

# Symantec™ Client Firewall Client Guide



# Symantec™ Client Firewall Client Guide

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Documentation version 5.1

## Copyright Notice

Copyright © 2003 Symantec Corporation.

All Rights Reserved.

Any technical documentation that is made available by Symantec Corporation is the copyrighted work of Symantec Corporation and is owned by Symantec Corporation.

NO WARRANTY. The technical documentation is being delivered to you AS-IS, and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained therein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical errors. Symantec reserves the right to make changes without prior notice.

No part of this publication may be copied without the express written permission of Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014.

## Trademarks

Symantec, the Symantec logo, and LiveUpdate are U.S. registered trademarks of Symantec Corporation. Symantec Client Firewall, Symantec Client Security, and Symantec Security Response are trademarks of Symantec Corporation.

Other brands and product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

# Technical support

As part of Symantec Security Response, the Symantec global Technical Support group maintains support centers throughout the world. The Technical Support group's primary role is to respond to specific questions on product feature/function, installation, and configuration, as well as to author content for our Web-accessible Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering as well as Symantec Security Response to provide Alerting Services and Virus Definition Updates for virus outbreaks and security alerts.

Symantec technical support offerings include:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and Web support components that provide rapid response and up-to-the-minute information
- Upgrade insurance that delivers automatic software upgrade protection
- Content Updates for virus definitions and security signatures that ensure the highest level of protection
- Global support from Symantec Security Response experts, which is available 24 hours a day, 7 days a week worldwide in a variety of languages
- Advanced features, such as the Symantec Alerting Service and Technical Account Manager role, offer enhanced response and proactive security support

Please visit our Web site for current information on Support Programs. The specific features available may vary based on the level of support purchased and the specific product that you are using.

## Licensing and registration

If the product that you are implementing requires registration and/or a license key, the fastest and easiest way to register your service is to access the Symantec licensing and registration site at [www.symantec.com/certificate](http://www.symantec.com/certificate). Alternatively, you may go to [www.symantec.com/techsupp/ent/enterprise.html](http://www.symantec.com/techsupp/ent/enterprise.html), select the product that you wish to register, and from the Product Home Page, select the Licensing and Registration link.

## Contacting Technical Support

Customers with a current support agreement may contact the Technical Support group via phone or online at [www.symantec.com/techsupp](http://www.symantec.com/techsupp).

When contacting the Technical Support group, please be sure to have the following information available:

- Product release level
- Hardware information
- Available memory, disk space, NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description
  - Error messages/log files
  - Troubleshooting performed prior to contacting Symantec
  - Recent software configuration changes and/or network changes

## Customer Service

To contact Enterprise Customer Service online, go to [www.symantec.com](http://www.symantec.com), select the appropriate Global Site for your country, then choose Service and Support. Customer Service is available to assist with the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates such as address or name changes
- General product information (such as features, language availability, dealers in your area)
- Latest information on product updates and upgrades
- Information on upgrade insurance and maintenance contracts
- Information on Symantec Value License Program
- Advice on Symantec's technical support options
- Nontechnical presales questions
- Missing or defective CD-ROMs or manuals

# Contents

Chapter 1	Introducing Symantec Client Firewall	
	About Symantec Client Firewall .....	10
	Symantec Client Firewall and Symantec Client Security .....	11
	Symantec Client Firewall features .....	12
Chapter 2	Installing Symantec Client Firewall	
	System requirements .....	14
	Before installation .....	15
	Disabling the Windows XP firewall .....	15
	Starting and running the installation program .....	16
	If you need to uninstall Symantec Client Firewall .....	19
Chapter 3	Symantec Client Firewall basics	
	Accessing Symantec Client Firewall .....	22
	Working with Symantec Client Firewall .....	23
	Symantec Client Firewall user levels .....	23
	Connecting to a network .....	24
	Responding to Symantec Client Firewall alerts .....	25
	Adjusting the Reporting Level .....	34
	Using AlertTracker .....	34
	Customizing Symantec Client Firewall .....	35
	About general options .....	36
	About Advanced Options .....	37
	Keeping current with LiveUpdate .....	42
	Where to find troubleshooting information .....	43

<b>Chapter 4</b>	<b>Protecting your privacy</b>	
	About protecting your privacy .....	46
	Enabling or disabling Privacy Control .....	46
	Identifying confidential information to protect .....	47
	Tips on entering confidential information .....	47
	Adding confidential information .....	47
	Modifying or removing confidential information .....	48
	Customizing Privacy Control .....	48
	Setting the Privacy Level .....	49
	Adjusting individual Privacy Control settings .....	49
<b>Chapter 5</b>	<b>Controlling access to protected computers</b>	
	About controlling access .....	54
	Organizing computers into network zones .....	54
	Enabling file and printer sharing .....	54
<b>Chapter 6</b>	<b>Monitoring Symantec Client Firewall</b>	
	About monitoring Symantec Client Firewall .....	58
	Reviewing Current Status .....	59
	Reviewing the Symantec Client Firewall Event Log .....	60
	About Symantec Client Firewall Event Log entries .....	61
	Viewing the Symantec Client Firewall Event Log .....	61
	Filtering events in the Symantec Client Firewall Event Log .....	61
	Refreshing the Symantec Client Firewall Event Log .....	62
	Clearing the Symantec Client Firewall Event Log .....	62
	Changing the size of the Symantec Client Firewall Event Log .....	63
	Adjusting the width of a column .....	64
	Reviewing Internet access statistics .....	64
	Resetting counters .....	65
	Setting the statistics that display in the Statistics window .....	65
	Keeping the Statistics window visible .....	66
	Printing or saving logs and statistics .....	67
<b>Chapter 7</b>	<b>Guarding against intrusion attempts</b>	
	About guarding against intrusion attempts .....	70
	How Symantec Client Firewall protects against network attacks .....	70
	Monitoring communications with Symantec Client Firewall .....	71
	Analyzing communications with Intrusion Detection .....	71
	Ensuring that Symantec Client Firewall and Intrusion Detection are enabled .....	73

Customizing firewall protection .....	74
Changing the Security Level slider .....	75
Changing individual security settings .....	75
Customizing firewall rules .....	78
Priorities for firewall rule processing .....	79
Default firewall rules .....	79
Creating new firewall rules .....	80
Creating firewall rules manually .....	84
Elements of a firewall rule .....	84
Adding firewall rules .....	88
Changing an existing firewall rule .....	89
Customizing Intrusion Detection .....	90
Excluding specific network activity from being monitored .....	90
Enabling or disabling AutoBlock .....	91
Excluding specific computers from AutoBlock .....	92
Restricting a blocked computer .....	92
Unblocking computers .....	93

## Index



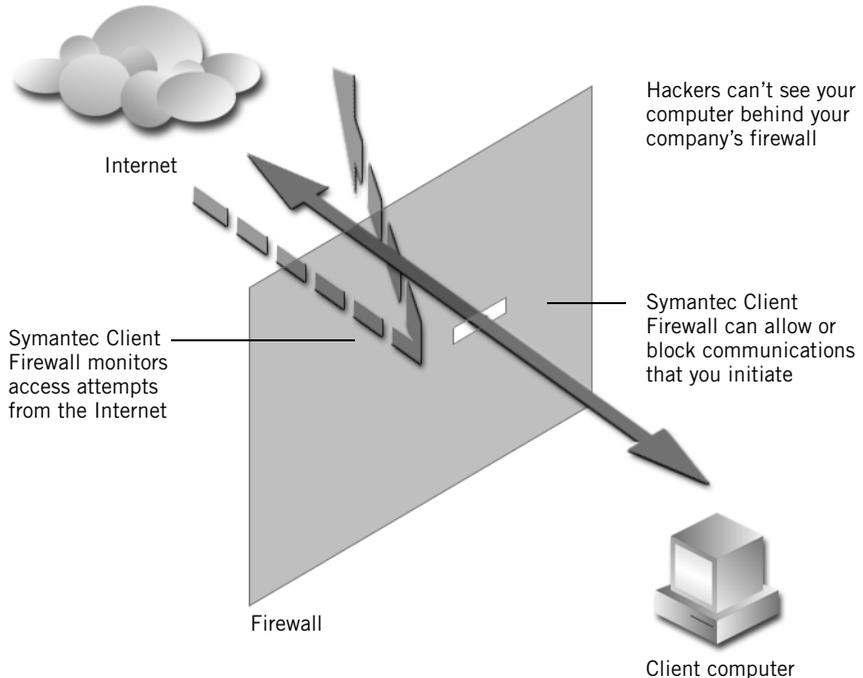
# Introducing Symantec Client Firewall

This chapter includes the following topics:

- [About Symantec Client Firewall](#)
- [Symantec Client Firewall and Symantec Client Security](#)
- [Symantec Client Firewall features](#)

## About Symantec Client Firewall

Symantec Client Firewall protects computers from hackers, protects your privacy, and eliminates unwanted sources of network traffic.



Symantec Client Firewall provides a barrier between your computer and the Internet. A firewall prevents unauthorized users from accessing privately owned computers and networks connected to the Internet.

Symantec Client Firewall prevents unauthorized access to your computer when you are on the Internet, detects possible hacker attacks, protects your personal information, and eliminates unwanted sources of network traffic.

# Symantec Client Firewall and Symantec Client Security

Symantec Client Firewall is a component of Symantec Client Security. At the client level, Symantec Client Security includes the following forms of protection:

- Virus protection
- Content filtering
- Firewall
- Intrusion detection

These forms of protection protect the network at the client level by identifying and removing *blended threats*. Blended threats use multiple methods of attack including worms, email and application vulnerabilities, and network shares to gain control of systems. Code Red and Nimda are examples of blended threats.

Symantec Client Security also protects against the following types of threats:

- File, boot, and macro viruses
- Remote control Trojan horses
- Mass mailer viruses, such as Love Letter/Melissa
- Active network infectors

See the Reference Area of the Symantec Security Response Web site for more information:

<http://sarc.com/>

## Symantec Client Firewall features

[Table 1-1](#) lists the features available in Symantec Client Firewall.

**Table 1-1** Symantec Client Firewall features

Feature	Description
Internet Status	<p>Provides a snapshot of your computer's network activity that you can use to identify ongoing attack attempts and review how program settings affect your protection.</p> <p>See <a href="#">"Monitoring Symantec Client Firewall"</a> on page 57.</p>
Client Firewall	<p>Protects your computer from Internet hackers and unauthorized intrusions. Makes your computer virtually invisible to others on the Internet.</p> <p>Protects remote and mobile users from hacker attacks and prevents these systems from being used by hackers to gain back-door access to the corporate network.</p> <p>See <a href="#">"Guarding against intrusion attempts"</a> on page 69.</p>
Intrusion Detection	<p>Detects and blocks malicious traffic and attempts by outside users to attack your computer.</p> <p>See <a href="#">"Guarding against intrusion attempts"</a> on page 69.</p>
Privacy Control	<p>Gives you several levels of control over the kinds of information that users and Web browsers can send over the Internet.</p> <p>See <a href="#">"Protecting your privacy"</a> on page 45.</p>

# Installing Symantec Client Firewall

This chapter includes the following topics:

- [System requirements](#)
- [Before installation](#)
- [Starting and running the installation program](#)
- [If you need to uninstall Symantec Client Firewall](#)

## System requirements

To use Symantec Client Firewall, your computer must have one of the following Windows operating systems installed:

- Windows 98/98SE
- Windows Me
- Windows NT version 4.0 Workstation with Service Pack 6a or later
- Windows 2000 Professional
- Windows XP Professional or Windows XP Home Edition

Your computer must meet the following minimum requirements.

### Windows 98/Me

- Intel Pentium processor at 150 MHz
- 32 MB of RAM
- 60 MB of available hard disk space
- Internet Explorer 5.0 or later
- CD-ROM or DVD-ROM drive
- Microsoft Windows Internet support

### Windows NT 4.0 Workstation

- Service Pack 6a or later
- Intel Pentium processor at 150 MHz
- 64 MB of RAM
- 60 MB of available hard disk space
- Internet Explorer 5.0 or later
- CD-ROM or DVD-ROM drive
- Microsoft Windows Internet support

## Windows 2000 Professional Workstation

- Intel Pentium processor at 150 MHz
- 64 MB of RAM
- 60 MB of available hard disk space
- Internet Explorer 5.0 or later
- CD-ROM or DVD-ROM drive
- Microsoft Windows Internet support

## Windows XP Professional/Home Edition

- Intel Pentium processor at 300 MHz or higher
- 128 MB of RAM
- 60 MB of available hard disk space
- Internet Explorer 5.0 or later
- CD-ROM or DVD-ROM drive
- Microsoft Windows Internet support

# Before installation

The Symantec Client Firewall install program triggers the uninstall of the following products:

- Symantec Desktop Firewall version 2.01
- Norton Personal Firewall version 2.5
- Norton Personal Firewall version 2002

You must uninstall all other versions before installing Symantec Client Firewall.

Quit all other Windows programs before installing Symantec Client Firewall. Other active programs may interfere with the installation and reduce your protection.

## Disabling the Windows XP firewall

Windows XP includes a firewall that can interfere with Symantec Client Firewall protection features. You must disable the Windows XP firewall before installing Symantec Client Firewall.

### To disable the Windows XP firewall

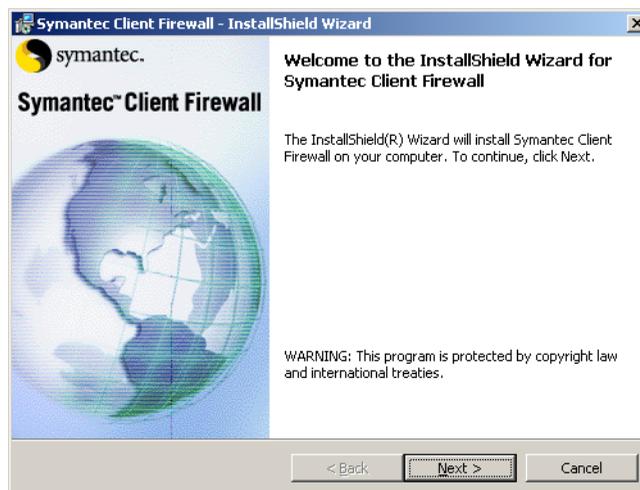
- 1 On the Windows XP taskbar, click **Start > Control Panel**.
- 2 In the Control Panel, double-click **Network Connections**.
- 3 In the Network Connections window, right-click the active connection, then click **Properties**.
- 4 On the Advanced tab, in the Internet Connection Firewall section, uncheck **Protect my computer and network by limiting or preventing access to this computer from the Internet**.
- 5 Click **OK** to close the settings window.

## Starting and running the installation program

You install Symantec Client Firewall using the Symantec Client Firewall CD.

### To start the Symantec Client Firewall installation program

- 1 Insert the Symantec Client Firewall CD into your CD-ROM drive.
- 2 Click **Install Symantec Client Firewall**.



- 3 On the Welcome screen, click Next.



- 4 In the License Agreement window, click I accept the terms in the license agreement.  
If you decline, you cannot continue with the installation.
- 5 Click Next.



- 6 Select whether or not you want to run LiveUpdate after the installation is done.

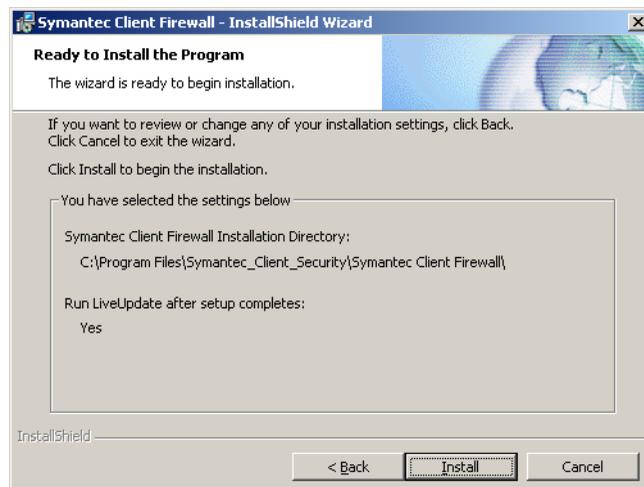
LiveUpdate keeps Symantec Client Firewall up to date with the latest program and protection updates.

- 7 Click Next.



- 8 Click **Change** to select a folder into which you want to install Symantec Client Firewall, if it is other than the default location.

- 9 Click Next.



- 10 Verify the options that you specified, then click **Install** to begin installing Symantec Client Firewall.
- 11 If you chose to run LiveUpdate after installation, follow the instructions in the LiveUpdate Wizard.
- 12 When LiveUpdate is done, click **Finish**.



- 13 Click **Finish**.  
A prompt appears telling you that you must restart your computer to complete the installation.
- 14 Click **Reboot Now** or **Cancel Reboot**.  
You must reboot before the computer is protected by Symantec Client Firewall.

## If you need to uninstall Symantec Client Firewall

If you need to uninstall Symantec Client Firewall from your computer, use the Add/Remove Programs feature in the Control Panel.

---

**Note:** During the uninstallation, Windows may indicate that it is installing software. This is a general Microsoft installer message and can be ignored.

---

## Uninstall Symantec Client Firewall components

You can uninstall Symantec Client Firewall and LiveUpdate.

### To uninstall Symantec Client Firewall

- 1 On the Windows taskbar, click **Start > Settings > Control Panel**.
- 2 In the Control Panel, double-click **Add/Remove Programs**.
- 3 In the list of currently installed programs, click **Symantec Client Firewall**.
- 4 Do one of the following:
  - In Windows XP/2000/Me, click **Change/Remove**.
  - In Windows 98/NT, click **Add/Remove**.
- 5 Click **Yes** to confirm that you want to uninstall the product.

If you have no other Symantec products on your computer, you should also uninstall LiveUpdate.

### To uninstall LiveUpdate

- 1 On the Windows taskbar, click **Start > Settings > Control Panel**.
- 2 In the Control Panel, double-click **Add/Remove Programs**.
- 3 In the list of currently installed programs, click **LiveUpdate**.
- 4 Do one of the following:
  - In Windows XP/2000/Me, click **Change/Remove**.
  - In Windows 98/NT, click **Add/Remove**.
- 5 Click **Yes** to confirm that you want to uninstall the product.

# Symantec Client Firewall basics

This chapter includes the following topics:

- [Accessing Symantec Client Firewall](#)
- [Working with Symantec Client Firewall](#)
- [Customizing Symantec Client Firewall](#)
- [Where to find troubleshooting information](#)

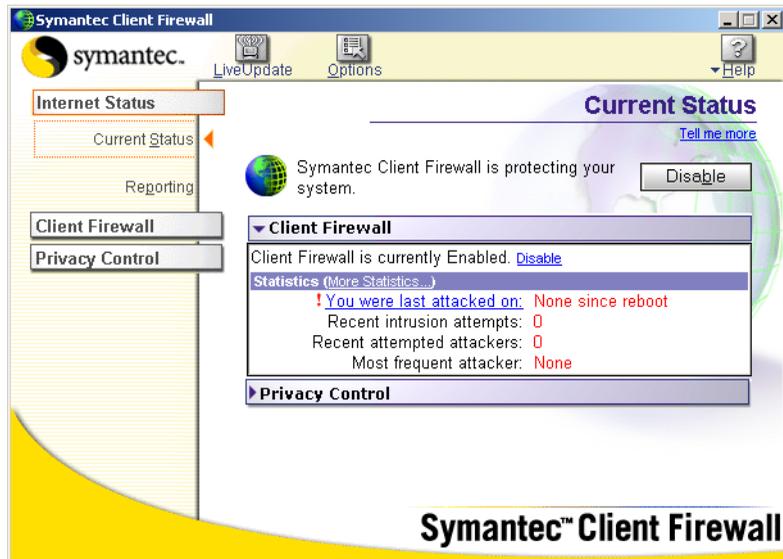
# Accessing Symantec Client Firewall

After installation, Symantec Client Firewall automatically protects any computer on which it is installed. You do not have to start the program to be protected.

Launch Symantec Client Firewall to change protection settings or monitor its activities.

## To access Symantec Client Firewall

- ◆ Do one of the following:
  - In the Windows System Tray, double-click the Symantec Client Firewall icon.
  - On the Windows taskbar, click **Start > Programs > Symantec Client Security > Symantec Client Firewall**.
  - On the Windows XP taskbar, click **Start > All Programs > Symantec Client Security > Symantec Client Firewall**.



# Working with Symantec Client Firewall

Symantec Client Firewall works in the background, so you may only interact with the program when it alerts you of new network connections and possible problems. You can control the number of alerts that you receive and how the program resolves potential security problems.

## Symantec Client Firewall user levels

Your user level determines which features you can use. User levels are defined by your system administrator.

The Admin user level type can perform all of the tasks listed in [Table 3-1](#). The capabilities of Normal and Restricted user types are also listed.

**Table 3-1** Symantec Client Firewall user access levels

Task	Normal user type	Restricted user type
Enable/Disable all components within Symantec Client Firewall protection, including the firewall, Intrusion Detection, and Privacy Control		
Enable/Disable Privacy Control	✓	
Enable/Disable Intrusion Detection		
Enable/Disable AutoBlocking		
Enable/Disable Automatic Internet Access Control and silent rule creation	✓	
Add and remove data for Confidential Information Blocking (CIB)	✓	
Add/modify/delete Admin rules		
Add/modify/delete User type rules	✓	
Modify Admin and User rule priorities		
Modify User rule priorities	✓	
Remove computers from the Currently Blocked by AutoBlock window		
Add computers from the Currently Blocked by AutoBlock to the Restricted Zone		

**Table 3-1** Symantec Client Firewall user access levels

Task	Normal user type	Restricted user type
Add/Remove computers to Restricted and Trusted Zones		
Exclude signatures from being monitored by Intrusion Detection		
Exclude IP addresses from being blocked by AutoBlock		
Run the Application Scan	✓	
Access Advanced Options		
Uninstall Symantec Client Firewall		
Modify Symantec Client Firewall settings		
Modify Privacy Control settings	✓	
Change Reporting Level	✓	
View Event Log	✓	
Modify Event Log		
View Statistics	✓	
Reset Statistics Values		
Clear Intrusion Detection status		
Run LiveUpdate	✓	✓
Access Help files	✓	✓
Access online tutorials and technical support Web site	✓	✓

## Connecting to a network

Every time that you use Windows file sharing to exchange files with someone in your office, print to a shared printer, or connect to the Internet using a modem, broadband, LAN, or VPN connection, your computer joins a network of other computers. When you are part of a network, your computer is vulnerable to attacks. Symantec Client Firewall automatically monitors all new network connections to ensure that your computer is safe.

Normally, your computer connects to a network because of an action that you take. Some wireless access cards automatically scan for and connect to any

network in range. If you travel with a laptop that is equipped with a wireless access card, you may discover that your computer joins wireless networks in airports and other public places.

Whenever you join a network, Symantec Client Firewall automatically begins monitoring the connection. You do not need to make any changes in order to be protected. Symantec Client Firewall notifies you of the new connection and logs it in its Event Log.

---

**Note:** Windows NT users are not alerted to new connections, but all network traffic is still protected.

---

## Responding to Symantec Client Firewall alerts

Symantec Client Firewall monitors communication activities to and from your computer. It lets you know when an activity that may compromise your security is taking place.



When an alert appears, read it before you make a decision. Identify what type of alert it is and the Threat Level. Once you understand the risks, you can make a choice.

Take as much time as you need to make your choice. Your computer is safe from attack while the alert is active.

Symantec Client Firewall shows the following types of alerts:

- Security Alerts
- Internet Access Control alerts
- Settings Alerts
- ActiveX Alerts
- Java Alerts
- Cookie Alerts
- Confidential Information Alerts

## Responding to Security Alerts

Security Alerts appear when someone attempts to access your computer. It may be a hacker or someone on your own network. Security Alerts can signal that your computer is being attacked or that a malicious user is attempting to bypass Symantec Client Firewall protection.

---

**Note:** Security alerts include alerts generated by Intrusion Detection.

---



When a Security Alert is activated, Symantec Client Firewall immediately blocks communication with the attacking computer. Security Alerts can also trigger AutoBlock, which blocks all communication from the attacking computer for 30 minutes—even if subsequent communication is benign. This prevents attackers from accessing your computer.

See [“Guarding against intrusion attempts”](#) on page 69.

Not every Security Alert represents an attempt to attack your computer. There are many harmless events that occur on the Internet that cause Security Alerts.

### To respond to a Security Alert

- 1 In the Security Alert window, review the description of the threat and the Threat Level.
- 2 For additional information about the threat, click **Details**.
- 3 Select one of the following:
  - Yes: Learn more about this type of threat.
  - No: Do not learn about this threat.
- 4 If you don't want to receive alerts about this threat, check **Don't create a Security Alert for this threat again**.
- 5 Click **OK** to close the alert.

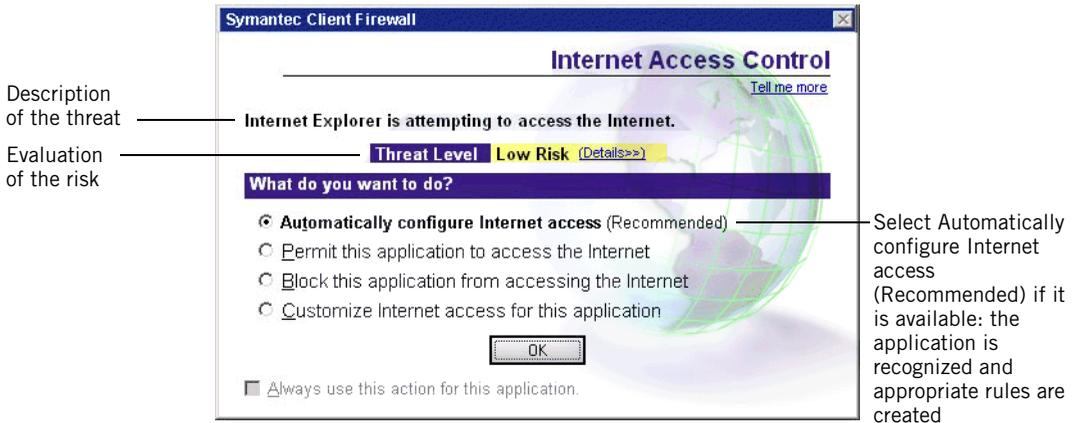
If you decide that Symantec Client Firewall is blocking a legitimate activity, make the appropriate changes to your firewall protection or reporting.

See [“Customizing firewall protection”](#) on page 74.

## Responding to Internet Access Control alerts

Internet Access Control alerts appear when Symantec Client Firewall identifies a program on your computer that is attempting to access the Internet. If you did not trigger the program or are not running the application with which the program is associated, this could be an indication that a Trojan horse or other

remote-control program is attempting to send information without your knowledge.



You can minimize the number of Internet Access Control alerts by performing an Application Scan, or by enabling Automatic Internet Access Control. When this option is enabled, Symantec Client Firewall creates rules for applications that it recognizes without interrupting your work.

See “[Scanning for Internet-enabled applications](#)” on page 81.

**To respond to an Internet Access Control alert**

- 1 In the Internet Access Control alert window, review the description of the threat and the Threat Level.
- 2 For additional information about the threat, click **Details**.
- 3 Select the action that you want to take.

Automatically configure Internet access (Recommended)	Symantec Client Firewall recognizes the application and has appropriate access rules in its database. This is almost always the best option.
Permit this application to access the Internet	Gives the program full access to the Internet. This is not as safe as Automatically configure Internet access, but it is appropriate for many applications that Symantec Client Firewall does not recognize.
Block this application from accessing the Internet	Blocks all Internet access for the application. This is the appropriate choice if you don't recognize the application and the risk is high.

Customize Internet access for this application Starts the Add Rule Wizard. Select this option if you understand how the application accesses the Internet and you want to create specific rules to control its access.

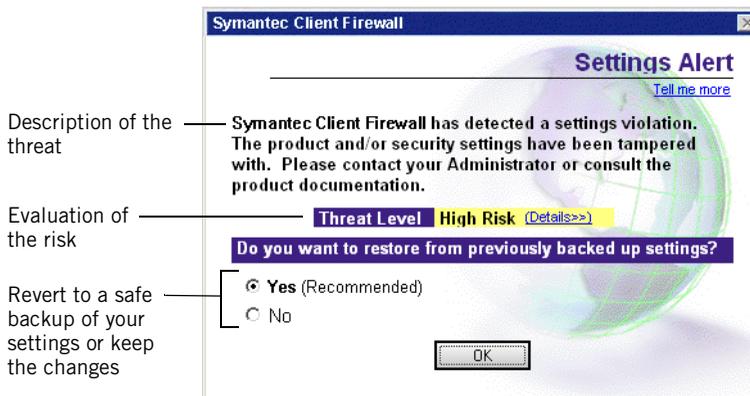
- 4 If you don't want to receive alerts about this threat, check **Always use this action for this application**.
- 5 Click **OK** to close the alert.

If you decide that Symantec Client Firewall is notifying you about a legitimate application, make the appropriate changes to your Internet Access Control settings.

## Responding to Settings Alerts

Settings Alerts appear when someone attempts to change Symantec Client Firewall settings by modifying the Windows Registry. Settings Alerts can indicate that an attacker is attempting to disable Symantec Client Firewall protection.

All Symantec Client Firewall settings are encrypted to prevent users from making changes using Registry editing tools. Encryption means that the information is encoded with a mathematical formula, scrambling the data into an unreadable format. Symantec Client Firewall also maintains a complete backup of its settings. If any settings are modified in, or deleted from, the Registry, you can revert to the backup.

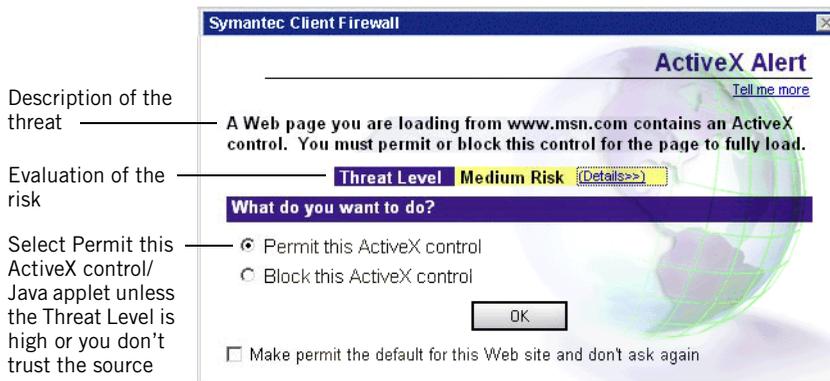


### To respond to a Settings Alert

- 1 In the Settings Alert window, review the description of the threat and the Threat Level.
- 2 For additional information about the threat, click **Details**.
- 3 Select one of the following:
  - **Yes (Recommended)**: Revert to a backup copy of Symantec Client Firewall settings.
  - **No**: Use the changed Registry settings.  
Be careful when choosing to use the changed settings. This may let an attacker damage your computer or view information on your hard disk. Even if the Settings Alert isn't part of an attack, manually changing Registry settings can cause your computer to behave unpredictably.
- 4 Click **OK** to close the alert.

### Responding to Java and ActiveX Alerts

Java applets and ActiveX controls are Web page components that do more than show text or graphics. Common applications of these components are pop-up menus and up-to-date stock quotes. Java applets and ActiveX controls can also be used by malicious sites to copy information from your computer or damage your operating system.



### To respond to a Java or ActiveX Alert

- 1 In the Java or ActiveX Alert window, review the description of the threat and the Threat Level.
- 2 For additional information about the threat, click **Details**.
- 3 Select one of the following:
  - **Permit this ActiveX control (or Java applet):** Let the ActiveX control or Java applet run. Only choose this option if you trust the Web site.
  - **Block this ActiveX control (or Java applet):** Prevent the ActiveX control or Java applet from running. While this is always the safer option, it might prevent the Web page from appearing or functioning correctly. If you select block, and the Web page does not appear or function correctly, click the **Refresh** button in your browser, then click **Permit this ActiveX control (or Java applet)**.
- 4 Click **OK** to close the alert.

Many reputable sites use ActiveX controls and Java applets as part of their navigation. If you receive a large number of alerts when visiting trusted sites, you can change the Java Applet and ActiveX Control Security Levels.

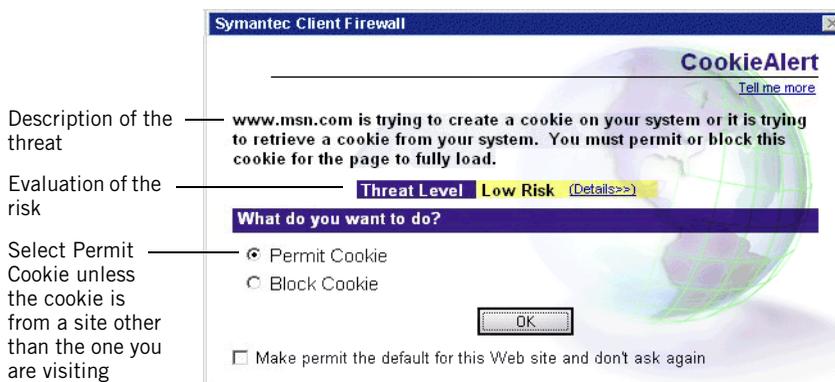
See [“Setting Java and ActiveX Security Levels”](#) on page 76.

### Responding to Cookie Alerts

Cookies are small files stored on your computer that Web sites use to track your visits. Because cookies are used so often and present a small security risk, you should not block all cookies. However, cookies can present significant risks to your privacy.

Cookie Alerts appear when you have the Privacy Level set to High or Cookie Blocking set to Medium. To block all cookies, and not see Cookie Alerts, change Cookie Blocking to High: Block Cookies. Expect repeated Cookie Alerts from pages on which you block cookies.

See “Changing the Cookie Blocking setting” on page 50.



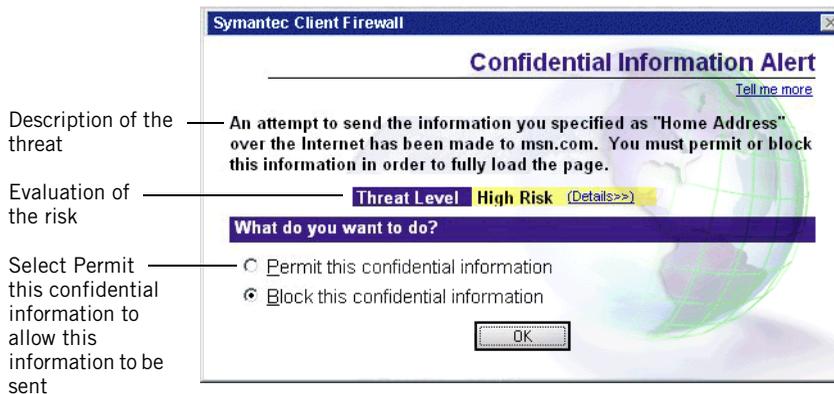
### To respond to a Cookie Alert

- 1 In the Cookie Alert window, review the description of the threat and the Threat Level.
- 2 For additional information about the threat, click **Details**.
- 3 Select one of the following:
  - **Permit Cookie:** Allow access to the cookie. Cookies from the Web site that you are visiting are usually harmless and may be necessary for the Web pages to function.
  - **Block Cookie:** Block access to the cookie. Cookies that are from Web sites other than the one that you are visiting are commonly used to track your Internet usage, and can usually be blocked without affecting the operation of the Web site that you are visiting.
- 4 Click **OK** to close the alert.

## Responding to Confidential Information Alerts

Confidential Information Alerts appear when you attempt to send protected information to a Web site that does not use secure, encrypted communications, or when you send protected information using an instant messenger program.

Symantec Client Firewall may recognize unimportant information as confidential information. For example, you might be entering an item number in which the last four digits match the last four digits of your credit card number. In this case, permit the attempt to send the information.



### To respond to a Confidential Information Alert

- 1 In the Confidential Information Alert window, review the description of the threat and the Threat Level.
- 2 For additional information about the threat, click **Details**.
- 3 Select one of the following:
  - **Permit this confidential information:** Send the information. If you select this option, a malicious user may be able to intercept this information.
  - **Block this confidential information:** Stop the attempt to send the information.
- 4 Click **OK** to close the alert.

## Adjusting the Reporting Level

The Reporting Level slider lets you control the amount of information that Symantec Client Firewall logs and the number of alerts that it displays.

### To adjust the Reporting Level

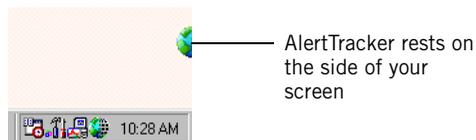
- 1 Open Symantec Client Firewall.
- 2 In the Symantec Client Firewall window, in the left pane, click **Internet Status > Reporting**.
- 3 Use the Reporting slider to set the Reporting Levels.

Minimal	Reports possible attacks, attempts to send confidential information, and potential Trojan horse activity
Medium	Reports all events in the Minimal category, plus attempts by applications to access the Internet
High	Reports all events in the Medium category, plus warnings about blocked ports, cookies, and interactive Web content

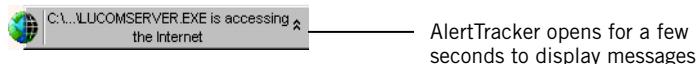
## Using AlertTracker

AlertTracker keeps you up to date on the actions that Symantec Client Firewall takes.

AlertTracker attaches to either side of the screen on your primary monitor. You can hide AlertTracker if you don't want it to appear on your screen.



Many of the Internet events that Symantec Client Firewall monitors are not significant enough to trigger alerts. When one of these small events occurs, AlertTracker displays a message for a few seconds and then returns to the side of the screen. If you miss an AlertTracker message, you can review a list of recent messages.



AlertTracker notifies you every time that your computer joins a network. If your computer is equipped with a wireless connectivity card, this is an easy way to tell when your computer has joined a public wireless network.

### Use AlertTracker

You can review recent AlertTracker messages. You can also move the location where AlertTracker appears on your screen. If you prefer, you can hide AlertTracker.

#### To review recent AlertTracker messages

- 1 On the Windows desktop, double-click AlertTracker.
- 2 To the right of the first message, click the Up Arrow if it appears.
- 3 Select a message to see the Symantec Client Firewall Event Log.  
See [“Reviewing the Symantec Client Firewall Event Log”](#) on page 60.

#### To move AlertTracker

- ◆ Drag the half globe to the side of the screen on which you want it to appear.

#### To hide AlertTracker

- ◆ In the Windows System Tray, right-click the Symantec Client Firewall icon, then click **Hide AlertTracker**.

If you hide AlertTracker, you will not be notified when your computer joins a network. Information about the connection will still appear in the Event Log.

## Customizing Symantec Client Firewall

The default settings for Symantec Client Firewall provide a safe, automatic, and efficient way of protecting your computer in a general corporate environment.

#### To customize Symantec Client Firewall

- 1 Open Symantec Client Firewall.
- 2 At the top of the Symantec Client Firewall window, click **Options**.
- 3 Select the tab on which you want to change options.

## About general options

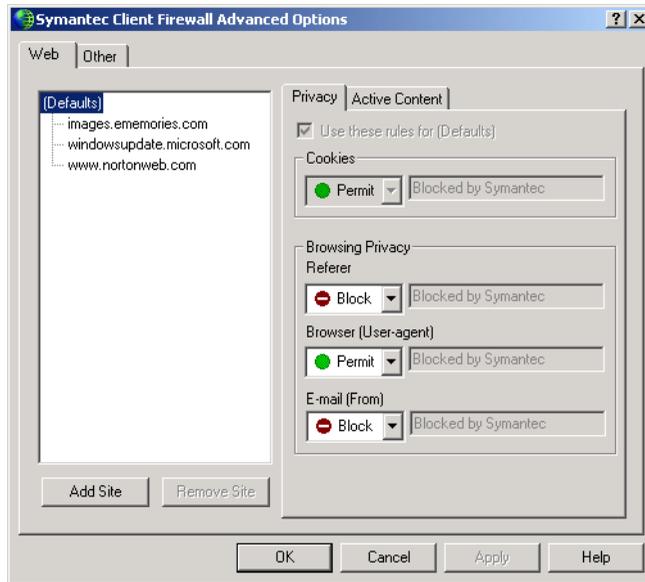
The general options listed in [Table 3-2](#) let you control visual elements of Symantec Client Firewall, view information about past actions that the program has taken to protect your computer, and set advanced options.

**Table 3-2** General options

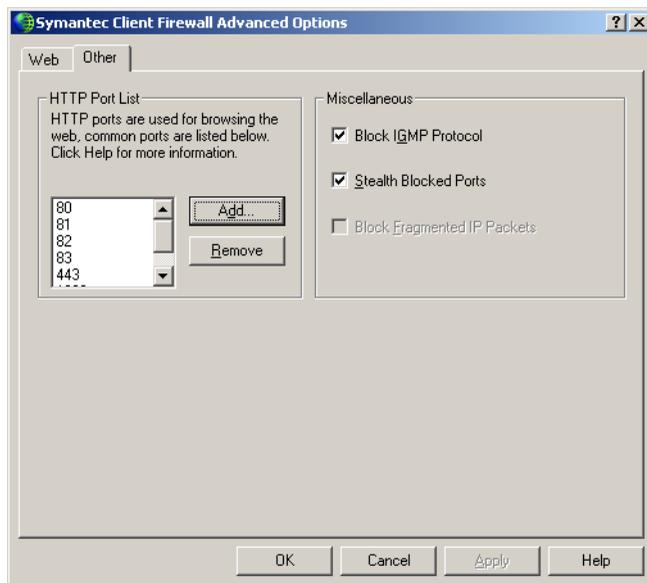
Option	Description
Show Taskbar Icon	Displays a Symantec Client Firewall icon on the Windows taskbar that gives you access to program settings.
Show the AlertTracker	Toggles the AlertTracker on and off.
Startup	Lets you select whether to run Symantec Client Firewall manually or automatically whenever Windows starts.
View Event Log	Displays a detailed list of recent Symantec Client Firewall activity.  See <a href="#">“Reviewing the Symantec Client Firewall Event Log”</a> on page 60.
View Statistics	Displays realtime network counters that track your Internet usage and any actions that Symantec Client Firewall takes.  See <a href="#">“Reviewing Internet access statistics”</a> on page 64.
Clear Status	Resets information displayed in the Current Status window.  See <a href="#">“Reviewing Current Status”</a> on page 59.
Advanced Options	Opens the Advanced Options window, where you can configure settings for individual Web sites and make changes to ports and monitoring behavior.

## About Advanced Options

The Advanced Options dialog box has two main tabs: Web and Other. The Web tab contains two panes. The left pane is a hierarchical list of Web sites for which you have defined site-specific settings. The right pane shows the Privacy and Active Content settings defined for the currently selected site.



The Other tab contains the HTTP port list and miscellaneous options.



## Understanding the list of Web sites

The list of Web sites is organized into a treelike structure that can be up to three levels deep. At the top of the site list is (Defaults). The (Defaults) item reflects the Privacy and Active Content settings that are applied to all sites.

The second-level entries are either domain names or site names. Domain names are high-level names that can contain several Web sites. For example, the domain `ajax.com` includes the site names `www.ajax.com` and `news.ajax.com`.

The third-level entries are specific site names within a domain listed on the second level. When you add a domain name to the site list, any sites within the domain are organized as third-level entries beneath the domain name. If you remove a domain, all of the site entries beneath that domain become second-level entries.

## Adding a site or domain to the list of sites

The sites listed in the Advanced Options dialog box on the Web tab are sites for which you have made site-specific settings. Before you make site-specific settings, add the site to the list.

**To add a site or domain to the list of sites**

- 1 Open Symantec Client Firewall.
  - 2 At the top of the Symantec Client Firewall window, click **Options > Advanced Options**.
  - 3 On the Web tab, in the left pane, click **Add Site**.
  - 4 Do one of the following:
    - To create settings that apply to a specific Web site, type the Web site name. For example, service.symantec.com.
    - To create settings that apply to all servers within a domain, type the domain name. For example, symantec.com.
- The new site or domain name is added to the site list on the Web tab in the left pane.
- 5 When you are done adding sites, click **OK**.

**Configuring site-specific settings**

You can configure site-specific settings for Privacy and Active Content (such as scripts, Java applets, ActiveX controls, and animated images).

**To configure site-specific settings**

- 1 Open Symantec Client Firewall.
- 2 At the top of the Symantec Client Firewall window, click **Options > Advanced Options**.
- 3 On the Web tab, in the left pane, select the site for which you want to configure settings.
- 4 In the right pane, select the option that you want to change.
- 5 Click **OK**.

## Removing a site or domain from the list of sites

When you remove a site or domain, the site-specific or domain-specific settings are deleted.

### To remove a site or domain from the list of sites

- 1 Open Symantec Client Firewall.
- 2 At the top of the Symantec Client Firewall window, click **Options > Advanced Options**.
- 3 On the Web tab, in the left pane, select the site name or domain name.
- 4 Click **Remove Site**.
- 5 In the confirmation dialog box, click **Yes**.

## Changing the HTTP port list

HTTP ports are the ports that your Web browser uses to download Web pages. The default port for HTTP is port 80, but there are several other ports commonly used for HTTP. The HTTP port list contains the most common port numbers by default. You can add or remove ports from this list, which specifies the ports to filter for Java and ActiveX blocking, script blocking, confidential information, and so on.

### To add or remove ports from the HTTP port list

- 1 Open Symantec Client Firewall.
- 2 At the top of the Symantec Client Firewall window, click **Options > Advanced Options**.
- 3 On the Other tab, select one of the following:
  - Add: Add ports.
  - Remove: Remove ports.
- 4 Click **OK**.

## Blocking IGMP

IGMP (Internet Group Membership Protocol) is used to establish memberships in multicast groups. Your computer reports to a nearby router that it wants to receive messages addressed to a specific multicast group.

IGMP does not present a major security risk, but Symantec Client Firewall lets you block the protocol entirely. This might be a good idea if you do not use any applications that require IGMP. If you have problems receiving multicast

information, such as movies or PowerPoint presentations, ensure that IGMP is not blocked.

#### **To block IGMP**

- 1 Open Symantec Client Firewall.
- 2 At the top of the Symantec Client Firewall window, click **Options > Advanced Options**.
- 3 On the Other tab, check **Block IGMP Protocol**.
- 4 Click **OK**.

### **Giving blocked ports a stealth appearance**

You can configure Symantec Client Firewall to not respond to scans of blocked ports. When this option is active, your computer is invisible to other computers on the Internet.

#### **To give blocked ports a stealth appearance**

- 1 Open Symantec Client Firewall.
- 2 At the top of the Symantec Client Firewall window, click **Options > Advanced Options**.
- 3 On the Other tab, check **Stealth Blocked Ports**.
- 4 Click **OK**.

### **Blocking fragmented IP packets**

Sometimes, IP packets are broken up into fragments as they are transmitted over the Internet. This can be a normal function of Internet communications, but it happens rarely. Fragmented IP packets can be used in attacks on computers.

On some operating systems, Symantec Client Firewall can block all fragmented IP packets to guard against your computer from being attacked by them:

- For computers running under Windows 9x/NT, this feature is available. By default, it is disabled but can be configured.
- For computers running under Windows 2000/XP, this feature is unavailable.

### To block fragmented IP packets

- 1 Open Symantec Client Firewall.
- 2 At the top of the Symantec Client Firewall window, click **Options > Internet Security > Advanced Options > Other**.
- 3 Check **Block Fragmented IP Packets**.
- 4 Click **OK**.

### Accessing Tray Menu options

Tray Menu options let you control the contents of the menu that appears when you right-click the Symantec Client Firewall taskbar icon. You can display or hide any of the following:

- Options
- Advanced Options
- View Event Log
- View Statistics

### To access Tray Menu options

- 1 Open Symantec Client Firewall.
- 2 At the top of the Symantec Client Firewall window, click **Options**.
- 3 Click **Tray Menu**.

## Keeping current with LiveUpdate

Symantec products depend on current information to protect your computer from newly discovered threats. Symantec makes this information available to you through LiveUpdate. Using your Internet connection, LiveUpdate downloads program updates and protection updates to your computer.

Use LiveUpdate options to enable Automatic LiveUpdate and define how updates should be applied.

### About program updates

Program updates are minor improvements to your installed product. These differ from product upgrades, which are newer versions of entire products.

LiveUpdate automates the process of downloading and installing program updates. It saves you the trouble of locating and downloading files from an Internet site, then installing them, and deleting the leftover files from your disk.

## Obtaining program and protection updates

Use LiveUpdate regularly to obtain protection updates. Program updates are released on an as-needed basis.

---

**Note:** If you connect to the Internet through America Online (AOL), CompuServe, or Prodigy, connect to the Internet first, and then run LiveUpdate.

---

### To obtain updates using LiveUpdate

- 1 Open Symantec Client Firewall.
- 2 At the top of the Symantec Client Firewall window, click **LiveUpdate**.
- 3 Click **Next** to locate updates.
- 4 If updates are available, click **Next** to download and install them.
- 5 When the installation is complete, click **Finish**.

## Where to find troubleshooting information

The Symantec Web site includes a troubleshooter, updates, patches, online tutorials, and knowledge base articles. Point your browser to [www.symantec.com/techsupp/](http://www.symantec.com/techsupp/)



# Protecting your privacy

This chapter includes the following topics:

- [About protecting your privacy](#)
- [Enabling or disabling Privacy Control](#)
- [Identifying confidential information to protect](#)
- [Customizing Privacy Control](#)

## About protecting your privacy

Every time that you browse the Internet, computers and Web sites collect information about you. Some of this information comes from forms that you fill out and choices that you make on pages. Other information comes from your browser, which automatically provides information about the Web page that you last visited and the type of computer that you're using.

Many Web sites store information they collect in cookies that are placed on your hard disk. When you return to a site that has set a cookie on your computer, the Web server opens and reads the cookie.

Most cookies are harmless. Sites use them to personalize Web pages, remember choices that you have made on the site, and deliver optimized pages for your computer. However, sites can also use cookies to track your Internet usage and browsing habits.

Malicious users can also collect personal information without your knowledge. Any time that you send information over the Internet, the data must pass through a number of computers before it reaches its destination. During transmission, it's possible for third parties to intercept and steal this information.

Computers include some basic security features, but they might not be enough to protect your personal information. Privacy Control helps protect your privacy by giving you several levels of control over cookies and limiting the information that your browser sends to Web sites.

Privacy Control can also ensure that you don't send private information, such as credit card numbers, over the Internet unless it is encrypted, or you specifically allow it.

## Enabling or disabling Privacy Control

Some Web-based services may need to access browser information that Privacy Control automatically blocks. You can disable Privacy Control to let Web sites gather information from your browser.

### To enable or disable Privacy Control

- 1 Open Symantec Client Firewall.
- 2 In the Symantec Client Firewall window, in the left pane, click **Privacy Control**.
- 3 Check or uncheck **Enable Privacy**.

# Identifying confidential information to protect

Many Web sites ask for your name, email address, and other personal information. While it is generally safe to provide this information to large, reputable sites, malicious sites can use this information to invade your privacy. It is also possible for people to intercept information sent via the Web, email, and instant messenger programs.

Privacy Control lets you create a list of information that you want to remain private. If you attempt to send protected information over the Internet, Symantec Client Firewall can warn you about the security risk or block the connection.

## Tips on entering confidential information

Because Symantec Client Firewall blocks personal information exactly the way that you enter it into the program, it is better to enter only partial numbers. For example, a phone number could be typed as 888-555-1234, but it could also be typed without dashes (8885551234) or with spaces (888 555 1234), or even in two or more separate fields. One common aspect of these formats is that the last four digits (1234) are always together. Therefore, you can have better protection by protecting the last four digits than you have by protecting the entire number.

Entering partial information has two advantages. First, you are not entering a complete number where someone might find it. Second, it lets Symantec Client Firewall block your private information on sites that use multiple text boxes for phone or credit card numbers.

## Adding confidential information

You must add information that you want to protect to the Symantec Client Firewall Confidential Information list.

### To add confidential information

- 1 Open Symantec Client Firewall.
- 2 In the Symantec Client Firewall window, in the left pane, click **Privacy Control**.
- 3 Click **Confidential Info**.
- 4 In the Confidential Information dialog box, click **Add**.
- 5 In the Add Confidential Information dialog box, under Type Of Information To Protect, select a category.

- 6 In the Descriptive Name text box, type a description to help you remember why you are protecting the data.
- 7 In the Information To Protect text box, type the information that you want to block from being sent over nonsecure Internet connections.
- 8 Click OK.

## Modifying or removing confidential information

You can modify or remove confidential information at any time.

### To modify or remove confidential information

- 1 Open Symantec Client Firewall.
- 2 In the Symantec Client Firewall window, in the left pane, click **Privacy Control**.
- 3 Click **Confidential Info**.
- 4 Select the confidential information that you want to change or remove.
- 5 Select one of the following:
  - Modify
  - Remove
- 6 Click OK.

## Customizing Privacy Control

Privacy Control protects four areas listed in [Table 4-1](#).

**Table 4-1** Privacy Control protection areas

Protection	Description
Confidential Information	Blocks specific strings of text that you do not want sent over the Internet
Cookie Blocking	Stops Web sites from retrieving personal information stored in cookie files
Browser Privacy	Protects information about your browsing habits
Secure Connections	Prevents you from establishing secure connections to online stores and other Web sites

There are two ways to adjust Privacy Control settings:

- Set the Privacy Level: Use the slider in the main Privacy Control pane to select preset security levels.
- Adjust individual Privacy Control settings: Customize your protection by manually adjusting individual settings.

## Setting the Privacy Level

Symantec Client Firewall offers preset security levels that help you set several Privacy Control options at one time. The Privacy Level slider lets you select minimal, medium, or high protection.

### To set the Privacy Level

- 1 Open Symantec Client Firewall.
- 2 In the Symantec Client Firewall window, in the left pane, click **Privacy Control**.
- 3 Move the **Privacy Level** slider to the Privacy Level that you want.

High	Blocks all personal information and displays an alert each time that a cookie is encountered.
Medium (recommended)	Displays an alert if confidential information is typed into a Web form or instant messenger program. Conceals your browsing from Web sites. Does not block cookies.
Minimal	Does not block confidential information or cookies, but conceals your browsing from Web sites.

## Adjusting individual Privacy Control settings

You can change the settings for Confidential Information, Cookie Blocking, Browser Privacy, and Secure Connections if the Privacy Level settings do not meet your needs.

---

**Note:** When you customize settings, the Privacy Level sliders disappear. To make the Privacy Level sliders reappear, click Default Level.

---

## Changing the Confidential Information setting

Change the Confidential Information setting to control how Symantec Client Firewall handles attempts to send information on the Confidential Information list over the Internet.

### To change the Confidential Information setting

- 1 Open Symantec Client Firewall.
- 2 In the Symantec Client Firewall window, in the left pane, click **Privacy Control**.
- 3 Click **Custom Level**.
- 4 Select the Confidential Information setting that you want.

High	Blocks all confidential information
Medium	Alerts you each time that you attempt to send confidential information to a nonsecure Web site or through an instant messenger program
None	Does not block confidential information

- 5 Click **OK**.

## Changing the Cookie Blocking setting

Change the Cookie Blocking setting to control how Symantec Client Firewall handles sites that attempt to place cookies on your computer.

---

**Note:** Two types of cookies exist, persistent and nonpersistent. Symantec Client Firewall treats both types the same way.

---

**To change the Cookie Blocking setting**

- 1 Open Symantec Client Firewall.
- 2 In the Symantec Client Firewall window, in the left pane, click **Privacy Control**.
- 3 Click **Custom Level**.
- 4 Select the Cookie Blocking setting that you want.

High	Blocks all cookies
Medium	Alerts you each time that a cookie is encountered
None	Allows cookies

- 5 Click OK.

**Enabling or disabling Browser Privacy**

Browser Privacy prevents Web sites from learning the type of browser that you are using, the Web site that you last visited, and other information about your browsing habits. Some Web sites that depend on Java Script may not work correctly if they cannot identify the type of browser that you are using.

**To enable or disable Browser Privacy**

- 1 Open Symantec Client Firewall.
- 2 In the Symantec Client Firewall window, in the left pane, click **Privacy Control**.
- 3 Click **Custom Level**.
- 4 In the Customize Privacy Settings dialog box, check or uncheck **Enable Browser Privacy**.
- 5 Click OK.

## Disabling or enabling secure Web connections

When you visit a secure Web site, your browser sets up an encrypted connection with the Web site. By default, Symantec Client Firewall lets any account use secure connections. If you want to ensure that you are not sending confidential information to secure Web sites, you can disable secure Web connections.

---

**Note:** If you disable secure Web connections, your browser will not encrypt any information that it sends. You should only disable secure Web connections if you are using the Confidential Information filter.

---

### To disable or enable secure Web connections

- 1 Open Symantec Client Firewall.
- 2 In the Symantec Client Firewall window, in the left pane, click **Privacy Control**.
- 3 Click **Custom Level**.
- 4 In the Customize Privacy Settings dialog box, check or uncheck **Enable Secure Connections (https)**.
- 5 Click **OK**.

# Controlling access to protected computers

This chapter includes the following topics:

- [About controlling access](#)
- [Organizing computers into network zones](#)
- [Enabling file and printer sharing](#)

## About controlling access

Symantec Client Firewall monitors all connections, including those made among computers in your office. After installation, you may need to adjust some settings to share files, printers, and other resources with other computers in your office.

## Organizing computers into network zones

Symantec Client Firewall lets you organize computers on your local network and the Internet into two zones: Trusted and Restricted.

Computers that you place in the Trusted zone are not regulated by Symantec Client Firewall. They have as much access to your computer as they would have if Symantec Client Firewall was not installed. Only use the Trusted zone for computers on your local network with which you need to share files and printers. If a computer in your Trusted zone is attacked, and an attacker takes control of it, it poses a risk to your computer and all other computers in your Trusted zone.

Computers that you place in the Restricted zone are prevented from accessing your computer at all. If a computer is in the Restricted zone, all communication between it and any computers that you have protected with Symantec Client Firewall is automatically blocked.

In most cases, you will want to add all of the computers in your office to your Trusted zone. Only add external computers to your Trusted zone if you know that their users can be trusted and they have firewall software installed.

## Enabling file and printer sharing

Microsoft networking provides file and printer sharing. By default, Symantec Client Firewall prevents any computers from accessing these services on a protected computer.

To share files and give access to printers on your local network, you can enable file and printer sharing. If you enable these features on your local network, they are still protected from malicious users on the Internet.

---

**Note:** Before enabling file and printer sharing on your local network, ensure that each shared resource is protected by a secure password.

---

**To enable file and printer sharing**

- 1** Open Symantec Client Firewall.
- 2** In the Symantec Client Firewall window, in the left pane, click **Client Firewall > Internet Access Control**.
- 3** Click **Configure > System-Wide Settings**.
- 4** In the System-Wide Settings dialog box, select the entry for Windows file sharing or printer sharing.
- 5** Click **Modify**.
- 6** In the Modify Rule dialog box, on the Action tab, click **Permit Internet access**.
- 7** Click **OK**.
- 8** In the System-Wide Settings dialog box, click **OK**.



# Monitoring Symantec Client Firewall

This chapter includes the following topics:

- [About monitoring Symantec Client Firewall](#)
- [Reviewing Current Status](#)
- [Reviewing the Symantec Client Firewall Event Log](#)
- [Reviewing Internet access statistics](#)
- [Printing or saving logs and statistics](#)

## About monitoring Symantec Client Firewall

Symantec Client Firewall maintains records of every incoming and outgoing Internet connection and any actions that the program takes to protect your computer. You should periodically review this information to spot potential security violations.

There are three sources of Symantec Client Firewall information:

- Current Status window: Recent Web- and firewall-related activities
- Symantec Client Firewall Event Log: Users' Internet activities and any actions Symantec Client Firewall has taken
- Statistics window: Statistics of network activity and actions that Symantec Client Firewall has taken

When reviewing logged information, check for:

- Recent attacks in the Current Status window
- Many denied access attempts, especially from a single IP address
- Sequences of port numbers from the same IP address, possibly indicating a port scan (attackers trying many ports on your computer, looking for one that they can access)
- Excessive network activity by unknown programs

It is normal to see some denied access attempts on a random basis (not all from the same IP address, and not to a sequence of port numbers). You may also see logged access attempts made due to activity on your own computer such as connecting to an FTP server and sending email.

If you see any of the above patterns, it could be evidence of an attack.

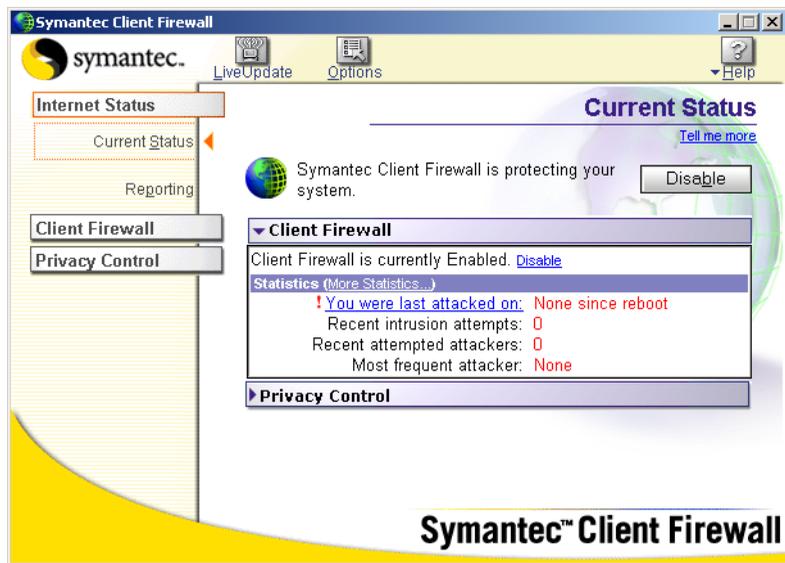
See [“Guarding against intrusion attempts”](#) on page 69.

## Reviewing Current Status

The Current Status window provides a snapshot of your computer's network activity since the last time you started Windows. Use this information to identify ongoing attack attempts and review how your Privacy Control settings affect your protection.

### To review Current Status

- 1 Open Symantec Client Firewall.
- 2 In the Symantec Client Firewall window, in the left pane, click **Internet Status > Current Status**.



- 3 In the middle of the Current Status window, select the category that you want to review.

Client Firewall	Displays any recent attacks on this computer, including the time of the most recent attack and the IP address of the attacking computer
Privacy Control	Displays the number of cookies that have been blocked, and the number of times confidential information has been blocked

## Reviewing the Symantec Client Firewall Event Log

The Symantec Client Firewall Event Log contains information about Web sites that you have visited, actions that the firewall has taken, and any alerts that have been triggered. This Event Log includes details about some of the activity reported in the Current Status window.

The Symantec Client Firewall Event Log is organized onto the eight tabs listed in [Table 6-1](#).

**Table 6-1** Symantec Client Firewall Event Log tabs

Tab	Information
Content Blocking	Details about Java applets and ActiveX controls blocked by Symantec Client Firewall.
Connections	A history of all TCP/IP network connections made with this computer. Connections are logged when the connection is closed.
Firewall	Communication intercepted by the firewall, including rules that were processed, alerts displayed, unused ports blocked, and AutoBlock events.
Intrusion Detection	Whether Intrusion Detection is active, the attack signatures being monitored, and the number of intrusions that occurred and were blocked.
Privacy	The cookies that have been blocked, including the name of the cookie and the Web site that requested the cookie. The information listed is dependent on the cookie settings.
System	When Symantec Client Firewall has been enabled or disabled, connection activity, and when rules, pRules settings, and Intrusion Detection settings have been updated by an administrator.
Web History	URLs visited by the computer, providing a history of Web activity.
Alerts	All alert activity, including normal Internet Access Control alerts and security alerts triggered by possible attacks on the Symantec Client Firewall client computer.

## About Symantec Client Firewall Event Log entries

Standard Event Log information includes:

- **Date:** The date of the event.
- **Time:** The time of the event. The most recent event is listed first.
- **Message:** The event that was logged. This appears on the Content Blocking, Firewall, Privacy, System, and Alerts tabs.

## Viewing the Symantec Client Firewall Event Log

You can view the Event Log in any Symantec Client Firewall window.

### To view the Symantec Client Firewall Event Log

- 1 Open Symantec Client Firewall.
- 2 At the top of the Symantec Client Firewall window, click **Options**.
- 3 Click **View Event Log**.
- 4 In the Event Log dialog box, select the tab that you want to review.
- 5 Click **OK** to close the Event Log.

## Filtering events in the Symantec Client Firewall Event Log

You can filter events to select the types of System events that are displayed. The options include Error, Warning, Information, Alert, and System events.

### To filter events in the Event Log

- 1 Open Symantec Client Firewall.
- 2 At the top of the Symantec Client Firewall window, click **Options**.
- 3 Click **View Event Log**.
- 4 On the System tab, check each event type that you want to include in the display.
- 5 Click **OK** to close the Event Log.

## Refreshing the Symantec Client Firewall Event Log

The Event Log automatically refreshes when you move from tab to tab. To view network events occurring since you began viewing the Event Log, manually refresh it.

### To refresh the Event Log

- ◆ In the Event Log window, click **Refresh**.

## Clearing the Symantec Client Firewall Event Log

If you actively use the Internet, or if other computers frequently connect to your computer, the Event Log may include information about hundreds of connections. This can make it difficult to identify intruder activity or assess the impact of any changes that you make to Symantec Client Firewall settings.

Clear Event Log tabs to remove logged information. This lets you see how settings changes affect your protection. You can clear a single Event Log tab or clear the entire Event Log at once.

### Clear events

You can clear events on a single Event Log tab or for the entire Event Log. You can also have Symantec Client Firewall clear the Event Log every time that the computer starts.

#### To clear events on a single Event Log tab

- 1 Open Symantec Client Firewall.
- 2 At the top of the Symantec Client Firewall window, click **Options**.
- 3 Click **View Event Log**.
- 4 On the tab that you want to clear, on the Log menu, click **Clear Tab**.

#### To clear the entire Event Log

- 1 Open Symantec Client Firewall.
- 2 At the top of the Symantec Client Firewall window, click **Options**.
- 3 Click **View Event Log**.
- 4 On the Log menu, click **Clear All Tabs**.

**To automatically clear the Event Log when the computer starts**

- 1 Open Symantec Client Firewall
- 2 At the top of the Symantec Client Firewall window, click **Options**.
- 3 Click **View Event Log**.
- 4 On the Log menu, click **Clear All Tabs Upon Logoff**.  
This automatically clears the contents of every Event Log file each time that the computer restarts. If **Clear All Tabs Upon Logoff** is already clicked, you do not need to do anything.

## Changing the size of the Symantec Client Firewall Event Log

The Event Log stores the information for each tab in a separate file. You can change the size of Event Log files to manage the amount of hard disk space that they occupy. When the files reach their maximum size, new events overwrite the oldest events.

By default, Symantec Client Firewall Event Log files are 128 KB. If you want to see information spanning a longer period, increase the size of the log. If you need to recover hard disk space, reduce the size. Changing the size of a log file clears all of the information in that log.

**To change the size of the Event Log**

- 1 Open Symantec Client Firewall.
- 2 At the top of the Symantec Client Firewall window, click **Options**.
- 3 Click **View Event Log**.
- 4 On the tab displaying the log that you want to configure, on the Log menu, click **Change Log File Size**.
- 5 Select a file size.
- 6 Click **OK**.

When you are finished changing the log file sizes, you must restart your computer for the changes to take effect.

## Adjusting the width of a column

You can change the width of the columns in the Symantec Client Firewall Event Log.

### To adjust the width of a column in the Event Log

- 1 Open Symantec Client Firewall.
- 2 At the top of the Symantec Client Firewall window, click **Options**.
- 3 Click **View Event Log**.
- 4 On the tab that you want to view, point to the boundary line on the right side of the column heading.  
The cursor changes from a pointer to a cross-hair.
- 5 Drag the boundary line to the desired width.

## Reviewing Internet access statistics

The Symantec Client Firewall Statistics window contains realtime network counters that track your Internet usage and any actions that Symantec Client Firewall takes.

Symantec Client Firewall includes information on the statistics listed in [Table 6-2](#).

**Table 6-2** Symantec Client Firewall statistics

Statistic	Details
Network	TCP and UDP bytes sent and received, the number of open network connections, and the highest number of simultaneous open network connections since the program started
Web	Graphics, cookies, and requests for browser information that have been blocked, the number of bytes and packets that have been processed, and the number of HTTP connections
Firewall TCP Connections	The number of blocked and permitted TCP connections
Firewall UDP Datagrams	The number of blocked and permitted UDP connections
Firewall Rules	The number of communication attempts blocked, permitted, or not matched by firewall rules

**Table 6-2** Symantec Client Firewall statistics

Statistic	Details
Network Connections	Information about current connections, including the application that is using the connection, the protocol being used, and the addresses or names of the connected computers
Last 60 Seconds	The number of network and HTTP connections and the speed of each connection type

**To review Internet access statistics**

- 1 Open Symantec Client Firewall.
- 2 At the top of the Symantec Client Firewall window, click **Options**.
- 3 Click **View Statistics**.

## Resetting counters

Reset the counters to clear all of the statistics and begin accumulating them again. This helps you see if a configuration change affects the statistics.

**To reset counters**

- 1 Open Symantec Client Firewall.
- 2 At the top of the Symantec Client Firewall window, click **Options**.
- 3 Click **View Statistics**.
- 4 On the View menu, click **Reset Values**.

## Setting the statistics that display in the Statistics window

You can view all Symantec Client Firewall statistics at once or display only certain categories.

**To set the statistics that display in the Statistics window**

- 1 Open Symantec Client Firewall.
- 2 At the top of the Symantec Client Firewall window, click **Options**.
- 3 Click **View Statistics**.
- 4 On the View menu, click **Options**.

- 5 In the Symantec Client Firewall Statistics Options window, select one or more categories of statistics that you want to display.
- 6 Click OK.

## Configuring Statistics window columns

The Statistics window can display information in one or two columns. Both window layouts contain the same statistics.

### To configure Statistics window columns

- 1 Open Symantec Client Firewall.
- 2 At the top of the Symantec Client Firewall window, click **Options**.
- 3 Click **View Statistics**.
- 4 Do one of the following:
  - To automatically adjust between a one and two column display, based on the current window width, on the View menu, click **Columns > Automatic**.
  - To always display a single column, on the View menu, click **Columns > One**.
  - To always display two columns, on the View menu, click **Columns > Two**.

## Keeping the Statistics window visible

You can keep the Statistics window visible, even when an application runs in a full-screen window. This can be useful for spotting unusual network activity that may indicate a problem.

### To keep the Statistics window visible

- 1 Open Symantec Client Firewall.
- 2 At the top of the Symantec Client Firewall window, click **Options**.
- 3 Click **View Statistics**.
- 4 On the View menu, click **Always On Top**.

# Printing or saving logs and statistics

As you access the Internet, older information in the Symantec Client Firewall Event Log and access statistics is overwritten with newer data. To preserve older Internet usage information, or to include this information in word-processing or other documents, print or export the Event Log and statistics.

## Print or save logs and statistics

You can print or save logs and statistics.

### To print log information

- 1 Open Symantec Client Firewall.
- 2 At the top of the Symantec Client Firewall window, click **Options**.
- 3 Click **View Event Log**.
- 4 On the tab containing the information that you want to print, on the Log menu, click **Print Tab**.
- 5 Repeat step 4 to print another tab.
- 6 Click **OK** when you have finished printing.

### To print statistics information in a text file

- 1 Open Symantec Client Firewall.
- 2 At the top of the Symantec Client Firewall window, click **Options**.
- 3 Click **View Statistics**.
- 4 On the File menu, click **Print**.
- 5 In the Print window, click **Print**.

### To save log information in a text file

- 1 Open Symantec Client Firewall.
- 2 At the top of the Symantec Client Firewall window, click **Options**.
- 3 Click **View Event Log**.
- 4 On the tab containing the information that you want to save, on the Log menu, click **Save Tab As**.

- 5 Specify a location and name for the text file.
- 6 Click **Save**.
- 7 To save information on another tab, repeat steps 4-6.

**To save statistics to a text file**

- 1 Open Symantec Client Firewall.
- 2 At the top of the Symantec Client Firewall window, click **Options**.
- 3 Click **View Statistics**.
- 4 On the File menu, click **Save**.
- 5 Specify a location and name for the text file.
- 6 Click **Save**.

# Guarding against intrusion attempts

This chapter includes the following topics:

- [About guarding against intrusion attempts](#)
- [How Symantec Client Firewall protects against network attacks](#)
- [Ensuring that Symantec Client Firewall and Intrusion Detection are enabled](#)
- [Customizing firewall protection](#)
- [Customizing firewall rules](#)
- [Customizing Intrusion Detection](#)

## About guarding against intrusion attempts

Network attacks take advantage of the way that computers transfer information. Symantec Client Firewall can protect your computer by monitoring the information that comes into and out of your computer and blocking any attack attempts.

Information travels across the Internet in the form of *packets* (small bundles of data). Along with the data, each packet includes a header that contains information about the sending computer, the intended recipient, how the data in the packet should be processed, and the port that should receive the packet.

Ports are channels that divide the stream of information coming from the Internet into separate paths that are handled by individual applications. When Internet applications run on a computer, they listen to one or more ports and accept information sent to these ports.

Network attacks are designed to take advantage of weaknesses in specific Internet applications. Attackers use tools that send packets containing malicious programming code to a particular port. If an application that is vulnerable to this attack is listening to that port, the code can let the attacker gain access to, disable, or even take control of the computer. The programming code that is used to generate the attacks may be contained inside of a single packet or span several packets.

## How Symantec Client Firewall protects against network attacks

Symantec Client Firewall protects your computer from intrusion attempts, malicious Web content, and *Trojan horses* (malicious programming hidden inside otherwise safe-looking applications). Symantec Client Firewall creates a shield that blocks or limits attempts to view information on your computer. It also monitors all incoming and outgoing information for data patterns typical of an attack.

## Monitoring communications with Symantec Client Firewall

Symantec Client Firewall monitors communications between your computer and other computers on the Internet. It also protects your computer against common security problems such as those listed in [Table 7-1](#).

**Table 7-1** Common security problems

Problem	Protection
Improper connection attempts	Warns you of any connection attempts from other computers and attempts by applications on your computer to connect to other computers
Trojan horses	Maintains a list of common Trojan horses
Security and privacy incursions by malicious Web content	Monitors all Java applets and ActiveX controls and lets you choose whether to run or block the application
Port scans	Cloaks inactive ports on your computer and detects port scans
Intrusions	Detects and blocks malicious traffic and attempts by outside users to attack your computer

You can control the level of protection by using the Security Level slider. You can also control how Symantec Client Firewall reacts to improper connection attempts, Trojan horses, and malicious Web content.

See “[Customizing firewall protection](#)” on page 74.

## Analyzing communications with Intrusion Detection

Intrusion Detection scans each packet that enters and exits your computer for *attack signatures* (arrangements of information that identify an attacker’s attempt to exploit a known operating system or application vulnerability).

[Table 7-2](#) lists the attacks that Symantec Client Firewall monitors.

**Table 7-2** Monitored attacks

Attack	Description
Bonk	An attack on the Microsoft TCP/IP stack that can crash the attacked computer

**Table 7-2** Monitored attacks

Attack	Description
RDS_Shell	A method of exploiting the Remote Data Services component of the Microsoft Data Access Components that lets a remote attacker run commands with system privileges
WinNuke	An exploit that can use NetBIOS to crash older Windows 95/98/NT computers

Because attacks may span packets, Intrusion Detection examines packets in two different ways. It scans each packet individually looking for patterns that are typical of an attack. It also monitors the packets as a stream of information, which lets it identify attacks spread across multiple packets.

If the information matches a known attack, Intrusion Detection automatically discards the packet and severs the connection with the computer that sent the data. This protects your computer from being affected in any way.

You can modify how Intrusion Detection responds to attacks by excluding attack signatures from being monitored and by enabling or disabling AutoBlock, which automatically blocks all communication from an attacking computer. By excluding certain network behavior from blocking, you can continue to be productive, even while your computer is under attack.

Along with protecting your computer against attacks, Symantec Client Firewall also monitors all of the information that your computer sends to other computers. This ensures that your computer cannot be used to attack other users or be exploited by zombie programs. *Zombies* are programs that can be secretly installed and run remotely to aid in a collective attack on another computer. If Symantec Client Firewall detects that your computer is sending information that is typical of an attack, it immediately blocks the connection and warns you about the possible problem.

To reduce the number of warnings that you receive, Symantec Client Firewall only monitors attacks that are targeted at ports that your computer uses. If an attacker attempts to connect to your computer via an inactive port or a port that has been blocked by the firewall, Symantec Client Firewall will not notify you because there is no risk of an intrusion.

Symantec Client Firewall does not scan for intrusions by computers in your Trusted zone. However, Intrusion Detection does monitor the information that you send to Trusted computers for signs of zombies and other remote control attacks.

Intrusion Detection relies on an extensive list of attack signatures to detect and block suspicious network activity. Run LiveUpdate regularly to ensure that your list of attack signatures is up to date.

See “Keeping current with LiveUpdate” on page 42.

## Ensuring that Symantec Client Firewall and Intrusion Detection are enabled

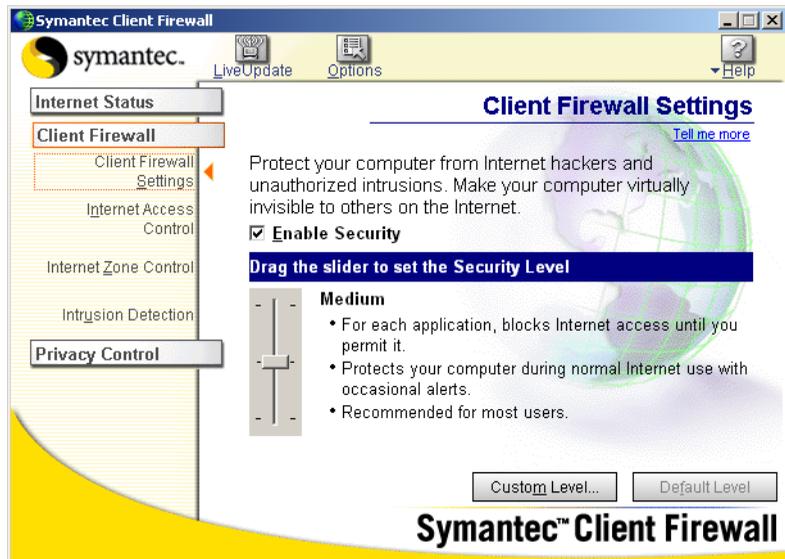
The firewall and Intrusion Detection are automatically enabled when you install Symantec Client Firewall. It is unlikely that you need to change any settings. However, you can ensure that the firewall and Intrusion Detection are working by following these steps.

### Ensure that Symantec Client Firewall and Intrusion Detection are enabled

You can enable or disable Symantec Client Firewall and Intrusion Detection.

#### To ensure that the firewall is enabled

- 1 Open Symantec Client Firewall.



- 2 In the Symantec Client Firewall window, in the left pane, click **Client Firewall > Client Firewall Settings**.
- 3 Check **Enable Security** to activate the firewall.

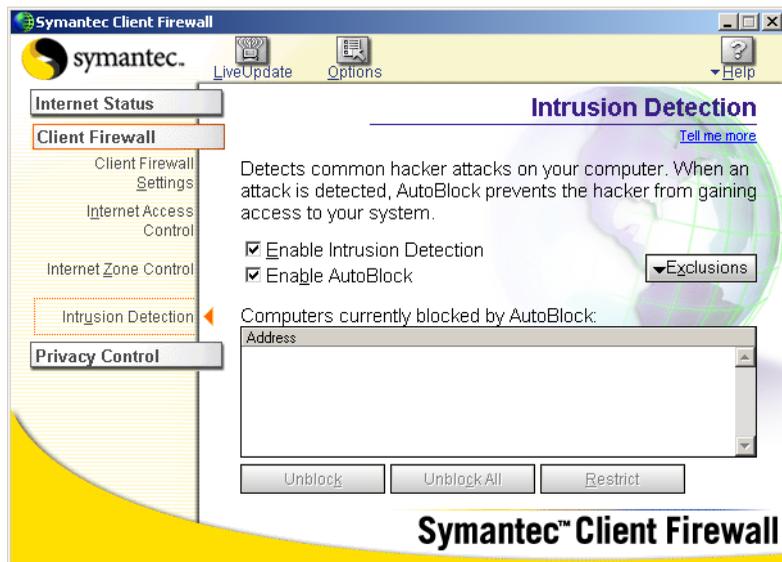
---

**Note:** Disabling the firewall also disables Intrusion Detection.

---

**To ensure that Intrusion Detection is enabled**

- 1 Open Symantec Client Firewall.



- 2 In the Symantec Client Firewall window, in the left pane, click **Client Firewall > Intrusion Detection**.
- 3 Check **Enable Intrusion Detection** to activate Intrusion Detection.

## Customizing firewall protection

The default firewall settings should provide you with adequate protection. If the default protection is not appropriate, you can customize the firewall using the Security Level slider. The slider lets you select preset groups of security settings. You can also customize the firewall by changing individual security settings.

## Changing the Security Level slider

The Security Level slider lets you select Minimal, Medium, or High security settings. When you change the slider position, the protection level changes. Changing the Security Level slider does not affect the protection provided by Intrusion Detection.

### To change the Security Level slider

- 1 Open Symantec Client Firewall.
- 2 In the Symantec Client Firewall window, in the left pane, click **Client Firewall > Client Firewall Settings**.
- 3 Move the slider to the Security Level that you want.

High	<p>The firewall blocks everything until you allow it. If you have done an Application Scan, you should not be interrupted frequently with Internet Access Control alerts.</p> <p>See <a href="#">“Scanning for Internet-enabled applications”</a> on page 81.</p> <p>You are alerted each time that an ActiveX control or Java applet is encountered. Unused ports do not respond to connection attempts, giving them a stealth appearance.</p>
Medium (recommended)	<p>The firewall blocks everything until you allow it. If you have done an Application Scan, you should not be interrupted frequently with Internet Access Control alerts.</p> <p>ActiveX controls and Java applets run without warning. Unused ports do not respond to connection attempts, giving them a stealth appearance.</p>
Minimal	<p>The firewall blocks connection attempts by Trojan horse programs. ActiveX controls and Java applets run without warning.</p>

## Changing individual security settings

If the Security Level options do not meet your needs, you can change the settings for the firewall, Java, and ActiveX protection levels. Changing an individual setting overrides the Security Level, but it does not affect the other security settings.

---

**Note:** When you customize settings, the Security Level sliders disappear. To make the Security Level sliders reappear, click Default Level.

---

## Changing firewall settings

Symantec Client Firewall monitors connections between your computer and computers on the Internet and blocks any potentially hazardous connections.

### To change firewall settings

- 1 Open Symantec Client Firewall.
- 2 In the Symantec Client Firewall window, in the left pane, click **Client Firewall > Client Firewall Settings**.
- 3 Click **Custom Level**.
- 4 Select the setting that you want.

High	Blocks all communication that you do not specifically allow. You must create firewall rules for every application that requests Internet access.
Medium	Blocks many ports that are used by harmful applications. However, it can also block useful applications when they use the same ports.
None	Disables Symantec Client Firewall and allows all Internet communications.

## Setting Java and ActiveX Security Levels

Java applets and ActiveX controls make Web sites more interactive. Many Web sites rely on ActiveX controls and Java applets to perform and appear correctly. Most of these applications are safe and do not threaten your computer or data.

However, ActiveX controls can have total access to your data, depending on how they are programmed. They can copy data from your hard disk and transmit it over the Internet while you are online. They can delete files, intercept messages, capture passwords, or gather banking numbers and other important data.

The only way to prevent bad applications from running on your computer is to block them from downloading. However, blocking all Java applets and ActiveX controls prevents many Web sites from appearing or running correctly.

### To set Java and ActiveX Security Levels

- 1 Open Symantec Client Firewall.
- 2 In the Symantec Client Firewall window, in the left pane, click **Client Firewall > Client Firewall Settings**.
- 3 Click **Custom Level**.
- 4 Select the Java Applet Security Level or ActiveX Control Security Level that you want.

High	Blocks your browser from running any Java applets or ActiveX controls over the Internet. This is the safest, but most inconvenient, option. Some Web sites might not operate properly using this setting.
Medium	Prompts you when Java applets and ActiveX controls are encountered. This lets you temporarily or permanently allow or block each Java applet or ActiveX control that you encounter. It can be bothersome to respond every time that you encounter a Java applet or ActiveX control, but it lets you decide which ones to run.
None	Lets Java applets and ActiveX controls run whenever you encounter them.

### Enabling Internet Access Control alerts

Internet Access Control alerts give you control when an application tries to connect to the Internet but no firewall rule exists for it. When a connection attempt is made, an Internet Access Control alert appears, and you can permit or block the application from accessing the Internet.

Disable this option to block applications from accessing the Internet when there are no specific firewall rules in place for them.

### To enable Internet Access Control alerts

- 1 Open Symantec Client Firewall.
- 2 In the Symantec Client Firewall window, in the left pane, click **Client Firewall > Client Firewall Settings**.
- 3 Click **Custom Level**.
- 4 Check **Enable Access Control Alerts**.

## Enabling alerts for unused ports

Symantec Client Firewall blocks access to the unused ports on your computer. For example, if someone tries to connect to your computer using Symantec pcAnywhere and you don't have a Symantec pcAnywhere host running, no response is made to acknowledge the connection attempt, so the inquiring computer learns nothing.

You can enable alerts to appear when attempts are made to access unused ports on your computer. These alerts are useful for solving problems when you are configuring advanced programs and features, such as Internet Connection Sharing.

### To enable alerts for unused ports

- 1 Open Symantec Client Firewall.
- 2 In the Symantec Client Firewall window, in the left pane, click **Client Firewall > Client Firewall Settings**.
- 3 Click **Custom Level**.
- 4 Check **Alert when unused ports are accessed**.

## Customizing firewall rules

Firewall rules control how Symantec Client Firewall protects your computer from malicious incoming traffic, applications, and Trojan horses. The firewall automatically checks all data coming in or out of your computer against these rules. Rules fall into three categories:

- **System:** Control system-wide protection
- **Application:** Block or permit applications from accessing the Internet
- **Trojan horse:** Protect against malicious applications

---

**Note:** To customize firewall rules, you must be assigned a user level of Administrator or Normal User. See [“Symantec Client Firewall user levels”](#) on page 23 for a list of user levels and associated rights.

---

## Priorities for firewall rule processing

When a computer attempts to connect to your computer, or when your computer attempts to connect to a computer on the Internet, Symantec Client Firewall compares the type of connection with its list of firewall rules.

Firewall rules are processed in a set order based on their types and the users who created them. The order of priority appears in [Table 7-3](#).

**Table 7-3** Rule processing priority

Priority	Rule type	User type
First	System-wide	Administrator
Second	Application	Administrator
Third	System-wide	User
Fourth	Application	User
Fifth	Trojan	Administrator
Sixth	Trojan	User

## Default firewall rules

A number of firewall rules are predefined and enabled when you install Symantec Client Firewall. These rules provide basic network functionality as well as protect you from known Internet risks. The default firewall rules listed in [Table 7-4](#) appear in the system-wide settings and in Trojan horse settings.

**Table 7-4** Examples of default firewall rules

Rule	Description
Default Inbound DNS Default Outbound DNS	Permits the use of the domain name system (DNS).
Default Inbound Bootp Default Outbound Bootp	Permits the use of the Bootp service. (Bootp is short for bootstrap protocol, which enables a computer to discover its own IP address.)
Default Inbound NetBIOS Name Default Inbound NetBIOS Default Outbound NetBIOS	Controls the use of the NetBIOS name service and the NetBIOS datagram service that are used in file sharing on the Microsoft Network.

**Table 7-4** Examples of default firewall rules

Rule	Description
Default Inbound Loopback Default Outbound Loopback	Permits inbound and outbound loopback connections to the localhost address of 127.0.0.1. It is usually safe to permit loopback or local connections because the connection originator is typically a trusted application on your own computer. Even with this firewall rule enabled, remote computers are never allowed access to the localhost address by the underlying network.
Default Inbound ICMP Default Outbound ICMP	Permits all types of outbound and safe types of inbound ICMP messaging. ICMP messages provide status and control information.
Default Block Back Orifice 2000 Trojan Default Block NetBus Trojan	Protects you from known remote-access Trojan horse programs. This firewall rule is automatically enabled.

## Creating new firewall rules

Symantec Client Firewall includes Internet Access Control, which automatically creates firewall rules as you use the Internet. You can also create and modify rules manually. There are four ways to create firewall rules with Internet Access Control:

- **Scan for Internet-enabled applications:** Find and configure access for all Internet applications on a computer at once. This is the quickest way to set up firewall rules.
- **Enable Automatic Internet Access Control:** Automatically configure access for well-known applications the first time that you run them.

- Add applications individually: Closely manage the list of applications that can access the Internet.
- Respond to Internet Access Control alerts: Symantec Client Firewall warns you when an application attempts to access the Internet for the first time. You can then allow or block Internet access for the application.

---

**Warning:** Creating a Block All rule blocks your computer's access to the network. This may cause unexpected behavior. For example, your computer may not be able to receive virus definitions file updates. To resolve this issue, you will need to create the BootPC and the BootPS permit rules above the Block All rule. Both of these rules are included in the default system-wide rules.

---

## Scanning for Internet-enabled applications

Scanning for Internet-enabled applications is the quickest way to set up firewall rules with Internet Access Control. Symantec Client Firewall scans the computer for applications that it recognizes and lets you select appropriate settings for each application.

### To scan for Internet-enabled applications

- 1 Open Symantec Client Firewall.
- 2 In the Symantec Client Firewall window, in the left pane, click **Client Firewall > Internet Access Control**.
- 3 Click **Configure**.
- 4 Click **Application Scan**.
- 5 Select the disk or disks on your computer that you want to scan.
- 6 Click **Next**.
- 7 In the Application Scan window, do one of the following:
  - Check applications that you want to add to the Internet Access Control list.
  - Click **Check All** to add all Internet-enabled applications at once.
- 8 Click **Finish**.

## Enabling Automatic Internet Access Control

Symantec Client Firewall maintains a list of Internet applications that are generally safe to use. When Automatic Internet Access Control is active, Symantec Client Firewall automatically creates new access rules for recognized applications the first time that they run.

If an unknown application attempts to access the Internet, Symantec Client Firewall warns you. You can then choose to allow or block Internet access for the application.

Symantec regularly updates the list of recognized applications. Symantec Client Firewall users should run LiveUpdate regularly to ensure that their list is up-to-date.

See [“Keeping current with LiveUpdate”](#) on page 42.

### To enable Automatic Internet Access Control

- 1 Open Symantec Client Firewall.
- 2 In the Symantec Client Firewall window, in the left pane, click **Client Firewall > Internet Access Control**.
- 3 Click **Configure**.
- 4 Check **Enable Automatic Internet Access Control**.
- 5 Click **Yes**.

## Adding an application to Internet Access Control

You can add applications to Internet Access Control that will strictly control an application’s ability to access the Internet. This overrides any settings made by Automatic Internet Access Control.

### To add an application to Internet Access Control

- 1 Open Symantec Client Firewall.
- 2 In the Symantec Client Firewall window, in the left pane, click **Client Firewall > Internet Access Control**.
- 3 Click **Add**.
- 4 Select the application’s executable file.  
Executable file names typically end in `.exe`.

- 5 Click **Open**.
- 6 In the Internet Access Control window, select one of the following:
  - Permit this application access to the Internet: Allow all access attempts by this program.
  - Block this application from accessing the Internet: Deny all access attempts by this program.
  - Customize Internet access for this application: Create rules controlling how this application accesses the Internet.  
See “[Customizing firewall rules](#)” on page 78.
- 7 If you want to see the kinds of risks that this application could pose to your computer, click **Details**.
- 8 Click **OK**.

## Changing Internet Access Control settings

After using Symantec Client Firewall for a while, you may find that you need to change access settings for applications. For example, you can choose to block any future Internet connections by an application or grant Internet access to a blocked application. Any changes override settings made by Automatic Internet Access Control.

### To change Internet Access Control settings

- 1 Open Symantec Client Firewall.
- 2 In the Symantec Client Firewall window, in the left pane, click **Client Firewall > Internet Access Control**.
- 3 Select the application that you want to change.
- 4 Click **Modify**.
- 5 In the Internet Access Control window, select the settings that you want.

Permit	Allow Internet access attempts by this application.
Block	Deny Internet access attempts by this application.
Customize	Control the types of information that this application can send and receive.
- 6 Click **OK**.

## Creating firewall rules manually

While Symantec Client Firewall automatically creates most of the firewall rules that you need, you may want to add specific rules. Only experienced Internet users should create their own firewall rules.

## Elements of a firewall rule

Firewall rules define specific types of communication that are either allowed or blocked. [Table 7-5](#) lists several settings for defining a firewall rule.

**Table 7-5** Firewall settings

Setting	Description
Action	<p>Specifies whether the rule permits, blocks, or monitors the type of network communication defined within the rule.</p> <p>Permit Internet Access: Allows communication of this type to take place.</p> <p>Block Internet Access: Prevents communication of this type from taking place.</p> <p>Monitor Internet Access: Updates the Firewall tab in the Symantec Client Firewall Event Log. Rule processing then continues until a match is found. If there is no match, the communication is either blocked by default or an Internet Access Control alert appears.</p> <p>Monitor Internet Access lets you log communication activity. For example, suppose that you have a Permit firewall rule that lets your FTP server communicate with any network address. You could track how often users at a particular network address connect to your FTP server by setting up a monitor rule to log instances of FTP server communication to and from that network address. The FTP server monitor rule must precede the FTP server permit rule.</p>

**Table 7-5** Firewall settings

Setting	Description
Connections	<p data-bbox="677 319 1225 402">Specifies whether the rule applies to inbound network communication, outbound network communication, or network communication in either direction.</p> <p data-bbox="677 423 1209 506">Connections to other computers: The rule applies to outbound connections from your computer to another computer.</p> <p data-bbox="677 527 1209 611">Connections from other computers: The rule applies to inbound connections from another computer to your computer.</p> <p data-bbox="677 631 1180 715">Connections to and from other computers: The rule applies to inbound connections as well as outbound connections.</p>

**Table 7-5** Firewall settings

Setting	Description
Computers	<p>Specifies the computers and network adapters to which this rule applies.</p> <p>The computers that you specify are other computers with which you want to control communications with your computer.</p> <p>Any computer: The rule applies to all computers.</p> <p>Only computers specified below: The rule applies only to computers, sites, and domains listed.</p> <p>Adapters: The rule applies to a specific network adapter in your computer. The IP address of the network adapter to which the rule should apply is specified.</p> <p>This is useful if your computer has more than one IP address. If, for example, your computer has a connection to a local network as well as a connection to the Internet, it probably has two IP addresses.</p> <p>This setting lets you apply rules to one of your computer's IP addresses. For example, if your computer is connected to a home network and to the Internet, you might want to set up a rule that permits file sharing on the home network, while another rule blocks file sharing over the Internet.</p> <p>If your local network uses DHCP so that your computer might get a different IP address each time that it starts, enter a network address using an IP address and a subnet mask that identifies all of the possible IP addresses that your computer might use. See your system administrator for the appropriate values.</p>

**Table 7-5** Firewall settings

Setting	Description
Communications: Protocols	<p>Specifies the communications protocols that this rule controls.</p> <p>TCP: The rule applies to TCP (Transmission Control Protocol) communications.</p> <p>UDP: The rule applies to UDP (User Datagram Protocol) communications.</p> <p>TCP and UDP: The rule applies to both TCP and UDP communications.</p> <p>ICMP: The rule applies to ICMP (Internet Control Message Protocol) communications. Only applies to system-wide rules and Trojan Horse rules.</p>
Communications: Ports	<p>Specifies the types of communications, or ports, that are controlled by this rule.</p> <p>All types of communications (all ports): The rule applies to communications using any port.</p> <p>Only the types of communications or ports listed below: The rule applies to the ports listed. You can add ports to, or remove ports from, the list.</p>
Tracking	<p>Specifies whether the program should notify you or create a Symantec Client Firewall Event Log entry when a network communication event matches the criteria set for this rule.</p> <p>Do not track this rule: No record of the actions of this rule are made.</p> <p>Create an Event Log entry: An entry is created in the Symantec Client Firewall Event Log when a network communication event matches this rule.</p> <p>Notify me with an AlertTracker message: An AlertTracker message appears when a network communication event matches this rule.</p> <p>Display Security Alert: A Security Alert dialog box appears when a network communication event matches this rule.</p>
Type	<p>Specifies the rule as an Administrator or User rule.</p> <p>See <a href="#">“Priorities for firewall rule processing”</a> on page 79.</p>

**Table 7-5** Firewall settings

Setting	Description
Description	Specifies the name of the rule so that you can differentiate this rule from other rules.

## Adding firewall rules

Before adding a new firewall rule, you must first determine whether you want to add a firewall rule that controls system-wide access to the Internet or a firewall rule to control an application.

- System-wide rules control system-wide access to the Internet. For example, the rules that provide protection against someone connecting to your computer using Microsoft networking are system-wide rules.
- Application rules control one application's access to the Internet. Use application rules when you have an application that needs access to the Internet.

### Adding a system-wide firewall rule

You can create firewall rules that apply to all of the applications on your computer.

#### To add a system-wide firewall rule

- 1 Open Symantec Client Firewall.
- 2 In the Symantec Client Firewall window, in the left pane, click **Client Firewall > Internet Access Control**.
- 3 Click **Configure**.
- 4 Click **System-Wide Settings**.
- 5 Click **Add**.
- 6 Follow the on-screen instructions.

## Adding an application rule

You can create firewall rules that apply to specific applications on your computer.

### To add an application rule

- 1 Open Symantec Client Firewall.
- 2 In the Symantec Client Firewall window, in the left pane, click **Security > Internet Access Control**.
- 3 Click **Add**.
- 4 Select the executable file for the application.
- 5 Click **Open**.
- 6 Follow the on-screen instructions.

## Changing an existing firewall rule

You can change firewall rules if they are not functioning the way that you want.

### To change an existing firewall rule

- 1 Open Symantec Client Firewall.
- 2 In the Symantec Client Firewall window, in the left pane, click **Client Firewall > Internet Access Control**.
- 3 To change a system-wide rule, click **Configure**, then click **System-Wide Settings**.
- 4 Select the rule that you want to change.
- 5 Click **Modify**.
- 6 Follow the on-screen instructions.

## Removing a firewall rule

Remove firewall rules when they are no longer necessary.

### To remove a firewall rule

- 1 Open Symantec Client Firewall.
- 2 In the Symantec Client Firewall window, in the left pane, click **Client Firewall > Internet Access Control**.
- 3 To remove a system-wide rule, click **Configure**, then click **System-Wide Settings**.
- 4 Select the rule that you want to remove.
- 5 Click **Remove**.
- 6 Click **OK**.

# Customizing Intrusion Detection

The default Intrusion Detection settings should provide you with adequate protection. If the default protection is not appropriate, you can customize Intrusion Detection settings.

You can customize Intrusion Detection by excluding specific network activity from monitoring, enabling, or disabling AutoBlock, and restricting blocked computers.

## Excluding specific network activity from being monitored

In some cases, benign network activity may appear similar to a Symantec Client Firewall attack signature. If you receive repeated warnings about possible attacks, and you know that these attacks are being triggered by safe behavior, you can create an exclusion for the attack signature that matches the benign activity.

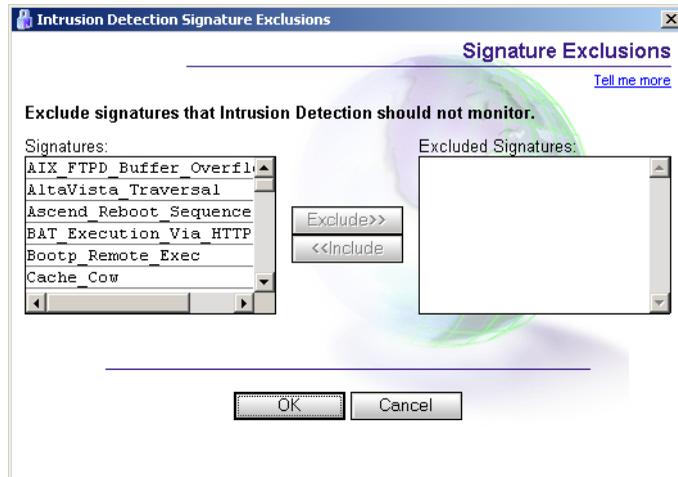
---

**Note:** Each exclusion that you create leaves your computer vulnerable to attacks. Be very selective when excluding attacks. Only exclude behavior that is always benign.

---

### To exclude attack signatures from being monitored

- 1 Open Symantec Client Firewall.
- 2 In the Symantec Client Firewall window, in the left pane, click **Client Firewall > Intrusion Detection**.
- 3 Click **Exclusions > Signature Exclusions**.



- 4 In the Signatures list, select the attack signature that you want to exclude.
- 5 Click **Exclude**.
- 6 When you are done excluding signatures, click **OK**.

## Enabling or disabling AutoBlock

When Symantec Client Firewall detects an attack, it automatically blocks the connection to ensure that your computer is safe. The program can also activate AutoBlock, which automatically discards all incoming communication from the attacking computer for a set period of time, even if the incoming communication does not match an attack signature. By default, AutoBlock stops all inbound communications from the attacking computer for 30 minutes. While AutoBlock stops all incoming communication from the remote computer, it does not stop you from sending information to the attacking computer.

#### **To enable or disable AutoBlock**

- 1 Open Symantec Client Firewall.
- 2 In the Symantec Client Firewall window, in the left pane, click **Client Firewall > Intrusion Detection**.
- 3 Check or uncheck **Enable AutoBlock**.

## Excluding specific computers from AutoBlock

Some normal Internet activities will be repeatedly recognized by Symantec Client Firewall as attacks. For example, some Internet service providers scan the ports of your computer to ensure that you are within their service agreements. To prevent normal activities from interrupting your Internet use, you can exclude them from being blocked by AutoBlock.

#### **To exclude activities from AutoBlock**

- 1 Open Symantec Client Firewall.
- 2 In the Symantec Client Firewall window, in the left pane, click **Client Firewall > Intrusion Detection**.
- 3 Click **Exclusions > IP Addresses**.
- 4 In the Currently blocked list, select the IP address that you want to exclude.
- 5 Click **Exclude**.
- 6 When you are done excluding IP addresses, click **OK**.

## Restricting a blocked computer

You can add a blocked computer to your Restricted zone to permanently prevent that computer from accessing your computer. Computers added to the Restricted zone do not appear on the blocked list because Symantec Client Firewall automatically rejects any connection attempts by restricted computers.

#### **To restrict a blocked computer**

- 1 Open Symantec Client Firewall.
- 2 In the Symantec Client Firewall window, in the left pane, click **Client Firewall > Intrusion Detection**.
- 3 In the list of computers that are currently blocked by AutoBlock, select the computer to add to the Restricted zone, then click **Restrict**.

## Unblocking computers

In some cases, Symantec Client Firewall may recognize normal activity as an attack. If you can't communicate with computers that you should be able to communicate with, they may be on the list of computers currently blocked by AutoBlock.

If a computer that you need to access appears on the list of computers currently blocked by AutoBlock, unblock it. If you have changed your protection settings and want to reset your AutoBlock list, you can unblock all of the computers on the AutoBlock list at once.

### To unblock computers currently blocked by AutoBlock

- 1 Open Symantec Client Firewall.
- 2 In the Symantec Client Firewall window, in the left pane, click **Client Firewall > Intrusion Detection**.
- 3 Do one of the following:
  - To unblock one computer, select its IP address, then click **Unblock**.
  - To unblock all computers on the AutoBlock list, click **Unblock All**.



# Index

## A

- access Symantec Client Firewall 22
- active content, protection from 71
- ActiveX controls 30, 76
- alerts
  - ActiveX 30
  - Confidential Information 33
  - cookie 31
  - Internet Access Control 27, 82
  - Intrusion Protection 73
  - Java 30
  - new network connection 24
  - Security 26
  - Settings 29
  - Symantec Client Firewall 77
- AlertTracker 34
- AOL 43
- attack signatures
  - about 71
  - excluding 90
- attacks
  - blocking 70
  - network 71
  - signatures 71
- AutoBlock
  - about 27
  - enabling and disabling 91
  - excluding computers 92
- Automatic LiveUpdate 42

## B

- blocking
  - computers 91
  - confidential information 47
  - cookies 32, 50
  - email addresses 51
  - Internet-enabled applications 28
- bootp service 79
- browser privacy 51

## C

- change
  - firewall rules 78
  - Internet Access Control settings 83
  - Symantec Client Firewall settings 35
- CompuServe 43
- computer
  - blocking 91
  - exclude from AutoBlock 92
  - requirements 14
- Confidential Information
  - alert 33
  - options 50
- Cookie Blocking options 50
- cookies 31, 50, 59
- Current Status 59

## D

- desktop icon 22
- DNS (Domain Name System) firewall rules 79
- domains
  - adding to list 38
  - removing from list 40

## E

- enabling
  - Automatic LiveUpdate 42
  - Browser Privacy 51
  - file and print sharing 54
  - Intrusion Detection 74
  - Privacy Control 46
  - secure Web connections 52
  - Symantec Client Firewall 73
- encryption 29, 52
- Event Log
  - See also* statistics
  - clearing events 62
  - contents 60

**E**  
Event Log (*continued*)

- exporting information from 67, 68
- filtering events 61
- printing 67, 68
- viewing 61

**F**

- file sharing 54
- firewall rules
  - adding 88
  - default 79
  - processing order 79
  - removing 90
  - settings for 84

**I**

- ICMP 80
- icon in notification area 22
- Internet Access Control
  - alerts 27, 77
  - creating firewall rules with 80
  - enabling alerts 77
  - settings 77, 83
- Internet access statistics
  - about 64
  - configuring 65
  - contents 64
  - exporting information from 67, 68
  - printing 67, 68
  - resetting 65
- Internet Control Message Protocol. *See* ICMP
- Internet Zone Control 54
- Internet-enabled applications 27, 81, 88
- Intrusion Detection
  - about 71
  - configuring 90

**J**

- Java applets 30, 76

**L**

- LiveUpdate options 42
- localhost 80
- loopback connections 80

**N**

- NetBIOS, default firewall rule 79
- notification area icon 22

**O**

- operating systems 14
- options
  - LiveUpdate 42
  - Symantec Client Firewall 35

**P**

- packets 70
- ports
  - about 70
  - hiding 78
  - scans 71
  - unused alerts 78
- preferences for Symantec Client Firewall 35
- printers, sharing 54
- Privacy Control 46
- privacy levels 46
- Prodigy Internet connection 43

**R**

- removing Symantec Client Firewall 19
- required computer configuration 14
- rights for users and administrators 23
- risks from zombie programs 72

**S**

- scans
  - for Internet-enabled applications 81
  - port 71
- secure Web connections, disabling and enabling 52
- security
  - attacks 70
  - levels 74
- Security Alerts 26
- settings
  - site-specific 39
  - Symantec Client Firewall 74
- Settings Alerts 29
- statistics 64
- status checking 59
- stealth ports 78

- Symantec Client Firewall
  - Advanced Options 37
  - alerts 77
  - as a component of Symantec Client Security 11
  - checking status 59
  - customizing 78
  - general options 36
  - options 35
  - security settings 74
  - wireless connections 24
- Symantec Client Security 11
- system
  - requirements 14
  - tray icon 22

## T

- Trojan horse programs 71, 80

## U

- uninstalling Symantec Client Firewall 19
- user access levels 23

## W

- Web sites
  - adding to list 38, 40
  - list of 38
  - removing from list 40
- Windows
  - operating systems 14
  - Registry 29
- wireless connections, protecting 24
- Wizard
  - Add Rule 29
  - LiveUpdate 19

## Z

- zombie programs 72
- zones
  - Restricted 54, 92
  - Trusted 54