Endpoint Security Client

User Guide
Version R71

December 24, 2008
## Contents

### Preface
- Who Should Use This Guide ................................................................. 8
- Summary of Contents ........................................................................... 9
- More Information .................................................................................. 11
- Feedback .............................................................................................. 11

### Chapter 1
**Introduction to Endpoint Security Client**

- Tour of the Control Center ................................................................. 14
- Getting around the Control Center .................................................... 14
- System Tray Icons .............................................................................. 15
- Overview Panel .................................................................................. 16
- Using the Overview Main Tab ............................................................. 17
- Setting Preferences .......................................................................... 18
- Understanding the Product Info Tab ................................................. 20
- Responding to alerts ......................................................................... 21
- New Program Alerts ....................................................................... 21
- New Network and VPN Alerts ......................................................... 22
- Compliance Alerts .......................................................................... 22

### Chapter 2
**VPN**

- VPN Basics ....................................................................................... 24
- Obtaining Authentication Credentials .............................................. 24
- Compact and Extended VPN Interfaces ........................................ 25
- Configuring Profiles and Sites .......................................................... 26
- Managing Connection Profiles ........................................................ 27
- Managing VPN Sites ....................................................................... 31
- Managing Certificates ..................................................................... 36
- Managing Entrust Certificates .......................................................... 36
- Creating Check Point Certificates .................................................... 38
- Renewing Check Point Certificates .................................................. 40
- Configuring Connection Options ..................................................... 41
  - Auto-Connect ............................................................................. 41
  - Secure Domain Logon ................................................................. 42
  - Auto Local Logon ................................................................... 43
- Proxy Settings (Visitor Mode) ............................................................ 43
- Advanced Configuration Options ...................................................... 45
  - Connecting and Disconnecting ..................................................... 45
  - Connecting Through a Hot-Spot ................................................... 46
  - Suspending Popup Messages ........................................................ 47
  - Enabling Office Mode ................................................................. 47
  - Enabling Hub Mode ................................................................ 48
  - Enabling Connectivity Enhancements ......................................... 48
- Connection Status ........................................................................... 49
# Program Control

Understanding Program Control ................................................................. 96
Program Access Control ............................................................................. 96
Program Authentication ............................................................................... 97
Setting Program Control Options ................................................................ 98
Setting Program Control Level .................................................................. 98
Enabling Automatic Lock .......................................................................... 99
Configuring Program Access .................................................................... 100
Setting Program Access Permissions ......................................................... 100
Customizing Program Control Settings ...................................................... 101
Setting Specific Permissions ..................................................................... 102
Using the Programs List ............................................................................ 103
Adding Programs to the Programs List ....................................................... 104
Granting Internet Access Permissions to Programs .................................... 105
Granting Server Permission to Programs .................................................... 105
Granting Pass-lock Permission to Programs ................................................. 106
Granting Send Mail Permission to Programs .............................................. 106
Advanced Program Control ....................................................................... 106
Disabling Outbound Mail Protection .......................................................... 107
Setting Filter Options ................................................................................ 107
Setting Authentication Options ................................................................. 108
Allowing Others to Use Programs ............................................................... 108
Managing Program Components ............................................................... 109
Using Programs with the Client ................................................................. 110
Using Antivirus Software .......................................................................... 110
Using Browsers ........................................................................................ 111
Using Chat ................................................................................................ 112
Using E-mail ............................................................................................. 112
Using Internet Answering Services ............................................................. 112
Using File Sharing .................................................................................... 113
Using FTP .................................................................................................. 113
Using Streaming Media ............................................................................ 113
Using Games ............................................................................................ 114
Using Remote Control .............................................................................. 115
Using VNC ............................................................................................... 115
Using Voice over IP .................................................................................. 116
Using Web Conferencing ......................................................................... 116

---

Adding to the Trusted Zone ...................................................................... 85
Adding to the Blocked Zone ....................................................................... 87
Blocking and Unblocking Ports .................................................................. 88
Default Port Permission Settings ............................................................... 88
Adding Custom Ports .................................................................................. 89
Configuring VPN Connection for Firewall ................................................ 90
Supported VPN Protocols ......................................................................... 90
Configuring VPN Connection Automatically ............................................. 90
Configuring VPN Connection Manually .................................................... 91

---

Chapter 5
Chapter 6  
**Full Disk Encryption**

Authenticating Full Disk Encryption ................................................................. 118
Ensuring That Your Computer Has Not Been Tampered With .......................... 118
Authenticating First Time .................................................................................. 118
Optional Full Disk Encryption Features ............................................................... 124
  Synchronizing Passwords .................................................................................. 124
  Full Disk Encryption Single Sign-on ................................................................. 126
Windows Integrated Logon .................................................................................. 127
Using the Full Disk Encryption Panel ............................................................... 128
  Viewing Status and Encryption Information .................................................. 128
  Changing Your Authentication Credentials .................................................... 131
  Changing the Language Used in the Interface ................................................ 131
  Languages Supported ....................................................................................... 133
  Fallback Languages ......................................................................................... 133
  Characters Supported in the Preboot Environment ........................................ 136

Chapter 7  
**Media Encryption**

Encryption Policy Manager .................................................................................. 138
  Using the EPM ................................................................................................. 138
Encrypting Media ................................................................................................. 139
Decrypting Media ................................................................................................. 141
Changing the Encrypted Device Password ........................................................ 141
Removable Media Manager .................................................................................. 142
  Using the Removable Media Manager ............................................................ 142
  Removable Media Manager Alert .................................................................. 143
  Authorizing Removable Media ....................................................................... 143
Device Manager .................................................................................................. 144
  Using the Device Manager ............................................................................ 144
Program Security Guard ..................................................................................... 145
  Using the Program Security Guard ............................................................... 145
Centralized Auditing and Alerts ......................................................................... 146
Maintenance Section .......................................................................................... 146

Chapter 8  
**E-mail Protection**

Outbound MailSafe Protection ........................................................................... 148
  Enabling Outbound MailSafe Protection ....................................................... 148
Customizing Outbound MailSafe Protection ...................................................... 149
  Enabling MailSafe by Program ..................................................................... 149
Setting MailSafe Options ................................................................................... 150

Chapter 9  
**Policies**

Policy Types .......................................................................................................... 152
Understanding Policy Arbitration ...................................................................... 153
Viewing Available Policies .................................................................................. 153
Using the Policies Panel ....................................................................................... 153
Resolving Slow Startup .............................................................................. 191
Internet Connection Troubleshooting ............................................................... 192
Connecting to the Internet Fails after Installation ......................................... 192
Allowing ISP Heartbeat Messages ............................................................... 193
Connecting Through an ICS Client .............................................................. 194
Connecting Through a Proxy Server .......................................................... 194

Glossary
Preface

In This Chapter

Who Should Use This Guide  page 11
Summary of Contents  page 12
More Information  page 13
Feedback  page 13
Who Should Use This Guide

This User Guide is intended for administrators responsible for maintaining network security within an enterprise, including policy management and user support.

This User Guide assumes a basic understanding of

- System administration.
- The underlying operating system.
- Internet protocols (IP, TCP, UDP, and so on).
## Summary of Contents

This guide contains the following chapters:

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction to Endpoint Security Client</td>
<td>Describes Endpoint Security main window, icons, shortcut keys, and the Overview panel; and explains how to respond to the first alerts.</td>
</tr>
<tr>
<td>VPN</td>
<td>Describes Virtual Private Networking features and configurations with Endpoint Security.</td>
</tr>
<tr>
<td>Anti-virus and Anti-spyware</td>
<td>Describes Endpoint Security protection against viruses and spyware and explains how to handle infections and how to schedule scans.</td>
</tr>
<tr>
<td>Firewall</td>
<td>Describes Endpoint Security firewall protection, and explains how to use Security Zones for easy firewall configuration.</td>
</tr>
<tr>
<td>Program Control</td>
<td>Describes how to control permissions for program access and use.</td>
</tr>
<tr>
<td>E-mail Protection</td>
<td>Describes Outbound MailSafe Protection, how to enable it and how to customize it.</td>
</tr>
<tr>
<td>Policies</td>
<td>Describes different types of policies (personal or corporate), and explains how Endpoint Security enforces the polices and arbitrates between them.</td>
</tr>
<tr>
<td>Alerts and Logs</td>
<td>Describes Endpoint Security alerts and explains how to handle them; describes the Alert Advisor and how to use it; explains how to use and customize the logs.</td>
</tr>
</tbody>
</table>

This guide contains the following additional information:

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alert Reference</td>
<td>This appendix is a reference guide for different types of alerts, why they appear and how to handle to them.</td>
</tr>
<tr>
<td>Troubleshooting</td>
<td>Provides basic and advanced troubleshooting scenarios and tips.</td>
</tr>
<tr>
<td>Glossary</td>
<td>Glossary of terms used in this guide and in Check Point products.</td>
</tr>
</tbody>
</table>
More Information

For additional technical information about Check Point products, and for the latest version of this document, see the Check Point Support Center at http://support.checkpoint.com/.

Feedback

Check Point is engaged in a continuous effort to improve its documentation. Please help us by sending your comments to:

cp_techpub_feedback@checkpoint.com
Check Point Endpoint Security™ is the first and only single agent that combines all essential components for total security on the endpoint: highest-rated firewall, Anti-virus, Anti-spyware, full disk encryption, media encryption with port protection, network access control (NAC), program control and VPN.

Check Point Endpoint Security protects PCs and eliminates the need to deploy and manage multiple agents, reducing total cost of ownership.

In This Chapter

Tour of the Control Center page 17
Overview Panel page 19
Responding to alerts page 24
Tour of the Control Center

The Control Center provides one-stop access to the security features that keep your computer safe.

To launch the Control Center, select **Settings** from the Endpoint Security system tray menu.

Getting around the Control Center

*Figure 1-1* Endpoint Security Control Center

The left menu provides access to the available panels.

To get help, click **Help**.
**System Tray Icons**

The icons displayed in the system tray let you monitor your security status and Internet activity on the fly, and access your security settings in just a few clicks. Right-click any of the icons below to access a shortcut menu.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>![VPN icon]</td>
<td>VPN is connected.</td>
</tr>
<tr>
<td>![Security icon]</td>
<td>Security scan, encryption, or change in client settings is in progress.</td>
</tr>
<tr>
<td>![Attention icon]</td>
<td>Attention needed (for example: client is out of compliance with policy, application error, or reboot needed).</td>
</tr>
</tbody>
</table>
Overview Panel

The Overview panel provides quick access to the most urgent issues and offers quick scanning of the status of different areas of protection and connection.

In This Section

- Using the Overview Main Tab page 20
- Setting Preferences page 21
- Understanding the Product Info Tab page 23

To open the Overview panel:
1. Right-click the Endpoint Security tray icon.
2. Select Settings.

The Endpoint Security Control Center opens, displaying the Overview panel, Main tab.
Using the Overview Main Tab

The Main tab of the Overview panel tells you whether your firewall, program, and e-mail security settings are enabled and provides a summary of security activity. From the Main tab you can:

- See at a glance if your computer is secure
- See a summary of the client's activity
- See if your version of the client is up to date
- Access the product tutorial

**VPN**
Shows whether you are connected to the VPN, if you have VPN installed on your Endpoint Security client.

**Anti-virus / Anti-spyware**
Shows whether each protection is turned on, and if so, how many viruses or spies were treated.

**Firewall**
Indicates whether your firewall is on and displays the number of firewall alerts and Internet Lock alerts that have occurred since the last reset. If a warning is displayed, click the underlined warning text to go immediately to the panel where you can adjust your settings.

**Program Control**
Indicates whether program control is configured safely and displays the number of program alerts that have occurred since the last reset. Endpoint Security client will warn you if program control is disabled.

**E-mail Protection**
Indicates whether MailSafe is enabled and displays the number of attachments that have been quarantined since the last reset. If a warning is displayed, click the underlined warning text. You are taken to the panel where you can adjust your settings.
Setting Preferences

The Overview/Preferences tab provides access to common settings.

In This Section

- Checking for Endpoint Security Updates
- Setting User-Level Password
- Setting General Preferences
- Setting Contact Preferences

Checking for Endpoint Security Updates

If your service agreement include product updates, you can check for, download, and install updates to Endpoint Security.

To check for Endpoint Security updates:

1. Open Overview/Preferences.
2. Click Check for Update.

Setting User-Level Password

By setting a user-level password, you prevent anyone but you from shutting down or uninstalling Endpoint Security client, or changing your security settings. Setting a password will not prevent other people from accessing the Internet from your computer.

If your version of Endpoint Security client was installed by an administrator with an installation password, that administrator can access all functions.

When you set a password for the first time, be sure to log out before leaving your computer. Otherwise, others can still change your settings.

This setting also allows others to use programs and access the Internet, but prevents them from changing your security settings. For example, you may want to prevent your children from changing the Endpoint Security settings but still allow them to use new programs without knowing your password.

Note - Other users will not be able to use programs that are already on your Blocked Programs list.
To set or change a Endpoint Security client password:
1. Open Overview/Preferences.
2. Click Set Password.
3. Type your password and password verification in the fields provided.
4. Select Allow others to use programs without a password.
5. Click OK.

Note - Valid passwords are between 6 and 31 characters long. Valid characters include A-Z, a-z, 0-9, and characters !,@,#,$,%,^,&,*.

After you have set a password, you must log in before you can change settings, shut down the TrueVector security engine, or uninstall Endpoint Security.

Setting General Preferences

By default, the client starts automatically when you turn on your computer. Use the settings in the General area to change the automatic startup option.

To set general display preferences:
1. Open Overview/Preferences.
2. In the General area, specify your preferences.
   - Load Endpoint Security software at startup: Endpoint Security client starts automatically when you turn on your computer.
   - Protect the Check Point Endpoint Security client: Prevents Trojan horses from sending Keyboard and Mouse requests to the client.

Warning - To ensure maximum security, disable the Protect the client feature only if you are having problems with your keyboard or mouse while using remote access programs.
Setting Contact Preferences

Setting contact preferences ensures that your privacy is protected when the client communicates with Check Point (for example, to check automatically for updates).

To set contact preferences:
1. Open **Overview|Preferences**.
2. In the Contact area, specify your preferences.
   - **Alert me with a pop-up before I make contact**: Displays a warning before contacting Check Point to deliver registration information, get product updates, research an alert, or access DNS to look up IP addresses.
   - **Hide my IP address when applicable**: Prevents your computer from being identified when you contact Check Point.
   - **Hide the last octet of my IP address when applicable**: Omits the last section of your IP address (for example, 123.456.789.XXX) when you contact Check Point.

Note - If you are participating in the Check Point Secure Community, you will not be alerted before sending anonymous data.

Understanding the Product Info Tab

The **Overview|Product Info** tab shows the version information for the following components:
- Endpoint Security client (also includes date and time of installation)
- TrueVector Security Engine
- Driver
- VPN Engine (if relevant)
- Anti-virus Engine
- Anti-spyware Engine
Responding to alerts

When you first start using the client, it is not unusual to see a number of alerts. Endpoint Security client is learning your program and network configurations, and giving you the opportunity to set up your security the way you want it.

How you respond to an alert depends upon the type of alert displayed. For information on responding to a particular type of alert, see Appendix A, “Alert Reference”.

New Program Alerts

The majority of the initial alerts you see will be New Program 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 Program alert to give access permission to programs 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 programs 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 program 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 (XREF:TBD). At any time, you can assign permissions to specific programs and services from the Programs List, accessed by selecting Program Control|Programs tab (XREF:TBD).

If you are seeing many server program alerts, you may want to run a spyware scan as an added precaution (XREF:TBD).

**New Network and VPN Alerts**

Other initial alerts you may 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 Trusted Zone, port/protocol permission, and program permissions correctly so that you can work securely over your network.

**Compliance Alerts**

Compliance alerts occur when Endpoint Security server operating in conjunction with Endpoint Security client determines that your computer is non-compliant with enterprise security requirements. Depending on the type of non-compliance, your ability to access the corporate network may be restricted or even terminated.

Computers that are running the correct types and versions of required software are said to be compliant with enterprise security requirements. When on the other hand Endpoint Security determines that a computer is non-compliant, it:

- Displays a Compliance alert (but only if the display of Compliance alerts is enabled in the currently active enterprise security policy)
- Directs you to a Web page that tells you how to make the endpoint computer compliant

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

- If the non-compliant condition does not require immediate remediation, your access to the corporate network may be restricted: You can continue to access some corporate network resources before you perform the steps necessary to make your computer compliant.
- If the non-compliant condition requires immediate remediation, your access to the corporate network may be terminated. In this case, you may only be able to access the Web page that tells you how to make your computer compliant with corporate security requirements.
A virtual private network (VPN) lets you use the internet to connect remotely to your company’s private network or intranet. VPNs allow private and secure communication while using public networks such as the Internet for transmission.

In This Chapter

- VPN Basics  page 27
- Configuring Profiles and Sites  page 29
- Managing Certificates  page 39
- Configuring Connection Options  page 44
- Advanced Configuration Options  page 48
- Connection Status  page 52
VPN Basics

Endpoint Security VPN lets you connect securely to your enterprise network when you are working remotely. After your computer and the VPN site prove their identities (or authenticate), all subsequent communication is encrypted and secure. 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 feature 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 Main panel displays information about any current VPN connection (if any) and about the status of your remote connection to Endpoint Security server. From the Main panel, you can 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.

Obtaining Authentication Credentials

When you connect to a site, and supply identification details, you are supplying authentication credentials. There are many authentication methods available. The recommended way to authenticate is through the use of certificates. A certificate and your password (to open the certificate) are your authentication credentials.

Contact your system administrator to send you with 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.
- Alternative authentication methods, such as a user name and password, or SecurID card.
Compact and Extended VPN Interfaces

Your administrator can deploy Endpoint Security client with either a compact or an extended version of the VPN interface. You can also 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. Depending on which view you use, you will see differences in the interface.

To switch between extended and compact views:

1. If you are switching from extended to compact view, you must first:
2. Delete all sites (see “Deleting Sites” on page 38).
3. Disable Auto Local Logon (see “Auto Local Logon” on page 46).
4. Disable Secure Domain Logon (see “Secure Domain Logon” on page 45).
5. Do one of the following:
   - In the Endpoint Security client Control Center, open the VPN panel | Main and click VPN Settings | Advanced.
   - Right-click the Endpoint Security system tray icon, select VPN Options | VPN Settings Advanced.
6. In the Product View section, select Extended View or Compact View and click OK.
7. 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.
Configuring Profiles and Sites

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.

Before Endpoint Security VPN connects to a site it needs to obtain information regarding the site's structure, 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 structure (or topology). During this process you are requested to prove who you are, 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. After this process of defining a site is complete, regular connections can take place.

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.

In This Section

- Managing Connection Profiles  page 30
- Managing VPN Sites  page 34
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 may 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 do 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 (see "Compact and Extended VPN Interfaces" on page 28).

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:
   - Open VPN|Main and click VPN Settings|Connections tab.
   - Right-click or double-click on the system tray icon, select Connect to VPN, click Options, and select the Connections tab.

2. 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.
Managing Connection Profiles

Exporting and Importing Profiles
You can export (save) and import existing profiles. For example, if your administrator creates a profile and asks you to import it.

To export a profile:
1. Open VPN\Main and click VPN Settings\Connections tab.
2. 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. Open VPN\Main and click VPN Settings\Connections tab.
2. 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 that you cannot change profiles while connected to 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 to 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. Open VPN|Main and click VPN Settings|Connections tab.
2. Right-click the desired profile and select Create Shortcut.
   Double-click the shortcut on your desktop to initiate a VPN connection.
Viewing Profile Properties

Open the Profile Properties window to check or modify a profile.

To view profile properties:
1. Open VPN|Main and click VPN Settings|Connections tab.
2. Right-click the desired profile and choose Properties.

The Profile Properties window appears with the following tabs:

- **General**: Site name, site description, and selected 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. You can delete only profiles that you created; you cannot delete a profile downloaded by your network administrator.

To delete profiles:
1. Open VPN|Main and click VPN Settings|Connections tab.
2. Right-click the desired profile and select Delete Profile.
3. In the confirmation window, click Yes.
Managing VPN Sites

Before you can establish a VPN connection, you must define a destination site (a VPN server or device) to which to connect. A site definition tells the client how to connect to the VPN site. During the initial connection, which differs from all subsequent connections, you must prove your identity by supplying a certificate or through some other means of authentication. The client then obtains the site’s structure (or topology). After the site is defined, regular connections can take place.

Defining Sites

You must define a site before you can establish a VPN connection. 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, work through 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 created the certificate or received one from your administrator (see “Managing Certificates” on page 39).

Preparing:

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

1. Open VPN|Main and click 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. Open VPN|Main and click VPN Settings|Connections.
2. If you are in extended view, click NewSite; or, if you are in compact view, click Define Server.

The Site Wizard window appears.
To define a site in the Site Wizard:

1. Provide the VPN site IP address or host name.
2. Select **Display Name** and provide a display name.
3. Click **Next**.
   Wait for the client to identify the site.
4. Select the method of authentication. (Your administrator should have provided you with the necessary information.) The choices and subsequent actions are:
   - **User name and Password**: Click **Next** to advance to the User Details window. Provide 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. (Optionally, you can click **View Certificate** to see the certificate.) 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. (For example, if you choose Use PinPad card, type your user name and passcode.) Click **Next**.
   - **Challenge Response**: Click **Next** to advance to the Challenge Response window. Provide your user name and click **Next**.
5. Choose the desired connectivity setting (Standard or Advanced) and click **Next**.
   The next window shows the certificate fingerprint and distinguished names (DN).
6. If your administrator gave you the site fingerprint and DN, compare them to those in the window. If they match, click **Next**.
7. Click **Finish**.
**Viewing Site Properties**

Open the Site Properties window to view or modify a site definition.

- **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 36).
- **Advanced**: Enable the NAT-T protocol (see “Enabling Connectivity Enhancements” on page 51).

To view site properties:

1. Open VPN|Main and click VPN Settings|Connections tab.
2. Right-click the desired site (not the profile, but the site that holds the profile) and choose Properties.

**Changing Authentication Methods**

Your administrator may ask you to change your VPN authentication method and should then provide you with authentication credentials (for example, a new certificate or a user name and password). If your laptop acts as a terminal for other users (each user connecting to the site with their own unique certificates, you will need to switch certificates as the need arises. Note that you cannot change authentication methods while connected to a VPN site.

To change authentication methods:

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 panel and click Disconnect.
2. Open VPN|Main and click VPN Settings|Connections tab.
3. Select a site and click Properties.
   
   The Site Properties window opens.
4. Open the Authentication tab and choose the appropriate authentication method from the Scheme drop-down list.
5. Provide the information appropriate for your authentication method. For example, if you are using a certificate, click Browse and choose the certificate.
6. 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.

**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. Open VPN\Main and click VPN Settings|Connections tab.
2. Select the desired site and then click Options|Update Site
   - If you are not connected to the site, the client prompts you to connect. You must be connected to complete the update (see “Connecting and Disconnecting” on page 48).

**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. Open VPN\Main and click VPN Settings|Connections tab.
2. Disconnect your VPN connection.
3. Select the desired site and then click Options|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. Note that by deleting a site, you also delete all associated profiles.

To delete sites:
1. Open **VPN|Main** and click **VPN Settings|Connections** tab.
2. Disconnect your VPN connection.
3. Select the site and then click **Delete**.
4. In the confirmation window that appears, click **Yes**.
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. All certificate functions are available in both the compact and extended versions of the VPN interface.

In This Section

Managing Entrust Certificates  page 39
Creating Check Point Certificates  page 41
Renewing Check Point Certificates  page 43

Managing Entrust Certificates

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

To use an Entrust certificate for authentication, perform the following Entrust procedures.

Enabling Entrust Entelligence

To enable Entrust Entelligence:

1. Open VPN>Main and click VPN Settings>Certificates tab.
2. Clear the Don’t use Entrust Entelligence check box.
**Initiating Entrust Certificates**

To initiate the creation of an Entrust certificate, register with the Entrust certificate authority by sending an .ini file (entrust.ini) to the certificate authority. The entrust.ini file contains information about the Entrust CA in the appropriate format.

**To initiate an Entrust certificate:**

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

**Creating Entrust Certificates**

This section explains how to create an Entrust certificate. Before you begin, make sure your administrator has given you a reference number and authorization code, which are required for completing the process.

**To create an Entrust certificate:**

1. Open **VPN|Main** and click **VPN Settings|Certificates** tab.
2. In the Entrust Certificates section, click **Create**.
   - The Create User window appears.
3. Click **Save to File**. Then click **Browse** to select the directory in which to save the certificate.
4. 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

5. Specify your profile parameters by entering the **Reference Number** and **Authorization code** supplied by your system administrator.

6. Click **OK**.

7. In the confirmation window that appears, click **OK** again.

---

**Creating 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.

PKCS#12 is a standard portable format (with a p12 extension) for transporting and storing private keys and certificates. CAPI (CryptoAPI) is a cryptographic application programming interface from Microsoft. You can access a Microsoft Certificate authority using Microsoft Internet Explorer to store and retrieve CAPI certificates. Endpoint Security can retrieve and store this type of certificate. Your administrator may also give you a hardware token for storing certificates. Hardware tokens provide greater security, since the private key used to encrypt the connection resides only on the hardware token.

Before you begin, get 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 as a PKCS#12 file, follow the instructions in this section.

To create a PKCS#12 file:
1. Open VPN|Main and click VPN Settings|Certificates.
2. Click Create Certificate.
   The Check Point Certificate window appears.
3. Select Store as a file (PKCS #12). 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.

To create a hardware or software token:
1. Open VPN|Main and click VPN Settings|Certificates.
2. 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.
   Each CSP uses its own unique configuration windows. Any deviations from the remaining instructions are due to differences in the CSP implementation. For details, consult your CSP’s documentation.
5. Provide the connection site IP address or host name and the registration key. Click Next.
Renewing Check Point Certificates

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**.

**Renewing Check Point Certificates**

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

**To renew a certificate:**
1. Open **VPN/Main** and click **VPN Settings/Certificates**.
2. 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.
Configuring Connection Options

In This Section

Auto-Connect  page 44
Secure Domain Logon  page 45
Auto Local Logon  page 46
Proxy Settings (Visitor Mode)  page 46

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

Auto-Connect

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.

By default, if the client detects traffic destined for the site, it connects to the site and encrypts the traffic. If the client is not connected to the site, it drops the connection unless you override this default. If you override the default, the traffic is sent clear. In connect mode, you are not prompted to connect to the site.

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.

In Auto-Connect mode, when the client detects traffic destined for the site, it automatically connects. 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|Options tab.
2. 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

In a Windows environment, your account may belong to a domain controlled by a domain controller. (A domain controller is 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 Gateway.

When you try to establish a VPN connection to a Windows domain, the client sends your login credentials to the domain controller for verification. By default, the client establishes the VPN connection only after the login process, which means traffic to and from the domain controller is not encrypted. 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|Options tab.
2. Select Enable Secure Domain Logon and click OK.
Auto Local Logon

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. Your password for the VPN site is encrypted using your password as a key. 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 in the manner of a terminal.

To enable Auto Local Logon:
1. Open VPN | Main and click VPN Settings | Options tab.
2. 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.

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, formally known as TCP Tunneling. If you are going to configure proxy settings, contact your system administrator for a valid user name and password to use to access the proxy.

Visitor Mode tunnels all client-to-Gateway communication through a regular TCP connection on port 443. All required VPN connectivity (IKE, IPsec, etc.) between the Client and the Server is tunneled inside this TCP connection. This means that the peer Gateway needs to run a Visitor Mode (TCP) server on port 443.
To configure proxy settings:

1. Open VPN\Main and click VPN Settings|Options tab.
2. 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, the "Use a proxy server for this connection" option is selected. 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.
Advanced Configuration Options

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

In This Section

- Connecting and Disconnecting
- Connecting Through a Hot-Spot
- Suspending Popup Messages
- Enabling Office Mode
- Enabling Hub Mode
- Enabling Connectivity Enhancements

Connecting and Disconnecting

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. Do one of the following:
   - Right-click the Endpoint Security icon in the system tray and select Connect to VPN.
   - In Endpoint Security|VPN, 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.

Connecting Through a Hot-Spot

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 in order 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:
  - Successfully connect to the network
  - Ten minutes pass
  - Three failed connection attempts

To enable hot-spot registration:

Do one of the following:

- Right-click the system tray icon and select Register to Hot Spot/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.

Note - If the Register to Hotspot/Hotel option is not available, this feature has been disabled by your network administrator.
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. This popup message can be suspended.

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.

To suspend pop-up messages:
1. Right-click the Endpoint Security icon in the system tray.
2. From the pop-up menu select *VPN Options*|*Suspend Auto-Connect Popups.*
   The Suspend Popup Messages window opens.
3. Select the popup suspension option you want.
4. Click **OK**.

Enabling Office Mode

Office Mode causes the gateway to assign your computer a temporary IP address that is guaranteed 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.

Note: when Office Mode is enabled with Auto-Connect Mode, you must re-initiate the connection after auto-connect succeeds.

To enable Office mode:
1. Open *VPN*|*Main* and click *VPN Settings*|*Connections* tab.
2. Right-click the profile and choose **Properties**.
   The Profile Properties window appears.
3. Click the **Advanced** tab, select **Office Mode**, and click **OK**.
Enabling Hub Mode

Hub Mode enables Endpoint Security VPN to use the site gateway as a router. Traffic from Endpoint Security VPN is not forwarded to the internal site but to another gateway. Use this procedure if your system administrator instructs you to enable Hub Mode.

To enable Hub mode:
1. Open VPN>Main and click VPN Settings>Connections tab.
2. Right-click the profile and choose Properties.
   The Profile Properties window appears.
3. Click the Advanced tab, select Route all traffic through gateway, and click OK.

Enabling Connectivity Enhancements

Connectivity enhancements include NAT traversal and Visitor Mode options.

VPN connection negotiations might result in the production of large packets. Some NAT devices may not fragment large packets correctly, making the connection impossible. To resolve this issue, there are several methods that may be used:

• **NAT-T**: NAT-T is based on IETF RFC 3193 and draft-02 of the IETF NAT-T specification. When a remote user initiates a VPN session with a Gateway, the remote host informs the Gateway that it is able to communicate using NAT-T. During the initial negotiation, both peers attempt to detect whether the traffic passed through a NAT device. If a NAT device is detected between the peers, communication between them switches to UDP port 4500. NAT-T is not supported using Aggressive Mode. UDP port 4500 must be enabled, because it will be used for the entire VPN session.

• **IKE over TCP**: IKE over TCP solves the problem of large UDP packets created during IKE phase I. The IKE negotiation is performed using TCP packets. TCP packets are not fragmented; in the IP header of a TCP packet, the DF flag ("do not fragment") is turned on. A full TCP session is opened between the remote host and the Gateway for the IKE negotiation during phase I.

• **Force UDP Encapsulation**: This method adds a special UDP header that contains readable port information to the IPSec packet. The new port information is not the same as the original. The port number 2746 is included in both the source and destination ports. The NAT device uses the source port for the hide operation but the destination address and port number remains the same. When the peer Gateway sees 2746 as the port number in the destination address, the Gateway calls a routine to decapsulate the packet.
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**

Endpoint Security client provides the following categories of information about the current connection:

- **Status Summary**: The client connection status, the gateway IP address, and the current computer's IP address.
- **Connections**: The name, IP address, site name, and tunnel properties of each available gateway. The active gateway is designated "(Primary)".
- **Gateway information**: The client displays basic data for each available gateway: the gateway name, gateway IP address, the site name or IP address, and whether Hub mode is active.
- **UDP Encapsulation**: Enables Endpoint Security client to overcome problems created by a Hide NAT device.
- **Visitor Mode/Office Mode**: 1) Sometimes the client needs to connect through a gateway that limits connections to port 80 or 443. Visitor Mode ensures all traffic between the client and the site is tunneled inside a regular TCP connection on port 443, required for VPN. 2) Sometimes the client is assigned a private IP address that conflicts with an identical address on the network behind the remote VPN peer. Office Mode prevents 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**: IP compression reduces the size of the data being sent, for significant performance improvement. IP compression is important for Endpoint Security client users with slow links, such as dial-up.
• IKE over TCP: IKE negotiation typically takes place over UDP. However, during the IKE negotiation between the client and the site, large UDP packets might be created. If these large packets are fragmented along the way, the IKE negotiation fails. TCP packets are not, as a rule, fragmented, so if large IKE packets are created, enable this option.

• Tunnel MTU Properties: Relates to the size of the packets that can be sent across the physical network. When the client is communicating across multiple routers with a site, it is the smallest Maximum Transmission Unit (MTU) of all the routers that is important. The current MTU is displayed here.

• Computer: The current computer's connection status and other connection information.

• Active Connection Settings: A summary of the current profile, including the site to which to connect, the gateway hostname, and the internet protocol specifications.

• Name: The 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.

• Profile Gateway: Name of the gateway specified in the connection profile.

• Selected Gateway: The actual gateway that was chosen for the connection. This may differ from the gateway defined in the connection profile.

• Gateway defined in the connection profile: Name of the defined gateway. It may differ from the Selected Gateway. For example, if the gateway in the profile did not respond, but a backup gateway took the connection.

• 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 Maximum Transmission size of packets 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. Open VPN(Main and click VPN Settings(Advanced tab.
2. Select Enable Logging.
Enabling Logging
Chapter 3

Anti-virus and Anti-spyware

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

In This Chapter

- Endpoint Security Anti-virus and Anti-spyware  page 57
- Scanning  page 59
- Advanced Options  page 65
Endpoint Security Anti-virus and Anti-spyware

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. Files can be scanned as they are opened, closed, executed, or as part of a full computer-wide scan. If a virus is detected, it is rendered harmless, either by repairing or denying access to the infected file.

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.

In This Section

- Enabling Anti-virus and Anti-spyware page 57
- Viewing Virus and Spyware Protection Status page 58
- Updating Anti-virus and Anti-spyware page 58

Enabling Anti-virus and Anti-spyware

If you chose not to turn on the Anti-virus protection feature in the Configuration Wizard following installation, you can turn it on manually.

**Warning** - The Endpoint Security client antivirus protection feature is incompatible with other virus protection software. Before you turn on the antivirus protection feature, uninstall any other antivirus software from your computer, including suite products that include virus protection among their features. Endpoint Security client can automatically uninstall some antivirus applications for you. If you are using a program that cannot be uninstalled automatically, use Add/Remove Programs from the Windows Control Panel.

To enable virus and spyware protection:

1. Open **Anti-virus/spyware|Main**.
2. In the **Anti-virus** area, click **On**.
3. In the **Anti-spyware** area, click **On**.
Viewing Virus and Spyware Protection Status

To view the status of your virus and spyware protection, see Overview | Main, or Anti-virus/spyware/Main.

The Main tab of the Anti-virus / Anti-spyware panel displays the status of your virus and spyware protection. From this area you can:

• Verify that virus and spyware protection is turned on.
• The dates and times of your last scans.
• Update definition files.
• Invoke a scan.
• View results of latest scan.
• Access advanced settings.

Updating Anti-virus and Anti-spyware

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. Therefore, the computer is vulnerable to viruses and spyware whenever its database of virus definition files becomes outdated.

In Anti-virus/spyware/Main, you can see if the Anti-virus or the Anti-spyware needs to be updated.

To get updates on demand:
1. Open Anti-virus/spyware/Main.
2. If Update overdue appears in either the Anti-virus or the Anti-spyware section, click Update Now.
Scanning

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

- In Anti-virus/spyware\Main tab, click Scan for Viruses, Scan for Spyware, or Scan for Viruses/Spyware.
- Right-click a file on your computer and choose Scan with Check Point Anti-virus.
- Schedule a system scan to run once or at regular intervals.
- Open a file (if On-Access scanning is enabled).

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 antivirus 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, you can schedule system scans to run at a time when you are least likely to be using your computer.

**Note** - Clicking Pause during a scan 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 Options button is disabled.

In This Section

- Understanding Scan Results  page 60
- Treating Files Manually  page 61
- Submitting Viruses and Spyware to Check Point  page 62
- Viewing Quarantine Items  page 63
- Viewing Logs  page 64
**Understanding Scan Results**

The results of the scan are displayed in the Scan Results window.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the virus/spyware.</td>
</tr>
<tr>
<td>Treatment</td>
<td>Specifies the treatment applied to the infection/spyware: Quarantined or Deleted.</td>
</tr>
<tr>
<td>Risk</td>
<td>Indicates the risk level of the infection.</td>
</tr>
<tr>
<td></td>
<td><strong>High</strong>: Poses a security threat. All viruses are considered High risk.</td>
</tr>
<tr>
<td></td>
<td><strong>Med</strong>: Potential privacy breach.</td>
</tr>
<tr>
<td></td>
<td><strong>Low</strong>: Adware or other benign, but annoying software.</td>
</tr>
<tr>
<td>Path</td>
<td>Location of the virus/spyware.</td>
</tr>
<tr>
<td>Type</td>
<td>Specifies whether the infection was caused by a virus, worm, or trojan; or the spyware was keylogging software or tracking cookie.</td>
</tr>
<tr>
<td></td>
<td><strong>Status</strong>: Indicates whether the file has been repaired, deleted, or remains infected. If the client was unable to treat the item, a What to do next link may appear here. This link will direct you to further information and instructions.</td>
</tr>
<tr>
<td></td>
<td><strong>Information</strong>: Provides more details. To get more information about a virus or spyware, click the Learn more link.</td>
</tr>
<tr>
<td>Detail</td>
<td><strong>Active Items</strong>: Infections/spyware found during the scan that could not be treated automatically. To accept the suggested treatments in the Treatment column, click Apply.</td>
</tr>
<tr>
<td></td>
<td><strong>Auto Treatment</strong>: Items already treated; you do not need to take further action.</td>
</tr>
</tbody>
</table>
Treating Files Manually

If you do not have automatic treatment enabled, or if a file could not be repaired automatically, you can handle it manually from the Scan details window.

To treat a file manually:
1. In the Scan Results window, select the item you want to treat.
2. In the Treatment column, choose a treatment option (see Table 3-2).
3. Click Close, when you have finished treating files.

Table 3-2  Treatment Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Treatment Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Repair</td>
<td>Tries to repair the selected file.</td>
</tr>
<tr>
<td>Quarantine</td>
<td>Appends the extension .z16 to the infected file to render it harmless. The file is placed in Quarantine.</td>
</tr>
<tr>
<td>Rename</td>
<td>Allows you to rename the file so that it will not be found by future scans. Use this option only if you are sure that the file is in fact not a virus.</td>
</tr>
<tr>
<td>Delete</td>
<td>Deletes the selected file.</td>
</tr>
<tr>
<td>Delete on Reboot</td>
<td>Deletes the selected file when your computer is next restarted.</td>
</tr>
<tr>
<td>Ignore Always</td>
<td>Instructs the client to ignore the file in all future scans.</td>
</tr>
<tr>
<td>Ignore Once</td>
<td>Instructs the client to remove the item from the list and take no further action.</td>
</tr>
</tbody>
</table>

Note - If the results of a scan contain Error, No treatment available, or Treatment failed, there is not yet a way to automatically remove the virus without risking the integrity of your computer or other files.

Recommendation - To find manual treatment procedures, enter the name of the virus, with the word “removal” into a search engine, such as Google or Yahoo, to locate removal instructions. Check Point is constantly researching viruses and developing safe ways to remove them.
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.

Warning - 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 Quarantine Items

In some cases, items detected during a virus or spyware 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 spyware in quarantine:**
1. Open **Anti-virus/spyware**.
2. Open the **Quarantine** tab.
3. Choose **Viruses** or **Spyware** from the Quarantined View drop-down list.

**Table 3-3** Quarantine Information for Viruses

<table>
<thead>
<tr>
<th>Infection</th>
<th>Name of the virus.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Days in Quarantine</td>
<td>Number of days the file has been in quarantine.</td>
</tr>
<tr>
<td>Path</td>
<td>Location of the virus on your computer.</td>
</tr>
</tbody>
</table>

**Table 3-4** Quarantine Information for Spyware

<table>
<thead>
<tr>
<th>Type</th>
<th>Type of spyware: keylogging or cookie.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the spyware.</td>
</tr>
<tr>
<td>Risk</td>
<td>The risk level of the infection: whether Low, for adware; or a serious threat, for keylogging software.</td>
</tr>
<tr>
<td>Days in Quarantine</td>
<td>Number of days the file has been in quarantine.</td>
</tr>
</tbody>
</table>

**Handling Quarantine Items**

You can move viruses or spyware into, and out of, quarantine.

**To delete or restore an item in quarantine:**
1. Open **Anti-virus/spyware|Quarantine**.
2. Choose **Spyware** or **Viruses** from the Quarantined View drop-down list.
3. Select the item from the list.
   - To send the item to the Recycle Bin, click **Delete**.
   - To send the item to its original path, click **Restore**. Use carefully.
   - To send an item to Check Point for analysis, select the item and then click **More Info**.
Viewing Logs

By default, all virus and spyware events are recorded in the Log Viewer.

**To view logged Virus events:**

1. Open **Alerts & Logs Log Viewer**.
2. From the Alert Type drop-down list, select **Anti-virus** or **Anti-spyware**.

<table>
<thead>
<tr>
<th>Log Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date</td>
<td>Date of the infection.</td>
</tr>
<tr>
<td>Type</td>
<td>Type of event that occurred:</td>
</tr>
<tr>
<td></td>
<td>Viruses</td>
</tr>
<tr>
<td></td>
<td>Update</td>
</tr>
<tr>
<td></td>
<td>Scan</td>
</tr>
<tr>
<td></td>
<td>Treatment</td>
</tr>
<tr>
<td></td>
<td>E-mail</td>
</tr>
<tr>
<td></td>
<td>Spyware</td>
</tr>
<tr>
<td></td>
<td>Adware</td>
</tr>
<tr>
<td></td>
<td>Browser Help Object</td>
</tr>
<tr>
<td></td>
<td>Dialer</td>
</tr>
<tr>
<td></td>
<td>Keylogger</td>
</tr>
<tr>
<td></td>
<td>Spy cookie</td>
</tr>
<tr>
<td>Virus/Spyware Name</td>
<td>The common name of the virus (for example, <em>iloveyou.exe</em>) or spyware (for example, <em>NavExcel</em>).</td>
</tr>
<tr>
<td>Filename</td>
<td>The name of the infected file, the name of files being scanned, or the name and version number of update and/or engine.</td>
</tr>
<tr>
<td>Action Taken</td>
<td>How the virus was handled by the client:</td>
</tr>
<tr>
<td></td>
<td>Updated, Update cancelled, Update Failed</td>
</tr>
<tr>
<td></td>
<td>Scanned, Scan cancelled, Scan Failed</td>
</tr>
<tr>
<td></td>
<td>File Repaired, File Repair Failed</td>
</tr>
<tr>
<td></td>
<td>Quarantined, Quarantine Failed</td>
</tr>
<tr>
<td></td>
<td>Deleted, Delete Failed</td>
</tr>
<tr>
<td></td>
<td>Restored, Restore Failed</td>
</tr>
<tr>
<td></td>
<td>Renamed, Rename Failed</td>
</tr>
<tr>
<td>Actor</td>
<td>Whether the action was manual or automatic.</td>
</tr>
<tr>
<td>E-mail</td>
<td>If the virus was detected in e-mail, the e-mail address of the sender.</td>
</tr>
</tbody>
</table>
Advanced Options

The Advanced Options button is enabled if the only active policy is the Personal Policy (see “Policies” on page 154).

If an Enterprise or Disconnected Policy is active, the features of this option are controlled by your system administrator.

Therefore, you will be able to control the Advanced Options of your own client only if the Enterprise Policy was not yet received and there is no contact with the Endpoint Security server, or the assigned policy consists only of an Enterprise Policy and your client is disconnected from the server.

In This Section

- Scheduling Scans  page 66
- Updating Virus and Spyware Definitions  page 67
- Specifying Scan Targets  page 68
- On-Access Scanning  page 69
- Specifying Spyware Detection Methods  page 69
- Enabling Automatic Virus Treatment  page 70
- Enabling Automatic Spyware Treatment  page 70
- Repairing Archived Files  page 71
- Virus Scan Options  page 71
- Antivirus Exceptions List  page 72
- Anti-spyware Exceptions List  page 73
Scheduling Scans

Scanning your computer for viruses and spyware is one of the most important things you can do to protect the integrity of your data and computing environment. Scanning is most effective when performed at regular intervals, so it often makes sense to schedule it as a task to run automatically. If your computer is not on when the scheduled scan is set to occur, the scan will occur fifteen minutes after your computer is restarted.

To schedule a scan:
1. Open Anti-virus/spyware|Main.
2. In the Anti-virus area, click the click to schedule link.
   The Advanced Options window appears.
3. In the Scan Schedule options, select the Scan for viruses check box, then specify a day and time for the scan.
4. Specify the scan frequency: daily, weekly, or monthly.
5. Select the Scan for spyware check box, then specify a day and time for the scan.
6. Specify the scan frequency.
7. Click OK.

Note - If you select a weekly repeating schedule, the scan will run on the day of the week based on the starting date. For example, if the starting date is November 4, 2008, the scan will run every subsequent Tuesday.
Updating Virus and Spyware Definitions

Every virus or spyware application contains a definition file, with information to identify and locate viruses and spyware on your 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. Therefore, your computer is vulnerable to viruses and spyware whenever its database of virus definition files becomes outdated.

By enabling the automatic update feature, you will always receive the latest definition files when they are available.

To enable automatic updates:
1. Open Anti-virus/spyware\Main.
2. Click Advanced Options.
   The Advanced Options window appears.
3. Open the Updates options.
4. Select the Enable automatic anti-virus updates check box.
5. Select the Enable automatic anti-spyware updates check box.
6. In the Set update frequency drop-down list, specify when the client should check for updates and download and install them if available.
7. Click OK.

In Anti-virus/spyware\Main, you can see if the Anti-virus or the Anti-spyware needs to be updated.

To get updates on demand:
1. Open Anti-virus/spyware\Main.
2. If Update overdue appears in either the Anti-virus or the Anti-spyware section, click the click to update link; or click Update Now.
Specifying Scan Targets

You can specify which drives, folders, and files are scanned when a system scan occurs. Exclude or include an item in the scan by selecting the check box beside it. By default, the client only scans local hard drives.

**To specify scan targets:**
1. Open Anti-virus/spyware|Main.
2. Click Advanced Options.
   - The Advanced Options window appears.
3. Open Virus Management|Scan Targets.
4. Select the drives, folders, and files to be scanned.
5. Select the Scan boot sectors for all local drives check box and then click OK.
6. Select the Scan system memory check box and then click OK.

The following table explains the icons shown in the Scan Targets window.

**Table 3-6 Icons Indicating Scan Targets**

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The selected disk, all sub-folders and files will be included in the scan.</td>
</tr>
<tr>
<td></td>
<td>The selected disk, all sub-folders and files will be excluded from the scan.</td>
</tr>
<tr>
<td></td>
<td>The selected disk will be included in the scan, but one or more sub-folders or files will be excluded.</td>
</tr>
<tr>
<td></td>
<td>The selected folder will be excluded from the scan, but one or more sub-folders or files will be included.</td>
</tr>
<tr>
<td></td>
<td>The selected folder will be included in the scan. A gray check mark indicates that scanning of the folder or file is enabled because scanning has been enabled for a higher level disk or folder.</td>
</tr>
<tr>
<td></td>
<td>The selected folder will be excluded from the scan. A gray &quot;x&quot; mark indicates that scanning of the folder or file is disabled because scanning has been disabled for a higher level disk or folder.</td>
</tr>
<tr>
<td>Other</td>
<td>RAM DISK and any unknown drives. Specify other drives to scan.</td>
</tr>
</tbody>
</table>
On-Access Scanning

On-Access scanning protects your computer by detecting and treating viruses that may be dormant on your computer. On-Access scanning is enabled by default and supplies the most active form of virus protection. Files are scanned for viruses as they are opened, executed, or closed, allowing immediate detection and treatment of viruses.

Note - On-access scan will only scan for viruses in an archive (compressed file, such as those with a .zip extension.) when the file is opened. Unlike other types of files, archives are not scanned when moved from one location to another.

To enable on-access scanning:
1. Open Anti-virus/-spyware|Main.
2. Click Advanced Options.
3. Open Virus Management|On-Access Scanning and then select the Enable On-Access Scanning check box.
4. Click OK.

Specifying Spyware Detection Methods

In addition to default detection that searches your computer's registry for active spyware, there are methods to detect latent spyware and hard-to-find spyware.

To specify spyware detection methods:
1. Open Anti-virus/spyware|Main.
2. Click Advanced Options.
4. Select the Scan for tracking cookies check box.
5. Under Maximum strength detection options, select whether the scan should be more in-depth, or faster:
   • Intelligent quick scan: selected by default.
   • Full system scan: scans the local file system.
   • Deep-inspection scan: scans every byte of data on your computer.
The Full System Scan and the Deep-Inspection Scan may adversely affect performance. Select one of these options only if you suspect that undetected spyware is present.

6. Click **OK**.

**Enabling Automatic Virus Treatment**

When a virus infection is detected, the Scan window offers the available treatment options, such as Quarantine, Repair, or Delete. By default, the client automatically attempts to treat files that contain viruses. If a file cannot be repaired, the Scan window will inform you so that you can take the appropriate action.

**To enable automatic virus treatment:**

1. Open **Anti-virus/-spyware|Main**.
2. Click **Advanced Options**.
3. Open **Virus Management|Automatic Treatment**.
4. Select the auto treatment option you want:
   - Alert me - Do not treat automatically
   - Try to repair, and alert me if repair fails
   - Try to repair, quarantine if repair fails (recommended)
5. Click **OK**.

**Enabling Automatic Spyware Treatment**

When spyware is detected, the Scan window offers the available treatment options, such as Quarantine or Delete. The Scan window will display the suggested treatment of spyware so that you can take the appropriate action.

**To enable automatic spyware treatment:**

1. Open **Anti-virus/spyware|Main**.
2. Click **Advanced Options**.
3. Open **Spyware Management|Automatic Treatment**.
4. Select the **Enable automatic spyware treatment** check box and click **OK**.
Repairing Archived Files

If the infected file is located in an archive file (such as a .zip file), the client will not be able to treat it while the file is still included in the archive.

To repair a file in an archive:
1. Make sure “On-Access Scanning” is enabled.
2. Open the file that was specified in the Scan Results window from within an archival utility, such as WinZip.
   
   On-Access scanning will scan the file for infections. The Scan Results window will appear with the results of the scan.

Virus Scan Options

You can configure your virus scan to ignore any file larger than a specified size (default setting is 8 MB). This option improves scan time without increasing risk, as virus files are usually smaller than 8 MB. While large files ignored by the scan may contain viruses, your computer is still protected if you have On-Access scan enabled.

You can also enable the extended database. This database includes a comprehensive list of malware in addition to the standard virus list. However, some malware listed in the extended database may also be listed in the standard Anti-spyware database; some suspected malware may be scanned twice. Also, the extended database malware list may include programs that you consider to be benign.

To specify virus scan options:
1. Open Anti-virus/spyware|Main.
2. Click Advanced Options.
   
   The Advanced Options window appears.
3. Open Virus Management|Scan Options.
4. Select the Skip if the object is greater than check box and enter a maximum object size in the MB field.
5. In the **Set scanning priority** drop-down, select an option:
   - High (Faster scans, slower PC)
   - Medium
   - Low (Slower scans, faster PC)
6. Click **OK**.

### Antivirus Exceptions List

Although some programs considered to be suspicious by the extended database have the potential to harm your computer or to make your data vulnerable to hackers, there are many potentially benign applications that still will be detected as viruses during a scan. If you are using one of these applications, you can exclude it from antivirus scans by adding it to the Exceptions list.

**To add programs to the Exceptions list:**

- In the Scan Results list, click the program and choose **Ignore Always**, or do the following:
  1. Open **Anti-virus/spyware|Main**.
  2. Click **Advanced Options**.
  3. Open **Virus Management|Exceptions**.
  4. In the Virus Treatment Exceptions area, click **Add File**.
     The Add Exception window opens. It shows examples of exceptions that can be added.
  5. Provide an exception such as in the examples, or click **Browse** and select the file, folder, or drive to exclude from the scan.
  6. Click **OK**.

If you accidentally add a virus to the exceptions list, you can remove it.

**To remove viruses from the Exceptions list:**

1. Open **Anti-virus/spyware|Main**.
2. Click **Advanced Options**.
3. Open **Virus Management|Exceptions**.
4. Select the virus you want to remove and click **Remove from List**.
5. Click **OK**.
Anti-spyware Exceptions List

Although some spyware have the potential to harm your computer or data, there are many benign applications that may be detected as spyware during a scan. If you are using one of these applications (for example, voice recognition software), you can exclude it from spyware scans by adding it to the Exceptions list.

To add programs to the Exceptions list:

- In the Scan Results list, right-click the program and choose Ignore Always.

If you accidentally add spyware to the exceptions list, you can remove it.

To remove spyware from the exceptions list:

1. Open Anti-virus/spyware\Main.
2. Click Advanced Options.
3. Open Spyware Management\Exceptions.
4. Select the spyware application you want to remove and click Remove from List.
5. Click OK.
Chapter 4

Firewall Protection is your front line of defense against Internet threats. The client's default zones and security levels give you immediate protection against the vast majority of threats.

In This Chapter

Understanding Firewall Protection: page 75
Understanding Zones: page 76
Configuring New Network Connections: page 78
Integrating with Network Services: page 80
Choosing Security Levels: page 82
Setting Advanced Security Options: page 83
Managing Zone Traffic: page 87
Blocking and Unblocking Ports: page 91
Configuring VPN Connection for Firewall: page 93
Understanding Firewall Protection

In buildings, a firewall is a barrier that prevents a fire from spreading. In computers, the concept is similar. There are a variety of "fires" out there on the Internet—hacker activity, viruses, worms, and so forth. A firewall is a system that stops these attempts to damage your computer.

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

- What Zone did the traffic come from and what port is it addressed to?
- Do the rules for that Zone allow traffic through that port?
- Does the traffic violate any global rules?
- Is the traffic authorized by a program on your computer (Program Control settings)?

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

Endpoint Security client keeps track of the good, the bad, and the unknown out on the Internet by using virtual containers, called Zones, to classify the computers and networks that connect to your computer.

The Internet Zone is the "unknown." All the computers and networks in the world belong to this Zone—until you move them to one of the other Zones.

The Trusted Zone is the "good." It contains all the computers and networks you trust and want to share resources with—for example, the other machines on your local or home network.

The Blocked Zone is the "bad." It contains computers and networks you distrust.

When another computer wants to communicate with your computer, the client looks at the Zone it is in to help decide what to do.

Zones Manage Firewall Security

The client uses security levels to determine whether to allow or block inbound traffic from each Zone. Open the Firewall panel, Main tab to view and adjust security levels.

**High Security Setting**

High security places your computer in stealth mode, making it invisible to hackers. High security is the default configuration Internet Zone.

In High security, file and printer sharing is disabled; but outgoing DNS, outgoing DHCP, and broadcast/multicast are allowed, so that you are able to browse the Internet. All other ports on your computer are closed except when used by a program that has access permission and/or server permission.

**Medium Security Setting**

Medium security places your computer in component learning mode, where the client quickly learns the MD5 signatures of many frequently used program components without interrupting your work with multiple alerts. Medium security is the default setting for the Trusted Zone.
In Medium security, file and printer sharing is enabled, and all ports and protocols are allowed. (If Medium security is applied to the Internet Zone, however, incoming NetBIOS traffic is blocked. This protects your computer from possible attacks aimed at your Windows networking services.) At Medium security, you are no longer in stealth mode.

We recommend that you use the Medium security setting for the first few days of normal Internet use after installing the client. After a few days of normal use, the client will have learned the signatures of the majority of the components needed by your Internet-accessing programs, and will remind you to raise the Program Authentication level to High.

No security level is necessary for the Blocked Zone, because no traffic to or from that Zone is allowed.

Note - Advanced users can customize high and medium security for each Zone by blocking or opening specific ports. See “Blocking and Unblocking Ports” on page 91.

Zones Provide Program Control

Whenever a program requests access permission or server permission, it is trying to communicate with a computer or network in a specific Zone. For each program you can grant or deny the following permissions:

- Access permission for the Trusted Zone.
- Access permission for the Internet Zone.
- Server permission for the Trusted Zone.
- Server permission for the Internet Zone.

By granting access or server permission for the Trusted Zone, you enable a program to communicate only with the computers and networks you have put in that Zone. This is a highly secure strategy. Even if a program is tampered with, or given permission accidentally, it can only communicate with a limited number of networks or computers.

By granting access or server permission for the Internet Zone, however, you enable a program to communicate with any computer or network, anywhere.
Configuring New Network Connections

If your computer connects to a network, decide whether to place that network in the Trusted Zone or in the Internet Zone.

Placing a network in the Trusted Zone enables you to share files, printers, and other resources with other computers on that network. Networks you know and trust, such as your home or business LAN, should go in the Trusted Zone.

Placing a network in the Internet Zone prevents you from sharing resources with other computers on that network and protects you from the security risks associated with resource sharing. Unknown networks should go in the Internet Zone.

The Network Configuration Wizard helps you make this decision by determining whether the detected network is public or private.

Using the Network Configuration Wizard

When your computer connects to a new network, a Network Configuration Wizard appears, displaying the IP address of the detected network and whether it is public or private.

The IP address of the network is used to determine whether it is a private network or a public network.

- A private network is usually a home or business Local Area Network (LAN). Private networks are placed in the Trusted Zone by default.
- A public network is usually a much larger network, such as that associated with an ISP. Public networks are placed in the Internet Zone by default.

To configure your network connection using the Network Configuration Wizard:

1. Choose the Zone you want this network in and then click Next.

   By default, the client places private networks in the Trusted Zone, and public networks in the Internet Zone.

2. Name the network. The name you enter here will be displayed in the Zones tab of the Firewall panel.

   **Note** - If you prefer not to use the Network Configuration Wizard, click Cancel in any Wizard screen. A New Network alert will appear. The detected network will be placed in the Internet Zone, even if it is a private network.

To enable your computer to connect to the Internet through a proxy server, add the proxy to your Trusted Zone. See “Adding to the Trusted Zone” on page 88.
Disabling the Network Configuration Wizard

The Network Configuration Wizard is enabled by default. If you prefer to use the New Network Alert to configure new networks, you can disable the Network Configuration Wizard.

To disable the Network Configuration Wizard:

1. In screen four of the Wizard, select the **Do not show this Wizard the next time a new network is detected** check box.
2. Click **Finish**.
Integrating with Network Services

If you are working on a home or business network, you may want to share files, network printers, or other resources with other people on the network, or send and receive e-mail through your network’s mail servers. Use the instructions in this section to enable safe resource sharing.

Enabling File and Printer Sharing

To share printers and files with other computers on your network, you will need to configure Endpoint Security client to allow access to the computers with which you plan to share resources.

To configure the client for file and printer sharing:
1. Add the network subnet (or, in a small network, the IP address of each computer you are sharing with) to your Trusted Zone. See “Adding to the Trusted Zone” on page 88.
2. Set the Trusted Zone security level to Medium. This allows trusted computers to access your shared files. See “Choosing Security Levels” on page 82.
3. Set Internet Zone security to High. This makes your computer invisible to non-trusted machines.

Connecting to Network Mail Servers

Endpoint Security client is configured to automatically work with Internet-based mail servers using POP3 and IMAP4 protocols, when you give your e-mail client permission to access the Internet.

Some mail servers, such as Microsoft Exchange, include collaboration and synchronization features that might require you to trust the server for those services to correctly function.

To configure the client for mail servers with collaboration and synchronization:
1. Add the network subnet or IP address of the mail server to your Trusted Zone.
2. Set the Trusted Zone security level to Medium. This allows server collaboration features to work.
3. Set Internet Zone security level to High. This makes your computer invisible to non-trusted machines.
Enabling Internet Connection Sharing

If you are using Windows' Internet Connection Sharing (ICS) option, or a third-party connection sharing program, you can protect all of the computers that share the connection from inbound threats by installing Endpoint Security client on the gateway machine only. However, to receive outbound protection, or to see alerts on the client machines, you must have Endpoint Security client installed on the client machines as well.

**Note** - Before you configure the client, use your ICS software to set up the gateway and client relationships. If you use hardware such as a router to share your Internet connection rather than Microsoft’s Internet Connection Sharing (ICS), ensure that the local subnet is in the Trusted Zone.
Choosing Security Levels

The default firewall security levels (High for the Internet Zone, Medium for the Trusted Zone) protect you from port scans and other hacker activity, while allowing you to share printers, files, and other resources with trusted computers on your local network. In most cases, you do not have to make any adjustment to these defaults. You are protected as soon as Endpoint Security client is installed.

To set the security level for a Zone, open Firewall Main and drag the sliders to the setting you want.

Table 4-1 Internet Zone Security

<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HIGH</td>
<td>This is the default setting. Your computer is in stealth mode, making it invisible to other computers. Access to Windows NetBIOS services, file and printer shares is blocked. Ports are blocked unless you have provided permission for a program to use them.</td>
</tr>
<tr>
<td>MED</td>
<td>Your computer is visible to other computers. Access to Windows services, file and printer shares is allowed. Program permissions are still enforced.</td>
</tr>
<tr>
<td>LOW</td>
<td>Your computer is visible to other computers. Access to Windows services, file and printer shares is allowed. Program permissions are still enforced.</td>
</tr>
</tbody>
</table>

Table 4-2 Trusted Zone Security

<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HIGH</td>
<td>Your computer is in stealth mode, making it invisible to other computers. Access to Windows (NetBIOS) services, file and printer shares is blocked. Ports are blocked unless you have provided permission for a program to use them.</td>
</tr>
<tr>
<td>MED</td>
<td>This is the default setting. Your computer is visible to other computers. Access to Windows services, file and printer shares is allowed. Program permissions are still enforced.</td>
</tr>
<tr>
<td>LOW</td>
<td>Your computer is visible to other computers. Access to Windows services, file and printer shares is allowed. Program permissions are still enforced.</td>
</tr>
</tbody>
</table>
Setting Advanced Security Options

Advanced security options enable you to configure the firewall for a variety of special situations, such as gateway enforcement and Internet Connection Sharing (ICS).

In This Section

- Setting Gateway Security Options  page 83
- Setting ICS Options  page 84
- Setting General Security Options  page 85
- Setting Network Security Options  page 86

Setting Gateway Security Options

Some companies require their employees to use Endpoint Security client when connecting to the Internet through their corporate gateway. When the **Automatically check the gateway** control is selected, the client checks for any compatible gateways and confirms that it is installed so that gateways requiring the client will grant access.

You can leave this option selected even if you are not connecting through a gateway. Your Internet functions will not be affected.

**To set automatic gateway check:**

1. Open **Firewall/Main**.
2. Click **Advanced**.
   - The Advanced Settings window opens.
3. In the Gateway Security area, check the **Automatically check the gateway for security enforcement** checkbox.
4. Click **OK**.
Setting ICS Options

If you are using ICS (Internet Connection Sharing), use these controls to configure Endpoint Security client to recognize the ICS gateway and clients.

To set Internet Connection Sharing preferences:

1. Open Firewall/Main.
2. Click Advanced.

The Advanced Settings window opens.

3. In the Internet Connection Sharing area, choose your security settings.
   - This computer is not on an ICS/NAT net: Internet Connection sharing is disabled.
   - This is a client of an ICS/NAT gateway running Endpoint Security: The client automatically detects the IP address of the ICS gateway and displays it in the Gateway Address field. You also can type the IP address into the field.
     Select the Forward alerts from gateway to this computer checkbox to log and display alerts on the client computer that occur on the gateway.
   - This computer is an ICS/NAT gateway: The client automatically detects the IP address of the ICS gateway and displays it in the Local Address field. You also can type the IP address into the field.
     Select Suppress alerts locally if forwarded to clients to suppress alerts forwarded from the gateway to clients.

4. Click OK.
Setting General Security Options

These controls apply global rules regarding certain protocols, packet types and other forms of traffic (such as server traffic) to both the Trusted Zone and the Internet Zone.

To modify general security settings:
1. Open Firewall|Main.
2. Click Advanced.
3. In the General Settings area, choose your security settings.

Table 4-3 General Security Settings

<table>
<thead>
<tr>
<th>Security Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block all fragments</td>
<td>Blocks all incomplete (fragmented) IP data packets. Hackers sometimes create fragmented packets to bypass or disrupt network devices that read packet headers. <strong>Caution</strong>: If you select this option, the client will silently block all fragmented packets without alerting you or creating a log entry. Do not select this option unless you are aware of how your online connection handles fragmented packets.</td>
</tr>
<tr>
<td>Block trusted servers</td>
<td>Prevents all programs on your computer from acting as servers to the Trusted Zone. Note that this setting overrides permissions granted in the Programs panel.</td>
</tr>
<tr>
<td>Block Internet servers</td>
<td>Prevents all programs on your computer from acting as servers to the Internet Zone. Note that this setting overrides permissions granted in the Programs panel.</td>
</tr>
<tr>
<td>Enable ARP protection</td>
<td>Blocks all incoming ARP (Address Resolution Protocol) requests except broadcast requests for the address of the target machine. Also blocks all incoming ARP replies except those in response to outgoing ARP requests.</td>
</tr>
<tr>
<td>Filter IP traffic over 1394</td>
<td>Filters FireWire traffic. You must restart your computer if you select this option.</td>
</tr>
<tr>
<td>Allow VPN Protocols</td>
<td>Allows the use of VPN protocols (ESP, AH, GRE, SKIP) even when High security is applied. With this option disabled, these protocols are allowed only at Medium security.</td>
</tr>
</tbody>
</table>
Automatic network detection helps you configure your Trusted Zone easily so that traditional local network activities such as file and printer sharing aren't interrupted. The client detects only networks to which you are physically connected. Routed or virtual network connections are not detected.

You can set the client to silently include every detected network in the Trusted Zone; or to ask you in each case whether to add a newly detected network.

### Setting Network Security Options

To specify Network settings:

1. Open **Firewall** | **Main**.
2. Click **Advanced**.
3. In the Network settings area, choose your security settings.

<table>
<thead>
<tr>
<th><strong>Table 4-3</strong> General Security Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Security Setting</strong></td>
</tr>
<tr>
<td>Allow uncommon protocols at high security</td>
</tr>
<tr>
<td>Lock hosts file</td>
</tr>
<tr>
<td>Disable Windows Firewall</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Table 4-4</strong> Network Security Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Include networks in the Trusted Zone upon detection</strong></td>
</tr>
<tr>
<td><strong>Exclude networks from the Trusted Zone upon detection</strong></td>
</tr>
<tr>
<td><strong>Ask which Zone to place new networks in upon detection</strong></td>
</tr>
</tbody>
</table>
Managing Zone Traffic

The Zones tab contains the traffic sources (computers, networks, or sites) you have added to the Trusted Zone or Blocked Zone. It also contains any networks that the client has detected. If you are using a single, non-networked PC, the traffic source list displays only your ISP (Internet Service Provider) network, which should be in the Internet Zone.

To open the Zone traffic list, click Firewall Zones.

In This Section

Viewing Zone Traffic page 87
Modifying Zone Traffic Sources page 88
Adding to the Trusted Zone page 88
Adding to the Blocked Zone page 90

Viewing Zone Traffic

The zone traffic list displays the traffic sources and the Zones to which they belong.

Table 4-5 Information of Zone Traffic Source List

<table>
<thead>
<tr>
<th>Zone Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name you assigned to this computer, site, or network.</td>
</tr>
<tr>
<td>IP Address/Site</td>
<td>The IP address or host name of the traffic source.</td>
</tr>
<tr>
<td>Entry Type</td>
<td>The type of traffic source: Network, Host, IP, Site, or Subnet. <strong>Warning</strong> - Allowing or blocking traffic for the Host traffic type may enable security settings to be bypassed, particularly in networks where hosts received dynamically assigned IP addresses.</td>
</tr>
<tr>
<td>Zone</td>
<td>The Zone to which the traffic source is assigned: Internet, Trusted, or Blocked.</td>
</tr>
</tbody>
</table>

87
Modifying Zone Traffic Sources

From the Zone traffic source list, you can move the traffic source from one Zone to another, add, edit, or remove a traffic source.

To change the Zone of a traffic source:
1. Open Firewall Zones.
2. Locate the traffic source.
3. Click in the Zone column and choose a Zone.
4. Click Apply.

To add, remove, or edit a traffic source:
1. Open Firewall Zones.
2. In the Name column, click the traffic source, then click Add, Edit, or Remove.
3. Click Apply.

Adding to the Trusted Zone

The Trusted Zone contains computers you trust want to share resources with. For example, if you have three home PCs that are linked together in an Ethernet network, you can put each individual computer or the entire network adapter subnet in the Trusted Zone. The Trusted Zone’s default medium security settings enable you to safely share files, printers, and other resources over the home network. Hackers are confined to the Internet Zone, where high security settings keep you safe.

Note - Note that allowing or blocking traffic for the Host traffic type may allow security settings to be bypassed, particularly in networks where hosts received dynamically assigned IP addresses.

To add a single IP address:
1. Open Firewall Zones.
2. Click Add and choose IP address.
   The Add IP Address window appears.
3. Select Trusted from the Zone drop-down list.
4. Provide the IP address and a description, and then click OK.
Adding to the Trusted Zone

To add an IP range:
1. Open Firewall|Zones.
2. Click Add and choose IP address.
   The Add IP Range window appears.
3. Select Trusted from the Zone drop-down list.
4. Provide the beginning IP address in the first field, and the ending IP address in the second field.
5. Provide a description.
6. Click OK.

To add a subnet:
1. Open Firewall|Zones.
2. Click Add and choose Subnet.
   The Add Subnet window appears.
3. Select Trusted from the Zone drop-down list.
4. Provide the IP address in the first field, and the Subnet mask in the second field.
5. Provide a description.
6. Click OK.

To add to a Host or Site to the Trusted Zone:

   Note - To see the IP addresses before adding the site, click Lookup. If the IP addresses associated with the host name are changed after you place the host in the Trusted Zone, those IP addresses are not added to the Trusted Zone.

1. Open Firewall|Zones.
2. Click Add, then select Host/Site. The Add Host/Site window appears.
3. Select Trusted from the Zones drop-down list.
4. Provide the fully qualified host name in the Host name field.
5. Provide a description of the host and site.
6. Click OK.
   The client resolves the host name you enter with its IP address(es) and adds those IP addresses to the Trusted Zone.
To add a network to the Trusted Zone:
1. Open Firewall > Zones.
2. In the Zone column, click the row containing the network, then select Trusted.
3. Click Apply.

**Note** - The client automatically detects new network connections and helps you add them to the right Zone. For more information, see Network Configuration.

**Adding to the Blocked Zone**

To add to the Blocked Zone, follow the instructions for adding to the Trusted Zone, but select Blocked from the drop-down list in step 3.
Blocking and Unblocking Ports

The client's default security levels determine which ports and protocols are allowed and which are blocked. If you are an advanced user, you can change the definition of the security levels by changing port permissions and adding custom ports.

Default Port Permission Settings

The default configuration for High security blocks all inbound and outbound traffic through ports not being used by programs you have given access or server permission except:

- DHCP broadcast/multicast
- Outgoing DHCP (port 67) - on Windows 9x systems
- Outgoing DNS (port 53) - If the computer is configured as an ICS gateway

<table>
<thead>
<tr>
<th>Traffic Type</th>
<th>Security levels</th>
<th>Traffic Type</th>
<th>Security levels</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>HIGH</td>
<td>MED</td>
<td>LOW</td>
</tr>
<tr>
<td>DNS outgoing</td>
<td>block</td>
<td>n/a</td>
<td>allow</td>
</tr>
<tr>
<td>DHCP outgoing</td>
<td>block</td>
<td>n/a</td>
<td>allow</td>
</tr>
<tr>
<td>broadcast/ multicast</td>
<td>allow</td>
<td>allow</td>
<td>allow</td>
</tr>
<tr>
<td><strong>ICMP</strong></td>
<td></td>
<td></td>
<td><strong>UDP</strong></td>
</tr>
<tr>
<td>incoming (ping echo)</td>
<td>block</td>
<td>allow</td>
<td>allow</td>
</tr>
<tr>
<td>incoming (other)</td>
<td>block</td>
<td>allow</td>
<td>allow</td>
</tr>
<tr>
<td>outgoing (ping echo)</td>
<td>block</td>
<td>allow</td>
<td>allow</td>
</tr>
<tr>
<td>outgoing (other)</td>
<td>block</td>
<td>allow</td>
<td>allow</td>
</tr>
<tr>
<td>IGMP</td>
<td></td>
<td></td>
<td>outgoing</td>
</tr>
<tr>
<td>incoming</td>
<td>block</td>
<td>allow</td>
<td>allow</td>
</tr>
<tr>
<td>outgoing</td>
<td>block</td>
<td>allow</td>
<td>allow</td>
</tr>
</tbody>
</table>

Table 4-6 Default Access Permissions for Traffic Types
To change a port's access permission:

1. Open Firewall|Main.

2. In either the Internet Zone Security or the Trusted Zone Security area, click Custom.

   The Custom Firewall Settings window appears.

3. Scroll to locate High and Medium security settings.

4. To block or to allow a specific port or protocol, select the relevant check box.

5. Click OK.

   **Note** - Be aware that when you select a traffic type in the High security settings list, you are choosing to ALLOW that traffic type to enter your computer under High security, thus decreasing the protection of the HIGH security level. Conversely, when you select a traffic type in the Medium security settings list, you are choosing to BLOCK that traffic type under Medium security, thus increasing the protection of the MED security level.

### Adding Custom Ports

You can allow communication through additional ports at High security, or block additional ports at Medium security by specifying individual port numbers or port ranges.

**To specify additional ports:**

1. Open Firewall|Main.

2. In either the Trusted Zone or Internet Zone area, click Custom.

   The Custom Firewall settings window appears.

3. Scroll to the security level (High or Medium) to which you want to add ports.

4. Select port type that is marked with *none selected*: incoming UDP, outgoing UDP, incoming TCP, or outgoing TCP.

5. Provide the port or port ranges you want to allow or block in the Ports field, separated by commas. For example, 139, 200-300.

6. Click OK.
Configuring VPN Connection for Firewall

Endpoint Security client is compatible with many types of VPN client software and can automatically configure the connection for certain VPN clients.

In This Section

- Supported VPN Protocols
- Configuring VPN Connection Automatically
- Configuring VPN Connection Manually

Supported VPN Protocols

The client monitors the VPN protocols listed in the following table.

<table>
<thead>
<tr>
<th>Networking Protocol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AH</td>
<td>Authentication Header Protocol</td>
</tr>
<tr>
<td>ESP</td>
<td>Encapsulating Security Payload protocol</td>
</tr>
<tr>
<td>GRE</td>
<td>Generic Routing Encapsulation protocol</td>
</tr>
<tr>
<td>IKE</td>
<td>Internet Key Exchange protocol</td>
</tr>
<tr>
<td>IPSec</td>
<td>IP Security protocol</td>
</tr>
<tr>
<td>L2TP</td>
<td>Layer 2 Tunneling protocol. L2TP is a more secure variation of PPTP.</td>
</tr>
<tr>
<td>LDAP</td>
<td>Lightweight Directory Access protocol</td>
</tr>
<tr>
<td>PPTP</td>
<td>Point-to-Point Tunneling protocol</td>
</tr>
<tr>
<td>SKIP</td>
<td>Simple Key Management for Internet Protocol</td>
</tr>
</tbody>
</table>

Configuring VPN Connection Automatically

When VPN traffic is detected, an Automatic VPN Configuration alert is displayed. Depending upon the type of VPN activity detected, and whether the client was able to configure your VPN connection automatically, you may see an Automatic VPN Configuration alert.
For detailed information about the types of Automatic VPN Configuration alerts you may see and how to respond to them, see “New Program Alerts” on page 180.

For example, manual action may be required if the loopback adaptor or the IP address of the VPN gateway falls within a range or subnet that you have blocked.

**Configuring VPN Connection Manually**

If your VPN connection cannot be configured automatically, the client displays a Manual Action Required alert, informing you of manual changes needed to configure your connection.

**In This Section**

- Adding VPN Resources to Trusted Zone
- Unblocking the VPN Gateway
- Allowing VPN Protocols
- Granting Access Permission to VPN Software

**Adding VPN Resources to Trusted Zone**

You must add the VPN gateway to the Trusted Zone. In addition, there may be other VPN-related resources that need to be in the Trusted Zone for your VPN to function properly.

**Required Resources**

The resources below are required by all VPN computers and must be added to the Trusted Zone.

- VPN Concentrator
- Remote host computers connected to the VPN client (if not included in the subnet definitions for the corporate network)
- Corporate Wide Area Network (WAN) subnets that will be accessed by the VPN client computer
- Corporate LANs that will be accessed by the VPN computer

**Other VPN Resources**

The resources below may or may not be required, depending on your specific VPN implementation.

- DNS servers
Configuring VPN Connection Manually

- Local host computer's NIC loopback address (depending on Windows version). If you specify a local host loopback address of 127.0.0.1, do not run proxy software on the local host.
- Internet Gateway
- Local subnets
- Security servers (for example, RADIUS, ACE, or TACACS servers)

Unblocking the VPN Gateway

If the VPN gateway falls within a range or subnet that you have blocked, you must manually unblock the range.

To unblock an IP range or subnet:
1. Open Firewall | Zones.
2. In the Zone column, select the blocked IP range or subnet.
3. Select Trusted.
4. Click Apply.

Allowing VPN Protocols

To ensure proper configuration of your VPN software with Endpoint Security client, you will need to modify your general security settings to allow VPN protocols.

To allow VPN protocols:
1. Open Firewall | Main.
2. Click Advanced.
3. In the General settings area, select the Allow VPN protocols check box.
4. Click OK.

Note - If your VPN program uses protocols other than GRE, ESP, and AH, also select the Allow uncommon protocols at high security check box.

Granting Access Permission to VPN Software

Grant access permission to the VPN client and any other VPN-related programs.
To grant permission to your VPN program:
1. Open Program Control\Programs.
2. In the Programs column, select your VPN program. If your VPN program is not listed, click Add to add it to the list.
3. In the Access column, click below Trusted and choose Allow.

To grant access to VPN-related components:
1. Open Program Control\Components.
2. In the Components column, select the VPN component for which you want to grant access.
3. In the Access column, select Allow.
Chapter 5

Program Control

Program control protects you by making sure that only programs you trust can access the Internet. You can use the Program alerts to configure program permissions as they are needed, or use the Programs tab to establish permissions ahead of time. Advanced users can also control the ports that each program is permitted to use.

In This Chapter

- Understanding Program Control  page 99
- Setting Program Control Options  page 101
- Configuring Program Access  page 103
Understanding Program Control

Everything you do on the Internet - from browsing Web pages to downloading MP3 files - is managed by specific programs on your computer.

Hackers exploit this fact by planting malware on your computer. Malware can be sent as e-mail attachments, that are installed as soon as you open them. You may also download and install malware that has been disguised as an update to a legitimate program.

Once on your machine, malware can wreak havoc in a variety of ways. It may raid your address book and send itself to everyone in it. It may listen for connection requests from the Internet, then the hacker can contact it and give it instructions, effectively taking control of your computer.

To protect your computer from these threats, the Program Control feature uses Program Authentication (verifies that your programs haven't been tampered with) and Program Access Control (provides access or server permission only when you tell it to).

Program Access Control

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 check box 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.

For more information, see “Program Alerts” on page 180.
Program Authentication

Whenever a program on your computer attempts to access the Internet, Endpoint Security client authenticates it with its Smart Checksum. If the program has been altered since the last time it accessed the Internet, the client displays a Changed Program alert.

You decide whether the program should be allowed access or not. For added security, the client also authenticates the components, such as DLL files, associated with the program’s main executable file. If a component has been altered since the last time permission was granted, the client displays a Program Component alert, similar in appearance to the Changed Program alert.

For more information, see “Changed Program Alerts” on page 182.
Setting Program Control Options

When you're using Endpoint Security client, no program on your computer can access the Internet or your local network, or act as a server, unless you give it permission to do so.

Setting Program Control Level

Use the program control level to regulate the number of Program alerts you will see when you first begin using the client.

To set the global program control level:
1. Open Program Control|Main.
2. In the Program Control area, click the slider and drag it to the desired setting:
   - **HIGH**: Advanced program and component control and Application Interaction Control are enabled.
     - You may see a large number of alerts.
     - Programs and components are authenticated.
     - Program permissions are enforced.
   - **MED**: Advanced program control and Application Interaction Control are disabled.
     - Fewer alerts display.
     - Component learning mode is active.
     - Programs are authenticated; components are learned.
     - Program permissions are enforced.
   - **LOW**: Advanced program control is disabled.
     - Program and Component Learning Mode is active.
     - No program alerts are displayed.
   - **OFF**: Program control is disabled.
     - No programs or components are authenticated or learned.
     - No program permissions are enforced.
     - All programs are allowed access/server rights.
     - No program alerts are displayed.

Check Point recommends the **Medium** setting for the first few days of normal use. This component learning mode enables the client to quickly learn the MD5 signatures of many frequently used components without interrupting your work. Use
this setting until you have used Internet-accessing programs (for example, browser, e-mail, and chat) at least once with the client running; then change your Program Control setting to High.

Enabling Automatic Lock

The automatic Internet lock protects your computer if you leave it connected to the Internet for long periods even when you're not actively using network or Internet resources.

When the lock engages, only traffic initiated by programs to which you have given Pass-lock permission is allowed. All traffic to and from your computer is stopped, including DHCP messages, or ISP heartbeats, used to maintain your Internet connection. As a result, you may lose your Internet connection.

You can set the Internet lock to engage:

- When your screen saver engages, or
- After a specified number of minutes of network inactivity.

**To enable or disable the automatic lock:**

1. Open Program Control | Main.
2. In the Automatic Lock area, select On or Off.

**To set automatic lock options:**

1. Open Program Control | Main.
2. In the Automatic Lock area, click Custom.
   The Custom Lock Settings window appears.
3. Specify the lock mode to use.
   - **Lock after ___ minutes of inactivity**: Engages automatic lock after the specified number of minutes has passed. Specify a value between 1 and 99.
   - **Lock when screensaver activates**: Engages automatic lock whenever your screen is activated.
Configuring Program Access

You can configure program access automatically or manually. Using the Program Wizard, you can automatically configure Internet access for some of the most commonly used programs.

Setting Program Access Permissions

Endpoint Security client displays a New Program alert when a program on your computer tries to access the Internet or local network resources for the first time. It displays a Server Program alert when a program tries to act as a server for the first time. You can configure the client to automatically allow or block new programs without displaying an alert. For example, if you are sure you have given access permission to all the programs you want, you can automatically deny access to any program that asks for permission.

To set connection attempt permissions for new programs:
1. Open Program Control|Main.
2. Click Advanced.
   The Advanced Program Settings window opens.
3. In the Connection Attempts area, specify your preferences for each Zone.
   • **Always allow access**: Allows all new programs access to the specified Zone.
   • **Always deny access**: Denies programs access to the specified Zone.
   • **Always ask for permission**: Displays an alert asking for permission for the program to access the specified Zone.

Note - Settings for individual programs can be established in the Programs tab. Settings in this panel apply ONLY to programs not yet listed in the Programs tab.
To set server attempt permissions for new programs:

1. Open Program Control | Main.
2. Click Advanced.
3. In the Server Attempts area, specify your preferences for each Zone.
   - **Always accept the connection:** Allows all programs attempting to act as a server.
   - **Always deny the connection:** Denies all programs attempting to act as a server.
   - **Always ask before connecting:** Displays an alert asking for permission for the program to act as a server.

**Customizing Program Control Settings**

By default, the client always asks you whether to block or to allow connection attempts and server access attempts for the Internet and Trusted Zones. If the TrueVector Service is running, but the client is not, program access is denied by default.

You can customize program control by setting global program properties.

**To set global program properties:**

1. Open Program Control | Main.
2. Click Advanced, then open the Alerts & Functionality tab.
3. Specify global program options.
   - **Show alert when Internet access is denied:** Displays a Blocked Program alert when the client denies access to a program. To have access denied silently, clear this option.
   - **Deny access if permission is set to "ask" and the TrueVector service is running but the client is not:** Protects the client application from the rare event of an independent process (such as a Trojan horse) shutting down the client but leaving the TrueVector service running.
   - **Require password to allow a program temporary Internet access:** Prompts you to enter a password to grant access permission. Requires that you be logged in to respond Yes to a Program alert. To allow access without a password, clear this option.
Setting Specific Permissions

By setting the Program Control level to High, Medium, or Low, you specify globally whether programs and their components must request permission before accessing the Internet or before acting as a server.

You can also specify different settings for an individual program. For example, if you wanted to allow access to a particular program, but keep security High for all other programs, you could set the permission for that program to Allow.

In This Section

- Using the Programs List page 106
- Adding Programs to the Programs List page 107
- Granting Internet Access Permissions to Programs page 108
- Granting Server Permission to Programs page 108
- Granting Pass-lock Permission to Programs page 109
- Granting Send Mail Permission to Programs page 109
- Advanced Program Control page 109
- Disabling Outbound Mail Protection page 110
- Setting Filter Options page 110
- Setting Authentication Options page 111
- Allowing Others to Use Programs page 111
Using the Programs List

The programs list contains the programs that have tried to access the Internet or the local network and tells you which Zone the program is in, whether the program can act as a server, and whether the program can send e-mail. As you use your computer, the client detects every program that requests network access and adds it to the programs list.

To access the programs list:
- Open Program Control|Programs.

The Access, Server, and Send Mail columns indicate whether a specific program is allowed to access the Internet, to act as a server, and to send e-mail.

Table 5-1 Program Permission Icons

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓</td>
<td>The program is allowed access/server rights. To change the permission, click the icon and choose either Block or Ask.</td>
</tr>
<tr>
<td>?</td>
<td>The client will display a Program alert when the program asks for access and/or server rights. To change the permission, click the icon and choose either Allow or Block.</td>
</tr>
<tr>
<td>✗</td>
<td>The program is denied access/server rights. To change the permission, click the icon and choose either Allow or Ask.</td>
</tr>
<tr>
<td></td>
<td>The program is currently active.</td>
</tr>
<tr>
<td></td>
<td>The program has pass-lock permission: it can continue to access the Internet when the Internet Lock is engaged. To change the permission, click the icon and choose Normal.</td>
</tr>
</tbody>
</table>
Adding Programs to the Programs List

If you want to specify access or server permission for a program that does not appear on the programs list, you can add the program to the list and set permissions.

To add a program to the programs list:
1. Open Program Control|Programs.
2. Click Add.
   The Add Program window appears.
3. Select the program you want to add and click Open.
   Be sure to select the program’s executable file.

To edit a program on the programs list:
1. Open Program Control|Programs.
2. Right-click a program in the Programs column and choose one of the available options:
   • Changes Frequency: The client uses only file path information to authenticate the program. The MD5 signature will not be checked. Caution: This is a Low security setting.
   • Options: Opens the Program Options dialog box, in which you can customize security options and create expert rules for programs.
   • Properties: Opens your operating system's properties dialog box for the program.
   • Remove: Deletes the program from the list.
Granting Internet Access Permissions to Programs

There are different ways a program can be granted permission to access the Internet: through a response to an alert, through manual configuration in the programs list, and by automatic configuration by the client.

Many of your most commonly used programs can be automatically configured for safe Internet access. To determine whether a program was configured manually or automatically, select the program in the Programs List and refer to the Entry Details field.

Built-in rules ensure a consistent security policy for each program. Programs with access to the Internet Zone also have access to the Trusted Zone. Programs with server permission in a Zone also have access permission for that Zone. This is why (for example) selecting Allow under Trusted Zone/Server automatically sets all of the program’s other permissions to Allow.

To grant a program permission to access the Internet:
1. Open Program Control|Programs.
2. In the Programs column, click the program and choose Allow.

Granting Server Permission to Programs

Exercise caution when granting permission for programs to act as a server, as Trojan horses and other types of malware often need server rights. Permission to act as a server should be reserved for programs you know and trust, and that need server permission to operate properly.

To grant a program permission to act as a server:
1. Open Program Control|Programs.
2. In the Programs column, click the program and choose Allow.
Granting Pass-lock Permission to Programs

When the Internet Lock is engaged, programs given pass-lock permission can continue to access the Internet. If you grant pass-lock permission to a program, and that program uses other applications to perform its functions (for example, services.exe), be sure to give those other programs pass-lock permission as well.

To grant pass-lock privilege:
1. Open Program Control|Programs.
2. Click in the Lock column of the program and choose Pass Lock.

Granting Send Mail Permission to Programs

To enable your e-mail program to send e-mail messages and to enable protection against e-mail threats, grant send mail permission to your e-mail program. For more information, see “E-mail Protection” on page 150.

To grant send mail permission to a program:
1. Open Program Control|Programs.
2. In the list, click in the Send Mail column of the program and choose Allow.

Advanced Program Control

Advanced Program Control tightens your security by preventing unknown programs from using trusted programs to access the Internet, and by preventing hackers from using the Windows CreateProcess and OpenProcess functions to manipulate your computer.

By default, the following applications are allowed to use other programs to access the Internet:
- Endpoint Security
- MS Word, Excel, PowerPoint, and Outlook

To enable Advanced Program Control for a program:
1. Open Program Control|Programs.
2. In the Programs column, select a program.
3. Click Options.
Disabling Outbound Mail Protection

By default, Outbound Mail protection is enabled for all programs. Because the ability to send e-mail is not a characteristic of all programs, you may choose to disable Outbound Mail protection for any program that does not require it.

To disable Outbound Mail protection for a program:

1. Open Program Control | Programs.
2. Select a program from the list and then click Options.
   The Program Options window appears.
3. Open the Security tab.
4. Clear the Enable Outbound E-mail Protection for this program check box.

For more information, see “Outbound MailSafe Protection” on page 151.

Setting Filter Options

By default, Privacy protection and Web Filtering is disabled for all programs. You can enable these features for a program from the Program Options window.

To enable Privacy protection and Web Filtering for a program:

1. Open Program Control | Programs.
2. Select a program from the list and then click Options.
3. Open the Security tab.
4. In the Filter Options area, select the Enable Privacy for this program check box.

For more information, see Chapter 7, “Privacy.”
Setting Authentication Options

By default, all programs are authenticated by their components. You can specify authentication options for a program from the Program Options window.

Allowing Others to Use Programs

You may want to prevent your children from changing your security settings, but still allow them to use new programs.

To allow access to programs without using a password:

1. Open Overview/Preferences.
2. Click Set Password.
3. Select the Allow others to use programs without a password (unless the program permission is set to "Block") check box.

With this option selected, users must provide a password before they will be allowed to change your settings. However, without providing a password, users will be able to allow Internet access for new programs and programs whose permissions are set to "Ask". For programs explicitly blocked by you, access will continue to be denied.

4. Click OK.
Managing Program Components

For each program on your computer, you can specify whether the client will authenticate the base executable only, or the executable and the components it loads. In addition, you can allow or deny access to individual program components.

The Components List contains the program components for allowed programs that have tried to access the Internet or the local network. The Access column indicates whether the component is always allowed access, or whether the client should alert you when that component requests access.

As you use your computer, the client detects the components that are used by your programs and adds them to the Components List.

**To access the Components List:**
- Open Program Control|Components.

**To grant access permission to a program component:**
1. Open Program Control|Components.
2. Select a component from the list and then click in the Access column and choose Allow.
Using Programs with the Client

To ensure that your other software programs are compatible with the client, you may need to modify the program’s configuration settings.

Many of your most commonly used programs can be configured automatically for Internet access. To see if the programs you use can be automatically configured, consult the list in the Program Wizard. Although in some cases Internet access can be configured automatically, many programs also require server access rights.

In This Section

Using Antivirus Software ............................................ page 113
Using Browsers .......................................................... page 114
Using Chat ............................................................... page 115
Using E-mail .............................................................. page 115
Using Internet Answering Services ......................... page 115
Using File Sharing ........................................................ page 116
Using FTP ................................................................. page 116
Using Streaming Media ............................................... page 116
Using Games ............................................................. page 117
Using Remote Control ................................................. page 118
Using VNC ................................................................. page 118
Using Voice over IP ..................................................... page 119
Using Web Conferencing ............................................ page 119

Using Antivirus Software

For antivirus software to receive updates, it must have access permission for the Trusted Zone.

To receive automatic updates from your antivirus software vendor, add the domain that contains the updates (e.g., update.avsupdate.com) to your Trusted Zone. See “Adding to the Trusted Zone” on page 88.
For your browser to work properly, it must have access permission for the Internet Zone and Trusted Zone. Before granting permission, make sure that you understand how to configure your browser's security for optimal protection and have the latest service packs installed for the browser you are using.

**To grant access your browser access permission, do any of the following:**
- Run the Program Wizard.
  - The client will automatically detect your default browser and prompt you to grant it Internet Zone access.
- Grant access to the program directly. See “Granting Internet Access Permissions to Programs” on page 108.
  - Answer Yes when a Program alert for the browser appears.

**Microsoft Internet Explorer**

If you are using Windows 2000, you may need to allow Internet access rights to the Services and Controller Application (the file name is typically services.exe).

**To grant Internet access permission to the Services and Controller Application:**
1. Open **Program Control**|**Programs**.
2. In the **Programs** column, locate **Services and Controller Application**.
3. Click in the **Access** column and choose **Allow**.

**Mozilla Browsers**

Netscape Navigator versions above 4.73 will typically experience no problems running concurrently with the client. If you are using Navigator version 4.73 or higher, or Mozilla Firefox, and still experience difficulty accessing the Web with the client active, check the browser Preferences to make sure you are not configured for proxy access.
Using Chat

Chat and instant messaging programs (for example, AOL Instant Messenger) may require server permission to operate properly.

To grant server permission to your chat program:

- Answer Yes to the Server Program alert.
- Grant server permission to the program (see “Granting Server Permission to Programs” on page 108).

**Warning** - We strongly recommend that you set your chat software to refuse file transfers without prompting first. File transfer within chat programs is a means to distribute malware such as worms, viruses, and Trojan horses. Refer to your chat software vendor’s help files to learn how to configure your program for maximum security.

Using E-mail

For your e-mail program (for example, Microsoft Outlook) to send and receive mail, it must have access permission for the Zone the mail server is in. In addition, some e-mail client software may have more than one component requiring server permission. For example, Microsoft Outlook requires that both the base application (OUTLOOK.EXE) and the Messaging Subsystem Spooler (MAPISP32.exe) to have server permission.

To securely give e-mail programs access:

1. Add the local mail server to the Trusted Zone (see “Adding to the Trusted Zone” on page 88).
2. Limit the e-mail program access to the Trusted Zone.
3. Add the remote mail server (host) to the Trusted Zone.

To learn how to give a program permission to access or act as a server to the Trusted Zone, see “Setting Program Control Options” on page 101.

**Note** - You can also heighten security by limiting the ports that your e-mail program can use. See “Default Port Permission Settings” on page 91.

Using Internet Answering Services

To use Internet answering machine programs (such as CallWave) with the client:
1. Give the program server permission and access permission for the Internet Zone.
2. Add the IP address of the vendor's servers to the Trusted Zone.
3. Set the security level for the Internet Zone to medium.

**Note** - To find the server IP address, contact the vendor's technical support.

**Using File Sharing**

File sharing programs, such as Napster, Limewire, AudioGalaxy, or any Gnutella client software, must have server permission for the Internet Zone to work with the client.

**Using FTP**

To use FTP (File Transfer Protocol) programs, you may need to adjust your FTP client program settings.

**To enable FTP with the client:**

1. Enable passive or PASV mode in your FTP client.
   This tells the client to use the same port for communication in both directions. If PASV is not enabled, the client may block the FTP server's attempt to contact a new port for data transfer.
2. Add the FTP sites you use to the Trusted Zone (see “Adding to the Trusted Zone” on page 88).
3. Give Trusted Zone access permission to your FTP client program (see “Setting Program Access Permissions” on page 103).

**Using Streaming Media**

Applications that stream audio and video, such as RealPlayer, Windows Media Player, and QuickTime, must have server permission for the Internet Zone to work with the client. See “Granting Server Permission to Programs” on page 108.
Using Games

To play games over the Internet while using the client, you may have to adjust the program permissions and security levels.

**Program Permission**

Internet games require access permission, server permission, or both, to the Internet Zone.

The easiest way to grant access is to answer Yes to the program alert of game program. However, many games run in "exclusive" full screen mode, which prevents you from seeing the alert.

**To solve this problem:**

- **Set the game to run in a window.**
  
  This will allow you to see the alert, if the game is running at a resolution lower than that of your desktop. If the alert appears but you cannot respond to it because your mouse is locked to the game, press the Windows key on your keyboard. After granting the game program Internet access, reset the game to run full-screen.

- **Use Software Rendering Mode.**
  
  By changing your rendering mode to "Software Rendering," you can allow Windows to display the alert on top of your game screen. After allowing the game Internet access, you can change back to your preferred rendering device.

- **Use Alt+Tab.**
  
  Press Alt+Tab (or Alt+Enter, depending on environment) to toggle back into Windows. This leaves the game running, but allows you to respond to the alert. Once you have allowed Internet access, press Alt+Tab again to restore your game. Note: This may cause some applications in crash (especially in Glide or OpenGL); however, the problem should be corrected for the next run.

**Security Level and Zone**

Some Internet games, particularly those that use Java, applets, or other Web-based portal functionality, may not work properly when your Internet Zone security level is set to High. High security will also prevent remote game servers from seeing your computer. To solve these problems, you can:

- **Change your Internet Zone security level to Medium, or**
• Add the game server you're connecting to your Trusted Zone (see page 88). The documentation from the game manufacturer's Web site should indicate the IP address or host name of the server.

**Warning** - Trusting game servers means trusting the other players in the game. Endpoint Security client does not protect you from attacks instigated by fellow gamers in a trusted environment. Make sure that you understand how to configure your browser's security for optimal protection and have the latest service packs installed for the browser you are using.

**Using Remote Control**

If your computer is either the host or the client of a remote access system such as PCAnywhere or Timbuktu, configure the remote control.

**To configure remote access:**

1. Add the IP addresses of the hosts or clients to your Trusted Zone (see “Adding to the Trusted Zone” on page 88).
2. Add the subnet of the network you are accessing remotely to your Trusted Zone.
3. If a dynamic IP address is assigned to the remote machine, add the DHCP server address or range of addresses to the Trusted Zone.

**Warning** - If your remote control client or host is on a network not under your control (for example on a business or university LAN), perimeter firewalls or other features of the network may prevent you from connecting. If you still have problems connecting after following the instructions above, contact your network administrator for assistance.

**Using VNC**

**To enable VNC and Endpoint Security to work together:**

1. On both the server and viewer (client) machine, do one of the following:
   
   • If you know the IP address or subnet of the viewer (client) you will be using for remote access, and it will always be the same, add that IP or subnet to the Trusted Zone (see “Adding to the Trusted Zone” on page 88).
   
   • If you do not know the IP address of the viewer, or it will change, give the program access permission and server permission for the Trusted and Internet Zones (see “Setting Program Access Permissions” on page 103).

When prompted by VNCviewer on the viewer machine, provide the name or IP address of the server machine, followed by the password. You should be able to connect.
2. On the viewer (client) machine, run VNCviewer to connect to the server machine. Do not run in "listen mode."

Warning - If you enable VNC access by giving it server permission and access permission, be sure to set and use your VNC password to maintain security. We recommend adding the server and viewer IP addresses to the Trusted Zone, rather than giving the application Internet Zone permission.

Using Voice over IP

To use Voice over IP (VoIP) programs with the client, you must to do one or both of the following, depending on the program:

1. Give the VoIP application server permission and access permission.
2. Add the VoIP provider's servers to the Trusted Zone. To learn the IP addresses of these servers, contact your VoIP provider's customer support.

Using Web Conferencing

If you experience problems using a Web conferencing program, such as Microsoft Netmeeting:

1. Add the domain or IP address that you connect to, to the Trusted Zone (see "Adding to the Trusted Zone" on page 88).
2. Disable the web conferencing program's "Remote Desktop Sharing" option.
Full Disk Encryption is a policy-based, enterprise security software solution that combines boot protection, preboot authentication and strong encryption to ensure only authorized users are granted access to information stored in desktop and laptop PCs.

Full Disk Encryption is deployed and administered across the network. As encryption is both automatic and transparent, security is enforced without requiring special efforts from users.

In This Chapter

- Authenticating Full Disk Encryption  page 121
- Optional Full Disk Encryption Features  page 127
- Using the Full Disk Encryption Panel  page 131
Authenticating Full Disk Encryption

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 dialog box opens.

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

Ensuring That Your Computer Has Not Been Tampered With

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 First Time

The following sections explain how to access a Full Disk Encryption-protected computer as a new user.

Assume that your administrator has configured a temporary user account and password for you. Then the first time you authenticate to Full Disk Encryption, you must use the temporary user account name and password.

Once you have successfully entered the temporary user account name and password, Full Disk Encryption prompts you to enter your personal (new) user account name and fixed password (or to use a dynamic token or smart card for authentication). These are the credentials you will use in the future, instead of the temporary user account name and password. Your administrator will inform you of your user name and of requirements for the password.

Instead of a temporary user account, your administrator can have configured your personal user account and a password, or configured a dynamic token or smart card for your authentication. The administrator will inform you how you are to authenticate the first time.
**Using a Fixed Password**

A fixed password is a private string of characters, known only to you and Full Disk Encryption, which you use each time you want to access the computer.

Your Full Disk Encryption administrator will tell you which user account name and password to use the first time you access the Full Disk Encryption-protected computer.

**To authenticate yourself with a fixed password:**


   **Reminder:** If you did not personally start the computer, press **CTRL**+**ALT**+**DEL** to ensure that your computer has not been tampered with. Your computer restarts and Full Disk Encryption re-displays the *User Account Identification* dialog box.

2. In the *User account name* field, enter the user account name you received from your administrator.

3. In the *Password* field, enter the password you received from your administrator. The password is obscured with asterisks (*) when entered. Click **OK**.

   If your administrator has configured your ordinary user account instead of a temporary account, please continue with step 6.

   If your administrator has configured a temporary user account for you, Full Disk Encryption informs you that you must change to your regular user name and set a new password. Click **OK** to close the message box.

   You will now enter your personal (new) user account name and fixed password. These are the credentials you will use in the future, instead of the temporary user account name and password that you just used.

   The Temporary User dialog box opens.

4. Enter your personal user account name and click **OK**.

5. Enter and confirm the fixed password you want to use and click **OK**.

   Full Disk Encryption confirms that you have successfully accessed the computer for the first time using your Full Disk Encryption credentials.

6. Click **Continue** to close the dialog box. Full Disk Encryption now allows Windows to start.
**Using a Dynamic Token**

A dynamic token is a password you generate using a password token every time you want to be authenticated by Full Disk Encryption.

*Note* - Your Full Disk Encryption administrator will provide you with a dynamic token, the information you need to use it, and a username.

**To authenticate yourself using a dynamic token:**

1. Start your Full Disk Encryption-protected computer. The **User Account Identification** dialog box opens.
   
   **Reminder:** If you did not personally start the computer, press **CTRL+ALT+DEL** to ensure that your computer has not been tampered with. Your computer restarts and Full Disk Encryption re-displays the **User Account Identification** dialog box.

2. In the **Username** account name field, enter the username you received from your administrator and press **TAB**.
   
   Full Disk Encryption recognizes that you will be using a dynamic token to authenticate yourself and displays the **User Account Identification** dialog box.

3. In the dynamic token, enter the Full Disk Encryption challenge to generate a response.

4. Enter the response in the **Response** field and click **OK**.
   
   Full Disk Encryption confirms that you have successfully accessed the computer for the first time using your Full Disk Encryption credentials.

5. Click **Continue** to close the dialog box. Full Disk Encryption now allows Windows to start.
Using a Smart Card/USB Token

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

Note - Your Full Disk Encryption administrator will supply you with your smart card/USB token, the information you need to use it, and, if necessary, a temporary username and password to use the first time you access the Full Disk Encryption protected computer. Ensure that your smart card/USB token is connected to your computer before you start to authenticate yourself.

To authenticate yourself using a smart card/USB token:

1. Connect your smart card/USB token to your Full Disk Encryption-protected computer.

2. Start your computer.

   The User Account Identification dialog box opens.

   Reminder: If you did not personally start the computer, press CTRL+ALT+DEL to ensure that your computer has not been tampered with. Your computer restarts and Full Disk Encryption re-displays the User Account Identification dialog box.

3. In the User account name field, enter the temporary user account name you received from your administrator and press the TAB key to move to the Password field.

4. Enter the password you received from your administrator and click OK.

   If your administrator has configured your ordinary user account instead of a temporary account, please continue with step 6.

   If your administrator has configured a temporary user account for you, Full Disk Encryption informs you that you must change to your regular user name and set a new password. Click OK to close the message box.

   The Temporary User dialog box opens.

5. Enter your new user account name and click OK.

   Full Disk Encryption recognizes that you have a user account that uses a smart card for authentication. It confirms that this is the first time you are logging on with the new user account name. The Logon Successful dialog box opens.

6. Click Continue.

   After Windows loads, the Change Credentials dialog box opens.
7. Select the certificate you want to use and click OK.

   **Note** - Do NOT choose the Personal Store certificate. If you do, you will not be able to authenticate yourself after restarting the computer.

   The ‘personal store’ from which you select a certificate is a container on your computer, not on the token. For this reason, it is not available before you have gained access to the operating system.

   Full Disk Encryption confirms that your user certificate has been updated.

8. Click OK.

9. Restart the computer when prompted to do so.

   After restarting, the Token Authentication dialog box opens.

10. Enter your PIN.

    The PIN is obscured with asterisks (*) when entered.

11. Click OK.

    **Note** - Regardless of the keyboard layout used, we recommend that you use smart card PINs that are comprised only of ASCII characters:

    !"#$%&'()*+,-./0123456789:;<=>?@
    ABCDEFGHIJKLMNOPQRSTUVWXYZ
    \[]^_`abcdefghijklmnopqrstuvwxyz{|}~

    The space character is also an ASCII character.

---

**What if I forget my password?**

If you forget your password, you can use the Full Disk Encryption Password Change option.

**To change your password:**


2. Enter your username and select Remote Help.

3. Call your Full Disk Encryption administrator or helpdesk to guide you through the password change process.
What if I don't have access to my token/smart card?

If you do not have access to your dynamic token or smart card, you can use the Full Disk Encryption One-time logon option.

To use the One-time logon option:

2. Enter your username and select Remote Help.
3. Select the One-Time Logon option to enable that function. Call your Full Disk Encryption administrator or helpdesk to guide you through the one-time logon process.
Optional Full Disk Encryption Features

This section describes some optional features which your administrator may have chosen to configure for your Full Disk Encryption installation. For example, depending on the configuration, you may or may not be able to use the same password for logging on to Windows as for authenticating yourself to Full Disk Encryption, or you may not have to enter your Full Disk Encryption credentials at all.

In This Section

- Synchronizing Passwords
- Full Disk Encryption Single Sign-on
- Windows Integrated Logon

Synchronizing Passwords

Using Full Disk Encryption's password synchronization, you can synchronize Windows and Full Disk Encryption passwords with each other, assuming that your administrator has enabled password synchronization for your user account.

Depending on the settings configured by your administrator, your passwords may be synchronized in one or both of the following ways:

- Using the Windows password when authenticating to Full Disk Encryption
  
  If this synchronization option has been configured for you, the Windows password is also used for Full Disk Encryption preboot authentication. Once synchronized, changing the Windows password will automatically change the Full Disk Encryption password to the new Windows password.

  (This setting is called Synchronize Windows Password to Preboot in the administrator’s application.)

- Using the Full Disk Encryption password when logging on to Windows
  
  If this synchronization option has been configured for you, the password used for Full Disk Encryption preboot authentication is used also for Windows authentication. Once synchronized, changing the Full Disk Encryption password will automatically change the Windows password to the new Full Disk Encryption password.

  (This setting is called Synchronize Preboot Password to Windows in the administrator’s application.)
Using the Windows Password for Full Disk Encryption

When your password synchronization policy has been changed so that you will use the Windows password to authenticate yourself to Full Disk Encryption, the passwords will be synchronized after you either

- Change your Windows password

or

- Log on to Windows for the first time after the policy change.

You will be prompted to enter your Full Disk Encryption password, and it will be synchronized with the Windows password.

Once the passwords have been synchronized, changing the Windows password will automatically change the Full Disk Encryption password to the new Windows password.

To synchronize the Full Disk Encryption password with the Windows password:

1. When you have either changed your Windows password or log on to Windows for the first time after the policy change, the Password Synchronization dialog box opens.

2. Enter your Full Disk Encryption password and click OK. Full Disk Encryption confirms that your password was changed.

   From now on, use your Windows password when authenticating yourself to Full Disk Encryption.

Using the Full Disk Encryption Password for Windows

When your password synchronization policy has been changed so that you will use the Full Disk Encryption password to log on to Windows, the passwords will be synchronized after you do either of the following:

- Change your Full Disk Encryption password

   When you change your Full Disk Encryption password, you will be prompted for your Windows password. It is then synchronized with your Full Disk Encryption password.

- Log on to Windows for the first time after the policy change

   The passwords are synchronized automatically.
Once the passwords have been synchronized, changing the Full Disk Encryption password will automatically change the Windows password to the new Full Disk Encryption password.

**Full Disk Encryption Single Sign-on**

The Single Sign-on (SSO) feature automatically logs you onto Windows once you have been authenticated by Full Disk Encryption.

*Note* - Your Full Disk Encryption administrator decides whether or not you will have access to SSO.

**First Logon after Enabling SSO**

After the administrator has enabled SSO for your Full Disk Encryption user account on a computer, Full Disk Encryption must learn your account’s credentials. This is done at the first logon after SSO is enabled. At this logon, you log on to Windows as usual. Full Disk Encryption then stores your credentials securely and uses them on subsequent logons where SSO has been enabled.

**De-selecting the SSO Option**

When the SSO option is not selected, no credentials are passed to Windows. This permits a different Windows user account to be used.

*Note* - When SSO has been turned off, no Windows credentials will be recorded or used, and the ‘chain’ is broken. When SSO is then turned back on, the previous credentials must be specified again for SSO to function again.

**SSO and Password Changes**

Periodically, it will be necessary to change your Windows password. Full Disk Encryption will look for Change Password dialog boxes to record the changes. When a Change Password dialog box is opened, Full Disk Encryption records what is entered into the new password field. When you next restart your computer, SSO will work as usual, as the new password has already been stored.

**Logging on with SSO Enabled**

Logging on when SSO is enabled is very similar to logging on without SSO. Just remember to select the **SSO Active** check box.
To log on with SSO enabled:

1. Authenticate yourself as usual in the User Account Identification dialog box.
2. Make sure that the SSO Active check box is selected, and click OK.

Your computer starts, and you are automatically logged on to Windows.

Note - If you do not want to use SSO, you may be able to clear the SSO Active option. This depends on the configuration options selected by your administrator.

Windows Integrated Logon

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

Note - Depending on the settings configured by your Full Disk Encryption administrator, you may not be able to start Windows in safe mode.

Depending on what settings your administrator has configured for your computer, you may need to authenticate yourself to Full Disk Encryption if you have:

- Removed your WIL-enabled computer from the network
- Added hardware devices to your WIL-enabled computer or in any way tampered with the hard drive
- Moved the hard drive to another computer
- Exceeded the allowed number of failed attempts to log on to Windows.

If the system detects any indications of these issues, WIL may be disabled automatically. The computer then restarts, and you must authenticate yourself to Full Disk Encryption before the operating system is loaded.
# Using the Full Disk Encryption Panel

This chapter describes how to use the Full Disk Encryption panel in Endpoint Security Client after you have authenticated yourself to Full Disk Encryption and gained access to the operating system. In the Full Disk Encryption panel, you can:

- View status and encryption information
- Change your Full Disk Encryption user credentials
- Change the language used in the Full Disk Encryption client user interface.

## Viewing Status and Encryption Information

You can view the status information of your Full Disk Encryption installation in the Full Disk Encryption panel.

**To view status information:**

- Open Full Disk Encryption|Main.

## Status Information

The Full Disk Encryption|Main panel displays the following status information.

<table>
<thead>
<tr>
<th>Status field</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Locally installed version</td>
<td>The version of Full Disk Encryption currently installed on this computer.</td>
</tr>
<tr>
<td>Preboot user account</td>
<td>The name of the user account that authenticated at preboot.</td>
</tr>
<tr>
<td>FDEMC user account</td>
<td>The name of the user account currently logged on to FDE Management Console (FDEMC), if applicable.</td>
</tr>
<tr>
<td>MI mode</td>
<td>Indicates whether this installation of Full Disk Encryption is running in MI mode or not. The possible values are: Yes or No.</td>
</tr>
<tr>
<td>Windows integrated logon</td>
<td>The current value specified for the Windows Integrated Logon setting. The possible values are: Enabled or Disabled.</td>
</tr>
<tr>
<td>Last recovery update</td>
<td>Date and time when the most recent recovery file was created.</td>
</tr>
</tbody>
</table>
### Table 6-1  Status Information (2 of 3)

<table>
<thead>
<tr>
<th>Status field</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last recovery file delivery</td>
<td>Date and time a recovery file was last copied to its target directory. The target directory is the directory specified under <strong>Recovery Path</strong> in the <strong>Install</strong> settings under <strong>System Settings</strong>.</td>
</tr>
<tr>
<td>Last log file update</td>
<td>Date and time the log file was last updated by Full Disk Encryption.</td>
</tr>
<tr>
<td>Last log file delivery</td>
<td>Date and time the local log file was last written by Full Disk Encryption. The file name of the local log file is the same as the name of the machine. The local log file is written to the directory or directories specified in <strong>Set Central Log Path(s)</strong> (<strong>Install</strong> settings under <strong>System Settings</strong>).</td>
</tr>
<tr>
<td>Last local edit</td>
<td>Date and time of the most recent change to a Local setting; also contains the group and the user account name of the user who made the change.</td>
</tr>
<tr>
<td>Last update profile</td>
<td>Date and time when the most recent update profile was downloaded and the path, including the profile name, from which it was downloaded.</td>
</tr>
<tr>
<td>License expire date</td>
<td>Date when the license expires. Expiration date is only used for evaluation versions of the product.</td>
</tr>
</tbody>
</table>
Encryption Information

The following Encryption information relevant to each volume is displayed:

Table 6-2  Encryption Information

<table>
<thead>
<tr>
<th>Text</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encrypting name nn%</td>
<td>Displays the progress of encryption, including the name of the encryption algorithm and the percentage of encryption completed.</td>
</tr>
<tr>
<td>Fully encrypted name</td>
<td>States that the volume is fully encrypted and the name of the algorithm used to encrypt it.</td>
</tr>
<tr>
<td>Decrypting nn%</td>
<td>Displays the progress of decryption as the percentage of decryption completed.</td>
</tr>
<tr>
<td>Unencrypted</td>
<td>States that the volume is unencrypted.</td>
</tr>
<tr>
<td>Error</td>
<td>An error has occurred during encryption or decryption.</td>
</tr>
</tbody>
</table>
Changing Your Authentication Credentials

Using the Full Disk Encryption panel, you can:

- Change your password if you authenticate yourself with a fixed password.
- Change your current authentication method (logon method) - fixed password, dynamic token, smart card. The authentication method or methods to which you can change are active under Logon method in the Full Disk Encryption - Change Credentials dialog, the others are dimmed because they are unavailable.

To change credentials:

1. Open Full Disk Encryption | Advanced.
2. Click Change.
   
The Full Disk Encryption Authentication dialog box opens.
3. Authenticate in the Full Disk Encryption authentication dialog. If you use a smart card for authentication, select Use inserted smart card.
   
   If you need to use Remote Help to authenticate, contact your Remote Help administrator, who will guide you through the Remote Help procedure.
   
   After successful authentication, the Full Disk Encryption - Change Credentials dialog will be displayed.
   
The Full Disk Encryption - Change Credentials dialog displays the logon methods that are available to you. The available methods can be:

a. Fixed Password
   
Enter and confirm a new password if you authenticate with a fixed password. If the Hide typing check box is selected, the characters you enter are disguised as asterisks (*), otherwise the actual characters entered are displayed. The dialog provides guidance on the validity of the password you enter.

b. Dynamic token
   
Enter the required information.

c. Smart card
Enter the required information.
4. Select the available **Logon method** to which you want to change.
5. Click **OK**.

### Changing the Language Used in the Interface

You can change the language used in the Full Disk Encryption client's preboot interface, system tray, recovery utility, and single sign-on interface (if single sign-on is active).

**To change the language used:**
1. Open Full Disk Encryption|Advanced.
2. From the **Select Language** drop-down menu, select the language you want to use.
3. Close Endpoint Security Client. The next time you start Full Disk Encryption, the preboot environment dialog will use the language you selected.
Languages Supported

The following languages are supported in Full Disk Encryption:

- Chinese (Simplified)
- Chinese (Taiwan)
- English
- French
- German
- Italian
- Japanese
- Spanish

Note - You can also choose the language of the operating system, which is listed as Operating System in the drop-down menu. See “Fallback Languages” on page 136. If Operating System is selected and the language of the operating system is not one of the supported languages, US English will be displayed.

Fallback Languages

If the operating system language is a non-supported variant of one of the eight supported languages, for example, French (Canada) or Chinese (Singapore), the language variant that will be used is the fallback language listed in the following table:

<table>
<thead>
<tr>
<th>ID</th>
<th>Selected Language</th>
<th>Fallback Language</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x0C04</td>
<td>Chinese (Hong Kong S.A. R.)</td>
<td>Chinese (Traditional)</td>
</tr>
<tr>
<td>0x1404</td>
<td>Chinese (Macau S.A.R.)</td>
<td>Chinese (Traditional)</td>
</tr>
<tr>
<td>0x0804</td>
<td>Chinese (People's Republic of China)</td>
<td>Chinese (Simplified)</td>
</tr>
<tr>
<td>0x0004</td>
<td>Chinese (Simplified)</td>
<td>Chinese (Simplified)</td>
</tr>
<tr>
<td>0x1004</td>
<td>Chinese (Singapore)</td>
<td>Chinese (Simplified)</td>
</tr>
<tr>
<td>0x0404</td>
<td>Chinese (Taiwan)</td>
<td>Chinese (Traditional)</td>
</tr>
<tr>
<td>0x7C04</td>
<td>Chinese (Traditional)</td>
<td>Chinese (Traditional)</td>
</tr>
<tr>
<td>0x0009</td>
<td>English</td>
<td>English (United States)</td>
</tr>
</tbody>
</table>
### Table 6-3  Fallback Languages

<table>
<thead>
<tr>
<th>ID</th>
<th>Selected Language</th>
<th>Fallback Language</th>
<th>ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x0C09</td>
<td>English (Australia)</td>
<td>English (United States)</td>
<td>0x0409</td>
</tr>
<tr>
<td>0x2809</td>
<td>English (Belize)</td>
<td>English (United States)</td>
<td>0x0409</td>
</tr>
<tr>
<td>0x1009</td>
<td>English (Canada)</td>
<td>English (United States)</td>
<td>0x0409</td>
</tr>
<tr>
<td>0x2409</td>
<td>English (Caribbean)</td>
<td>English (United States)</td>
<td>0x0409</td>
</tr>
<tr>
<td>0x1809</td>
<td>English (Ireland)</td>
<td>English (United States)</td>
<td>0x0409</td>
</tr>
<tr>
<td>0x2009</td>
<td>English (Jamaica)</td>
<td>English (United States)</td>
<td>0x0409</td>
</tr>
<tr>
<td>0x1409</td>
<td>English (New Zealand)</td>
<td>English (United States)</td>
<td>0x0409</td>
</tr>
<tr>
<td>0x3409</td>
<td>English (Republic of the Philippines)</td>
<td>English (United States)</td>
<td>0x0409</td>
</tr>
<tr>
<td>0x1C09</td>
<td>English (South Africa)</td>
<td>English (United States)</td>
<td>0x0409</td>
</tr>
<tr>
<td>0x2C09</td>
<td>English (Trinidad and Tobago)</td>
<td>English (United States)</td>
<td>0x0409</td>
</tr>
<tr>
<td>0x0809</td>
<td>English (United Kingdom)</td>
<td>English (United Kingdom)</td>
<td>0x0809</td>
</tr>
<tr>
<td>0x0409</td>
<td>English (United States)</td>
<td>English (United States)</td>
<td>0x0409</td>
</tr>
<tr>
<td>0x3009</td>
<td>English (Zimbabwe)</td>
<td>English (United States)</td>
<td>0x0409</td>
</tr>
<tr>
<td>0x000C</td>
<td>French</td>
<td>French (France)</td>
<td>0x040C</td>
</tr>
<tr>
<td>0x080C</td>
<td>French (Belgium)</td>
<td>French (France)</td>
<td>0x040C</td>
</tr>
<tr>
<td>0x0C0C</td>
<td>French (Canada)</td>
<td>French (France)</td>
<td>0x040C</td>
</tr>
<tr>
<td>0x040C</td>
<td>French (French)</td>
<td>French (France)</td>
<td>0x040C</td>
</tr>
<tr>
<td>0x140C</td>
<td>French (Luxembourg)</td>
<td>French (France)</td>
<td>0x040C</td>
</tr>
<tr>
<td>0x180C</td>
<td>French (Principality of Monaco)</td>
<td>French (France)</td>
<td>0x040C</td>
</tr>
<tr>
<td>0x100C</td>
<td>French (Switzerland)</td>
<td>French (France)</td>
<td>0x040C</td>
</tr>
<tr>
<td>0x0007</td>
<td>German</td>
<td>German (Germany)</td>
<td>0x0407</td>
</tr>
<tr>
<td>0x0C07</td>
<td>German (Austria)</td>
<td>German (Germany)</td>
<td>0x0407</td>
</tr>
<tr>
<td>0x0407</td>
<td>German (Germany)</td>
<td>German (Germany)</td>
<td>0x0407</td>
</tr>
<tr>
<td>0x1407</td>
<td>German (Liechtenstein)</td>
<td>German (Germany)</td>
<td>0x0407</td>
</tr>
<tr>
<td>0x1007</td>
<td>German (Luxembourg)</td>
<td>German (Germany)</td>
<td>0x0407</td>
</tr>
<tr>
<td>0x0807</td>
<td>German (Switzerland)</td>
<td>German (Germany)</td>
<td>0x0407</td>
</tr>
<tr>
<td>0x0010</td>
<td>Italian</td>
<td>Italian (Italy)</td>
<td>0x0410</td>
</tr>
<tr>
<td>0x0410</td>
<td>Italian (Italy)</td>
<td>Italian (Italy)</td>
<td>0x0410</td>
</tr>
<tr>
<td>0x810</td>
<td>Italian (Switzerland)</td>
<td>Italian (Italy)</td>
<td>0x0410</td>
</tr>
<tr>
<td>0x0011</td>
<td>Japanese</td>
<td>Japanese (Japan)</td>
<td>0x0411</td>
</tr>
<tr>
<td>ID</td>
<td>Selected Language</td>
<td>Fallback Language</td>
<td></td>
</tr>
<tr>
<td>-------</td>
<td>------------------------------------</td>
<td>--------------------</td>
<td></td>
</tr>
<tr>
<td>0x0411</td>
<td>Japanese (Japan)</td>
<td>Japanese (Japan)</td>
<td></td>
</tr>
<tr>
<td>0x000A</td>
<td>Spanish</td>
<td>Spanish (Spain)</td>
<td></td>
</tr>
<tr>
<td>0x2C0A</td>
<td>Spanish (Argentina)</td>
<td>Spanish (Spain)</td>
<td></td>
</tr>
<tr>
<td>0x400A</td>
<td>Spanish (Bolivia)</td>
<td>Spanish (Spain)</td>
<td></td>
</tr>
<tr>
<td>0x340A</td>
<td>Spanish (Chile)</td>
<td>Spanish (Spain)</td>
<td></td>
</tr>
<tr>
<td>0x240A</td>
<td>Spanish (Columbia)</td>
<td>Spanish (Spain)</td>
<td></td>
</tr>
<tr>
<td>0x140A</td>
<td>Spanish (Costa Rica)</td>
<td>Spanish (Spain)</td>
<td></td>
</tr>
<tr>
<td>0x1C0A</td>
<td>Spanish (Dominican Republic)</td>
<td>Spanish (Spain)</td>
<td></td>
</tr>
<tr>
<td>0x300A</td>
<td>Spanish (Ecuador)</td>
<td>Spanish (Spain)</td>
<td></td>
</tr>
<tr>
<td>0x440A</td>
<td>Spanish (El Salvador)</td>
<td>Spanish (Spain)</td>
<td></td>
</tr>
<tr>
<td>0x100A</td>
<td>Spanish (Guatemala)</td>
<td>Spanish (Spain)</td>
<td></td>
</tr>
<tr>
<td>0x480A</td>
<td>Spanish (Honduras)</td>
<td>Spanish (Spain)</td>
<td></td>
</tr>
<tr>
<td>0x080A</td>
<td>Spanish (Mexico)</td>
<td>Spanish (Spain)</td>
<td></td>
</tr>
<tr>
<td>0x4C0A</td>
<td>Spanish (Nicaragua)</td>
<td>Spanish (Spain)</td>
<td></td>
</tr>
<tr>
<td>0x180A</td>
<td>Spanish (Panama)</td>
<td>Spanish (Spain)</td>
<td></td>
</tr>
<tr>
<td>0x3C0A</td>
<td>Spanish (Paraguay)</td>
<td>Spanish (Spain)</td>
<td></td>
</tr>
<tr>
<td>0x280A</td>
<td>Spanish (Peru)</td>
<td>Spanish (Spain)</td>
<td></td>
</tr>
<tr>
<td>0x500A</td>
<td>Spanish (Puerto Rico)</td>
<td>Spanish (Spain)</td>
<td></td>
</tr>
<tr>
<td>0x0C0A</td>
<td>Spanish (Spain)</td>
<td>Spanish (Spain)</td>
<td></td>
</tr>
<tr>
<td>0x380A</td>
<td>Spanish (Uruguay)</td>
<td>Spanish (Spain)</td>
<td></td>
</tr>
<tr>
<td>0x200A</td>
<td>Spanish (Venezuela)</td>
<td>Spanish (Spain)</td>
<td></td>
</tr>
</tbody>
</table>
Characters Supported in the Preboot Environment

The following characters are supported in the Full Disk Encryption Preboot Environment:

"#$%&'()+,-./0123456789:;<=>?@
ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`
abcedfghijklmnopqrstuvwxyz{|}~äöü
ÄÖÜ

The following characters are supported in the Full Disk Encryption Preboot Environment:

αβγδεζηθικλμνξοπρστυψω

The following characters are supported in the Full Disk Encryption Preboot Environment:

กขฃคฅฆงจจฉชซฌญฎฏฐฒณ

The following characters are supported in the Full Disk Encryption Preboot Environment:

ๆ suitability the

The following characters are supported in the Full Disk Encryption Preboot Environment:

กขฃคฅฆงจจฉชซฌญฎฏฐฒณ

The following characters are supported in the Full Disk Encryption Preboot Environment:

กขฃคฅฆงจจฉชซฌญฎฏฐฒณ

The following characters are supported in the Full Disk Encryption Preboot Environment:

กขฃคฅฆงจจฉชซฌญฎฏฐฒณ

The following characters are supported in the Full Disk Encryption Preboot Environment:

กขฃคฅฆงจจฉชซฌญฎฏฐฒณ

The following characters are supported in the Full Disk Encryption Preboot Environment:

กขฃคฅฆงจจฉชซฌญฎฏฐฒณ

The following characters are supported in the Full Disk Encryption Preboot Environment:

กขฃคฅฆงจจฉชซฌญฎฏฐฒณ

The following characters are supported in the Full Disk Encryption Preboot Environment:

กขฃคฅฆงจจฉชซฌญฎฏฐฒณ

The following characters are supported in the Full Disk Encryption Preboot Environment:

กขฃคฅฆงจจฉชซฌญฎฏฐฒณ

The following characters are supported in the Full Disk Encryption Preboot Environment:

กขฃคฅฆงจจฉชซฌญฎฏฐฒณ

The following characters are supported in the Full Disk Encryption Preboot Environment:

กขฃคฅฆงจจฉชซฌญฎฏฐฒณ
Chapter 7

Media Encryption

Check Point Media Encryption is a unique solution that provides a policy driven mechanism for securing enterprise information and ensures data integrity. The product includes the following features, which have been defined by your system administrator.

Media Encryption is an integral component of the Check Point Endpoint Security Client. The Endpoint Security Client combines firewall, network access control, program control, anti-malware, data security, and remote access protections in a unified application with a common user interface.

In This Chapter

- Encryption Policy Manager  page 141
- Removable Media Manager  page 145
- Device Manager  page 147
- Program Security Guard  page 148
- Centralized Auditing and Alerts  page 149
- Maintenance Section  page 149
Encryption Policy Manager

The optional Encryption Policy Manager (EPM) allows users to encrypt and control access to data on removable media connected to their endpoint computers. The greatest threat when granting access to removable media storage devices is the loss of sensitive or proprietary information. The encryption policy manager can ensure that data can only be accessed by authorized staff on authorized systems.

The Encryption Policy Manager provides transparent encryption of removable media storage devices. This feature includes encrypting CD or DVD media when using the built-in software on the protected workstations. Unlike any other solution on the market, offline access can be granted to trusted users. Users will be able to access secure devices without the need to install any software onto third party systems using secure password authentication. This component will allow access on third party systems even with just basic user rights.

In This Section

Using the EPM
Encrypting Media
Decrypting Media
Changing the Encrypted Device Password

Using the EPM

Media Encryption secures removable media by encrypting some or all of the data stored thereon. You can encrypt and manage removable media by using the EPM Client.

To work with the Encryption Policy Manager, click Open in the EPM Client section on the Media Encryption panel.

The EPM Client window opens, showing connected removable media devices in the pane to the left.
Encrypting Media

To start the encryption process:

- **Automatic**: The encryption process begins automatically whenever non-encrypted media is inserted into a protected computer configured to permit access only to encrypted media.
- **Manual**: Click Import in the EPM Client window.

In either case, a wizard guides you through the process of encrypting removable media devices. This process creates an encrypted storage area on a user definable percentage of the device.

**Encrypting CDs and DVDs**

If permitted by your policy, Media Encryption can encrypt CDs and DVDs with the following limitations:

- Encryption of CDs is supported on Windows XP and Windows Vista.
- Encryption of DVDs is supported on Windows Vista.
- Import will be accessible only for RW and blank R/RW discs.
- Nothing can be added to or removed from once burnt CD/DVDs. Such CD/DVDs can be erased only.

The process of importing and exporting files to CD/DVDs is similar to that of other removable media described here. Two differences are that you cannot encrypt a partial disk and you cannot add or delete files. If you wish to remove information on a rewritable disk, you need to use the Export feature to completely erase it.

**Warning** - 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. Click Cancel to abort the encryption process.
To encrypt media:

1. Start the wizard by performing one of the steps described above.
2. Click Next to continue.
3. In the Media Properties window, enter a percentage of the media to encrypt.
4. In the Media Owner Information window, define the owner of the media device by selection one of the following 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 performing the encryption or click Browse to select a user from the active domain.
5. In the Password Protection window, enter and confirm an access password. Passwords must conform to rules established by the system administrator.
6. The Progress window displays the encryption progress. Depending on the type of media and the quantity of data, this process may take a long time.

   Warning - Do NOT under any circumstance remove the storage device during the encryption process. This would destroy your data and may damage the media.

7. When the Finish window opens, click Finish to complete the process. The EPM Client window returns.

   Note that the encrypted media status now appears as Encrypted and that the Import button is no longer available.

   The following information is displayed for the selected device:
   - EPM Status: The current status of the selected encrypted device
   - Media Size: The size of the selected device.
   - Date Created: The date the selected encrypted drive was created.
   - Date Accessed: The date the selected encrypted drive was last accessed.
   - Owner: The user ID of the user who created the encrypted device.
Decrypting Media

This section describes how to decrypt previously encrypted media. The policy typically permits only the owner or another authorized user to perform decryption.

To decrypt removable media:
1. In the EPM Client window, click Export. The EPM Media Export wizard opens.
2. If the Password window appears, enter the appropriate password.
3. When the Finish window opens, click Finish to complete the process. The EPM on the and may take some time depending on the size of device and type of device. By default you will no longer have access to the encrypted device when external to the organization’s network.

Warning - Do NOT under any circumstance remove the storage device during the encryption process. This would destroy your data and may damage the media.

Changing the Encrypted Device Password

To change the removable media access password for an encrypted device:
1. Select the required device in the EPM Client window left pane.
2. Click Set. The Password window opens.
3. Enter and confirm the new password.
   The password must meet the administrator-defined criteria, which you can access by clicking Policy Note.
4. Click OK.
Removable Media Manager

By centrally controlling access to removable media/IO devices, you can control access to removable media such as: floppy disks, external disk drives, PDAs, flash memory, digital cameras, etc. CD and DVD drives are protected by using Device Manager feature. The Removable Media Manager controls device access on all available ports including USB and Firewire.

All removable media must be authorized before access is permitted. The process of authorizing removable media involves storing a digital signature on the media itself. This signature must be present in order to access removable media from a protected endpoint computer.

Administrators control authorization by defining Removable Media Manager rules in the Media Encryption policy installed on protected endpoint computers. Rules define access rights for each type of removable media including prerequisites such as virus scanning and data authorization. Administrators may grant users permission to authorize removable media according to predefined conditions.

The digital signature is automatically updated during file transfers within the protected environment. If changes to the media are permitted outside of the organization, the device must be re-authorization before it can be used within the protected environment.

Media Encryption ensures that all devices are virus-free and prevents unauthorized importing and exporting of data. In addition, Media Encryption prevents users from gaining access to unauthorized hot-swap and plug-and-play devices.

In This Section

Using the Removable Media Manager page 145
Removable Media Manager Alert page 146
Authorizing Removable Media page 146

Using the Removable Media Manager

Media Encryption provides a policy driven mechanism for securing information and ensuring data integrity across all end points. User functionality is available in the Removable Media Manager section on the Media Encryption panel.
Removable Media Manager Alert

When the Removable Media Manager is enabled, all removable media must be authorized before access is permitted. Administrators control authorization by defining Removable Media Manager rules in the Media Encryption policy installed on protected endpoint computers.

If the policy permits users to authorize removable media, an alert appears:

ALERT unauthorized removable media detected

To authorize the removable media device from this window, click Authorize. The Media Import Wizard opens.

Click Ignore to close this alert, and the removable media cannot be accessed.

Authorizing Removable Media

If permitted by the policy, users can authorize removable media directly from an alert message or manually by clicking Scan from the Removable Media Manager section on the Media Encryption panel. In either case, the Media Import Wizard guides you through the authorization steps.

1. In the Welcome window, click Next to continue.
2. In the Virus Scanners window, select the scanners you wish to execute to ensure that the removable media is virus-free and contains only authorized file types.

   If the policy permits users to select scanners and to skip scanning, a window appears with the Skip Scan option. If you want to authorize removable media without scanning it, click Skip Scan. This is not recommended.

   If the removable media successfully passes the scan the Virus Scan Complete window opens.

   If the scan is unsuccessful, a window opens, displaying data and explaining why the scan failed. Access to the removable media is then blocked.

3. Click Next to continue.
4. When the Finish window appears, click Finish.
Device Manager

Media Encryption controls user access to devices connected to various ports on endpoint computers. This protection is available for IrDA, COM, USB, Firewire, and LPT ports.

By requiring permissions to access these devices, you can control access to removable media, CD/DVD drives, PDAs, Blackberries, Bluetooth devices and external hard disks. Device Manager prevents users from connecting unauthorized devices to computer ports and provides On/Off/read-only protection as opposed to the more granular approach offered by the Removable Media Manager (see page 145).

Using the Device Manager

Media Encryption controls user access to devices connected to various ports on endpoint computers. The Media Encryption policy specifies which devices are granted access and what type of access is permitted (Read only, Read/Write and Execute).

Device manager user options are located in the Device Manager section of the Media Encryption panel.

To view the policy rules for various devices, click View.

When Device Manager rules block access to a device or port, an alert appears.

ALERT unauthorized removable media detected
**Program Security Guard**

Media Encryption provides a profile-based file management solution. Administrators can prevent users from creating specific file types on local workstations and network drives. Restricted file types are specified by their extension and can be used to prevent the introduction of unlicensed or unauthorized software (.exe, .com, .dll, etc.), potentially malicious file types (.vbs, .scr, etc.) or simply unwanted file types (.mpg, .mp3, mov, avi, etc.). This protection applies to any external source including e-mail attachments and web downloads.

**Using the Program Security Guard**

Administrators can prevent users from creating specific file types on local workstations and network drives. Restricted file types are specified by their extension and can be used to prevent the introduction of unlicensed or unauthorized software (.exe, .com, .dll, etc.), potentially malicious file types (.vbs, .scr, etc.) or simply unwanted file types (.mpg, .mp3, mov, avi, etc.).

If a Program Security Guard rule blocks access to a file, a message appears.

*ALERT PSG*
Centralized Auditing and Alerts

Media Encryption provides detailed auditing of potential security breaches. All events are centrally logged in an SQL database with the ability to create structured queries and detailed reports.

Media Encryption enables the administrator to centrally audit all file operations on all removable storage including CDs and DVDs. The administrator can configure the auditing of certain events to produce e-mail alerts to defined addresses.

The Media Encryption auditing provides extensive tracking of user behavior and system security. To simplify audit analysis, fully configurable HTML reports can be generated from within the administration console detailing summary information across all audit events.

Maintenance Section

The Maintenance section of the Media Encryption panel allows you to manually update the Media Encryption policy and to test connectivity with the Media Encryption server.

To update the Media Encryption policy, click Update.

To test network connectivity with the Media Encryption server, click Test. This feature is useful for diagnosing client/server connection problems.
Chapter 8

E-mail Protection

Worms, viruses, and other threats often use e-mail to spread from computer to computer. MailSafe protects your contacts by preventing your e-mail from spreading malware.

MailSafe only protects SMTP protocol messages.

In This Chapter

- Outbound MailSafe Protection  page 151
- Enabling Outbound MailSafe Protection  page 151
- Customizing Outbound MailSafe Protection  page 152
Outbound MailSafe Protection

Outbound MailSafe protection alerts you if your e-mail program tries to send an unusually large number of messages (more than five e-mail messages within a two seconds), or tries to send a message to an unusually large number of recipients (more than fifty recipients). This prevents your computer from being used without your knowledge to send infected attachments to other people. In addition, Outbound MailSafe protection verifies that the program attempting to send the e-mail has permission to send e-mail messages.

Outbound MailSafe protection works with the following e-mail applications:

- Eudora
- Outlook
- Outlook Express
- Netscape Mail
- Pegasus Mail
- Juno

Enabling Outbound MailSafe Protection

For your security, Outbound e-mail protection is enabled by default. When Outbound protection is enabled, Outbound MailSafe settings apply to all programs with send mail privileges.

**To enable Outbound e-mail protection**

1. Open E-mail Protection\Main.
2. In the Outbound e-mail Protection area, select On.
Customizing Outbound MailSafe Protection

You can customize when MailSafe is activated. You can extend the time interval, increase the number of messages and recipients allowed, or specify the e-mail addresses that are allowed to send e-mail from your computer.

Enabling MailSafe by Program

When Outbound MailSafe protection is on, protection is enabled for all programs that have been granted permission to send e-mail (see “Setting Specific Permissions” on page 105).

You can customize Outbound MailSafe protection by enabling or disabling it for particular programs.

To enable Outbound MailSafe protection for a program:

1. Open Program Control > Programs.
2. In the Programs column, right-click a program name and then select Options.
3. Open the Security tab.
4. In the Outbound E-mail Protection area, select the Enable Outbound E-mail Protection for this program check box.
5. Click OK.
Setting MailSafe Options

To allow for legitimate e-mail messages that would activate MailSafe and thus not be sent (because of too many recipients or too many sends), customize Outbound MailSafe protection settings to better meet your individual needs.

Note - You must have Outbound E-mail Protection enabled to access these options.

To customize Outbound MailSafe protection settings:
1. Open E-mail Protection | Main.
2. Click Advanced.
   The Advanced E-mail Protection window appears.
3. In the Display Outbound E-mail Protection Alerts When area, choose your settings.
   • **Too many E-mails are sent at once**: Endpoint Security client displays an Outbound MailSafe protection alert when your computer attempts to send more than the specified number of e-mails within the specified time interval.
   • **A message has too many recipients**: Endpoint Security client displays an Outbound MailSafe protection alert when your computer attempts to send an e-mail message with more than the specified number of recipients.
   • **If the sender's address is not in this list**: Endpoint Security client displays an Outbound MailSafe protection alert when your computer attempts to send an e-mail whose originating address (the address in the From: field) does not appear on the list. To prevent the client from blocking all outgoing e-mail, make sure that your valid e-mail address appears on this list.
Policy Enforcement enables Endpoint Security client to protect your enterprise network by enforcing a security policy created by your network administrator. Enterprise policy enforcement occurs when the client is used in an Endpoint Security Server environment. With Endpoint Security, your administrator can send enterprise policies out to the computer users on the enterprise's local network. In this way, your enterprise can be sure that everyone on the network is adequately protected from Internet threats.

In This Chapter

Policy Types page 155
Understanding Policy Arbitration page 156
Policy Types

**Personal** Security Policy: Settings you choose for your firewall, program control, e-mail protection and other features in Endpoint Security client.

**Enterprise** Security Policy: Settings for the same security features, but created by your company's security administrator and assigned to users on the enterprise network.

**Disconnected** policy: Created by a security administrator, enforces certain enterprise security settings even when your computer is not connected to the corporate network.

A security administrator sends enterprise policies to the Endpoint Security clients on the corporate network.

If you are out of compliance with the enterprise policy, your computer may enforce restricted rules that limit your access. If this occurs, you will be directed to a Web page that provides instructions for getting your computer back into compliance. If you need further assistance, contact your system administrator.
Understanding Policy Arbitration

Your personal policy is active whenever the client is running. An enterprise policy may be active or inactive, depending on the situation.

When both your personal policy and an enterprise policy are active, Endpoint Security arbitrates between the two policies: the more restrictive of the two policy settings is enforced. For example, if your personal policy calls for the Internet Zone security level to be set to medium; and an active enterprise policy calls for it to be set to high, the high setting is enforced.

Because of policy arbitration, an active enterprise policy may block traffic that your personal policy is set to allow, or vice-versa. If you think Endpoint Security is blocking legitimate traffic that should be allowed, contact your system administrator.

Viewing Available Policies

Depending on how your administrator has configured your policy settings, you may only be able to view your personal, enterprise, and disconnected policies, or you might also be able to view any updates that have been made to your enterprise policy.

Using the Policies Panel

Use the Policies panel to:

- See which policies are installed, which is currently active, and the last time a policy was updated.
- Access a text version of policy settings for each enterprise policy and for your personal policy.

The Policies panel appears only if your version of Endpoint Security is configured to display it.

This panel might not be available to you because:

- Your version of Endpoint Security does not include Policies functionality.
- Your version includes Policy functionality, but your administrator has elected not to display the panel.
Table 9-1  Policy Panel Information

<table>
<thead>
<tr>
<th>Policy Panel Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Name</td>
<td>Name of the policy. <strong>Personal Policy</strong>: Settings you have established for the client by using the Control Center. Other policy names refer to enterprise policies that your administrator has installed on your computer.</td>
</tr>
<tr>
<td>Active</td>
<td>This column indicates whether the listed policy is currently active. <strong>Personal Policy</strong> is always active. The administrator can activate or deactivate an enterprise policy. When both your personal policy and another policy are active, Endpoint Security arbitrates between the two active policies.</td>
</tr>
<tr>
<td>Last Server Contact</td>
<td>For enterprise security policies, this column indicates the date and time that the client first established the current connection to an Endpoint Security Server, to enforce the listed enterprise policy. If the connection to the server is down, or the client is not enforcing an enterprise policy, this column displays <strong>Disconnected</strong>.</td>
</tr>
<tr>
<td>Author</td>
<td>The administrator who created and assigned the security policy. For the personal policy, this is listed as <strong>N/A</strong>.</td>
</tr>
<tr>
<td>Entry Detail Area</td>
<td>Details about the policy that is currently selected in the list.</td>
</tr>
<tr>
<td>Author</td>
<td>The administrator who created and assigned the security policy. For the personal policy, this is listed as <strong>N/A</strong>.</td>
</tr>
<tr>
<td>Entry Detail Area</td>
<td>Details about the policy that is currently selected in the list.</td>
</tr>
</tbody>
</table>
Chapter 10

Alerts and Logs

You can be notified by an alert each time the client acts to protect you; or only when an alert is likely to have resulted from malicious activity. You can choose to log all alerts, only high-rated alerts, or alerts caused by specific traffic types.

In This Chapter

- Understanding Alerts and Logs  page 159
- Setting Basic Alert and Log Options  page 162
- Showing or Hiding Alerts  page 163
- Setting Log Options  page 164
- Using Alert Advisor  page 170
Understanding Alerts and Logs

The client alert and logging features keep you aware of what is happening on your computer without being overly intrusive, and enable you to go back at any time to investigate past alerts.

About Alerts

Endpoint Security client generates two alert types: enterprise or personal, which correspond to settings or rules contained in the active policy.

Both policy types have three categories of alerts: informational, program, and network.

To learn how to respond to specific alerts, see Appendix A, “Alert Reference”.

Informational Alerts

Informational alerts tell you that the client has blocked a communication that did not fit your security settings.

Informational alerts do not require a decision from you.

Click OK to close the alert box.

Program Alerts

Program alerts ask you if you want to allow a program to access the Internet or local network, or to act as a server. Program alerts require a Yes or No response. The most common types of Program alerts are the New Program alert and the Repeat Program alert.

Click Yes to grant permission to the program.

Click No to deny permission.

New Network Alerts

New Network alerts occur when you connect to any network: a wireless home network, a business LAN, or an ISP network.

If you are on a home or local network, New Network alerts let you instantly configure the client to allow you to share resources with the network.
**Instant Messaging Alerts**

This section provides an explanation of the types of alert messages that may appear during an instant messaging session that is protected by Endpoint Security.

The table below lists the alert messages that can appear when using Endpoint Security. Consult the table for an explanation of why these alerts appear and to determine whether any action is required on your part. All alert messages appear in brackets [ ] in your instant messaging window.

<table>
<thead>
<tr>
<th>Alert Text</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session not encrypted because [contact's IM ID] disabled encryption</td>
<td>This alert appears when you have encryption enabled, but your contact has disabled encryption.</td>
</tr>
<tr>
<td>Session not encrypted because [contact's IM ID] is not protected by Endpoint Security</td>
<td>This alert appears in your instant messaging window when you are having a conversation with a contact who is not using Endpoint Security.</td>
</tr>
<tr>
<td>Link removed</td>
<td>This alert appears in the message recipients's window in place of a removed link.</td>
</tr>
<tr>
<td>Session encrypted</td>
<td>This alert appears at the beginning of an encrypted instant messaging conversation.</td>
</tr>
<tr>
<td>Potentially harmful content was removed from this message</td>
<td>This alert is appended to the filtered message.</td>
</tr>
<tr>
<td>Your message was blocked because you are not on [contact's IM ID]'s contact list</td>
<td>This alert appears when you attempt to send a message to someone who has Spam Blocker enabled, but who does not have you on his or her contact list.</td>
</tr>
<tr>
<td>A file transfer on [contact's IM ID]'s PC was blocked</td>
<td>This alert appears when you attempt to send a file to a contact, but the contact has blocked file transfers in Endpoint Security client.</td>
</tr>
</tbody>
</table>
About Event Logging

By default, the client creates a log entry every time traffic is blocked, whether an alert is displayed or not. Log entries record the traffic source and destination, ports, protocols, and other details. The information is recorded to a text file named ZALOG.txt, stored in the Internet Logs folder. Every 60 days, the log file is archived to a dated file, so that it does not become too large.

You can choose to prevent specific categories of events from being logged. For example, you may want to create log entries only for firewall alerts, or suppress entries for a particular type of Program alert.

<table>
<thead>
<tr>
<th>Alert Text</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Video transmission on [contact's IM ID]'s PC was blocked</td>
<td>This alert appears when a you attempt to transmit video to a contact, but the contact has blocked video transmission.</td>
</tr>
<tr>
<td>Potentially harmful formatting or scripting was removed from your last message</td>
<td>This alert appears when your contact set the Inbound protection option for Tags to Block, and you attempt to send a message to a contact that includes formatting or scripting.</td>
</tr>
<tr>
<td>A potentially harmful link was removed from your last message</td>
<td>This alert appears when your contact set the Inbound protection option for Active to Block, and you attempt to send a message to a contact that includes an executable link.</td>
</tr>
</tbody>
</table>

Table 10-1  Instant Messaging Alerts
Setting Basic Alert and Log Options

Basic alert and log options let you specify the type of event for which the client displays an alert and for which events it creates a log entry.

Setting Alert Event Level

The alert events Shown control, in the Main tab of Alerts & Logs, lets you control the display of alerts by rating. Program alerts are always displayed, because they ask you to decide whether to grant permission.

To set the alert event level:
1. Open Alerts & Logs | Main.
2. In the alert events Shown area, select the desired setting.
   - **High**: Displays an alert for every security event that occurs, both high-rated and medium-rated.
   - **Med**: Displays only high-rated alerts, which are most likely a result of hacker activity.
   - **Off**: Displays Program alerts only. Informational alerts are not displayed.

Setting Event and Program Logging Options

Use the Event Logging and Program Logging areas to choose what types of informational alerts and program alerts will be logged.

To enable or disable event logging and program logging:
1. Open Alerts & Logs | Main.
2. In the Event Logging area, select the desired setting.
   - **On**: Creates a log entry for all events.
   - **Off**: No events are logged.
3. In the Program Logging area, specify the log level.
   - **High**: Creates a log entry for all program alerts.
   - **Med**: Creates a log entry for high-rated program alerts only.
   - **Off**: No program events are logged.
Showing or Hiding Alerts

You can specify whether you want to be alerted to all security and program events, or if you only want to be notified of events that are likely a result of malicious activity.

Showing or Hiding Firewall Alerts

The Alert Events tab gives you more detailed control of alert display. You can specify for which types of blocked traffic Firewall and Program alerts are displayed.

To show or hide firewall or program alerts:
1. Open Alerts & Logs|Main.
2. Click Advanced.
   The Alert & Log Settings window appears.
3. Open the Alert Events tab.
4. In the Alert column, select the type of blocked traffic for which the client should display an alert.
5. Click Apply.

Enabling System Tray Alerts

When you choose to hide some or all informational alerts, the client can still keep you aware of those alerts by showing a small alert icon in the system tray.

To enable system tray alerts:
1. Open Alerts & Logs|Main.
2. Click Advanced.
3. Click the System Tray Alert tab.
4. Select the Enable system tray alert icon check box.
Setting Log Options

You can specify whether the client keeps track of security and program events by enabling or disabling logging for each type of alert.

In This Section

Formatting Log Appearance  page 164
Customizing Event Logging  page 164
Customizing Program Logging  page 165
Viewing Log Entries  page 165
Viewing the Text Log  page 168
Archiving Log Entries  page 169

Formatting Log Appearance

You can set the field separator for your text log files.

To format log entries:
1. Open Alerts & Logs.
2. Click Advanced.
   The Advanced Alerts and Log Settings window appears.
3. Open the Log Control tab.
4. In the Log Archive Appearance area, select the format to be used for logs: Tab, Comma, or Semicolon.

Customizing Event Logging

By default, the client creates a log entry when a high-rated firewall event occurs. You can customize firewall alert logging by suppressing or allowing log entries for specific security events, such as MailSafe quarantined attachments, Blocked non-IP packets, or Lock violations.

To create or suppress log entries based on event type:
1. Open Alerts & Logs/Main.
2. Click Advanced.
Customizing Program Logging

The Advanced Alerts and Logs window appears.

3. Select **Alert Events**.

4. In the **Log** column, select the type of event for which the client should create a log entry.

5. Click **Apply** to save your changes.

6. Click **OK** to close the Alert & Log Settings window.

**Customizing Program Logging**

By default, the client creates a log entry when any type of Program alert occurs. You can customize Program alert logging by suppressing log entries for specific Program alert types, such as New Program alerts, Repeat Program alerts, or Server Program alerts.

**To create or suppress log entries based on event type:**

1. Open **Alerts & Logs**|**Main**.

2. In the Program Logging area, click **Custom**.

3. In the **Program Logs** column, select the type of event for which the client should create a log entry.

4. Click **Apply** to save your changes.

5. Click **OK** to close the Alert & Log Settings window.

**Viewing Log Entries**

You can view log entries in a text file using a text editor or in the Log Viewer. Although the format differs slightly, the general information contained in the log is the same.

**To view the current log in the Log Viewer:**

1. Open **Alerts & Logs**|**Log Viewer**.

2. Select the number of alerts to display (from 1 to 99) in the alerts list.

   You can sort the list by any field by clicking the column header.

3. Click a log entry to view Log entry details.
**Log Viewer Fields**

At the top of the Log Viewer panel, the **Alert Type** drop down list allows you to view either Program or Firewall alerts.

<table>
<thead>
<tr>
<th>Table 10-2</th>
<th>Log Viewer Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Column Heading</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>Rating</td>
<td>Each alert is rated critical, high, or medium. Critical-rated and High-rated alerts are those likely to have been caused by hacker activity. Medium-rated alerts are likely to have been caused by unwanted but harmless network traffic.</td>
</tr>
<tr>
<td>Date / Time</td>
<td>The date and time the alert occurred.</td>
</tr>
<tr>
<td>Type</td>
<td>The type of alert: Firewall, Program, Malicious Code Detection, Lock Enabled, Scan, Update, or Treat.</td>
</tr>
<tr>
<td>Protocol</td>
<td>In the <strong>Alert Type</strong> drop-down list choose Firewall to view the Protocol column. Identifies the protocol used by the traffic that caused the alert condition.</td>
</tr>
<tr>
<td>Program</td>
<td>The name of the program attempting to send or receive data. (Applies only to Program alerts).</td>
</tr>
<tr>
<td>Source IP</td>
<td>The IP address of the computer that sent the traffic that the client blocked.</td>
</tr>
<tr>
<td>Destination IP</td>
<td>The address of the computer the blocked traffic was sent to.</td>
</tr>
<tr>
<td>Direction</td>
<td>The direction of the blocked traffic: <strong>Incoming</strong> or <strong>Outgoing</strong> to/from your computer.</td>
</tr>
<tr>
<td>Action Taken</td>
<td>How the traffic was handled by the client.</td>
</tr>
<tr>
<td>Count</td>
<td>The number of times an alert of the same type, with the same source, destination and protocol, occurred during a single session.</td>
</tr>
<tr>
<td>Source DNS</td>
<td>The domain name of the computer that sent the traffic that caused the alert.</td>
</tr>
<tr>
<td>Column Heading</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Destination DNS</td>
<td>The domain name of the intended addressee of the traffic that caused the alert.</td>
</tr>
<tr>
<td>Policy</td>
<td>The name of the policy containing the security setting or rule that caused the alert. Endpoint Security client recognizes three policy types: personal, enterprise, and disconnected.</td>
</tr>
<tr>
<td>Rule</td>
<td>In the Alert Type drop-down list choose Firewall to view the Rule column. When an alert was caused by conditions specified in a classic firewall rule, this column contains the name of the rule.</td>
</tr>
</tbody>
</table>
Viewing the Text Log

By default, alerts generated by Endpoint Security are logged in the file, ZAlog.txt. If you are using Windows95, Windows98 or Windows Me, the file is located in the following folder: (x):\Windows\Internet Logs. If you are using Windows NT or Windows 2000, the file is located in the following folder: (x):\Winnt\Internet Logs.

To view the current log as a text file:

1. Open Alerts & Logs\Main.
2. Click Advanced.
   The Advanced Alerts & Log Settings window opens.
3. Open the Log Control tab.
4. In the Log Archive Location area, click View Log.

Table 10-3  Text Log Information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Type of event recorded.</td>
<td>FWIN</td>
</tr>
<tr>
<td>Date</td>
<td>Date of the alert, in format yyyy/mm/dd</td>
<td>2001/12/31 (December 31, 2001)</td>
</tr>
<tr>
<td>Time</td>
<td>Local time of the alert. This field also displays the hours difference between local and Greenwich Mean Time (GMT).</td>
<td>17:48:00 -8:00GMT (5:48 PM, eight hours earlier than Greenwich Mean Time. GMT would be 01:48.)</td>
</tr>
<tr>
<td>Source</td>
<td>IP address of the computer that sent the blocked packet, and the port used; OR the program on your computer that requested access permission.</td>
<td>192.168.1.1:7138 (FW events) Microsoft Outlook</td>
</tr>
<tr>
<td>Destination</td>
<td>IP address and port of the computer to which the blocked packet was addressed.</td>
<td>192.168.1.101:0</td>
</tr>
<tr>
<td>Transport</td>
<td>Protocol (packet type) involved.</td>
<td>UDP</td>
</tr>
</tbody>
</table>
Archiving Log Entries

At regular intervals, the contents of ZAlog.txt are archived to a date-stamped file, for example, ZAlog2005.09.12.txt (for September 12, 2005). This prevents ZAlog.txt from becoming too large.

To view archived log files, use Windows Explorer to browse to the directory where your logs are stored.

**To set archive frequency:**
1. Open **Alerts & Logs|Main**
2. Click **Advanced**.
3. Open the **Log Control** tab.
4. Select the **Log Archive Frequency** check box.
   
   If this check box is not selected, Endpoint Security continues to log events for display in the Log Viewer tab, but does not archive them to the ZAlog.txt file.
5. In the Log Frequency area, specify the log frequency (between 1 and 60 days).

**Specifying Archive Location**

The ZAlog.txt file and all archived log files are stored in the same directory.

**To change the log and archive location:**
1. Open **Alerts & Logs|Main**.
2. Click **Advanced**.
   
   The Advanced Alerts & Log Settings window opens.
3. Open the **Log Control** tab.
4. In the Log Archive Location area, click **Browse** and select a location for the log and archive files.
Using Alert Advisor

Check Point AlertAdvisor is an online utility that enables you to analyze the possible causes of an alert, and helps you decide how to respond to a Program alert.

To use AlertAdvisor, click More Info in an alert pop-up.

Endpoint Security sends information about your alert to AlertAdvisor. AlertAdvisor returns an article that explains the alert and gives you advice on what, if anything, you need to do to ensure your security.

To submit an alert to AlertAdvisor:
1. Open Alerts & Logs | Log Viewer.
2. Right-click anywhere in the alert record you want to submit and choose More Info.
Appendix

Alert Reference

There are various types of alerts you may see while using Endpoint Security. This reference describes why Alerts happen, what they mean, and what to do about them.

In This Appendix

- Informational Alerts  page 173
- Program Alerts  page 180
Informational Alerts

Informational alerts tell you that Endpoint Security has blocked a communication that did not fit your security settings. They do not require a decision from you.

Firewall Alert/Protected

Firewall alerts are the most common type of informational alert. Firewall alerts inform you that the Endpoint Security firewall has blocked traffic based on port and protocol restrictions or other firewall rules.

Why Firewall Alerts Occur

Firewall alerts with a red band at the top indicate high-rated alerts. High-rated alerts often occur as a result of malicious activity.

Firewall alerts with an orange band at the top indicate medium-rated alerts. Medium-rated alerts are likely the result of harmless network traffic. For example, if your ISP is using ping to verify that you're still connected. However, they also can be caused by a hacker trying to find unprotected ports on your computer.

What you should do

If you're on a home or business network, and your Trusted Zone security is set to HIGH, normal LAN traffic such as NetBIOS broadcasts may generate firewall alerts. Try lowering Trusted Zone security to MEDIUM.

By default, Endpoint Security only displays high-rated firewall alerts. If your defaults have been changed, you may see a lot of medium-rated alerts. Try setting your alert display settings to MEDIUM.

If you receive a large number of firewall alerts, and you are working on a home network or business LAN, it is possible that normal network communications are being blocked. If this is happening, you can eliminate the alerts by placing your network in the Trusted Zone.
Reducing Firewall Alerts

Repeated alerts may indicate that a resource you want to trust is trying repeatedly to contact you. If you are receiving a lot of firewall alerts, but you do not suspect you are under attack, try the following troubleshooting steps:

- Determine if the source of the alerts should be trusted.
- Submit repeated alerts to AlertAdvisor to determine the source IP address that caused the alerts.
- If the alerts were caused by a source you want to trust, add it to the Trusted Zone.
- Determine if your Internet Service Provider is sending you "heartbeat" messages.
- Try the procedures suggested for managing ISP heartbeat (see page 196).

MailSafe Alert

MailSafe alerts let you know that Endpoint Security has quarantined a potentially dangerous outgoing e-mail message.

Why MailSafe Alerts Occur

A violation of Outbound MailSafe protection settings, such as an e-mail that has too many recipients, or too many e-mails within a short time, can cause a MailSafe alert to occur.

What you should do

- Examine the alert carefully. Does the activity noted describe actions you were recently performing? For example, did you recently attempt to send out a legitimate mailing to a large number of recipients, or to send many e-mails in a short period of time? If so, you may want to modify your Outbound MailSafe settings to better accommodate your needs, see "Outbound MailSafe Protection" on page 151.
- Verify that your e-mail address is listed on the approved sender's list. If you selected the if the sender's e-mail is not in this list option, and your e-mail is not on that list or is misspelled, add your valid e-mail address to the list.
Blocked Program Alerts

Blocked Program alerts tell you that Endpoint Security has prevented an application on your computer from accessing the Internet or Trusted Zone resources. By clicking OK, you're not allowing the program access, just acknowledging that you saw the alert.

Why Blocked Program Alerts Occur

Blocked Program alerts occur when a program tries to access the Internet or the Trusted Zone, even though you have explicitly denied it permission to do so.

What you should do

If the program that was blocked is one that you want to have access to the Internet Zone or Trusted Zone, use the Programs tab to give the program access permission.

Reducing Blocked Program Alerts

To turn off Blocked Program alerts, do one of the following:

- When you see a Blocked Program alert, select Do not show this window again before clicking OK. From then on, all Blocked Program alerts will be hidden. Note that this will not affect New Program, Repeat Program, or Server Program alerts.

- In the Program Control panel, click Advanced to access the Alerts & Functionality tab, then clear the Show alert when Internet access is denied check box.

Note - Turning off Blocked Program alerts does not affect your level of security.
Internet Lock Alerts

Internet Lock alerts let you know that Endpoint Security has blocked incoming or outgoing traffic because the Internet Lock is engaged. By clicking OK, you're not opening the lock; you're just acknowledging that you've seen the alert.

**Why Internet Lock Alerts Occur**

These alerts occur only when the Internet Lock is engaged.

**What you should do**

Click **OK** to close the alert pop-up.

If the Internet Lock has been engaged automatically (or accidentally), open it to prevent further alerts; see “Understanding Zones” on page 76.

You may want to give certain programs (for example, your browser) permission to bypass the Internet Lock, so that you can continue to perform some basic functions under the lock's higher security. See “Granting Pass-lock Permission to Programs” on page 109.

**Reducing Internet Lock Alerts**

If you are receiving a lot of Internet Lock alerts, it is possible that your Automatic Internet Lock settings are engaging the Internet Lock after every brief period of inactivity.

**To reduce the number of alerts, you can do one of the following:**

- Turn off the Automatic Internet Lock.
- Increase the interval of inactivity required to engage the Automatic Internet Lock to engage; see “Enabling Automatic Lock” on page 102.
Endpoint Security Policy Received Alerts

Policy Received alerts tell you that Endpoint Security has received a new enterprise policy from Endpoint Security Server.

Why Policy Received Alerts Occur

These alerts occur when your system administrator updates your enterprise policy and deploys that policy to your computer from Endpoint Security Server.

What you should do

Click **OK** to close the alert box. By doing this, you’re not changing your security settings.

Reducing Policy Received Alerts

It is unusual to see repeated Endpoint Security Policy Received alerts. If you are seeing such alerts, contact your system administrator, or disable alert display in the **Main** tab of the **Alerts & Logs** panel.

Compliance Alerts

Compliance alerts occur when Endpoint Security server operating in conjunction with the Endpoint Security client determines that your computer is non-compliant with enterprise security requirements. Depending on the type of non-compliance, your ability to access the corporate network may be **restricted** or even **terminated**.

Why Compliance Alerts Occur

These alerts appear when you are trying to connect to your corporate network and you are out of compliance with the enterprise policy stored in Endpoint Security Server.

What you should do

Compliance alerts, in conjunction with special Web pages, will tell you what you need to do to become compliant with security policy settings.

- If the non-compliant condition does not require immediate remediation, your access to the corporate network may be **restricted**: You can continue to access some corporate network resources, but you should perform the steps necessary to make your computer compliant as soon as possible.
• If the non-compliant condition requires immediate remediation, your access to the corporate network may be terminated. In this case, you may only be able to access the Web page that tells you how to make your computer compliant with corporate security requirements.

Click the link in the alert or corresponding Web page to begin the remediation process. Remediation generally involves installing a newer version of Endpoint Security or approved antivirus software. If you see a Compliance alert and you are unsure of how to make your computer compliant with corporate security, consult your system administrator.

**Note** - Your administrator has the option of configuring Endpoint Security to automatically install any applications required to bring your computer into compliance with corporate guidelines. In some cases, this might result in a program being installed on your computer without warning, and could require a reboot of your computer. If you experience an automatic system reboot or if a program attempts to install itself on your computer, consult your system administrator.

**Reducing Compliance Alerts**

You can avoid seeing Compliance alerts by keeping your computer is in compliance with the security policy established by your administrator.

**Connected/Disconnecting Alerts**

These alerts tell you when Endpoint Security logs into, or logs off from, Endpoint Security Server.

**Why Connected/Disconnected Alerts Occur**

These alerts are strictly informational. They inform you that Endpoint Security client has logged into Endpoint Security Server.

**What you should do**

When you see this alert, there's nothing you have to do to ensure your security. Click **OK** to dismiss the alert box.

However, if Endpoint Security repeatedly disconnects from Endpoint Security Server, and you think this might be due to a network problem, contact your system administrator.
Reducing Connected/Disconnected Alerts

In an Endpoint Security environment, it is normal to see a Protected alert when you start your computer or start Endpoint Security. To avoid see any informational alerts, turn off alerts in the Main tab of the Alerts & Logs panel.
Program Alerts

Most of the time, you are likely to see program alerts when you are actually using a program. For example, if you've just installed Endpoint Security, and you immediately open Microsoft Outlook and try to send an e-mail message, you'll get a program alert asking if you want Outlook to have Internet access. However, program alerts can also occur if a Trojan horse or worm on your computer is trying to spread.

New Program Alerts

New Program alerts enable you to set access permission for program that has not asked for Internet Zone or Trusted Zone access before.

If you click Yes, the program is allowed access.

If you click No, the program is denied access.

Why New Program Alerts Occur

New Program alerts occur when a program on your computer tries to initiate a connection with a computer in the Internet Zone or Trusted Zone, and that program has not already received access permission from you.

As you begin to work with Endpoint Security, you will probably see one or more New Program Alerts.

What you should do

Click Yes or No in the alert pop-up after answering these questions:

- Did you just launch a program or process that would reasonably require permission? If so, it's probably safe to click Yes. If not, continue.
- Do you recognize the name of the program in the Alert pop-up? If so, does it make sense for the program to need permission? If so, it's probably safe to click Yes. If not, or if you're not sure, continue.
- Click the More Info button in the alert box. This submits your alert information (for example, the name of the program and the address it was trying to reach) to AlertAdvisor, which then displays a Web page with information about the alert and the program. Use the AlertAdvisor information to help you decide if it's safe to answer Yes.
Repeat Program Alerts

- If you’re really not sure what to do, it’s best to click No. You can always grant permission later by going to the Programs tab.

Reducing New Program Alerts

You may see several New Program alerts soon after installing Endpoint Security. As you assign permissions to each new program, the number of alerts you see will decrease.

To keep from seeing Repeat Program alerts, select Remember this answer the next time I use this program.

Repeat Program Alerts

Repeat Program alerts occur when a program on your computer tries to initiate a connection with a computer in the Internet Zone or Trusted Zone, and that program has asked for permission before.

Why Repeat Program Alerts Occur

If you click Yes or No to a New Program alert without checking Remember this answer the next time I use this program, you'll see a Repeat Program alert the next time the program asks for access permission.

What you should do

You should respond to Repeat Program alerts in the same way you would to New Program alerts.

New Program alerts enable you to set access permission for program that has not asked for Internet Zone or Trusted Zone access before.

If you click Yes, the program is allowed access. If you click No, the program is denied access.

Note - If your browser does not have permission to access the Internet, you will be re-routed to this help file. To access AlertAdvisor, give your browser permission to access the Internet.
Reducing Repeat Program Alerts

To keep from seeing Repeat Program alerts, select Remember this answer the next time I use this program before clicking Yes or No in any New Program or Repeat Program alert. This sets the permission for the program to Allow or Block in the Programs tab.

Changed Program Alerts

Changed Program alerts warn you that a program that has asked for access permission or server permission before has changed somehow.

If you click Yes, the changed program is allowed access. If you click No, the program is denied access.

Why Changed Programs Alerts Occur

Some programs are configured to access the Internet regularly to look for available updates. Changed Program alerts can occur if you have updated a program since the last time it accessed the Internet. However, they can also occur if a hacker has tampered with the program.

Consult the documentation for your programs, or refer to the support Web sites of their vendors, to find out if the program has automatic update functionality.

What you should do

To determine how to respond to a Changed Program alert, consider these questions:

• Did you (or system administrator) recently upgrade the program that is asking for permission?

• Does it make sense for the program to need permission?

If you can answer "yes" to both questions, it’s probably safe to click Yes.

If you’re not sure, it’s safest to answer No. You can always grant permission later by going to the Programs tab; see “Setting Specific Permissions” on page 105.
Reducing Changed Program Alerts

Changed Program alerts are always displayed because they require a Yes or No response from you. If you are using a program whose checksum changes frequently, you can avoid seeing numerous alerts by having Endpoint Security check the program's file name only. See “Adding Programs to the Programs List” on page 107.

Program Component Alerts

Use the Program Component alert to allow or deny Internet access to a program that is using one or more components that haven't yet been secured by Endpoint Security. This helps protect you from hackers who try to use altered or faked components to get around your program control restrictions.

By clicking Yes, you allow the program to access the Internet while using the new or changed components. By clicking No, you prevent the program from accessing the Internet while using those components.

Why Program Component Alerts Occur

Program Component alerts occur when a program accessing the Internet or local network is using one or more components that Endpoint Security has not yet secured, or that has changed since it was secured.

Endpoint Security automatically secures the components that a program is using at the time you grant it access permission. This prevents you from seeing a Component alert for every component loaded by your browser. See “Program Authentication” on page 100.

What you should do

The proper response to a Program Component alert depends on your situation. Consider the following questions:

- Are any of the following true?
- You just installed or re-installed Endpoint Security.
- You recently updated the application that is loading the component (For the application name, look under Technical Information in the alert pop-up.)
- The application that is loading the component has an automatic update function.
• Someone else (for example, a systems administrator at your workplace) may have updated a program on your computer without your knowledge.

• Are you actively using the application that loaded the component?

If you can answer "yes" to both questions, it is likely that Endpoint Security has detected legitimate components that your browser or other programs need to use. It is probably safe to answer Yes to the Program Component alert.

By clicking Yes, you allow the program to access the Internet while using the new or changed components. If you cannot answer yes both questions, or if you feel unsure about the component for any reason, it is safest to answer No.

By clicking No, you prevent the program from accessing the Internet while using those components. If you're not sure what to do, or if you decide to answer No, investigate the component to determine if it is safe.

Reducing Program Component Alerts

You may receive a large number of component alerts if you raised the Program Authentication level to high soon after installing Endpoint Security. With authentication set to High, Endpoint Security cannot automatically secure the large number of DLLs and other components commonly used by browsers and other programs.

To reduce the number of alerts, lower the authentication level to medium for the first few days after installing Endpoint Security.

If you have been using Endpoint Security for more than a few days, it is very rare to see large numbers of program alerts.
Server Program Alerts

Server Program alerts enable you to set server permission for a program on your computer.

Why Server Program Alerts Occur

Server Program alerts occur when a program on your computer wants server permission for either the Internet Zone or Trusted Zone, and that program has not already received server permission from you.

Relatively few programs on your computer will require server permission. Some common types of programs that do are:

- Chat
- Internet Call Waiting
- Music file sharing (such as Napster)
- Streaming Media (such as RealPlayer)
- Voice-over-Internet
- Web meeting

If you are using the types of programs described above that require server permission to operate properly, grant permission before you start using the program (see “Granting Server Permission to Programs” on page 108).

Note - If your browser does not have permission to access the Internet, you will be re-routed to the online help. To access AlertAdvisor, give your browser permission to access the Internet (see “Granting Internet Access Permissions to Programs” on page 108).

What you should do

Before responding to the Server Program alert, consider the following:

- Did you just launch a program or process that would reasonably require permission? If so, it’s probably safe to click Yes. If not, continue.
- Do you recognize the name of the program in the alert pop-up, and if so, does it make sense for the program to need permission? If so, it’s probably safe to click Yes.
- Click the More Info button in the alert box. This submits your alert information (for example, the name of the program and the address it was trying to reach) to AlertAdvisor, which then displays a Web page with information about the
alert and the program. Use the AlertAdvisor information to help you decide if it's safe to answer Yes. For more information, see “Using Alert Advisor” on page 170.

- If you are still not certain that the program is legitimate and needs server permission, it is safest to answer No. If it becomes necessary, you can give the program server permission later by using the Programs tab. See “Granting Server Permission to Programs” on page 108.

Reducing Server Program Alerts

If you are using the types of programs described above that require server permission to operate properly, use the Programs tab in Endpoint Security to grant permission before you start using the program.

Advanced Program Alerts

Advanced Program alerts are similar to other Program alerts (New Program, Repeat Program, and Changed Program)--they inform you that a program is attempting to access the network.

However, they differ from other Program alerts in that the program is attempting to use another program to connect to the Internet, or is attempting to manipulate another program's functionality.

Why Advanced Program Alerts Occur

Advanced Program alerts occur in two situations: when a program on your computer tries to initiate a connection with a computer in the Internet Zone or Trusted Zone by instructing another program to connect; or when a program attempts to hijack the processes of another program by calling the OpenProcess function.

There are some legitimate programs associated with your operating system that may require access to another program. For example, if you were using Windows Task Manager to shutdown Microsoft Internet Explorer, Windows Task Manager would need to call the OpenProcess function on the Internet Explorer program to shut it down.

What you should do

How you should respond to an Advanced Program alert depends upon the cause of the alert. If the Advanced Program alert was caused by the OpenProcess function being called, you should determine whether the function was called by a legitimate program or by a malicious one. Verify that the program cited in the alert is one you
trust to carry out this function. For example, if you were attempting to shut down a program using Windows Task Manager when you received the Advanced Program alert, it is probably safe to answer Yes. Similarly, if the alert was caused by a program using another program to access the Internet and that program routinely requests such permission, is probably safe to answer Yes. If you are unsure as to the cause of the alert or the expected behavior of the program initiating the request, it is safest to answer No. After denying advanced permission to the program, perform an Internet search on the program’s file name. If the program is malicious, it is likely that information about it is available, including how to remove it from your computer.

Reducing Advanced Program Alerts

It is unusual to see a large number of Advanced Program alerts. If you receive repeated alerts, research the program name or names and consider either removing the program from your computer or providing the program with the necessary access rights.

Automatic VPN Configuration Alerts

Automatic VPN Configuration alerts occur when Endpoint Security detects VPN activity. Depending upon the type of VPN activity detected, and whether Endpoint Security was able to configure your VPN connection automatically, you may see one of three Automatic VPN Configuration alerts.

Why Automatic VPN Alerts Occur

Automatic VPN Configuration alerts occur when Endpoint Security detects VPN activity that it is not configured to allow.

What you should do

How you should respond to an Automatic VPN Configuration alert depends upon which Automatic VPN Configuration alert you encounter, whether you are running VPN software or not, and whether you want to configure Endpoint Security to allow your VPN connection

• If you are running VPN software on your computer and you want to configure the connection, select either:
  • Configure Endpoint Security to support this VPN connection, or
  • I am running VPN software and would like to configure Endpoint Security to support it
• If you are running VPN software but do not want Endpoint Security to configure your connection, select **Do not configure Endpoint Security to support this VPN connection**.

• If you are not running VPN software, select **I am not running VPN software**.

**Reducing VPN Configuration Alerts**

If you are running VPN software, the only way to see fewer of these alerts is to properly configure your Endpoint Security client to allow your VPN software and its required resources. See “Configuring VPN Connection Manually” on page 94.

**Manual Action Required Alerts**

A Manual Action Required alert informs you that further steps must be taken before Endpoint Security is properly configured to support your VPN connection.

**Why Manual Action Require Alerts Occur**

A Manual Action Required alert occurs when Endpoint Security is unable to configure your VPN connection automatically, or if further manual changes are required before automatic configuration can be completed.

**What you should do**

Manual Action Required alerts do not require a response from you. To configure VPN connection manually, see “Configuring VPN Connection Manually” on page 94 and follow the instructions for manual configuration.

**Reducing Manual Action Alerts**

It is unusual for you to see many Manual Action Required alerts. If you do see multiple alerts, either perform the required steps to properly configure your Endpoint Security to support your VPN connection, or remove the VPN software from your computer.
New Network Alerts

A New Network alert appears when Endpoint Security detects that you're connected to a network you haven't seen before. You can use the alert pop-up to enable file and printer sharing with that network. New Network alerts occur when you connect to any network--wireless home network, a business LAN, or your ISP.

The first time you use Endpoint Security, you will almost certainly see a New Network alert. This alert is a convenience tool designed to help you configure Endpoint Security.

Why New Network Alerts Occur

By default, Endpoint Security versions 3.5 and above display the Network Configuration Wizard, rather than the New Network alert, when a network is detected.

What you should do

How you respond to a New Network alert depends on your particular network situation. If you are connected to a home or business local network and you want to share resources with the other computers on the network, put the network in the Trusted Zone.

To add the new network to the Trusted Zone:

1. In the New Network alert pop-up, provide a name for the network (for example “Home NW”) in the Name box.
2. Select Trusted Zone from the Zone drop-down list.
3. Click OK.

Use caution if Endpoint Security detects a wireless network. It is possible for your wireless network adapter to pick up a network other than your own. Be sure that the IP address displayed in the New Network alert is yours before adding it to the Trusted Zone.

Warning - If you are not certain which network Endpoint Security has detected, write the IP address displayed in the alert box, and consult your home network documentation, systems administrator, or ISP to determine what network it is.
Appendix

Troubleshooting

In This Appendix

VPN Troubleshooting  page 191
Network Troubleshooting  page 193
Internet Connection Troubleshooting  page 195
VPN Troubleshooting

If you are having difficulty using VPN software with the client, refer to the table for troubleshooting tips provided in this section.

Table B-1  Troubleshooting VPN Issues

<table>
<thead>
<tr>
<th>If...</th>
<th>See...</th>
</tr>
</thead>
<tbody>
<tr>
<td>You can't connect to your VPN</td>
<td>Configuring Client for VPN Traffic</td>
</tr>
<tr>
<td>You have created expert firewall rules</td>
<td>VPN Auto-Configuration and Expert Rules</td>
</tr>
<tr>
<td>You are using a supported VPN client and Endpoint Security client does not detect it automatically the first time you connect</td>
<td>Automatic VPN Detection Delay</td>
</tr>
</tbody>
</table>

Configuring Client for VPN Traffic

If you cannot connect to your VPN, you may need to configure the client to accept traffic coming from your VPN.

To configure the client to allow VPN traffic:

1. Add VPN-related network resources to the Trusted Zone (see page 88).
2. Grant access permission to the VPN client and any other VPN-related programs on your computer (see page 105).
3. Allow VPN protocols (see page 94).

VPN Auto-Configuration and Expert Rules

If you have created expert firewall rules that block VPN protocols, Endpoint Security client will not be able to automatically detect your VPN when you initiate a connection. To configure your VPN connection, you will need to make sure that your VPN client and VPN-related components are in the Trusted Zone, and that they have permission to access the Internet. See page 93.
Automatic VPN Detection Delay

Endpoint Security client periodically polls your computer to determine if supported
VPN protocols are engaged. Upon detection, Endpoint Security client prompts you
to configure your connection automatically. If you have recently installed a VPN
client and have tried to connect, the client may not have detected your VPN
configuration. If you prefer the client to configure your connection automatically,
you can wait ten minutes. Then, try connecting again. If you prefer to connect right
away, you can configure your connection manually. See page 93.
Network Troubleshooting

If you are having difficulty connecting to your network or using networking services, refer to the table for troubleshooting tips provided in this section.

Table B-2  Troubleshooting Network Issues

<table>
<thead>
<tr>
<th>If...</th>
<th>See...</th>
</tr>
</thead>
<tbody>
<tr>
<td>You can't see the other computers in your Network Neighborhood, or they can't see you</td>
<td>Making Your Computer Visible on Local Network</td>
</tr>
<tr>
<td>You can't share files or printers over your home or local network</td>
<td>Sharing Files and Printers Locally</td>
</tr>
<tr>
<td>Your computer is on a LAN and takes a long time to start up when Endpoint Security client is installed</td>
<td>Resolving Slow Startup</td>
</tr>
</tbody>
</table>

Making Your Computer Visible on Local Network

If you can't see the other computers on your local network, or if they can't see your computer, it is possible that the client is blocking the NetBIOS traffic necessary for Windows network visibility.

To make your computer visible on the local network:

1. Add the network subnet (or, in a small network, the IP address of each computer you’re sharing with) to your Trusted Zone (see page 88).

2. Set the Trusted Zone security level to Medium, and the Internet Zone security level to High. This allows trusted computers to access your shared files, but blocks all other machines from accessing them (see page 82).

   Note - The client will detect your network automatically and display the New Network alert. You can use the alert to add your network subnet to the Trusted Zone; see page 189.

Sharing Files and Printers Locally

Endpoint Security client enables you to quickly and easily share your computer so that the trusted computers you’re networked with can access your shared resources, but Internet intruders can't use your shared resources to compromise your system.
To configure the client for secure sharing:

1. Add the network subnet (or, in a small network, the IP address of each computer you're sharing with) to your Trusted Zone (see page 88).

2. Set the Trusted Zone security level to Medium. This allows trusted computers to access your shared files (see page 82).

3. Set the Internet Zone security level to High. This makes your computer invisible to non-trusted computers.

Resolving Slow Startup

If the client is configured to load at startup, some users connected to the LAN may find that it takes several minutes for the startup process to finish.

In most cases, this is because your computer needs access to your network's Domain Controller to complete its startup and login process, and the client is blocking access because the Controller has not been added to the Trusted Zone.

To solve this problem, add the host name or IP address of your network's Domain Controller to the Trusted Zone.
Internet Connection Troubleshooting

If you are having difficulty connecting to the Internet, refer to the table for troubleshooting tips provided in this section.

<table>
<thead>
<tr>
<th>If...</th>
<th>See...</th>
</tr>
</thead>
<tbody>
<tr>
<td>You cannot connect to the Internet</td>
<td>Connecting to the Internet Fails after Installation</td>
</tr>
<tr>
<td>You can connect to the Internet but are disconnected after a short time</td>
<td>Allowing ISP Heartbeat Messages</td>
</tr>
<tr>
<td>Your computer is an Internet Connection Sharing (ICS) client and you can't connect to the Internet</td>
<td>Connecting Through an ICS Client</td>
</tr>
<tr>
<td>Your computer uses a proxy server to connect to the Internet and you can't connect to the Internet</td>
<td>Connecting Through a Proxy Server</td>
</tr>
</tbody>
</table>

Connecting to the Internet Fails after Installation

If you are unable to connect to the Internet after installing Endpoint Security client, the first troubleshooting step is to determine whether Endpoint Security client is the cause. If you are unable to follow the steps below, for example, if you can't clear the Load Endpoint Security at startup box, contact Check Point technical support.

To determine if Endpoint Security client is the cause of connection problems:

1. Open Overview/Preferences.
2. In the General area, clear Load Check Point Endpoint Security at startup.
   A warning window labeled Check Point TrueVector Service opens.
3. Click Yes.
4. Restart your computer, then try to connect to the Internet.
   - If you can connect: Your Endpoint Security client settings may be the cause of your connection problems. Make sure your browser has access permission.
   - If you cannot connect: Your Endpoint Security client settings are not the cause of your connection problems.
Allowing ISP Heartbeat Messages

Internet Service Providers (ISPs) periodically send heartbeat messages to their connected dial-up customers to make sure they are still there. If the ISP cannot determine that the customer is there, it might disconnect the customer so that the user's IP address can be given to someone else.

By default, Endpoint Security client blocks the protocols most commonly used for these heartbeat messages, which may cause you to be disconnected from the Internet. To prevent this from happening, you can identify the server sending the messages and add it to your Trusted Zone or you can configure the Internet Zone to allow ping messages.

Identifying Source of Heartbeat Messages

This is the preferred solution because it will work whether your ISP uses NetBIOS or ICMP to check your connection, and it allows you to maintain high security for the Internet Zone.

To identify the server your ISP uses to check your connection:
1. When your ISP disconnects you, click Alerts & Logs > Log Viewer.
2. In the alerts list, find the alert that occurred at the time you were disconnected.
3. In the Entry Detail area, note the Source DNS detected.
   - If you're not able to identify the server this way, contact your ISP to determine which servers need access permission.
4. After you have identified the server, add it to the Trusted Zone (see page 88).

Configuring Endpoint Security Client to Allow Pings

If your ISP uses ICMP echo (or ping) messages for connectivity checks, configure the client to allow ping messages from the Internet Zone.

To configure the client to allow ping messages:
1. Open Firewall > Main.
2. In the Internet Zone area, click Custom.
3. Select the Allow incoming ping (ICMP echo) check box.
4. Click OK.
5. Set the security level for the Internet Zone to Medium (see page 82).
Connecting Through an ICS Client

If you are using Windows' Internet Connection Sharing (ICS) option, or a third-party connection sharing program, and you are unable to connect to the Internet, make sure that Endpoint Security client is properly configured for the client and gateway machines. See “Enabling Internet Connection Sharing” on page 81.

Do not configure the client for Internet Connection Sharing if you use hardware such as a server or router, rather than a host PC.

Connecting Through a Proxy Server

If you connect to the Internet through a proxy server and you are unable to connect to the Internet, make sure that the IP address of your proxy server is in your Trusted Zone. See “Adding to the Trusted Zone” on page 88.
Glossary

Symbols & Numeric

1394
A very fast external bus standard that supports data transfer rates of up to 400Mbps (in 1394a) and 800Mbps (in 1394b). Products supporting the 1394 standard go under different names, depending on the company. Apple, which originally developed the technology, uses the trademarked name FireWire.

Access Permission
Access permission allows a program on your computer to initiate communications with another computer. This is distinct from server permission, which allows a program to "listen" for connection requests from other computers. You can give a program access permission for the Trusted Zone, the Internet Zone, or both.

Act as a Server
A program acts as a server when it "listens" for connection requests from other computers. Several common types of applications, such as chat programs, e-mail clients, and Internet Call Waiting programs, may need to act as servers to operate properly. However, some hacker programs act as servers to listen for instructions from their creators. The client prevents programs on your computer from acting as servers unless you grant server permission.

ActiveX Controls
ActiveX controls (developed by Microsoft) are a set elements such as a check boxes or buttons that offer options to users or run macros or scripts that automate a task.
**Ad Blocking**

A client feature that enables you to block banner, pop-up and other types of advertisements.

**Advanced Program Control**

Advanced Program Control is an advanced security feature that tightens your security by preventing unknown programs from using trusted programs to access the Internet.

**Alert Advisor**

Check Point AlertAdvisor is an online utility that enables you to instantly analyze the possible causes of an alert, and helps you decide whether to respond Yes or No to a Program alert. To use AlertAdvisor, click the More Info button in an alert pop-up. The client sends information about your alert to AlertAdvisor. AlertAdvisor returns an article that explains the alert and gives you advice on what, if anything, you need to do to ensure your security.

**Animated Ad**

An advertisement that incorporates moving images.

**Banner Ad**

An ad that appears in a horizontal banner across a Web page.

**Blocked Zone**

The Blocked Zone contains computers you want no contact with. The client prevents any communication between your computer and the machines in this Zone.

**Cache Cleaner**

Privacy feature that enables you to remove unwanted files and cookies from your computer on demand, or on a scheduled basis.
**Component**

A small program or set of functions that larger programs call on to perform specific tasks. Some components may be used by several different programs simultaneously. Windows operating systems provide many component DLLs (Dynamic Link Libraries) for use by a variety of Windows applications.

**Component Learning Mode**

The period after installation when program control is set to Medium. When in component learning mode, the client can quickly learn the MD5 signatures of many frequently used components without interrupting your work with multiple alerts.

**Cookie**

A small data file used by a Web site to customize content, remember you from one visit to the next, and/or track your Internet activity. While there are many benign uses of cookies, some cookies can be used to divulge information about you without your consent.

**Cookie Control**

Privacy feature that allows you to prevent cookies from being stored on your computer.

**DHCP**

Dynamic Host Configuration Protocol

A protocol used to support dynamic IP addressing. Rather than giving you a static IP address, your ISP may assign a different IP address to you each time you log on. This allows the provider to serve a large number of customers with a relatively small number of IP addresses.

**DHCP Broadcast/Multicast**

A type of message used by a client computer on a network that uses dynamic IP addressing. When the computer comes online, if it needs an IP address, it issues a broadcast message to any DHCP servers which are on the network. When a DHCP server receives the broadcast, it assigns an IP address to the computer.
**Dial-Up Connection**

Connection to the Internet using a modem and an analog telephone line. The modem connects to the Internet by dialing a telephone number at the Internet Service Provider's site. This is in distinction to other connection methods, such as Digital Subscriber Lines, that do not use analog modems and do not dial telephone numbers.

**DLL**

Dynamic Link Library

A library of functions that can be accessed dynamically (that is, as needed) by a Windows application.

**DNS**

Domain Name Server

A data query service generally used on the Internet for translating host names or domain names (like `www.yoursite.com`) into Internet addresses (like `123.456.789.0`).

**Embedded Object**

An object such as a sound file or an image file that is embedded in a Web page.

**Endpoint Security Server**

An Endpoint Security system by Check Point that enables systems administrators to manage computer security from a single location. Administrators create security policies, then deploy them to the Endpoint Security client applications running on their users' computers.

**Enterprise Policy**

A collection of security settings (firewall, program control, e-mail protection, and so forth) designed by a network administrator and delivered to the client by uploading from Endpoint Security Server. The endpoint user cannot change the enterprise policy.
G

Gateway

In networking, a combination of hardware and software that links two different types of networks. For example, if you are on a home or business Local Area Network (LAN), a gateway enables the computers on your network to communicate with the Internet.

H

Heartbeat Messages

Messages sent by an Internet Service Provider (ISP) to make that a dial-up connection is still in use. If it appears a customer is not there, the ISP might disconnect her so that her IP address can be given to someone else.

High-Rated Alerts

An alert that is likely to have been caused by hacker activity. High-rated Firewall alerts display a red band at the top of the alert pop-up. In the Log Viewer, you can see if an alert was high-rated by looking in the Rating column.

HTTP Referrer Header Field

An optional field in the message that opens a Web page, containing information about the "referring document." Properly used, this field helps Web masters administer their sites. Improperly used, it can divulge your IP address, your workstation name, login name, or even (in a poorly-implemented e-commerce site) your credit card number. By selecting Remove Private Header information in the Cookies tab, you prevent this header field from transferring any information about you.

I

ICMP

Internet Control Messaging Protocol

An extension of the Internet Protocol that supports error control and informational messages. The "ping" message is a common ICMP message used to test an Internet connection.
ICS

Internet Connection Sharing

ICS is a service provided by the Windows operating system that enables networked computers to share a single connection to the Internet.

Index.dat

Index.dat files keep copies of everything that was in your Temporary Internet, Cookies, and History folders even AFTER these files have been deleted.

Information Alerts

The type of alerts that appear when the client blocks a communication that did not match your security settings. Informational alerts do not require a response from you.

Internet Zone

The Internet Zone contains all the computers in the world—except those you have added to the Trusted Zone or Blocked Zone.

The client applies the strictest security to the Internet Zone, keeping you safe from hackers. Meanwhile, the medium security settings of the Trusted Zone enable you to communicate easily with the computers or networks you know and trust—for example, your home network PCs, or your business network.

IP Address

The number that identifies your computer on the Internet, as a telephone number identifies your phone on a telephone network. It is a numeric address, usually displayed as four numbers between 0 and 255, separated by periods. For example, 172.16.100.100 could be an IP address.

Your IP address may always be the same. However, your Internet Service Provider (ISPs) may use Dynamic Host Configuration Protocol (DHCP) to assign your computer a different IP address each time you connect to the Internet.

ISP

Internet Service Provider
A company that provides access to the Internet. ISPs provide many kinds of Internet connections to consumers and business, including dial-up (connection over a regular telephone line with a modem), high-speed Digital Subscriber Lines (DSL), and cable modem.

**Java Applet**

A Java applet is a small Internet-based program written in Java, which is usually embedded in an HTML page, and which can be executed within a Web browser.

**JavaScript**

A popular scripting language that enables some of the most common interactive content on Web sites. Some of the most frequently used JavaScript functions include Back and History links, changing images on mouse-over, and opening and closing browser windows. The default settings allow JavaScript because it is so common and because most of its uses are harmless.

**Mail Server**

The remote computer from which the e-mail program on your computer retrieves e-mail messages sent to you.

**MD5 Signature**

A digital "fingerprint" used to verify the integrity of a file. If a file has been changed in any way (for example, if a program has been compromised by a hacker), its MD5 signature will change as well.

**Medium-rated Alert**

An alert that was probably caused by harmless network activity, rather than by a hacker attack.

**MIME-type integrated object**

An object such as an image, sound file, or video file that is integrated into an e-mail message. MIME stands for Multipurpose Internet Mail Extensions.
Mobile Code

Executable content that can be embedded in Web pages or HTML e-mail. Mobile code helps make Web sites interactive, but malicious mobile code can be used to modify or steal data, and for other malevolent purposes.

Mobile-Code Control

A client feature that enables you to block active controls and scripts on the Web sites you visit. While mobile code is common on the Internet and has many benign uses, hackers can sometimes use it for malevolent purposes.

N

NetBIOS

Network Basic Input/Output System

A program that allows applications on different computers to communicate within a local network. By default, the client allows NetBIOS traffic in the Trusted Zone, but blocks it in the Internet Zone. This enables file sharing on local networks, while protecting you from NetBIOS vulnerabilities on the Internet.

P

Packet

A single unit of network traffic. On "packet-switched" networks like the Internet, outgoing messages are divided into small units, sent and routed to their destinations, then reassembled on the other end. Each packet includes the IP address of the sender, and the destination IP address and port number.

Pass-lock

When the Internet Lock is engaged, programs given pass-lock permission can continue accessing the Internet. Access permission and server permission for all other programs is revoked until the lock is opened.
**Persistent Cookie**

A cookie put on your hard drive by a Web site you visit. These cookies can be retrieved by the Web site the next time you visit. While useful, they create a vulnerability by storing information about you, your computer, or your Internet use in a text file.

**Personal Policy**

Your personal policy comprises all the security settings you can control through the client interface. For example, if you use the Zones tab to add a server to the Trusted Zone, that configuration becomes part of your personal policy.

**Ping**

A type of ICMP message (formally "ICMP echo") used to determine whether a specific computer is connected to the Internet. A small utility program sends a simple "echo request" message to the destination IP address, and then waits for a response. If a computer at that address receives the message, it sends an "echo" back. Some Internet providers regularly "ping" their customers to see if they are still connected.

**Pop-under Ad**

An ad that appears in a new browser window that opens under the window you're looking at, so you don't see the ad until you close the original browser window.

**Pop-up Ad**

An ad that appears in a new browser window that 'pops up' in front of the window you're looking at.

**Port**

A channel associated with the use of TCP or UDP. Some ports are associated with standard network protocols; for example, HTTP (Hypertext Transfer Protocol) is traditionally addressed to port 80. Port numbers range from 0 to 65535.

**Port Scan**

A technique hackers use to find unprotected computers on the Internet. Using automated tools, the hacker systematically scans the ports on all the computers in a range of IP addresses, looking for unprotected or "open" ports. Once an open port is located, the hacker can use it as an access point to break in to the unprotected computer.
Privacy Advisor

A small display that shows you when the client blocks cookies or mobile code, and enables you to un-block those elements for a particular page.

Private Header

A section of a Web page that contains information about the Web site, which can collect information about visitors to the site. Private header information enables sites you visit by clicking a link from another site to know what site you came from. If a site implements the use of private headers carelessly, private headers can transfer information that you’ve entered in a web form--for example, Social Security number, credit card, etc.).

Programs List

The list of programs to which you can assign Internet access and server permissions. The list is shown in the Programs tab of the Program Control panel. You can add programs to the list, or remove programs from it.

Protocol

A standardized format for sending and receiving data. Different protocols serve different purposes; for example SMTP (Simple Mail Transfer Protocol) is used for sending e-mail messages; while FTP (File Transfer Protocol) is used to send large files of different types. Each protocol is associated with a specific port, for example, FTP messages are addressed to port 21.

Public Network

A large network, such as that associated with an ISP. Public networks are placed in the Internet Zone by default.

Quarantine

MailSafe quarantines incoming e-mail attachments whose filename extensions (for example, .EXE or .BAT) indicate the possibility of auto-executing code. By changing the filename extension, quarantining prevents the attachment from opening without inspection. This helps protect you from worms, viruses, and other malware that hackers distribute as e-mail attachments.
Script
A series of commands that execute automatically, without the user intervening. These usually take the form of banners, menus that change when you move your mouse over them, and popup ads.

Security Levels
The High, Med., and Low settings that dictate the type of traffic allowed into or out of your computer.

Server Permission
Server permission allows a program on your computer to "listen" for connection requests from other computers, in effect giving those computers the power to initiate communications with yours. This is distinct from access permission, which allows a program to initiate a communications session with another computer. Several common types of applications, such as chat programs, e-mail clients, and Internet Call Waiting programs, may need server permission to operate properly. Grant server permission only to programs you're sure you trust, and that require it in order to work. If possible, avoid granting a program server permission for the Internet Zone. If you need to accept incoming connections from only a small number of machines, add those machines to the Trusted Zone, and then allow the program server permission for the Trusted Zone only.

Session Cookie
A cookie stored in your browser's memory cache that disappears as soon as you close your browser window. These are the safest cookies because of their short life-span.

Skyscraper Ad
An ad that appears in a vertical column along the side of a Web page.

Stealth Mode
When the client puts your computer in stealth mode, any uninvited traffic receives no response—not even an acknowledgement that your computer exists. This renders your computer invisible to other computers on the Internet, until a permitted program on your computer initiates contact.
Third Party Cookie

persistent cookie that is placed on your computer, not by the Web site you are visiting, but by an advertiser or other 'third party.' These cookies are commonly used to deliver information about your Internet activity to that third party.

VPN

Virtual Private Network

A VPN is a network that provides secure, private access to a LAN (such as your organization's network) over public infrastructure (such as the Internet), by tunneling the transmissions and data through encryption protocols and other security measures.