

User Guide for Zone Labs security software

version 6.5



A Check Point
COMPANY

Smarter Security™

© 2006 Zone Labs, LLC. All rights reserved.

© 2006 Check Point Software Technologies Ltd. All rights reserved.

Check Point, Application Intelligence, Check Point Express, the Check Point logo, AlertAdvisor, ClusterXL, Cooperative Enforcement, ConnectControl, Connectra, CoSa, Cooperative Security Alliance, FireWall-1, FireWall-1 GX, FireWall-1 SecureServer, FloodGate-1, Hacker ID, IMsecure, INSPECT, INSPECT XL, Integrity, InterSpect, IQ Engine, Open Security Extension, OPSEC, Policy Lifecycle Management, Provider-1, Safe@Home, Safe@Office, SecureClient, SecureKnowledge, SecurePlatform, SecurRemote, SecurServer, SecureUpdate, SecureXL, SiteManager-1, SmartCenter, SmartCenter Pro, Smarter Security, SmartDashboard, SmartDefense, SmartLSM, SmartMap, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartViewTracker, SofaWare, SSL Network Extender, TrueVector, UAM, User-to-Address Mapping, UserAuthority, VPN-1, VPN-1 Accelerator Card, VPN-1 Edge, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecurRemote, VPN-1 SecureServer, VPN-1 VSX, Web Intelligence, ZoneAlarm, Zone Alarm Pro, Zone Labs, and the Zone Labs logo, are trademarks or registered trademarks of Check Point Software Technologies Ltd. or its affiliates. All other product names mentioned herein are trademarks or registered trademarks of their respective owners. The products described in this document are protected by U.S. Patent No. 5,606,668, 5,835,726 and 6,496,935 and may be protected by other U.S. Patents, foreign patents, or pending applications.

Zone Labs, LLC.

A Checkpoint Company

475 Brannan, Suite 300

San Francisco, CA 94107

ZLD -0422-0650-2006-0601

Contents

Tables	ix
Figures	xi
Preface	xiii
About Zone Labs security software	xiv
About this guide	xv
Conventions	xv
Zone Labs User Forum	xv
Chapter 1 Installation and setup	1
System requirements and supported software	2
Hardware requirements and supported operating systems	2
Supported protocols for e-mail protection	2
Supported browser software	2
Supported IM clients	3
Installing Zone Labs security software	4
Installing ZoneAlarm	4
Installing Zone Labs security software	4
Upgrading from a previous version	6
Upgrading and the Windows XP SP2 Windows Firewall	6
Upgrading and IMsecure myVault settings	6
Upgrading and MailFrontier settings	6
Configuring basic options	7
Configuring program access permissions	7
Joining the DefenseNet community	7
Uninstalling Zone Labs security software	9
Chapter 2 Zone Labs security software basics	11
Tour of the Zone Labs security software Control Center	12
Getting around the Control Center	12
Using the dashboard	13
System Tray icons	15
Shortcut menu	15
Using the Status tab	16
Understanding Zones	18
Zones manage firewall security	18
Zones provide program control	19
Responding to alerts	20

New Program alerts	20
New Network and VPN alerts.	21
Setting product preferences.	22
Setting update options	22
Setting your password	22
Backing up and restoring security settings.	23
Setting general product preferences	23
Setting contact preferences	24
Setting product display and proxy server options.	25
Creating an online fraud protection profile.	26
Licensing, registration, and support	27
Updating your product license.	27
Registering Zone Labs security software	27
Accessing technical support	28
Chapter 3 Networking with Zone Labs security software.	29
Configuring a new network connection	30
Using the Network Configuration Wizard	30
Disabling the Network Configuration Wizard.	31
Using the Wireless Network Configuration Wizard	31
Disabling the Wireless Network Configuration Wizard.	31
Integrating with network services	33
Enabling file and printer sharing	33
Connecting to network mail servers	33
Enabling Internet Connection Sharing.	34
Configuring your VPN connection	35
Supported VPN protocols	35
Configuring your VPN connection automatically	35
Configuring your VPN connection manually	36
Adding a VPN gateway and other resources to the Trusted Zone.	37
Removing a VPN gateway from a blocked range or subnet.	37
Allowing VPN protocols	37
Granting access permission to VPN software	38
Chapter 4 Firewall protection.	39
Understanding Firewall protection.	40
Choosing security levels	41
Setting the security level for a Zone	41
Setting advanced security options.	42
Setting gateway security options	42
Setting ICS (Internet Connection Sharing) options	42
Setting general security options.	43
Setting network security options	44
Setting wireless network security options.	44
Managing traffic sources	46
Viewing the traffic source list	46
Modifying traffic sources	46
Adding to the Trusted Zone.	47
Adding to the Blocked Zone	48

Viewing logged Firewall events.	48
Blocking and unblocking ports	50
Default port permission settings	50
Adding custom ports	51
Understanding expert firewall rules.	53
How expert firewall rules are enforced.	53
Expert firewall rule enforcement rank	54
Creating expert firewall rules	55
Creating groups	57
Creating a location group	57
Creating a protocol group	57
Creating a day/time group	60
Managing Expert Firewall Rules.	61
Viewing the Expert Rules list.	61
Editing and re-ranking rules	62
Chapter 5 Program control	63
Understanding Program Control.	64
Setting program permissions automatically	64
Setting program permissions manually	65
Setting general program control options	67
Setting the program control level	67
Configuring OSFirewall protection	68
Enabling Component Control.	69
Setting the SmartDefense Advisor level.	69
Enabling the automatic lock	70
Viewing logged program events	71
Viewing logged OSFirewall events.	73
Configuring advanced program settings	74
Setting global program properties.	74
Setting access permissions for new programs	74
Setting permissions for specific programs	76
Using the programs list	76
Adding a program to the programs list.	79
Granting a program permission to access the Internet	80
Granting a program permission to act as a server	81
Granting send mail permission to a program	81
Setting program options for a specific program	82
Setting Advanced Program Control options.	82
Disabling Outbound Mail protection for a program.	82
Setting Filter options for a program	83
Setting authentication options.	83
Setting passlock permission for a program.	84
Managing program components.	85
Creating expert rules for programs.	87
Creating an expert rule for a Program	87
Sharing expert rules	88

Chapter 6	Spyware and Virus protection	89
	Spyware and Virus Protection	90
	Turning on virus and spyware protection	90
	Scheduling a scan	90
	Updating virus and spyware definitions	91
	Customizing virus protection options	93
	Specifying scan targets	93
	On-Access scanning	94
	E-mail Scanning	95
	Enabling automatic virus treatment	95
	Specifying virus detection methods	95
	Customizing spyware protection options	97
	Enabling automatic spyware treatment	97
	Specifying spyware detection methods	97
	Excluding spyware from scans	97
	Spy Site Blocking	98
	Preventing spyware attacks	98
	Performing a virus scan	99
	Understanding virus scan results	100
	Treating virus files manually	101
	Repairing files in an archive	101
	Submitting viruses and spyware to Zone Labs for review	102
	Viewing logged virus events	102
	Performing a spyware scan	104
	Understanding spyware scan results	105
	Errors in spyware scan results	106
	Viewing items in quarantine	106
	Viewing logged spyware events	107
	Viewing virus and spyware protection status	109
	Monitoring virus protection	110
	Monitoring Coverage	110
	Monitoring in ZoneAlarm, ZoneAlarm Pro, and ZoneAlarm Anti-Spyware	110
	Monitoring in ZoneAlarm Anti-virus and ZoneAlarm Security Suite	111
	Enabling and disabling Anti-virus Monitoring	111
	Viewing Status Messages in the Anti-virus Monitoring panel	112
	Viewing Anti-virus Monitoring alerts	112
Chapter 7	E-mail protection	115
	Understanding e-mail protection	116
	Inbound MailSafe protection	116
	Outbound MailSafe protection	117
	Enabling Inbound MailSafe protection	117
	Enabling Outbound MailSafe protection	117
	Customizing Inbound MailSafe protection	118
	Viewing the Attachments list	118
	Changing the quarantine setting for an attachment type	118
	Adding and removing attachment types	119
	Opening a quarantined attachment	120
	Customizing Outbound MailSafe protection	121
	Enabling Outbound MailSafe protection by program	121

Setting Outbound MailSafe protection options	121
Filtering junk e-mail	123
Allowing or blocking e-mail from specific senders	123
Allowing or blocking e-mail from specific companies	124
Adding contacts to the Allowed List	124
Scanning your Inbox	124
Allowing e-mail from distribution lists	124
Reporting junk e-mail	125
Reporting fraudulent e-mail	125
Specifying junk e-mail message options	126
Challenging e-mail from unknown senders	127
Specifying your outbound e-mail server	129
Customizing junk e-mail filter settings	130
Restoring e-mail incorrectly identified as junk	131
Viewing junk e-mail filter reports	132
Anti-virus protection for e-mail	133
Enabling E-mail scanning	133
How e-mail infections are handled	133
Chapter 8 Privacy protection	135
Understanding privacy protection	136
Setting general privacy options	137
Setting privacy protection levels	137
Applying privacy protection to programs other than browsers	137
Using Privacy Advisor	139
Setting privacy options for specific Web sites	140
Viewing the privacy site list	140
Adding sites to the privacy site list	141
Editing sites on the site list	141
Customizing cookie control	142
Blocking session cookies	142
Blocking persistent cookies	142
Blocking third-party cookies	143
Setting an expiration date for cookies	143
Customizing ad blocking	144
Specifying which ads to block	144
Setting ad void control options	144
Customizing mobile code control	146
Specifying which types of mobile code to block	146
Understanding Cache cleaner	147
Using Cache Cleaner	147
Customizing hard drive cleaning options	148
Customizing browser cleaning options	148
Chapter 9 Alerts and Logs	151
Understanding alerts and logs	152
About Zone Labs security software alerts	152
About event logging	159

Setting basic alert and log options	160
Setting the alert event level	160
Setting event and program logging options.	160
Controlling the number of alerts	161
Showing or hiding firewall alerts	161
Enabling system tray alerts	161
Game Mode	162
Setting event and program log options	164
Formatting log appearance	164
Customizing event logging	164
Customizing program logging	164
Viewing log entries	165
Viewing the text log	167
Archiving log entries	169
Using SmartDefense Advisor and Hacker ID.	170
Chapter 10 Identity protection	171
Understanding the ID Lock feature	172
How your personal information is protected	172
Setting the ID Lock protection level	173
About myVAULT	175
Adding data to myVAULT	175
Editing and removing myVAULT contents	177
Using the Trusted Sites list	178
Viewing the Trusted Sites list	178
Adding to the Trusted Sites list	179
Editing and removing trusted sites	179
Identity Protection Center	180
Chapter 11 Parental Control	181
Understanding Parental Control.	182
Enabling parental control and smart filtering.	183
Enabling or disabling parental control.	183
Enabling or disabling Smart Filtering	183
Setting timeout options	183
Choosing which content categories to block.	185
Chapter 12 Instant Messaging Security	191
IM Security Overview	192
Access	192
Blocking spam	192
Feature Control.	194
Inbound protection	194
Encrypting instant messaging traffic.	196
Setting IM Security options	199
Setting the protection level	199

	Viewing IM Security protection status	199
	Customizing protection settings	200
	Setting advanced IM Security options	200
	Viewing logged IM Security events	201
Appendix A	Alert reference	203
	Informational alerts	204
	Firewall alerts/Protected	204
	MailSafe alert	205
	Blocked Program alert	206
	Internet Lock alert	207
	Remote alert	208
	Program alerts	209
	New Program alert	210
	Repeat Program alert	211
	Changed Program alert	211
	Program Component alert	212
	Server Program alert	213
	Advanced Program alert	215
	Automatic VPN Configuration alert	215
	Manual Action Required alert	216
	OSFirewall alerts	218
	Medium-rated Suspicious Behavior alert	218
	High-rated Suspicious Behavior alert	218
	Malicious behavior alert	219
	ID Lock alert	220
	New Network alert	221
	Instant Messaging alerts	223
Appendix B	Keyboard shortcuts	225
	Navigation shortcuts	226
	Global function shortcuts	227
	Dialog box commands	229
	Button shortcuts	230
Appendix C	Troubleshooting	233
	VPN	234
	Configuring Zone Labs security software for VPN traffic	234
	VPN auto-configuration and expert rules	234
	Automatic VPN detection delay	234
	Networking	236
	Making your computer visible on your local network	236
	Sharing files and printers across a local network	236
	Resolving a slow start up	237
	Internet Connection	238
	Connecting to the Internet fails after installation	238

Allowing ISP Heartbeat messages	239
Connecting through an ICS client	239
Connecting through a proxy server	240
Unable to connect to program advice server	240
IM Security	241
IM programs not appearing in status	241
Anti-virus	242
Anti-virus feature installation problem	242
Anti-virus Monitoring alert	242
Resolving conflicts with anti-virus products	242
E-mail scanning or IM Security is unavailable	243
Third-party software	244
Anti-virus	244
Browsers	244
Chat and instant messaging programs	245
E-mail programs	246
Internet answering machine programs	246
File sharing programs	246
FTP programs	246
Games	247
Remote control programs	248
VNC programs	248
Streaming media programs	249
Voice over IP programs	249
Web conferencing programs	249
Appendix D Program behavior	251
Medium-rated suspicious behavior	252
High-rated suspicious behavior	253
Glossary	257
Index	269

Tables

Table 2-3: System Tray icons	15
Table 2-4: Update messages	17
Table 3-1: Supported VPN protocols	35
Table 3-2: Required VPN-related network resources	37
Table 4-1: Traffic source list fields	46
Table 4-2: Firewall event log fields	48
Table 4-3: Default access permissions for incoming and outgoing traffic types	50
Table 5-1: Program event log fields	71
Table 5-2: OSFirewall event log fields	73
Table 5-3: Program List symbols	79
Table 6-2: Icons indicating scan targets	93
Table 6-3: Virus event log fields	103
Table 6-4: Spyware event log fields	108
Table 9-6: Log viewer fields	166
Table 11-1: Parental Control categories	185
Table 12-6: Log Viewer field explanations	202
Table A-1: IM alert messages	223
Table B-1: Navigation shortcuts	226
Table B-2: Global shortcuts	227
Table B-3: Dialog box shortcuts	229
Table B-4: Keystrokes for activating buttons	230
Table C-1: Troubleshooting VPN problems	234
Table C-2: Troubleshooting network problems	236
Table C-3: Troubleshooting Internet connection problems	238
Table C-4: Troubleshooting IM Security problems	241
Table C-5: Troubleshooting Zone Labs Anti-virus problems	242

Table D-1: Medium-rated suspicious behavior guide 252

Table D-2: High-rated suspicious behavior guide 253

Figures

Figure 2-1: Zone Labs security software Control Center	12
Figure 2-2: Zone Labs security software dashboard	13
Figure 4-4: Expert firewall rule rank order	54
Figure 4-5: Expert Rules list	61
Figure 5-3: Programs list	77
Figure 5-4: Components List	85
Figure 6-1: Anti-virus and Anti-spyware status	92
Figure 6-2: Scan targets dialog box	93
Figure 6-3: Virus scan results dialog.	100
Figure 6-4: Spyware scan results dialog	105
Figure 6-5: Anti-virus Monitoring Status area in ZoneAlarm	112
Figure 7-1: Attachments list	118
Figure 7-2: The junk e-mail filter toolbar	123
Figure 7-3: Challenge options tab	128
Figure 7-4: Example of an infection report	133
Figure 8-1: Privacy Advisor	139
Figure 8-2: Privacy site list	140
Figure 9-1: Firewall alert.	153
Figure 9-2: New Program alert.	154
Figure 9-3: New Network alert.	155
Figure 9-4: ID Lock alert.	156
Figure 9-5: Medium-rated Suspicious Behavior alert	157
Figure 9-6: High-rated Suspicious Behavior alert	158
Figure 10-1: Transmission of myVAULT contents	173
Figure 10-2: Receipt of myVAULT contents	173
Figure 10-3: Trusted Sites list	178

Figure 12-1: Sending a voice transmission that is blocked	194
Figure 12-2: Blocking an incoming voice transmission	194
Figure 12-3: Sending an executable URL to a contact	195
Figure 12-4: Potentially harmful link removed.	195
Figure 12-5: Example of an encrypted conversation.	197
Figure 12-6: Example of an unencrypted conversation	197

Preface

- “About Zone Labs security software,” on page xiv
- “About this guide,” on page xv

About Zone Labs security software

Zone Labs security software is a family of security products that offers a wide range of features and benefits. This release supports the following versions of Zone Labs security software:

- **ZoneAlarm**

Offers firewall protection, limited MailSafe protection and Program Control, and Anti-virus Monitoring.

- **ZoneAlarm Anti-virus**

Includes the same features available in free ZoneAlarm, plus Anti-virus protection, Inbound and Outbound MailSafe protection, Program Control with SmartDefense Advisor, and OSFirewall protection.

- **ZoneAlarm Anti-Spyware**

Includes the same features available in free ZoneAlarm, plus Anti-spyware protection, Inbound and Outbound MailSafe Protection, Program Control with SmartDefense Advisor, and OSFirewall protection.

- **ZoneAlarm Pro**

Includes expert firewall protection, Inbound and Outbound MailSafe protection, Program Control with SmartDefense Advisor, Privacy control, Identity Protection, Anti-spyware protection, and OSFirewall protection.

- **ZoneAlarm Security Suite**




Includes the features available in ZoneAlarm Pro, plus IM Security, Parental Control, Identity Protection, Anti-virus protection, Junk E-mail Filtering, and offers protection for mobile laptop users and wireless home networks.

About this guide

This guide is intended for users of ZoneAlarm, ZoneAlarm Anti-virus, ZoneAlarm Pro, ZoneAlarm Anti-Spyware, and ZoneAlarm Security Suite. Throughout this guide, these products are collectively referred to as Zone Labs security software. In cases where a reference to a specific product is required, the product name is used.

Conventions

This guide uses the following formatting and graphics conventions.

Convention	Description
Bold	Used for user interface elements such as panels, tabs, fields, buttons, and menu options.
<i>Italic</i>	Used for file names and paths.
/	Used to separate panel and tab selections in procedures. Example: Select Overview Status , then click Add .
	Tip icon. Suggests alternative methods for accomplishing tasks or procedures.
	Note icon. Emphasizes related, reinforcing, or important information.
	Caution icon. Indicates actions or processes that can potentially damage data or programs.

Zone Labs User Forum

Connect with other users of Zone Labs security software. Ask questions, get answers, and see how fellow users get the most out of their Zone Labs security software. Visit: http://www.zonelabs.com/store/content/support/userForum/userForum_agreement.jsp

Chapter

Installation and setup

1

This chapter provides system requirements and instructions for installing, upgrading, configuring, and uninstalling Zone Labs security software.

Topics:

- “System requirements and supported software” on page 2
- “Installing Zone Labs security software” on page 4
- “Upgrading from a previous version” on page 6
- “Configuring basic options” on page 7
- “Uninstalling Zone Labs security software” on page 9

System requirements and supported software

This section lists hardware and software needed to run Zone Labs security software.

Hardware requirements and supported operating systems

The computer on which you install Zone Labs security software must have:

- One of the following operating systems and minimum RAM required:
 - Microsoft® Windows® XP, Home or Professional Edition, 128MB of RAM
 - Microsoft Windows 2000 Professional, 64MB of RAM
- 50MB of available hard-disk space
- Pentium® III 800Mhz or higher



The ideal resolution for Zone Labs security software is 1024 x 768 or higher. Some software screens might not display properly at resolutions of 800 x 600 or lower.

Supported protocols for e-mail protection

- HTTP (Junk e-mail filtering in conjunction with Outlook or Outlook Express)
- IMAP4 (Incoming only) - IMAP4 is not supported for virus scanning of e-mail.
- POP3 (Incoming only)
- SMTP (Outgoing only)

Supported browser software

- Internet Explorer 5.5, 6.0 SP1, 6.0 SP2
- Netscape Navigator 7.2, 8.1
- FireFox 1.00, 1.5
- Mozilla 1.4 and up
- MSN Explorer 6.0, 7.02
- AOL 9.0

Supported IM clients

- MSN 7.5.0299, 7.5.0324
- Windows Messenger 4.7.3001, 5.0.468, 5.1.0701
- Yahoo! IM 5.6.0.1351, 6.0.0.1643 - 6.0.0.1922, 7.0.0.xxx
- Yahoo! Japan IM 6.0.0.1703



Japan Yahoo IM does not support non-Japanese Yahoo's ID. Also, Japan IM uses a different process: *YPagerJ.exe*

- AOL Instant Messenger 5.9.x
- AOL9
- Triton (AIM) 1.0.4.1
- ICQ Pro 2003b (build 3916)
- ICQ Lite 5.04 build 2321, 5.1 build 3916
- Trillian Free (MSN/YIM/AIM/ICQ) 0.74i, 2.0.12 - 3.1
- Trillian Pro (MSN/YIM/AIM/ICQ) 2.0.12 - 3.1
- GAIM (MSN/YIM/AIM/ICQ) 1.0.0 - 1.5.0, 2.0.0 beta 3
- Miranda (MSN/YIM/ICQ) v0.4rc1, 0.4.0.3

Installing Zone Labs security software

The installation and setup process for Zone Labs security software involves installing the software files, running the configuration wizard to set basic protection options, and viewing the Tutorial.



If you have a previous version of Zone Labs security software installed, you may receive a security warning during installation. Click **OK** to dismiss these warnings before proceeding with installation.

Installing ZoneAlarm

Before you can begin the installation process, you must download ZoneAlarm from the Zone Labs Web site, then browse to the location on your computer where you saved the installation file.

1. Double-click the installation file you downloaded.

The installation program begins.

2. Either specify a location for the installation files, or click **Next** to continue.

The default location is *C:\Program Files\Zone Labs\ZoneAlarm*.

3. Type your name, company (optional), and e-mail address, then click **Next**.

4. Read and accept the license agreement, then click **Install**.

The installation program runs.

5. Click **Finish** to close the installation program.

6. Click **Yes** to start ZoneAlarm.

The License Wizard appears.

7. Select either the ZoneAlarm Pro trial or free ZoneAlarm, then click **Next**

When installing ZoneAlarm, you have the option to install a trial version of ZoneAlarm Pro, free for 15 days. During the trial period you will experience the advanced security protection available in ZoneAlarm Pro. At the end of the trial period, you can continue to use these advanced features by purchasing ZoneAlarm Pro, or you can revert to ZoneAlarm. When reverting to ZoneAlarm after the ZoneAlarm Pro trial, any custom settings you have created in ZoneAlarm Pro will be discarded.

Installing Zone Labs security software

Before you can begin the installation process, you will need to insert the Zone Labs security software CD into your CD-ROM drive, or if you downloaded the software from

the Zone Labs Web site, browse to the location on your computer where you saved the installation file.

To install Zone Labs security software:

1. Double-click the installation file.

The installation program begins.

2. Either specify a location for the installation files, or click **Next** to continue.

The default location is *C:\Program Files\Zone Labs\ZoneAlarm*.

3. Type your name, company (optional), and e-mail address, then click **Next**.

4. Read and accept the license agreement, then click **Install**.

5. Click **Finish** to close the installation program.

If you are upgrading from a previous version, you may be prompted to restart your computer to complete the installation process.

6. Click **OK** to restart your computer, or click **Cancel**.



If you click **Cancel**, remember to restart your computer later to complete the installation process.

Upgrading from a previous version

Zone Labs security software is designed for easy upgrade from version to version. In most cases, you do not need to uninstall your existing version before upgrading to version 6.5. However, if you are using any version of Integrity Client (for enterprise use only), you should first uninstall that product before upgrading.

Upgrading and the Windows XP SP2 Windows Firewall

If you are running Windows XP SP2 and upgrading to version 6.5, after upgrading you may need to manually turn the Windows XP SP2 Windows Firewall back on. In the Windows XP Help system, search for *firewall* to learn how to turn on the Windows XP Windows Firewall.

Upgrading and IMsecure myVault settings

If you are running the standalone version of IMsecure or IMsecure Pro and upgrading to ZoneAlarm Security Suite, the upgrade program has been designed for security reasons to not transfer Social Security, credit card, and Access PIN numbers.

Upgrading and MailFrontier settings

If you are running the standalone version of MailFrontier and upgrading to ZoneAlarm Security Suite, the upgrade process transfers your Address Book but other MailFrontier settings may be lost.

To upgrade from a previous version:

1. Double-click the installation file.

The installation program begins.

2. Select an upgrade option, then click **Next** to continue.

Upgrade	This option preserves your existing security settings and applies them to the new version. New features that are added during upgrade receive default settings.
Clean Install	This option discards your existing security settings and restores default settings.

Configuring basic options

After completing installation, you will see the Configuration Wizard. The Configuration Wizard appears only after installation and assists you in setting the basic Zone Labs security software options. You can use the Configuration Wizard to enable privacy protection, set new network detection behavior, specify alert settings, enable Anti-virus protection, and configure program permissions.

Configuring program access permissions

Zone Labs security software can configure many of the most popular programs in the following software categories:

- Instant Messaging programs
- Web browsers
- Microsoft Office
- E-mail
- Anti-virus
- Microsoft Windows processes
- Document utilities
- Zone Labs software applications

For more information about assigning permission to programs, see “Setting permissions for specific programs” on page 76.

Joining the DefenseNet community

Zone Labs security software users can help shape the future of Zone Labs security products by joining the DefenseNet community protection network and periodically sending anonymous configuration data to Zone Labs for analysis. By joining DefenseNet, you can help us focus our attention on the features and services that you use most often and to introduce new functionality that will provide even smarter security.

Configuration data is not collected from ZoneAlarm or ZoneAlarm Anti-virus users.



Even with the “Alert me before I make contact” preference selected in the **Overview|Preferences** tab, you will not be alerted before sending configuration data to Zone Labs.

The data collected is completely anonymous and is for Zone Labs internal use only and will not be shared with others. Of the millions of Zone Labs security software users, only a small percentage of users will have their information collected. The frequency of

data transmission depends upon the configuration of your computer. For most users, data will be sent once per day.

To send configuration data to Zone Labs, select **Yes, automatically and anonymously share my settings** in the Configuration Wizard.



If you later decide that you do not want to send anonymous data, select **Overview|Preferences**, in the Contact with Zone Labs area, then clear the **Share my settings anonymously...** check box.

Uninstalling Zone Labs security software

If you need to uninstall Zone Labs security software, run the uninstall program included with your installation rather than using the Windows Add/Remove Programs utility. This ensures that all traces of Zone Labs security software are removed from your computer.

You must be logged in as a user with administrator privileges in order to uninstall Zone Labs security software.



If you are upgrading, there is no need to uninstall your existing version. For more information, see “Installing Zone Labs security software” on page 4.

To uninstall Zone Labs security software:

1. Select **Start | Programs**.
2. Select **Zone Labs | Uninstall**.

The Uninstallation program begins.

Chapter

Zone Labs security software basics

2

This chapter provides an introduction to the main tools and concepts of Zone Labs security software.

Topics:

- “Tour of the Zone Labs security software Control Center,” on page 12
- “Understanding Zones,” on page 18
- “Responding to alerts,” on page 20
- “Setting product preferences,” on page 22
- “Licensing, registration, and support,” on page 27

Tour of the Zone Labs security software Control Center

The Zone Labs security software Control Center provides one-stop access to the security features that keep your computer safe. Zone Labs security software's major features are presented in a menu on the left side of the Control Center.

Getting around the Control Center

To move from feature to feature, first select the feature you want from the menu, then select the tab you want to view.

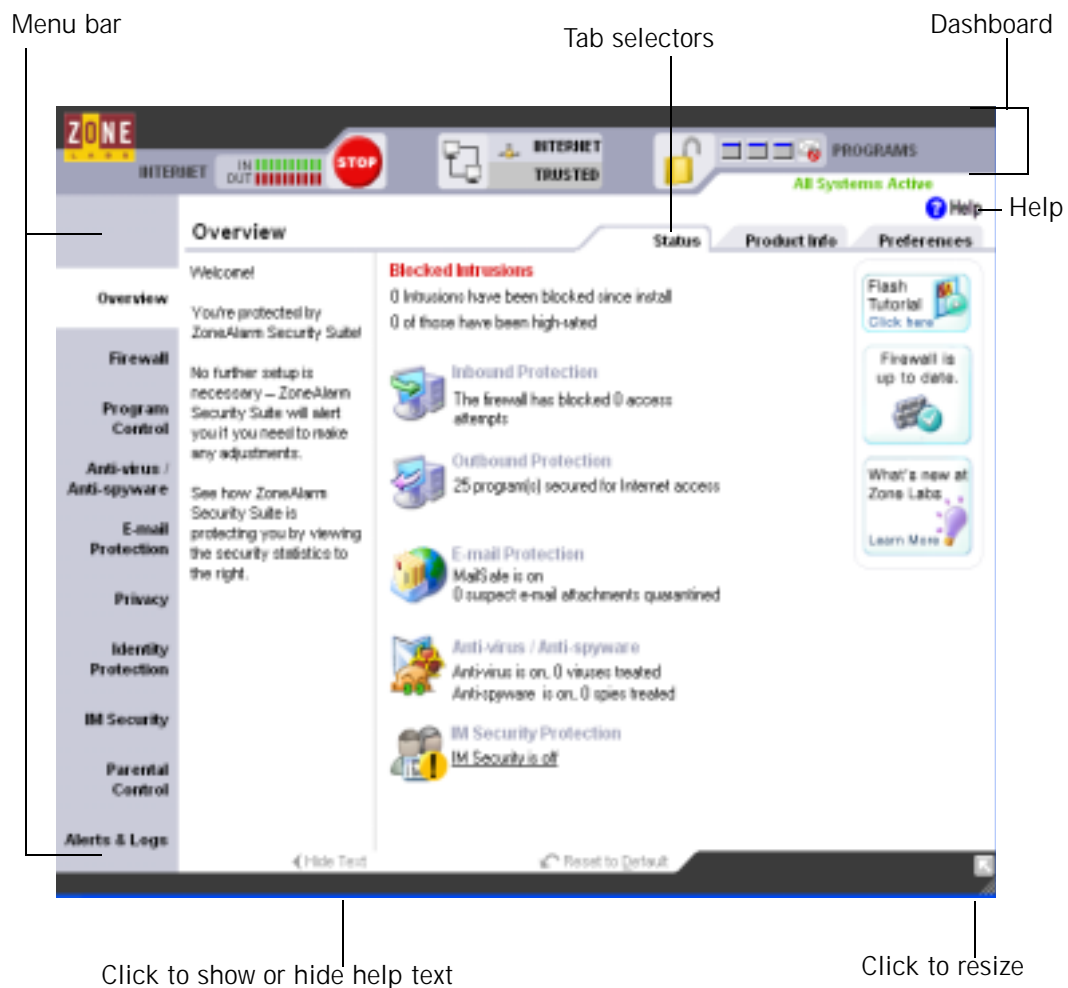


Figure 2-1: Zone Labs security software Control Center

Menu bar

The menu bar provides access to the available panels. The tools in each panel are arranged in two or more tabs.

Tab selectors

Click a tab selector to bring the tab you want to see to the top.

With the exception of the Overview panel, each panel in the Control Center has a Main tab and one or two other tabs. The Main tab contains the global controls for that panel.

Show /Hide Text

Click this link to show or hide instructional text for the selected tab. The text gives a brief explanation of the tab and its controls.

Help button

To get help with the controls on any panel, click the Help link in the upper-right corner. Zone Labs security software's online help system goes immediately to the help topic for the selected tab.

Using the dashboard

The dashboard provides constant access to basic security indicators and functions. The dashboard appears at the top of every panel.

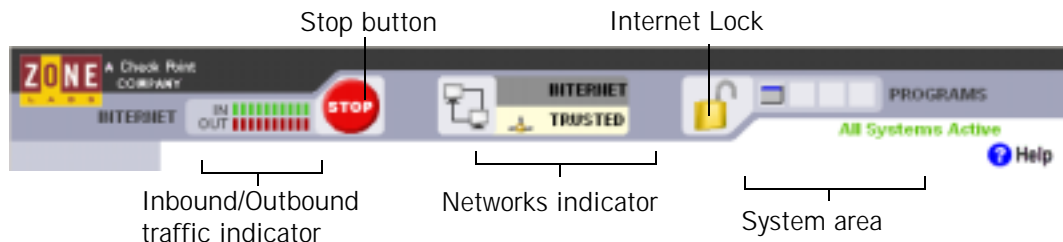


Figure 2-2: Zone Labs security software dashboard

Inbound/Outbound traffic indicator

The traffic indicator shows you when traffic leaves (red) or enters (green) your computer. This does not imply that the traffic is illegal or that any security problem has occurred.



Some applications access network resources in the background, so you may see network traffic occurring even when you aren't actively accessing the Internet.

Stop button

Click the Stop button to immediately block all network activity including Internet access. Clicking the Stop button on the dashboard instantly closes your computer to incoming and outgoing Internet traffic. Therefore, you should click the Stop button only if you believe your computer is under attack, otherwise, Zone Labs security software may block legitimate programs that require access, as well as *DHCP* (Dynamic Host Configuration Protocol) messages or ISP *heartbeat messages* used to maintain your Internet connection. To re-open access, click the **Stop** button again.

Internet Lock

The Internet Lock stops all traffic except traffic initiated by programs to which you have given *pass-lock* permission. Clicking the Internet Lock instantly blocks DHCP messages or ISP heartbeats used to maintain your Internet connection. As a result, you may lose your Internet connection. To reopen access, click the **Lock** button again.



You also can activate the Stop button and Internet Lock by right-clicking on the system tray icon and choosing either **Stop all Internet activity** or **Engage Internet Lock** from the shortcut menu.

Networks indicator

The networks indicator shows you when you have wired or wireless networks in either the Trusted Zone or Internet Zone.

Click the network symbol to go immediately to the Zones tab, where the settings for the network are stored.

Active Programs area

The active programs area displays the icons of programs that are currently open and that have accessed the Internet in your current session. To see information about a program displayed here, hover your mouse pointer over the icon.

The icon blinks when the program is sending or receiving data.

A hand symbol under the icon indicates that the program is active as server and is listening for connection requests.

System area

This area can display two messages.

■ All Systems Active

Indicates that Zone Labs security software is functioning normally.

■ Error Please Reboot

Indicates that you are not protected by Zone Labs security software because the underlying security process is not running. Restart your computer to allow Zone Labs security software to reset.

System Tray icons

The icons displayed in the system tray let you monitor your security status and Internet activity as frequently as you wish, and access your security settings in just a few clicks.









Icon	Description
	Zone Labs security software is installed and running.
	Your computer is sending (red band) or receiving (green band) network traffic. This does not imply that you have a security problem, or that the network traffic is dangerous.
	Zone Labs security software is running a spyware and/or virus scan. For details about scans, see "Performing a spyware scan," on page 104, or "Performing a virus scan," on page 99.
	Game Mode is activated, causing Zone Labs security software to suppress updates, scans, and most alerts. For details about this feature, see "Game Mode," on page 162.
	Zone Labs security software is receiving an update, such as an update of new spyware definitions or virus definitions.
	Zone Labs security software has blocked a communication, but your settings prevent a full-sized alert from being shown.
	(Yellow lock) The Internet Lock is engaged.
	(Red lock) The Stop button is engaged. You may also begin to see a lot of alerts.

Table 2-3: System Tray icons

Shortcut menu

Right-click any of the system tray icons to access a shortcut menu.

Engage Internet Lock

This menu option engages the Internet Lock and displays the yellow lock icon in the system tray. All Internet traffic initiated by programs without pass-lock permission is blocked. Provides the same function as clicking on the Internet Lock in the dashboard.

Stop All Internet Traffic

This menu option engages the Stop button and displays the red lock icon in the system tray. All Internet traffic is blocked. Provides the same function as clicking on the Stop button in the dashboard.

Game Mode / Stop Game Mode

The Game Mode option brings up the dialog that controls Game Mode. When activated, Game Mode causes Zone Labs security software to suppress updates, scans, and most alerts. Depending on your settings, Zone Labs security software will either deny or allow most program and network permission requests while Game Mode is active. You can use the Stop Game Mode option, which appears only while Game Mode

is active, to turn Game Mode off. For details about this feature, see “Game Mode,” on page 162.

Help

Displays help files.

View Scan

Displays the Scanning Status dialog box, which tracks the progress of spyware and virus scans. This menu option is available only during such scans.

About

Displays version information for the Zone Labs security software you have installed, including driver and engine information. If you are experiencing problems with your software you can copy this information to the clipboard and paste it into an e-mail to support.

Restore ...Control Center

Restores the Zone Labs security software Control Center to its full size. The label for this menu option reflects the version of Zone Labs security software you have installed (for example Zone Labs Anti-virus or ZoneAlarm Security Suite).

Shutdown...

Closes the Zone Labs security software application. The label for this menu option reflects the version of the Zone Labs security software you have installed (for example, Zone Labs Anti-virus or ZoneAlarm Security Suite).

Using the Status tab

The protection area of the Status tab tells you whether your security settings are enabled and provides a summary of security activity. From the Status tab you can:

- See at a glance if your computer is secure
- See a summary of Zone Labs security software’s activity
- See if your version of Zone Labs security software is up to date
- Access the product tutorial

To reset the alert counts in this area, click **Reset to Default** at the bottom of the panel.

Blocked intrusions

Shows you how many times the Zone Labs security software firewall and MailSafe have acted to protect you, and how many were *high-rated alerts*.

Inbound Protection

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

Outbound Protection

Indicates whether program control is configured safely and displays the number of program alerts that have occurred since the last reset. Zone Labs security software will warn you if program control is disabled.

Anti-virus Protection

Indicates whether your computer is protected against viruses and displays the number of viruses that have been treated to date. The Anti-virus Protection status only appears in ZoneAlarm Anti-virus and ZoneAlarm Security Suite. If you are using ZoneAlarm or ZoneAlarm Pro, you will see Anti-virus Monitoring status instead.

E-mail Protection area

Indicates whether MailSafe is enabled and displays the number of attachments that have been quarantined since the last reset. If a warning is displayed, click the underlined warning text to go immediately to the panel where you can adjust your settings.

Anti-virus / Anti-spyware

Indicates whether virus and spyware protection is enabled and displays the number of viruses and spies that have been treated.

IM Security Protection

Indicates whether Instant Messaging protection is enabled and displays the number of messages that have been scanned.

Update and tutorial information

When you purchase Zone Labs security software, you receive an automatic update subscription valid for one year.

The update box helps you make sure you're running the latest version of Zone Labs security software, and gives you quick access to product updates when they arrive.

Message	Meaning
"Check for update."	Click the link to see if there are any important updates to Zone Labs security software available for download.
"An update is available."	Your automatic update subscription indicates that an update to Zone Labs security software is available. Click the link to go to the Zone Labs Web site to download the update.
"Firewall is up to date"	You have the most up-to-date version of Zone Labs security software.
"Update subscription expired. Click to Renew."	Your automatic update subscription has expired. Click the link to go to the Zone Labs Web site to renew your subscription.

Table 2-4: Update messages

Click **Tutorial** to learn the basics of how Zone Labs security software works.

Understanding Zones

Zone Labs security software keeps track of the good, the bad, and the unknown out on the Internet by using virtual containers, called Zones, to classify the computers and networks that connect to your computer.

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

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

The *Blocked Zone* is the “bad.” It contains computers and networks you distrust.

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

To learn how to put a computer, network, or program in the Trusted Zone, see “Managing traffic sources,” on page 46.

Zones manage firewall security

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

High security setting

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

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

Medium security setting

Medium security places your computer in *component learning mode*, where Zone Labs security software quickly learn the MD5 signatures of many frequently used program components without interrupting your work with multiple alerts. Medium security is the default setting for the Trusted Zone.

In Medium security, file and printer sharing is enabled, and all ports and protocols are allowed. (If Medium security is applied to the Internet Zone, however, incoming NetBIOS traffic is blocked. This protects your computer from possible attacks aimed at your Windows networking services.) At Medium security, you are no longer in stealth mode.

We recommend that you use the Medium security setting for the first few days of normal Internet use after installing Zone Labs security software. After a few days of normal use, Zone Labs security software will have learned the signatures of the majority

of the components needed by your Internet-accessing programs, and will remind you to raise the Program Authentication level to High.

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



Advanced users can customize high and medium security for each Zone by blocking or opening specific ports. For more information, see “Blocking and unblocking ports,” on page 50.

Zones provide program control

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

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

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

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



Advanced users can specify the ports and protocols a particular program can use, the hosts it can access, and other details. For more information, see “Creating an expert rule for a Program,” on page 87.

Responding to alerts

When you first start using Zone Labs security software, it is not unusual to see a number of alerts. Don't worry! This doesn't mean you're under attack. It just means that Zone Labs security software is learning your program and network configurations, and giving you the opportunity to set up your security the way you want it.

How you respond to an alert depends upon the type of alert displayed. For information on responding to a particular type of alert, see Appendix A, "Alert reference," starting on page 203.

New Program alerts

The majority of the initial alerts you see will be New Program alerts. These alerts occur when a program on your computer requests access or server permission to the Internet or your local network. Use the New Program alert to give access permission to programs that need it—like your browser and e-mail program.



Use the check box labeled **Remember this answer** to give permanent permission to programs you trust.

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

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

If you do not recognize the program or process that is asking for server permission, search the Microsoft Support Web site (<http://support.microsoft.com/>) for information on the process to determine what it is and what it's used for. Be aware that many legitimate Windows processes, including those listed above, have the potential to be used by hackers to disguise worms and viruses, or to provide backdoor access to your system for Trojan horses. If you were not performing a function (such as browsing files, logging onto a network, or downloading files) when the alert appeared, then the safest approach is to deny server permission. At any time, you can assign permissions to specific programs and services from the Programs List, accessed by selecting **Program Control | Programs** tab.

To learn more about New Program alerts and how to respond to them, see "New Program alert," on page 210.

New Network and VPN alerts

The other initial alerts you may see are the New Network alert and VPN Configuration alerts. These occur when Zone Labs security software detects a network connection or VPN connection. They help you configure your Trusted Zone, port/protocol permission, and program permissions correctly so that you can work securely over your network. For details about these alerts and how to respond to them, see Appendix A, “Alert reference,” starting on page 203.

Setting product preferences

Use the Preferences tab to set or change your Zone Labs security software password, log in or log out, manage updates, set general options for the display of the Zone Labs security software Control Center, and configure privacy settings for communications with Zone Labs.

Setting update options

When you purchase Zone Labs security software you receive a year of free updates. You can check for updates manually, or set Zone Labs security software to check automatically.

To set check for update settings:

1. Select **Overview | Preferences**.
2. In the Check for Updates area, choose an update option.

Automatically	Zone Labs security software automatically notifies you when an update is available.
Manually	You monitor the Status tab for updates. To invoke an update check immediately, click Check for Update .

Setting your password

By setting a password, you prevent anyone but you from shutting down or uninstalling Zone Labs security software, or changing your security settings. Setting a password will not prevent other people from accessing the Internet from your computer.

The ability to create a password is not available in ZoneAlarm.

If your version of Zone Labs security software was installed by an administrator with an installation password, that administrator can access all functions.

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

To set or change a Zone Labs security software password:

1. Select **Overview | Preferences**.
2. Click **Set Password**.
3. Type your password and password verification in the fields provided.
4. Select **Allow others to use programs without a password (unless the program permission is set to "Block")** to allow others to use programs you haven't explicitly blocked, even if they don't have a password.

5. Click **OK**.



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

Once you have set a password, you must log in before you can change settings, shut down the TrueVector security engine, or uninstall Zone Labs security software.

Backing up and restoring security settings

You can back up your existing security settings to an XML file so that you can restore them later, should you need to.



The backup and restore feature should not be used to share settings among different computers or to distribute security policies. To do so could cause an extremely high number of alerts to appear due to differences among computers, applications, and Windows processes.

The ability to back up and restore settings is only available in ZoneAlarm Pro and ZoneAlarm Security Suite.

To back up security settings

1. Select **Overview | Preferences**.
2. In the Backup and Restore Security Settings area, click **Backup**.
3. Type a file name or select an existing file to overwrite.
4. Click **Save**.

To back up or restore security settings

1. Select **Overview | Preferences**.
2. In the Backup and Restore Security Settings area, click **Restore**.
3. Select the XML file which contains the settings you want to use.
4. Click **Open**.

Setting general product preferences

By default, Zone Labs security software starts automatically when you turn on your computer. Use the settings in the General area to change this and other options.

To set general display preferences:

1. Select **Overview | Preferences**.
2. In the General area, specify your preferences.

Load Zone Labs security software at startup	Zone Labs security software starts automatically when you turn on your computer.
Protect the Zone Labs security software client	Prevents Trojan horses from sending Keyboard and Mouse requests to Zone Labs security software. Note: To ensure maximum security, only disable this feature if you are having problems with your keyboard or mouse while using remote access programs.

3. In the General area, click **Options**.

The Options dialog box appears.

4. In the Display settings area, choose your display preferences.

Remember the last tab visited	Opens Zone Labs security software to the tab that you had open the last time you closed the Control Center.
Color-scheme	Allows you to change the default color scheme of the Control Center. Additional color choices are not available in ZoneAlarm.

5. In the Proxy Configuration area, enter the IP address of your proxy server information only if you are certain that it is necessary to do so.



Zone Labs security software automatically detects most proxy configurations, such as those configured through Internet Explorer, making it unnecessary to enter that information here. You should enter proxy information only if you have an uncommon proxy configuration, such as a scripted proxy, and if some product features such as anti-virus updates or instant messaging aren't working.

Setting contact preferences

Setting contact preferences ensures that your privacy is protected when Zone Labs security software communicates with Zone Labs (for example, to check automatically for updates).

To set contact preferences:

1. Select **Overview | Preferences**.

2. In the Contact with Zone Labs area, specify your preferences.

Alert me with a pop-up before I make contact	Displays a warning before contacting Zone Labs to deliver registration information, get product updates, research an alert, or access DNS to look up IP addresses. Note: There are certain situations in which you will not be notified before contact is made. Those include sending DefenseNet data to Zone Labs, contacting Zone Labs for program advice, when an anti-virus update is performed, or when monitoring your anti-virus status. The "Share setting anonymously..." setting below, turns off the DefenseNet transfer. All other settings can be disabled from the main tab of their respective panels.
Hide my IP address when applicable	Prevents your computer from being identified when you contact Zone Labs, LLC.
Hide the last octet of my IP address when applicable	Omits the last section of your IP address (for example, 123.456.789.XXX) when you contact Zone Labs, LLC.
Share my security settings anonymously with Zone Labs	Periodically sends anonymous configuration data to Zone Labs. For more information, see "Joining the DefenseNet community," on page 7. Note: Configuration data is not collected from ZoneAlarm or ZoneAlarm Anti-virus users.

Setting product display and proxy server options

You can use the Options dialog box to specify display setting options and proxy server information.

To set product display and proxy options:

1. Select **Overview | Preferences**.
2. In the **General** area, click **Options**.

The Options dialog box appears.

3. In the Display settings area, specify your preferences.

Remember the last tabs visited in the panels	Opens Zone Labs security software to the most recently viewed panel and tab the next time you open the Control Center.
Color-scheme	Allows you to change the default color scheme of the Control Center. Additional color choices are not available in ZoneAlarm.

4. Enter proxy server information, where necessary.

Zone Labs Security Software automatically detects most proxy configurations, such as those configured through Internet Explorer, making it unnecessary to enter that information here. You only need to enter your proxy information if you have an

uncommon proxy configuration, such as a scripted proxy, and if you find that some product features such as anti-virus updates aren't working.

Creating an online fraud protection profile

If you are an eBay user, you can protect yourself against online fraud by storing your online credentials in Zone Labs security software. Zone Labs security software protects your profile by making sure it is only sent to authorized eBay destinations.

To create your online protection profile in ZoneAlarm and ZoneAlarm Anti-virus:

1. Select **Overview | Preferences**.

2. In the eBay Protection Profile area, click **Password**.

The Alliance Partner Password dialog displays.

3. Select eBay from the Alliance Partner drop-down list.

4. Type your eBay password into the password and confirm fields, then click **OK**.

To enter your eBay password in ZoneAlarm Pro or ZoneAlarm Security Suite:

1. Select **ID Lock | myVAULT**, then click **Add**.

The Add information to myVAULT dialog appears.

2. Type a description of the item, then select **eBay password** from the category drop-down list.

3. Type your eBay password into the password and confirm fields, then click **OK**.

Asterisks will appear in place of the data you entered and an encrypted form of your eBay password will be stored in myVAULT. The original information is not stored on your computer.

4. Specify whether you want the information to be protected when using Web and E-mail.

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

For more information about how Zone Labs security software keeps passwords and other personal data safe, see Chapter 10, "Identity protection," starting on page 171.

Licensing, registration, and support

In order to receive support and updates for Zone Labs security software, you must have a valid license.

Updating your product license

If you have been using a trial or beta license key and have purchased a full license, or if your trial or beta is about to expire, you can purchase a full license from Zone Labs.

To purchase a license:

1. Select **Overview | Product Info**.
2. In the Licensing Information area, click **Buy Now!**

You will be directed to the Zone Labs Web site, where you can complete your product purchase.

To change your license key:

1. Select **Overview | Product Info**.
2. In the Licensing Information area, click **Change Lic**.
The License Information dialog appears.
3. In the space provided, either type or paste your license key.
4. Click **Apply**, then click **OK**.

Registering Zone Labs security software

Register Zone Labs security software to receive security news from Zone Labs.

To register Zone Labs security software:

1. Select **Overview | Product Info**.
2. In the Registration area, click **Change Reg**.
The Registration Information dialog appears.
3. Type your name, organization, and e-mail address in the fields provided.



The e-mail address you enter here is used to configure your Outbound MailSafe protection. Be sure to enter your e-mail address correctly. For more information, see "Setting Outbound MailSafe protection options," on page 121.

4. To be notified of product news and updates, select the check box labeled **Inform me of important updates and news**.
5. Click **OK**.

To change your registration information:

➤ Select **Overview|Prod Info**, then click **Change Reg.**

Accessing technical support

If you are eligible to receive technical support, you can access support resources, such as FAQs and known issues, directly from Zone Labs security software.

To access support resources:

1. Select **Overview | Prod Info**.

2. In the Support and Update Information area, click the **click here** link.

The Zone Labs Support Center Web site appears.

3. Click the **Support & Services** link, then select the product for which you need support.

Chapter

Networking with Zone Labs security software

3

If you're on a home network, business Local Area Network (LAN), or Virtual Private Network (VPN), or a wireless network, you want to ensure smooth communication with the network while still maintaining high security. The Network Configuration Wizard, automatic VPN configuration, and other features of Zone Labs security software help you to quickly set up your network environment.

Topics:

- “Configuring a new network connection,” on page 30
- “Integrating with network services,” on page 33
- “Configuring your VPN connection,” on page 35

Configuring a new network connection

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

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

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

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

🔒 Disabling the Wireless Network Configuration Wizard

Using the Network Configuration Wizard

When your computer connects to a new network, Zone Labs security software opens the Network Configuration Wizard, displaying the IP address of the detected network.

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

A private network is usually a home or business Local Area Network (LAN). Private networks are placed in the *Trusted Zone* by default.

A public network is usually a much larger network, such as that associated with an ISP. Public networks are placed in the *Internet Zone* by default.

To configure your network connection using the Network Configuration Wizard:

1. Choose the Zone you want this network in, then click **Next**.
2. Name the network. The name you enter here will be displayed in the Zones tab of the Firewall panel.




If you prefer not to use the Network Configuration Wizard, click Cancel in the Wizard screen. A New Network alert will appear. The detected network will be placed in the Internet Zone, even if it is a private network. For information on using the New Network alert, see “New Network alert,” on page 221.

Disabling the Network Configuration Wizard

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

To disable the Network Configuration Wizard:

-  In screen four of the Wizard, select the check box labeled **Do not show this Wizard the next time a new network is detected**, then click **Finish**.

Using the Wireless Network Configuration Wizard

When your computer connects to a new wireless network, Zone Labs security software opens the Wireless Network Configuration Wizard, then displays the IP address of the detected network.

The WEP (Wireless Encryption Protocol) setting on the wireless access point is used to determine whether it is a *secured* wireless network or an *unsecured* wireless network.

A secured wireless network is WEP enabled. WEP provides an initial barrier that can be easily penetrated by hackers. In order to truly secure the network, the wireless access point must have other features implemented, such as a limited access list or SSID (Service Set Identifier) broadcast disabled. Only place wireless networks that you know have a higher level of security and where you need to share resources or print in the *Trusted Zone*.

An unsecured wireless network may be completely unprotected and accessible by anyone. Unsecured networks are placed in the *Internet Zone* by default.

To configure a wireless connection:

1. Choose the Zone you want this network in, then click **Next**.
2. Name the network.

The name you enter in the Configuration Wizard displays in the Zones tab of the Firewall panel.




If you prefer not to use the Network Configuration Wizard, click Cancel in any Wizard screen. A New Network alert will appear. The detected network will be placed in the Internet Zone, even if it is a secured wireless network. For information on using the New Network alert, see "New Network alert," on page 221.

Disabling the Wireless Network Configuration Wizard

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

To disable the Wireless Network Configuration Wizard:

-  In screen four of the Wizard, select the check box labeled **Do not show this Wizard the next time a new network is detected**, then click **Finish**.

Integrating with network services

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

Enabling file and printer sharing

To share printers and files with other computers on your network, you will need to configure Zone Labs security software to allow access to the computers with which you plan to share resources.

To configure Zone Labs security software for file and printer sharing:

1. Add the network subnet (or, in a small network, the IP address of each computer you're sharing with) to your Trusted Zone.

See "Adding to the Trusted Zone," on page 47.

2. Set the Trusted Zone security level to Medium. This allows trusted computers to access your shared files.

See "Setting the security level for a Zone," on page 41.

3. Set Internet Zone security to High. This makes your computer invisible to non-trusted machines.

See "Setting the security level for a Zone," on page 41.

Connecting to network mail servers

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

Some mail servers, like Microsoft Exchange, include collaboration and synchronization features that might require you to trust the server in order for those services to work.

To configure Zone Labs security software for mail servers with collaboration and synchronization features:

1. Add the network subnet or IP address of the mail server to your Trusted Zone.
2. Set the Trusted Zone security level to Medium. This allows server collaboration features to work.
3. Set Internet Zone security level to High. This makes your computer invisible to non-trusted machines.

Enabling Internet Connection Sharing

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



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

Configuring your VPN connection

Zone Labs security software is compatible with many types of VPN client software and can automatically configure the connection for certain VPN clients.

Supported VPN protocols

Zone Labs security software monitors the VPN protocols listed in the table below.

Networking Protocol	Explanation and Comments
AH	Authentication Header Protocol
ESP	Encapsulating Security Payload protocol
GRE	Generic Routing Encapsulation protocol
IKE	Internet Key Exchange protocol
IPSec	IP Security protocol.
L2TP	Layer 2 Tunneling protocol. L2TP is a more secure variation of PPTP.
LDAP	Lightweight Directory Access protocol
PPTP	Point-to-Point Tunneling protocol
SKIP	Simple Key Management for Internet Protocol

Table 3-1: Supported VPN protocols

Configuring your VPN connection automatically

When VPN traffic is detected, an Automatic VPN Configuration alert is displayed. Depending upon the type of VPN activity detected, and whether Zone Labs security software was able to configure your VPN connection automatically, you may see one of three Automatic VPN Configuration alerts.

For detailed information about the types of Automatic VPN Configuration alerts you may see and how to respond to them, see “Automatic VPN Configuration alert,” on page 215.

For instance, manual action may be required if the loopback adaptor or the IP address of the VPN gateway falls within a range or subnet that you have blocked. For more information, see “Configuring your VPN connection manually,” on page 36.



If you have created an expert firewall rule that blocks VPN traffic, you will need to modify the expert rule to allow VPN traffic. See “Creating expert firewall rules,” on page 55.

Configuring your VPN connection manually

If your VPN connection cannot be configured automatically, Zone Labs security software displays a Manual Action Required alert informing you of the manual changes you need to make to configure your connection.

Refer to the following sections for manual configuration instructions:

- Adding a VPN gateway and other resources to the Trusted Zone
- Removing a VPN gateway from a blocked range or subnet
- Allowing VPN protocols
- Granting access permission to VPN software



If you have created an expert firewall rule that has blocked PPTP traffic and your VPN software uses PPTP, you will need to modify the expert rule. See “Creating expert firewall rules,” on page 55.

Adding a VPN gateway and other resources to the Trusted Zone

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

Required Resources	Other Resources
The resources below are required by all VPN client computers and must be added to the Trusted Zone.	The resources below may or may not be required, depending on your specific VPN implementation.
VPN Concentrator	DNS servers
Remote host computers connected to the VPN client (if not included in the subnet definitions for the corporate network)	Local host computer's NIC loopback address (depending on Windows version). If you specify a local host loopback address of 127.0.0.1, do not run proxy software on the local host.
Corporate Wide Area Network (WAN) subnets that will be accessed by the VPN client computer	Internet Gateway
Corporate LANs that will be accessed by the VPN computer	Local subnets
	Security servers (for example, RADIUS,ACE, or TACACS servers)

Table 3-2: Required VPN-related network resources

See “Adding to the Trusted Zone,” on page 47, to learn how to add resources to your computer’s Trusted Zone.

Removing a VPN gateway from a blocked range or subnet

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

To unblock an IP range or subnet:

1. Select **Firewall | Zones**.
2. In the Zone column, select the blocked IP range or subnet.
3. Select **Trusted** from the shortcut menu, then click **Apply**.

Allowing VPN protocols

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

To allow VPN protocols:

1. Select **Firewall | Main**, then click **Advanced**.

2. In the General settings area, select the check box labeled **Allow VPN protocols**.
3. Click **OK**.



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

Granting access permission to VPN software

Grant access permission to the VPN client and any other VPN-related programs.

To grant permission to your VPN program:

1. Select **Program Control | Programs**.
2. In the Programs column, select your VPN program.
3. In the Access column, click below Trusted, then select **Allow** from the shortcut menu.



If your VPN program is not listed, click **Add** to add it to the list.

To grant access to VPN-related components:

1. Select **Program Control | Components**.
2. In the Components column, select the VPN component for which you want to grant access.
3. In the Access column, select **Allow** from the shortcut menu.

If you are experiencing problems with your VPN connection, refer to the VPN troubleshooting tips in Appendix C, “Troubleshooting,” starting on page 233.

Chapter

Firewall protection

4

Firewall protection is your front line of defense against Internet threats. Zone Labs security software's default Zones and security levels give you immediate protection against the vast majority of threats. If you're an advanced user, custom port permissions and expert rules give you detailed control of traffic based on source, destination, port, protocol, and other factors.

Topics:

- "Understanding Firewall protection," on page 40
- "Choosing security levels," on page 41
- "Setting advanced security options," on page 42
- "Managing traffic sources," on page 46
- "Blocking and unblocking ports," on page 50
- "Understanding expert firewall rules," on page 53
- "Creating expert firewall rules," on page 55
- "Creating groups," on page 57
- "Managing Expert Firewall Rules," on page 61

Understanding Firewall protection

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

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

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

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

Choosing security levels

The default firewall *security levels* (High for the Internet Zone, Med. for the Trusted Zone) protect you from hacker activity (such as a *port scan*), while enabling you to share printers, files, and other resources with trusted computers on your local network. In most cases, you don't have to make any adjustment to these defaults. You're protected as soon as Zone Labs security software is installed!

Setting the security level for a Zone

Security levels make it easy to configure your firewall settings. You can apply a preconfigured security level (High, Medium, or Off) to each Zone, or you can specify the port and protocol restrictions for each level. See “Blocking and unblocking ports,” on page 50.

To set the security level for a Zone:

1. Select **Firewall | Main**.
2. In the Internet Zone Security area, click the slider and drag it to the desired setting.

High	Your computer is in stealth mode, making it invisible to other computers. Access to Windows <i>NetBIOS</i> (<i>Network Basic Input/Output System</i>) services, file and printer shares is blocked . Ports are blocked unless you have provided permission for a program to use them.
Med	Your computer is visible to other computers. Access to Windows services, file and printer shares is allowed . Program permissions are still enforced.
Off	Your computer is visible to other computers. Access to Windows services, file and printer shares is allowed . Program permissions are still enforced.

3. In the Trusted Zone Security area, click the slider and drag it to the desired area.

High	Your computer is in stealth mode, making it invisible to other computers. Access to Windows (NetBIOS) services, file and printer shares is blocked . Ports are blocked unless you have provided permission for a program to use them.
Med	Your computer is visible to other computers. Access to Windows services, file and printer shares is allowed . Program permissions are still enforced.
Off	Your computer is visible to other computers. Access to Windows services, file and printer shares is allowed . Program permissions are still enforced.

Setting advanced security options

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

Setting gateway security options

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

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

Setting ICS (Internet Connection Sharing) options

If you are using *ICS (Internet Connection Sharing)*, use these controls to configure Zone Labs security software to recognize the ICS gateway and clients.

To set Internet Connection Sharing preferences:

1. Select **Firewall | Main**.
2. Click **Advanced**.
3. In the Internet Connection Sharing area, choose your security settings.

This computer is not on an ICS/NAT network	Internet Connection sharing is disabled.
This is a client of an ICS/NAT gateway running Zone Labs security software	<p>Zone Labs security software automatically detects the IP address of the ICS gateway and displays it in the Gateway Address field. You also can type the IP address into the Gateway address field.</p> <p>Selecting Forward alerts from gateway to this computer will log and display alerts on the client computer that occur on the gateway.</p>
This computer is an ICS/NAT gateway	<p>Zone Labs security software automatically detects the IP address of the ICS gateway and displays it in the Local Address field. You also can type the IP address into the Gateway address field.</p> <p>Selecting Suppress alerts locally if forwarded to clients, will suppress alerts forwarded from the gateway to clients to also be displayed on the gateway.</p>

4. Click **OK**.

Setting general security options

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

To modify general security settings:

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

Block all fragments	Blocks all incomplete (fragmented) IP data packets. Hackers sometimes create fragmented packets to bypass or disrupt network devices that read packet headers. Caution: If you select this option, Zone Labs security software will silently block all fragmented packets without alerting you or creating a log entry. Do not select this option unless you are aware of how your online connection handles fragmented packets.
Block trusted servers	Prevents all programs on your computer from acting as servers to the Trusted Zone. Note that this setting overrides permissions granted in the Programs panel.
Block Internet servers	Prevents all programs on your computer from acting as servers to the Internet Zone. Note that this setting overrides permissions granted in the Programs panel.
Enable ARP protection	Blocks all incoming ARP (Address Resolution Protocol) requests except broadcast requests for the address of the target computer. Also blocks all incoming ARP replies except those in response to outgoing ARP requests.
Allow VPN Protocols	Allows the use of VPN protocols (ESP, AH, GRE, SKIP) even when High security is applied. With this option disabled, these protocols are allowed only at Medium security.
Allow uncommon protocols at high security	Allows the use of protocols other than ESP, AH, GRE, and SKIP, at High security.
Lock hosts file	Prevents your computer's hosts file from being modified by hackers through sprayer or Trojan horses. Because some legitimate programs need to modify your hosts file in order to function, this option is turned off by default.
Disable Windows Firewall	Detects and disables Windows Firewall. This option will only appear if you are using Windows XP with Service Pack 2.
Filter IP over 1394 traffic	Filters FireWire traffic.

4. Click **OK**.

Setting network security options

Automatic network detection helps you configure your Trusted Zone easily so that traditional local network activities such as file and printer sharing aren't interrupted. Zone Labs security software detects only networks that you are physically connected to. Routed or virtual network connections are not detected.

You can have Zone Labs security software silently include every detected network in the Trusted Zone; or ask you in each case whether to add a newly detected network.

To specify Network settings:

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

Include networks in the Trusted Zone upon detection	Automatically moves new networks into the Trusted Zone. This setting provides the least security.
Exclude networks from the Trusted Zone upon detection	Automatically blocks new networks from being added to the Trusted Zone and places them in the Internet Zone. This setting provides the most security.
Ask which Zone to place new networks in upon detection	Zone Labs security software displays a New Network alert or the Network Configuration Wizard, which give you the opportunity to specify the Zone.
Automatically put new unprotected wireless networks (WEP or WPA) in the Internet Zone	Puts unsecured wireless networks into the Internet Zone automatically, which prevents unauthorized access to your data from others accessing the network.

4. Click **OK**.

For more information about networking, see Chapter 3, "Networking with Zone Labs security software," starting on page 29.

Setting wireless network security options

Automatic wireless network detection helps you configure your Internet Zone to ensure that your computer remains secure without being interrupted each time a new wireless network is detected. Zone Labs security software detects only wireless networks that your computer is connected to. (Networks that you are not actually connected to may appear as available networks in your network neighborhood but the New Wireless Network Configuration Wizard only appears when you connect establish a connection to that network.)

You can have Zone Labs security software silently include every detected wireless network in the Internet Zone.

To specify Network settings:

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

Automatically put new unprotected wireless networks (WEP or WPA) in the Internet Zone	Zone Labs security software places new wireless networks in the Internet Zone when they are detected.
---	---

4. Click **OK**.

For more information about networking, see Chapter 3, “Networking with Zone Labs security software,” starting on page 29.

Managing traffic sources

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

Viewing the traffic source list

The traffic source list displays the traffic sources and the Zones they belong to. You can sort the list by any field by clicking the column header. The arrow (^) next to the header name indicates the sort order. Click the same header again to reverse the sort order.

Field	Description
Name	The name you assigned to this computer, site, or network
IP Address/Site	The IP address or host name of the traffic source
Entry Type	The type of traffic source: Network, Host, IP, Site, or Subnet
Zone	The Zone the traffic source is assigned to: Internet, Trusted, or Blocked

Table 4-1: Traffic source list fields

Modifying traffic sources

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

To change the Zone of a traffic source:

1. Select **Firewall | Zones**.
2. Locate the traffic source, then click in the **Zone** column.
3. Select a Zone from the shortcut menu, then click **Apply**.

To add, remove, or edit a traffic source:

1. Select **Firewall | Zones**.
2. In the Name column, click the traffic source, then click **Add**, **Edit**, or **Remove**.
3. Click **Apply**.

Adding to the Trusted Zone

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

To add a single IP address:

1. Select **Firewall | Zones**.
2. Click **Add**, then select **IP address** from the shortcut menu.

The Add IP Address dialog appears.

3. Select **Trusted** from the Zone drop-down list.
4. Type the IP address and a description in the boxes provided, then click **OK**.

To add an IP range:

1. Select **Firewall | Zones**.
2. Click **Add**, then select **IP address** from the shortcut menu.

The Add IP Range dialog appears.

3. Select **Trusted** from the Zone drop-down list.
4. Type the beginning IP address in the first field, and the ending IP address in the second field.
5. Type a description in the field provided, then click **OK**.

To add a subnet:

1. Select **Firewall | Zones**.
2. Click **Add**, then select **Subnet** from the shortcut menu.

The Add Subnet dialog appears.

3. Select **Trusted** from the Zone drop-down list.
4. Type the IP address in the first field, and the Subnet mask in the second field.
5. Type a description in the field provided, then click **OK**.

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

1. Select **Firewall | Zones**.
2. Click **Add**, then select **Host/Site**.

The Add Host/Site dialog appears.

3. Select **Trusted** from the Zones drop-down list.
4. Type the fully qualified host name in the **Host name** field.
5. Type a description of the host/site, then click **OK**.

To add a network to the Trusted Zone:

1. Select **Firewall | Zones**.
2. In the Zone column, click the row containing the network, then select **Trusted** from the shortcut menu.
3. Click **Apply**.



Zone Labs security software automatically detects new network connections and helps you add them to the right Zone. For more information, see Chapter 3, "Networking with Zone Labs security software," starting on page 29.

Adding to the Blocked Zone

To add to the Blocked Zone, follow the instructions for adding to the Trusted Zone, but select **Blocked** from the drop-down list in step 2.

Viewing logged Firewall events

By default, all Firewall events are recorded in the Log Viewer.

To view logged firewall events:

1. Select **Alerts & Logs | Log Viewer**.
2. Select **Firewall**, from the Alert Type drop-down list.

Table 5-2 provides an explanation the log viewer fields available for Firewall events.

Field	Information
Rating	Each alert is high-rated or medium-rated. High-rated alerts are those likely to have been caused by hacker activity. Medium-rated alerts are likely to have been caused by unwanted but harmless network traffic.
Date/Time	The date and time the alert occurred.
Type	The type of alert: Firewall, Program, ID Lock, or Lock Enabled.
Protocol	The communications protocol used by the traffic that caused the alert.

Table 4-2: Firewall event log fields

Field	Information
Program	The name of the program attempting to send or receive data. (Applies only to Program and ID Lock alerts).
Source IP	The IP address of the computer that sent the traffic that Zone Labs security software blocked.
Destination IP	The address of the computer the blocked traffic was sent to.
Direction	The direction of the blocked traffic. "Incoming" means the traffic was sent to your computer. "Outgoing" means the traffic was sent from your computer.
Action Taken	How the traffic was handled by Zone Labs security software.
Count	The number of times an alert of the same type, with the same source, destination, and protocol, occurred during a single session.
Source DNS	The domain name of the sender of the traffic that caused the alert.
Destination DNS	The domain name of the intended addressee of the traffic that caused the alert.

Table 4-2: Firewall event log fields

Blocking and unblocking ports

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

Default port permission settings

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

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

Traffic Type	Security levels		
	HIGH	MED	OFF
DNS outgoing	block	n/a	allow
DHCP outgoing	block	n/a	allow
broadcast/multicast	allow	allow	allow
ICMP			
incoming (ping echo)	block	allow	allow
incoming (other)	block	allow	allow
outgoing (ping echo)	block	allow	allow
outgoing (other)	block	allow	allow
IGMP			
incoming	block	allow	allow
outgoing	block	allow	allow
NetBIOS			
incoming	n/a	block	allow
outgoing	n/a	allow	allow
UDP (ports not in use by a permitted program)			
incoming	block	allow	allow
outgoing	block	allow	allow
TCP (ports not in use by a permitted program)			

Table 4-3: Default access permissions for incoming and outgoing traffic types

Traffic Type	Security levels		
	HIGH	MED	OFF
incoming	block	allow	allow
outgoing	block	allow	allow

Table 4-3: Default access permissions for incoming and outgoing traffic types

To change a port's access permission:

1. Select **Firewall | Main**.
2. In either the Internet Zone Security or the Trusted Zone Security area, click **Custom**.
The Custom Firewall Settings dialog appears.
3. Scroll to locate High and Medium security settings.
4. To block or to allow a specific port or protocol, click the check box beside it.



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

5. Click **Apply**, then click **OK**.

Adding custom ports

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

To specify additional ports:

1. Select **Firewall | Main**.

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

The Custom Firewall settings dialog appears.

Trusted Zone Internet Zone

Use this page to set custom security levels for the Internet Zone. Medium security allows all network traffic except traffic indicated by a check mark.

- Block other incoming ICMP
- Block outgoing ping (ICMP Echo)
- Block other outgoing ICMP
- Block incoming IGMP
- Block outgoing IGMP
- Block incoming UDP ports: (none selected)
- Block outgoing UDP ports: (none selected)
- Block incoming TCP ports: (none selected)
- Block outgoing TCP ports: (none selected)

Enter port numbers and/or port ranges separated by commas.
For example: 139,200-300

Ports:

Reset to Default OK Cancel Apply

Select one of these options, then specify the port number in the field that appears.

3. Scroll to the security level (High or Medium) to which you want to add ports.
4. Select the desired port type: incoming UDP, outgoing UDP, incoming TCP, or outgoing TCP.
5. Type the port or port ranges you want to allow or block in the Ports field, separated by commas. For example, 139, 200-300
6. Click **Apply**, then click **OK**.

Understanding expert firewall rules

Expert firewall rules are intended for users experienced with firewall security and networking protocols.

Expert rules do not take the place of other rules. They are an integral part of the multiple layer security approach and work in addition to other firewall rules.

Expert rules use four attributes to filter packets:

- Source and/or destination IP address
- Source and/or destination port number
- Network protocol/message type
- Day and Time

Source and destination addresses can be specified in a number of formats, including a single IP network address, a range of IP addresses, a subnet description, a gateway address, or a domain name.

Source and destination ports are used only for network protocols that use ports, such as UDP and TCP/IP. ICMP and IGMP messages, for example, do not use the port information.

Network protocols can be selected from a list of common IP or VPN protocols, or specified as an IP protocol number. For ICMP, the message type can also be specified.

Day and Time ranges can be applied to a rule to restrict access based on the day of the week and the time of day.

How expert firewall rules are enforced

It is important to understand how expert rules are enforced in combination with Zone rules, program permissions, and other expert rules.

Expert rules and Zone rules

Expert firewall rules are enforced before Zone firewall rules. That is, if a packet matches an expert rule, that rule is enforced, and Zone Labs security software skips evaluation of Zone rules.

Example: Imagine you have your Trusted Zone security level set to Medium. This allows outgoing NetBIOS traffic. However, you have also created an expert rule that blocks all NetBIOS traffic between the hours of 5PM and 7AM. Any outbound NetBIOS traffic during those hours will be blocked, in spite of the Trusted Zone setting.

Expert firewall rules and program permissions

Expert rules and Zone rules together are enforced in tandem with Program permissions. That is, if either your program permissions or Zone rules/expert firewall

rules determine that traffic should be blocked, it is blocked. Note that this means that you can use firewall rules to override or redefine program permissions.



Note that packets coming from the Blocked Zone will not be blocked if they are allowed by an Expert Firewall Rule.

Expert firewall rule enforcement rank

Within the realm of firewall rules, rule evaluation order becomes a factor. Zone Labs security software first checks expert firewall rules. If a match is found and a rule is enforced, the communication is marked as either blocked or allowed, and Zone Labs security software skips evaluation of Zone rules. If no expert firewall rule is matched, Zone Labs security software checks Zone rules to see if the communication should be blocked.

The enforcement rank of expert firewall rules is also important. Each rule has a unique rank number, and rules are evaluated in order of rank. Only the first rule that matches is executed. Consider these two rules:

			Name	Source	Destination	Protocol	Time	Conn
1			FTP Allow	My Computer	Trusted Zone	FTP	Any	
2			FTP Block	My Computer	Any	FTP	Any	

Figure 4-4: Expert firewall rule rank order

Rule 1 allows FTP clients in the Trusted Zone to connect to an FTP server on port 21. Rule 2 blocks all FTP clients from connecting on port 21, regardless of Zone. These two rules together allow clients in the Trusted Zone to use an FTP server on the client computer, but block all other FTP access.

If the order of the rules were reversed, Rule 2 would match first, and all FTP access would be blocked. Rule 1 would never have a chance to execute, so the FTP clients in the Trusted Zone would still be blocked.

Creating expert firewall rules

Creating expert firewall rules involves specifying the source or destination of the network traffic to which the rule applies, setting tracking options, and specifying the action of the rule: whether to block or to allow traffic that meets the specifications of the rule. You can create new rules from scratch, or you can copy an existing rule and modify its properties.

To create a new expert firewall rule:

1. Select **Firewall | Expert**, then click **Add**.

The Add rule dialog appears.

2. In the General area, specify the rule settings.

Rank	The order in which rules will be enforced. A rule with a rank of 1 is enforced first.
Name	Provide a descriptive name for the rule.
State	Specify whether the rule is enabled or disabled.
Action	Indicates whether to block or allow traffic that matches this rule.
Track	Indicates whether to log, alert and log, or do nothing when the expert rule is enforced.
Comments	Optional field for entering notes about the expert rule.

3. In the Source area, select a location from the list, or click **Modify**, then select **Add location** from the shortcut menu. You can add any number of sources to a rule.

My Computer	Applies the expert rule to traffic originating on your computer.
Trusted Zone	Applies the expert rule to network traffic from sources in your Trusted Zone.
Internet Zone	Applies the expert rule to network traffic from sources in your Internet Zone.
All	Applies the expert rule to network traffic coming from any source.
Host/Site	Applies the expert rule to network traffic coming from specified domain name.
IP Address	Applies the expert rule to network traffic coming from specified IP address.
IP Range	Applies the expert rule to network traffic coming from a computer within the specified IP range.
Subnet	Applies the expert rule to network traffic coming from a computer within the specified subnet.
Gateway	Applies the expert rule to network traffic coming from a computer on the specified gateway.
New Group	Choose this option, then click Add to create a new location group to apply to the expert rule.

Existing Group	Choose this option to select one or more location groups to apply to the expert rule, then click OK .
----------------	--

4. In the Destination area, select a location from the list, or click **Modify**, then select **Add location** from the shortcut menu.

Available location types are the same for Source and Destination locations.

5. In the Protocol area, select a protocol from the list, or click **Modify**, then select **Add Protocol**.

Add Protocol	Choose this option to add a protocol to the rule. Specify: TCP, UDP, TCP + UDP, ICMP, IGMP, or Custom.
New Group	Choose this option, then click Add to create a new protocol group to apply to the expert rule.
Existing Group	Choose this option to select one or more protocol groups to apply to the expert rule, then click OK .

6. In the Time area, select a time from the list, or click **Modify**, then select **Add Time**.

Day/Time Range	Choose this option to add a day/time range to the rule. Specify a description, time range and one or more days. Time range is specified using a 24 hour clock.
New Group	Choose this option, then click Add to create a new day/time group to apply to the expert rule.
Existing Group	Choose this option to select one or more day/time groups to apply to the expert rule, then click OK .

7. Click **OK**.

To create a new rule from an existing rule:

1. Select **Firewall | Expert**.
2. Select the expert firewall rule you want to duplicate, then either press **Ctrl+C** or right-click the rule and choose **Copy**.
3. Paste the copied rule either by pressing **Ctrl+V**, or by right-clicking and choosing **Paste**.



If a rule is currently selected in the list, the pasted rule will be inserted above the selected rule. If no rule is selected, the pasted rule will be inserted at the top of the rules list.

A "1" is appended to the name of the copied rule. If you paste a rule a second time, the number 2 is appended to the second rule copied.

4. Click **Apply** to save your changes.
5. Right-click the new rule and choose **Edit** to modify the rule properties as necessary.

Creating groups

Use groups to simplify the management of locations, protocols, and days/times that you use in your expert firewall rules.

Creating a location group

Use location groups to combine non-contiguous IP addresses and ranges, or different types of locations (for example, subnets and hosts), into an easily manageable set. You can then easily add that set of locations to any expert firewall rule.

To create a location group:

1. Select **Firewall | Expert**, then click **Groups**.

The Group Manager dialog appears.

2. Select the **Locations** tab, then click **Add**.

The Add Location Group dialog appears.

3. Specify the name and description of the location group, then click **Add** and select a Location type from the menu.

Host/Site	A description and host name of the Host/Site location, then click OK . Do not include http:// in the host name. Click Lookup to preview the site's IP address.
IP Address	A description and IP address of the IP Address location, then click OK .
IP Range	A description and beginning IP address and ending IP address of the IP Range location, then click OK .
Subnet	Specify a description, IP address, and Subnet Mask of the Subnet location, then click OK .
Gateway	Specify an IP address, MAC Address, and description of the Gateway location, then click OK .

4. Click **OK** to close the Group Manager dialog box.



Once created, the names of groups cannot be changed. For example, if you create a Location Group named "Home" and subsequently decide to call the group "Work", you would need to remove the group called "Home" and create a new group with the name "Work."

Creating a protocol group

Create a protocol group to combine well-known TCP/UDP ports, protocols, and protocol-specific message types (for example, ICMP message types), into sets that you

can easily add to expert rules. For example, you might create a group including POP3 and IMAP4 protocols in order to simplify the administration of your rules regarding e-mail traffic.

To create a Protocol group:

1. Select **Firewall | Expert**, then click **Groups**.

The Group Manager dialog appears.

2. Select the **Protocols** tab, then click **Add**.

The Add Protocol Group dialog appears.

3. Specify the name and description of the Protocols group, then click **Add**.

The Add Protocol dialog appears.

4. Select a protocol type from the Protocol drop-down list.

- TCP
- UDP
- TCP + UDP
- ICMP
- IGMP
- Custom

5. If you chose TCP, UDP, or TCP/UDP, in step 4, specify a destination, source and port number.

Name	Port number
FTP	21
Telnet	23
POP3	110
NNTP	119
NetBIOS Name	137
NetBIOS Datagram	138
NetBIOS Session	139
IMAP4	143
HTTPS	443
RTSP	554
Windows Media	1755
AOL	5190
Real Networks	7070

Other	Specify port number
FTP Data	20
TFTP	69
HTTP	80
DHCP	67
DHCP Client	68
SMTP	25
DNS	53

6. If you chose ICMP in step 4, specify a description, message name, and type number.

Message name	Type number
Source Quench	4
Redirect	5
Alt	6
Echo Request	8
Router Advertisement	9
Router Solicitation	10
Time Exceeded	11
Parameter Problem	12
Timestamp	13
Timestamp reply	14
Information request	15
Information reply	16
Address Mask Request	17
Address Mask Reply	18
Traceroute	30
Other	Specify type number

7. If you chose IGMP in step 4, specify a description, message name, and type number.

Membership Query	17
Membership Report (ver 1)	18
Cisco Trace	21
Membership Report (ver 2)	22
Leave Group (ver 2)	23
Multicast Traceroute Response	30

Multicast Traceroute	31
Membership Report (ver 3)	34
Other	Specify type number.

- 8.** If you chose **Custom** in step 4, specify a description, protocol type, and protocol number.

RDP	27
GRE	47
ESP	50
AH	51
SKIP	57
Other	Specify protocol number.

- 9.** Click **OK**, to close the Add Protocol dialog.

Creating a day/time group

To allow or block network traffic to or from your computer during specified periods of time, you can create a day/time group and then add it to an expert rule. For example, to block traffic coming from pop-up ad servers during business hours, you could create a group that blocks HTTP traffic coming from a specified domain during the hours of 9 AM and 5 PM, Monday through Friday.

To create a Day/Time group:

1. Select **Firewall | Expert**, then click **Groups**.

The Group Manager dialog appears.

2. Select the **Times** tab, then click **Add**.

The Add Time Group dialog appears.

3. Specify the name and description of the Time group, then click **Add**.

The Add Time dialog appears.

4. Specify a description of the time, then select a time and day range.

5. Click **OK**, then click **OK** to close the Group Manager.

Managing Expert Firewall Rules

From the Expert tab of the Firewall panel, you can view the status of existing expert rules, enable or disable rules, edit or remove rules, add new rules, change the order of rules, and create groups.

Viewing the Expert Rules list

The Expert Rules tab presents a list of all expert firewall rules. Rules are listed in order of enforcement priority (rank). The arrow buttons on the right-hand side move selected rules up and down the list, changing the enforcement order of the selected rules.

You also can change rank order of rules by dragging and dropping rules from one position to another.

For example, dragging and dropping rule 2 to the top of the list changes the rank of that rule to 1.

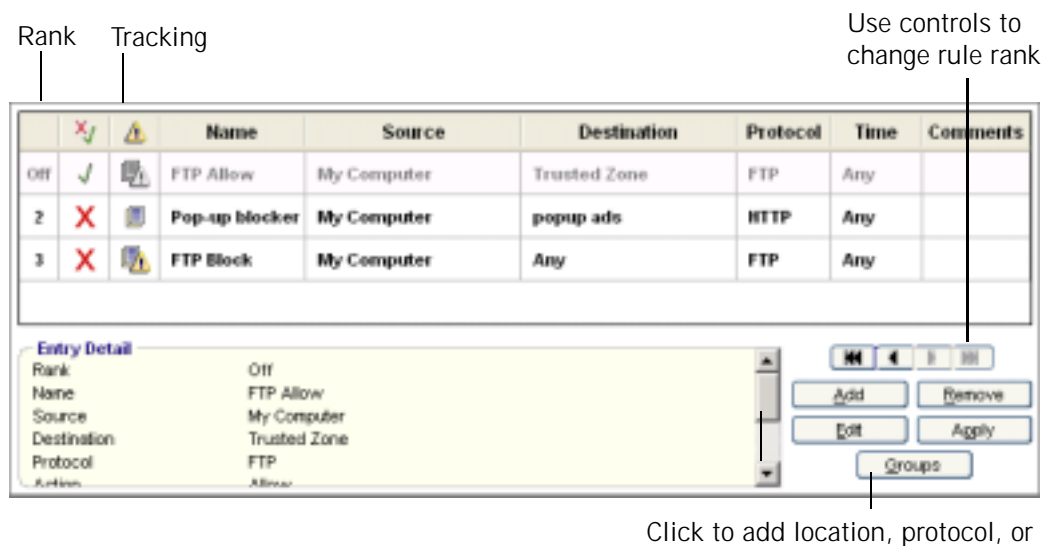


Figure 4-5: Expert Rules list

Rank

The enforcement priority of the rule. Rules are evaluated in order of rank, starting with number 1, and the first rule that matches will be enforced. Disabled rules will display “Off” instead of a rank number, but will retain their rank ordering in the list.

Action

A red ✗ means the rule will block network traffic; a green check mark ✓ means the rule will allow network traffic.

Track

None means no notification when the rule is applied. Log (📄) means a log entry will be created when the rule is applied. Alert and Log (📄🚨) means that an alert will be displayed and a log entry will be created when an expert rule is applied.

Name

A descriptive name for the rule.

Source

The source addresses and ports for the rule.

Destination

The destination addresses and ports for the rule.

Protocol

The network protocol to which the rule applies.

Time

The time period during which the rule is active.

Editing and re-ranking rules

You can edit or reorder existing expert rule from the Expert Rules list by selecting rules and dragging them into the desired rank. Note that if you have copied an expert rule into the rules for a Program, changing the expert rule does not automatically change the Program rule. For more information, see “Creating expert rules for programs,” on page 87.

To edit a rule:

1. Select **Firewall | Expert**.
2. Select the rule you want to edit, then click **Edit**.
The Edit Rule dialog appears.
3. Modify rule attributes as necessary, then click **OK**.

To change the rank of a rule:

1. Select **Firewall | Expert**.
2. Right-click the rule you want to move, then select **Move Rule**.

Move to Top	Moves the selected rule to the top of the Rules list.
Move to Bottom	Moves the selected rule to the bottom of the Rules list.
Move Up	Moves the selected rule one row up in the Rules list.
Move Down	Moves the selected rule one row down in the Rules list.

Chapter

Program control

5

Program Control protects you by making sure that only programs you trust can access the Internet or perform certain actions on your computer. You can assign program permissions manually or let Zone Labs security software assign permissions when program advice is available. Advanced users can control the ports that each program is permitted to use.

ZoneAlarm Security Suite includes the added protection of the Triple Defense Firewall, which prevents even trusted programs from carrying out potentially malicious behavior.

Topics:

- “Understanding Program Control,” on page 64
- “Setting general program control options,” on page 67
- “Configuring advanced program settings,” on page 74
- “Setting permissions for specific programs,” on page 76
- “Managing program components,” on page 85
- “Creating expert rules for programs,” on page 87

Understanding Program Control

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

Hackers exploit this fact by planting “malware”—literally, malicious software—on your computer. Malware can masquerade as harmless e-mail attachments or as updates to legitimate programs. Once on your computer, however, the malware can hijack trusted programs and carry out malicious activities under the guise of legitimacy.

Zone Labs security software protects your computer from hackers and malicious attacks by assigning policies to programs that indicate their level of trustworthiness, and specify the actions they are allowed to perform.

ZoneAlarm Security Suite provides the added feature of OSFirewall protection, which detects when programs try to use your operating system to perform suspicious actions on your computer.

Setting program permissions automatically

The SmartDefense Advisor and Program Control settings work together to ensure that good programs are given access and that bad programs are denied access. By default, Program Control is set to Medium and SmartDefense Advisor is set to Auto. With these defaults, Zone Labs security software assigns permission to programs automatically. For information about customizing Program Control and SmartDefense Advisor, see “Setting general program control options,” on page 67.

If SmartDefense Advisor and Program Control are set to their defaults, one of three things may occur when a program requests access for the first time:

- Access is granted - Access is granted if the program is known to be safe and requires the permissions it is asking for in order to function properly.
- Access is denied - Access is denied if the program is a known bad program or if the program does not require the permissions it is asking for.
- A New Program alert appears - Program alerts appear when you need to decide whether to allow or deny access to a program. The alert may contain a recommendation about whether to allow or deny access, and, if necessary, you can click **More info** to get details about the program to help you respond.

As long as SmartDefense Advisor is set to Auto, Zone Labs security software issues Program alerts only if no automatic setting is available. If you choose **Remember this setting** in a Program alert when allowing or denying program access, Zone Labs security software keeps your setting unless SmartDefense Advisor comes out with a different setting, or until you change the setting manually in the Programs tab. If you do not choose **Remember this setting**, Zone Labs security software will issue another Program alert the next time the program attempts the same action. For more information about Program alerts, see “Program alerts,” on page 209

Safe programs

Zone Labs security software validates your programs against a database of known safe programs and automatically assigns the permissions required for the programs to function properly. If you accepted the default program settings in the Configuration Wizard, Zone Labs security software is set up to automatically configure the most popular programs in the following general categories:

- Browsers (e.g., Internet Explorer, Netscape)
- E-mail applications (e.g., Microsoft Outlook, Eudora)
- Instant Messengers (e.g., AOL, Yahoo!)
- Anti-virus (e.g., Symantec, Zone Labs)
- Document utilities (e.g., WinZip[®] and Adobe[®] Acrobat[®])
- Zone Labs software applications

Even programs that are considered safe can be used by hackers to perform actions that are not. OSFirewall protection, available in ZoneAlarm Security Suite, displays alerts when it detects suspicious program behavior. For more information about these alerts, see “Program alerts,” on page 209.

Setting program permissions manually

If you want to assign permissions to programs on your own, or if Zone Labs security software was unable to assign permissions automatically, you can set permissions manually by using Program alerts, or by setting permissions for specific programs on the Programs tab of the Program panel.

Program alerts

When a program requests access for the first time, a New Program alert asks you if you want to grant the program access permission. When a program is detected to be listening to the ports on your computer, a Server Program alert is displayed.

Suspicious behavior alerts inform you that a trusted or unknown program on your computer is trying to perform an action that could be considered suspicious. For a list of actions that are considered suspicious, see “Program behavior,” on page 251.

To avoid seeing numerous alerts for the same program, select **Remember this setting** before clicking **Allow** or **Deny**. Zone Labs security software will continue to apply your Allow or Deny setting (without issuing alerts) unless you set SmartDefense Advisor to Auto and it has a setting different from yours.

Because Trojan horses and other types of malware often need server rights in order to do mischief, you should be particularly careful to give server permission only to programs that you know and trust, and that need server permission to operate properly. Several common types of applications, such as chat programs, e-mail clients, and Internet Call Waiting programs, may need server permission to operate properly. Grant

server permission only to programs you're sure you trust, and that require it in order to work.

If possible, avoid granting a program server permission for the Internet Zone. If you need to accept incoming connections from only a small number of machines, add those machines to the Trusted Zone, and then allow the program server permission for the Trusted Zone only.

For more information about program alerts, see “Program alerts,” on page 209.



You also can allow Zone Labs security software to automatically allow or deny all new programs without displaying an alert. For example, if you are sure you have given access permission to all the programs you want, you might automatically deny access to any other program that asks for permission. For more information, see “Setting access permissions for new programs,” on page 74.

Programs list

The Programs list allows you to set or customize permissions for specific programs based on your individual needs. For more information about using the Programs list and customizing permissions, see “Using the programs list,” on page 76.

Setting general program control options

When you're using Zone Labs security software, no program on your computer can access the Internet or your local network, or act as a server, unless it has permission to do so.

Setting the program control level

Zone Labs security software offers several methods of program control. Basic program control lets you determine access and server rights for individual programs. Advanced Program Control prevents malware from misusing trusted programs. Application Interaction Control alerts you if a process tries to use another process or a program tries to start another program. OSFirewall protection detects when programs try to use your operating system to perform suspicious actions on your computer. (This section explains how to set a general program control level, and how to customize settings for Advanced Application Control and Application Interaction Control. For details on OSFirewall, see "Configuring OSFirewall protection," on page 68.)

To limit the number of alerts you see and to benefit from Zone Labs' recommended program settings, use SmartDefense Advisor in conjunction with program control. For details on SmartDefense Advisor, see "Setting the SmartDefense Advisor level," on page 69.

To set the program control level:

1. Select **Program Control | Main**.
2. In the Program Control area, click the slider and drag it to the desired setting.

High	<p>With this setting, you may see a large number of alerts.</p> <ul style="list-style-type: none"> ◆ Programs must ask for Internet access and server rights. ◆ OSFirewall will monitor for suspicious behaviors. ◆ Advanced Program control and Application Interaction Control are enabled. ◆ By default, component control is disabled.*
Medium	<p>This is the default setting.</p> <ul style="list-style-type: none"> ◆ Programs must ask for Internet access and server rights. ◆ OSFirewall will monitor for suspicious behaviors. ◆ By default, component control is disabled.*
Low	<ul style="list-style-type: none"> ◆ Program control is in learning mode (no alerts are displayed). ◆ OSFirewall is disabled. ◆ By default, component control is disabled.*

Off	<p>Program control is disabled.</p> <ul style="list-style-type: none"> ◆ No programs or components are authenticated or learned. ◆ No program permissions are enforced. ◆ All programs are allowed access/server rights. ◆ All programs are allowed to perform suspicious behavior. ◆ No program alerts are displayed.
-----	---

* Component control is disabled by default. If you have turned component control on, it will remain enabled as long as program control is set to High, Medium, or Low. For information about component control, including directions for turning it on, see “Enabling Component Control,” on page 69.

To set custom program control options:

1. Select **Program Control | **Main**.**

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

The Custom Program Control Settings dialog appears.

3. On the Program Control tab, specify the settings to apply.

Enable Advanced Program Control	Prevents trusted programs from being used by untrusted programs to circumvent outbound protection.
Enable Application Interaction Control	Alerts you when a process attempts to use another process or any time a program launches another program.

4. Click **OK.**

Configuring OSFirewall protection

OSFirewall protection, which is enabled by default, detects when programs try to use your operating system to perform suspicious actions on your computer. You can also configure various OSFirewall Special System Protections, which determine whether programs on your computer can perform specific actions such as modifying your Internet Explorer home page or installing ActiveX controls.

To configure OSFirewall settings:

1. Select **Program Control | **Main**.**

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

3. In the Custom Program Control Settings dialog box that appears, select the **OSFirewall tab.**

4. Select or deselect **Enable OSFirewall, as desired. (Note that, to configure any OSFirewall Special System Protections in the next step, you must first enable OSFirewall.)**

5. Optionally, configure any OSFirewall Special System Protections. For any action in the list, click the State field and select **Allow**, **Deny**, **Ask**, or **Use Program Setting**. If you choose Use Program Setting, Zone Labs security software defers to SmartDefense Advisor settings or to your manual settings.
6. Click **Apply** to save the setting and leave the dialog open, or **OK** to save the setting and close the dialog.

Enabling Component Control

In addition to controlling permissions for all *programs* on a computer, advanced users may also want to monitor and, if desired, restrict individual *components* that these programs load (such as DLL files or ActiveX controls). Zone Labs security software keeps a list of components (used by allowed programs) that have tried to access the Internet or the local network. Depending on your program control and component control settings, Zone Labs security software can simply monitor components or it can alert you each time a new component attempts access. This section explains how to enable component control. For details about viewing the Components List and modifying component permissions manually, see “Managing program components,” on page 85.

By default, component control is turned off, though Zone Labs security software does add components to the Components List. If you enable component control and set program control to Medium, component control tracks components but does not restrict their activity. If you then reset program control to High, component control grants access to all previously known components but prompts you to allow or deny any components discovered subsequently. For advanced users concerned about component activity, the best practice is to install Zone Labs security software on a freshly set up computer, enable component control and set the program control level to Medium, and, after Zone Labs security software has had a chance to detect all normal components that require access, reset program control to High. (For information about the program control setting, see “Setting the program control level,” on page 67.)

To enable component control:

1. Select **Program Control | Main**.
2. In the Program Control area, click **Custom**.
The Custom Program Control Settings dialog appears.
3. On the Program Control tab, select **Enable component control**.
4. Click **OK**.

Setting the SmartDefense Advisor level

Whenever you use a program that requests access, SmartDefense Advisor queries the Zone Labs server to determine the policy for that program. You can choose to have SmartDefense Advisor set the permissions for the program automatically, or you can

configure program access manually. The SmartDefense Advisor level is set to Auto by default.

If you set SmartDefense Advisor to Auto and there is no advice available for a program, Zone Labs security software displays a Program alert prompting you to allow or deny access to the program. If you select **Remember this setting** when responding to such a Program alert, Zone Labs security software keeps your setting unless SmartDefense Advisor comes out with a different setting, or until you change the setting manually in the Programs tab.

For information about setting program permissions manually, see “Setting permissions for specific programs,” on page 76. You can set SmartDefense Advisor to Manual or Off and set *all* program permissions manually. Or, you can set SmartDefense Advisor to Auto and set manual program permissions *only* when SmartDefense Advisor does not recommend a policy.

To set the SmartDefense Advisor level

1. Select **Program Control | Main**.
2. In the SmartDefense Advisor area, choose your setting.

Auto	In Auto mode, SmartDefense Advisor automatically implements the recommendation returned from the server. Program Control must be set to Medium or High to set SmartDefense Advisor to Auto.
Manual	In Manual mode, you will receive Program alerts when programs request access and can set the permission on your own.
Off	SmartDefense Advisor will not contact the server for program advice.

Enabling the automatic lock

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

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

You can set the Internet lock to engage:

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

To enable or disable the automatic lock:

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

To set automatic lock options:

1. Select **Program Control | Main**.
2. In the Automatic Lock area, click **Custom**.

The Custom Lock Settings dialog appears.

3. Specify the lock mode to use.

Lock after n minutes of inactivity	Engages automatic lock after the specified number of minutes has passed. Specify a value between 1 and 99.
Lock when screensaver activates	Engages automatic lock whenever your screensaver is activated.

4. If desired, specify Internet access permissions for periods when the lock is engaged.

Allow pass-lock programs to access the Internet	Allows programs with pass-lock permission to access the Internet. Programs without pass-lock permission have no access. This is the default behavior when the lock is engaged.
Block all Internet access	Prevents all programs, regardless of pass-lock status, from accessing the Internet when the lock is engaged.

5. Click **OK**.

Viewing logged program events

By default, all Program events are recorded in the Log Viewer.

To view logged program events:

1. Select **Alerts & Logs | Log Viewer**.
2. Select **Program**, from the Alert Type drop-down list.

Table 5-1 provides an explanation of the log viewer fields available for Program events.

Field	Explanation
Rating	Event rating based on the Protection Level of the security option.
Date/Time	Date and time the event occurred.

Table 5-1: Program event log fields

Field	Explanation
Type	Type of program alert that occurred. Possible values for this column include: <ul style="list-style-type: none"> • Program Access • Repeat Program • New Program
Program	The program (displayed as the application file) that requested access. If a program name is unavailable, refer to the Description field of the Entry Details window.
Source IP	The IP address of the computer sending the request. If the source IP cannot be determined, this field may be left blank.
Destination IP	The IP address of the computer receiving the request. If the destination IP cannot be determined, this field may be left blank.
Direction	Specifies whether the request that caused the event was incoming, outgoing, or occurred as a result of internal traffic on your computer (data).
Action Taken	Specifies whether the request was Allowed or Blocked. Action is followed by /
Count	The number of times this action was taken.
Source DNS	The domain name server of the computer that is sending the request.
Destination DNS	The domain name server of the computer that is receiving the request.

Table 5-1: (Continued)Program event log fields

Viewing logged OSFirewall events

By default, all OSFirewall events are recorded in the Log Viewer.

To view logged OSFirewall events:

1. Select **Alerts & Logs | Log Viewer**.
2. Select **OSFirewall**, from the Alert Type drop-down list.

Table 5-2 provides an explanation of the log viewer fields available for OSFirewall events.

Field	Explanation
Rating	Event rating based on the Protection Level of the security option.
Date/Time	Date and time the event occurred.
Type	Type of OSFirewall alert that occurred. Possible values for this column include: <ul style="list-style-type: none"> • Process • Message • Module • Registry • File • Execution • Driver • Physical memory
Subtype	The specific event that initiated the Type of access requested (for example, OpenThread would be a subtype of Process).
Data	The path to the file that was attempting to be modified.
Program	Displays the path to the program that performed the behavior.
Action Taken	Specifies whether the request was Allowed or Blocked. Action is followed by /manual or /auto to indicate whether the action was performed by you or by SmartDefense Advisor.
Count	The number of times this action was taken.

Table 5-2: OSFirewall event log fields

Configuring advanced program settings

By default, Zone Labs security software always asks you whether to block or to allow connection attempts and server access attempts for the Internet and Trusted Zones. In addition, if the TrueVector service is running, but Zone Labs security software is not, program access is denied by default.

Setting global program properties

You can customize program control by specifying whether access is always allowed, always denied, or if you want to be asked, each time a program in either the Internet or Trusted Zone requests access.

To set global program properties:

1. Select **Program Control | Main**.
2. Click **Advanced**, then select the **Alerts & Functionality** tab.
3. Specify global program options.

Show alert when Internet access is denied	Displays a Blocked Program alert when Zone Labs security software denies access to a program. To have access denied silently, clear this option.
Deny access if permission is set to "ask" and the TrueVector service is running but Zone Labs security software is not	In rare cases, an independent process such as a Trojan horse could shut down the Zone Labs security software user interface, but leave the TrueVector service running. This setting prevents the application from hanging if this occurs.
Require password to allow a program temporary Internet access	Prompts you to enter a password to grant access permission. Requires that you be logged in to respond Yes to a Program alert. To allow access without a password, clear this option.

4. Click **OK**.

Setting access permissions for new programs

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

To set connection attempt permissions for new programs:

1. Select **Program Control | Main**.

2. Click *Advanced*.**3. In the Connection Attempts area, specify your preferences for each Zone.**

Always allow access	Allows all new programs access to the specified Zone.
Always deny access	Denies programs access to the specified Zone.
Always ask for permission	Displays an alert asking for permission for the program to access the specified Zone.



Settings for individual programs can be established in the Programs tab. Settings in this panel apply ONLY to programs not yet listed in the Programs tab.

To set server attempt permissions for new programs:

1. Select *Program Control* | *Main*.**2. Click *Advanced*.**

In the Server Attempts area, specify your preferences for each Zone.

Always accept the connection	Allows all programs attempting to act as a server.
Always deny the connection	Denies all programs attempting to act as a server.
Always ask before connecting	Displays an alert asking for permission for the program to act as a server.

Setting permissions for specific programs

In some cases, you may want to specify different settings for an individual program than the global program control level will allow. For example, if you wanted to allow access to a particular program, but keep security High for all other programs, you could set the permission for that program to **Allow**.



After you manually set permissions for a program, the permissions for that program will not change even if you later set the SmartDefense Advisor level to Auto. To benefit from automatic program advice, remove the program from the Programs List, then set the SmartDefense Advisor level to Auto.

Using the programs list

The programs list provides an overview of the programs on your computer that have tried to access the Internet or the local network. For each program, the program list provides detailed information about its current state, trustworthiness, and the functions it is allowed to perform. The programs list is organized in alphabetical order. You can sort the programs in the list by any column by clicking on column header. As you use your computer, Zone Labs security software detects every program that requests network access and adds it to the programs list. To access the Programs List, select **Program Control | Programs**.

Selecting a program name in the list displays program information in the yellow Entry Detail area below the list. This area provides details about the program, including its full name, the program's OSFirewall policy, and the date of the last policy update.

The SmartDefense Advisor and Trust Level columns indicate OSFirewall Protection for your computer and specify whether a program is allowed to perform operating system-

level actions like changing TCP/IP parameters, loading or installing drivers, or changing your browser's default settings.

status indicator

Active	Programs	Smart Defense Advisor	Trust Level	Access Trusted Internet	Server Trusted Internet	Send Mail
	Windows Update A...	Auto	?	?	?	?
	Windows NT Sessi...	Auto		✓	✓	?
	Windows NT Multipl...	Auto	?	?	?	?
●	Windows NT Logon...	Auto		?	?	?
	Windows Managem...	Auto	?	?	?	?
	Windows Explorer	Auto		✓	✓	?
	VMwareUser	Auto	?	?	?	?
	VMwareTray	Auto	?	✗	✗	✗
	VMware Tools Ser...	Auto	?	?	?	?
	Userinit Logon Appli...	Auto		✓	✓	?
	TrueVector Service	Auto	?	✗	✗	✗

Entry Detail	
Product name	Microsoft(R) Windows (R) 2000 Operating System
File name	C:\WINNT\system32\SERVICES.EXE
Policy	Automatically configured
Last policy update	4/22/2005 11:01:22

Figure 5-3: Programs list

Active

Indicates the current status of a program. A green circle indicates that the program is currently running.

Programs

The name of the program.

SmartDefense Advisor

The SmartDefense Advisor column indicates where the program policy comes from. The column may contain any of the following designations:

- **Auto**—SmartDefense Advisor determines the program policy, unless a recommendation is not available. (Note that, if SmartDefense Advisor is turned on, and you select **Remember this setting** when responding to a Program alert, the SmartDefense Advisor column will still say Auto, since the permissions will still change to conform to any SmartDefense Advisor recommendations that come out later.)
- **Custom**—You determined the program policy manually. If you change a program's permissions (by changing a value in any of the columns in the program's row, for example), the SmartDefense Advisor column displays "Custom" for that program.

- **System**—SmartDefense Advisor determines the program policy, and the program is used by your operating system.



Manually changing the policy for “System” programs could interfere with the normal functions of your computer.

Trust Level

The Trust Level determines the actions that a program is allowed to perform. The Trust Levels are Super, Trusted, Restricted, Ask, Kill, and No Enforcement.

A program’s Trust Level setting is determined by its policy. Zone Labs security software assigns policies to known programs automatically. The SmartDefense Advisor security team constantly monitors programs for changes in behavior and trustworthiness and updates the programs permissions accordingly. A program with a Trust Level setting of Super today, might have a Trust Level of Restricted tomorrow, if security experts determine that the program could pose a risk to your computer. Once a program’s policy setting has been changed from Auto to Custom, however, it will no longer be monitored for changes in Trust Level. For this reason, it is recommended that you keep the default settings for your programs. Refer to the table below for a description the symbols used in this list.

Access

The Access column refers to a program’s right to retrieve information from the Internet or networks in the Trusted Zone.

Server

Allows a program to passively listen for contact from the Internet or network. Few programs require server rights.

Send Mail

Allows a program to send and receive e-mail.

Refer to the table below for a description of the symbols used in this list..










Symbol	Meaning
	The program is currently active.
	The program is allowed access/server rights.
	When this symbol appears in the Access or Server columns, it means that Zone Labs security software will display a Program alert when the program asks for access, server rights. When this symbol appears in the Trust Level column, it means that Zone Labs security software will display a Suspicious Behavior alert when a program performs actions considered suspicious.
	The program is denied access/server rights.
	Super access. Program can perform suspicious actions without seeking permission. No alerts will be displayed.
	Trusted access. Trusted Programs can perform suspicious actions without seeking permission, but unknown programs must ask for permission.
	Restricted access. Program can perform trusted-level actions but cannot perform suspicious actions.
	No access. Programs marked with the No access (Kill) symbol cannot run.
	No enforcement. Program is not monitored at all and can perform any action whatsoever. This setting can pose a security risk.

Table 5-3: Program List symbols

For more information about what program actions are considered suspicious, see Appendix D, “Program behavior,” starting on page 251.

Adding a program to the programs list

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

To add a program to the programs list:

1. Select **Program Control | Programs**, then click **Add**.

The Add Program dialog appears.

2. Locate the program you want to add, then click **Open**.

Be sure to select the program's executable file (for example, program.exe).

To edit a program on the programs list:

1. Select **Program Control | Programs**.
2. Right-click a program in the Programs column and choose one of the available options.

Changes Frequently	If this option is selected, Zone Labs security software will use only file path information to authenticate the program. The MD5 signature will not be checked. Caution: This is a Low security setting.
Options	Opens the Program Options dialog box, in which you can customize security options and create expert rules for programs.
Properties	Opens your operating system's properties dialog box for the program.
Remove	Deletes the program from the list.

Granting a program permission to access the Internet

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

To grant a program permission to access the Internet:

1. Select **Program Control | Programs**.
2. In the Programs column, click the program for which you want to grant access, then select **Allow** from the shortcut menu.

For information about granting programs permission by responding to an alert, see "New Program alert," on page 210.



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

Granting a program permission to act as a server

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

To grant a program permission to act as a server:

1. Select **Program Control | Programs**.
2. In the Programs column, click the program for which you want to grant server access, then select **Allow** from the shortcut menu.

Granting send mail permission to a program

To enable your e-mail program to send e-mail messages and to enable protection against e-mail threats, grant send mail permission to your e-mail program. For more information about protecting your e-mail, see Chapter 7, “E-mail protection,” starting on page 115.

To grant send mail permission to a program:

1. Select **Program Control | Programs**.
2. Select a program from the list, then click in the **Send Mail** column.
3. Select **Allow** from the shortcut menu.



You also can access the Program Options dialog by right-clicking a program name and selecting **Options**.

Setting program options for a specific program

How a program is authenticated, whether it uses Outbound MailSafe protection, or is held to privacy standards, is determined globally by setting the Program Control level. You can modify these and other settings on a per-program basis from the Programs List.

Setting Advanced Program Control options

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

To enable Advanced Program Control for a program:

1. Select **Program Control | Programs**.
2. In the Programs column, select a program, then click **Options**.

The Program Options dialog appears.

3. Select the **Security tab**, then choose your Advanced Program Control options.

This program may use other programs to access the Internet	Allows the selected program to use other programs to access the Internet.
Allow Application Interaction	Allows the selected program to use OpenProcess and CreateProcess functions on your computer.

4. Click **OK**.

Disabling Outbound Mail protection for a program

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

To disable Outbound Mail protection for a program:

1. Select **Program Control | Programs**.
2. Select a program from the list, then click **Options**.

The Program Options dialog appears.

3. Select the **Security tab**.

4. Clear the check box labeled **Enable Outbound MailSafe Protection for this program**.



This check box will not appear unless the SendMail permission for this program is set to Allow.

5. Click **Apply** to save your changes, then click **OK**.

For more information about Outbound MailSafe Protection, see “Outbound MailSafe protection,” on page 117.

Setting Filter options for a program

When Parental Control and Privacy features are enabled globally, individual programs like Word Processing programs can still access restricted content unless filter options have also been enabled for that program. For example, although Parental Control blocks access to the site “<http://www.playboy.com>” from your browser, the site could still be accessed by clicking a URL within a Microsoft Word document unless Parental Control was also enabled for that program.

To enable filter options for a program:

1. Select **Program Control | Programs**.
2. Select a program from the list, then click **Options**.
The Program Options dialog appears.
3. Select the **Security** tab.
4. Under Filter Options, select the check box beside the protection you want, then click **OK**.

For more information about Privacy protection, see Chapter 8, “Privacy protection,” starting on page 135. For more information about Parental Control, see Chapter 11, “Parental Control,” starting on page 181.

Setting authentication options

You can specify whether a program is authenticated by using its full pathname or by its components. By default, all programs are authenticated by their components.

To specify an authentication method:

1. Select **Program Control | Programs**.
2. Select a program from the list, then click **Options**.
The Program Options dialog appears.
3. Select the **Security** tab.

4. Under Authentication, select the check box beside the option you want, then click **OK**.

Setting passlock permission for a program

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

To grant or revoke passlock permission:

1. Select **Program Control | Programs**.
2. Select a program from the list, then click **Options**.
3. Select the **Enable Pass Lock** check box.
4. Click **Apply**, then click **OK**.

Managing program components

In addition to controlling permissions for all *programs* on a computer, advanced users may also want to monitor and, if desired, restrict individual *components* that these programs load (such as DLL files or ActiveX controls). Zone Labs security software keeps a list of components (used by allowed programs) that have tried to access the Internet or the local network. Depending on your program control and component control settings, Zone Labs security software can simply monitor components or it can alert you each time a new component attempts access. This section explains how to access the Components List and how to change component permissions. For details about enabling component control, see “Enabling Component Control,” on page 69.

The Components List contains a list of program components for allowed programs that have tried to access the Internet or the local network. The Access column indicates whether the component is always allowed access, or whether Zone Labs security software should alert you when that component requests access. By default, the Components List is organized in alphabetical order, but you can sort the components in the list by any column by clicking on the Component column header.

To access the Components List:

➤ Select **Program Control | Components**.

Component ▲	Description	Access
activeds.dll	ADs Router Layer DLL	✓
actxprxy.dll	ActiveX Interface Marshaling Library	✓
adistres.dll	ADISTRES.DLL	✓
adsltdpc.dll	ADs LDAP Provider C DLL	✓
ADVAPI32.DLL	Advanced Windows 32 Base API	✓
alert.zap	Alerts Plugin Module	✓
atl.dll	ATL Module for Windows HT (Unicode)	✓
avifil32.dll	Microsoft AVI File support library	✓
blackbox.dll	Black Box	✓
browseic.dll	Shell Browser UI Library	✓

Entry Detail	
Component name	Alerts Plugin Module
File name	C:\PROGRAM FILES\ZONE LABS\ZONEALARM...
File type	Dynamic Link Library
Authentication	Manual
Version	4.0.81.0

[More Info](#)

Figure 5-4: Components List

To grant access permission to a program component:

1. Select Program Control | Components.

2. Select a component from the list, then click in the Access column.
3. Select **Allow** from the shortcut menu.

Creating expert rules for programs

By default, programs given access permission or server permission can use any port or protocol, and contact any IP address or host at any time. Conversely, programs that you block have no access rights at all. By creating expert rules for particular programs, you can heighten protection against hijacked programs by specifying ports and protocols, source and destination addresses, and time and day ranges during which activity is either allowed or denied. You can also apply tracking options to specific types of traffic in order to see alerts or generate log entries when allowed program traffic occurs, enable or disable rules at will, and apply multiple, ranked rules to a program.



If you created port rules for Programs in a version of Zone Labs security software, prior to 4.0, those port rules will be automatically converted to expert rules and visible in the Expert tab of the Program Options dialog. To access the Expert tab, select **Program Control|Programs**, then click **Options**.

Creating an expert rule for a Program

Expert rules for programs are enforced in the order they are ranked. Therefore, when you create expert rules for a program, make sure that the last rule you create for that program is a “Block All” rule.



For tips on setting up expert rules for your programs, visit the Zone Labs User Forum (<http://www.zonelabs.com/forum>) and search for “program rules”.

To create an expert rule for a program:

1. Select **Program Control|Programs**, then click **Options**.
2. Select **Expert Rules**, then click **Add**.

The Add rule dialog appears.

3. Create Expert Program rule.



The Add rule dialog contains the same fields and options that are available when you create Expert Firewall rules. Note, however, that IGMP and Custom protocols cannot be applied to expert rules for Programs. See “Creating expert firewall rules,” on page 55.

4. Click **OK**.

Sharing expert rules

Expert firewall rules (created in the Expert tab in the Firewall panel) cannot be directly applied to a single program. If the rule is enabled, it is applied globally. Similarly, an expert rule you created for one program cannot be directly applied to another program.

However, you can create a copy of the existing expert rule and apply it to any program. Note that none of the changes you make to the copy will be reflected in the original.

To apply an existing expert firewall rule to a program:

1. Select **Firewall | Expert**.
2. Select the rule you want to apply, then press **CTRL+C**.
3. Select **Program Control | Programs**.
4. In the Programs column, select the program to which you want to apply the expert rule, then click **Options**.
5. Select Expert Rules, then press **CTRL+V**.

The Expert rule is applied to the program.

6. Click **Apply**, then click **OK**.

To disable an Expert rule:

1. Select **Program Control | Programs**.
2. Select the program for which you want to disable an Expert Program rule, then right-click and select **Disable** from the shortcut menu.

The rule will be grayed-out.

3. Click **Apply**, then click **OK**.

Chapter

Spyware and Virus protection

6

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

Spyware Community Watch updates your signature database with information on the latest spyware outbreaks gathered from more than 30 million Zone Labs users.

The Anti-virus feature is only available in ZoneAlarm Anti-virus and ZoneAlarm Security Suite.

The Anti-spyware feature is only available in ZoneAlarm Anti-Spyware, ZoneAlarm Pro, and ZoneAlarm Security Suite.

Topics:

- “Spyware and Virus Protection,” on page 90
- “Customizing virus protection options,” on page 93
- “Customizing spyware protection options,” on page 97
- “Performing a virus scan,” on page 99
- “Performing a spyware scan,” on page 104
- “Viewing virus and spyware protection status,” on page 109
- “Monitoring virus protection,” on page 110

Spyware and Virus Protection

The Anti-spyware feature detects spyware components on your computer and either removes them automatically, or places them in quarantine so that you can remove them manually after assessing their risk.

The Anti-virus feature keeps known and unknown viruses from affecting your computer by scanning files and comparing them to a database of known viruses and against a set of characteristics that tend to reflect virus behavior. Files can be scanned as they are opened, closed, executed, or as part of a full computer-wide scan. If a virus is detected, Zone Labs security software renders it harmless, either by repairing or denying access to the infected file.

Turning on virus and spyware protection

If you are using ZoneAlarm Security Suite and you chose not to turn on the anti-virus protection feature in the Configuration Wizard following installation, you can turn it on manually.



The Zone Labs Anti-virus protection feature is incompatible with other virus protection software. Before you turn on the Anti-virus protection feature, you must uninstall any other anti-virus software from your computer, including suite products that include virus protection among their features. Zone Labs security software can automatically uninstall some anti-virus applications for you. If you are using a program that cannot be uninstalled automatically, you can uninstall it using Add/Remove Programs, accessible from the Windows Control Panel.

To enable virus and spyware protection:

1. Select **Anti-virus / Anti-spyware | Main**.
2. In the **Anti-virus** area, select **On**.
3. In the **Anti-spyware** area, select **On**.

Scheduling a scan

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

To schedule a scan:

1. Select **Anti-virus/Anti-spyware | Main**.
2. In the Anti-virus area, click **Advanced Options**.

The Advanced Options dialog appears.

3. Under Advanced Settings, select **Scan Schedule**.
4. Select the **Scan for viruses** check box, then specify a day and time for the scan.
5. Specify the scan frequency.
By default, a virus scan is performed once per week.
6. Select the **Scan for spyware** check box, then specify a day and time for the scan.
7. Specify the scan frequency.
By default, a spyware scan is performed once per week.
8. Click **OK**.

Updating virus and spyware definitions

Every virus or spyware application contains unique identification information, known as its definition file. These definition files are the maps used to locate viruses and spyware on your computer. As new viruses or spyware applications are discovered, Zone Labs security software updates its databases with the definitions files it needs to detect these new threats. Therefore, your computer is vulnerable to viruses and spyware whenever its database of virus definitions files becomes outdated. The **Details** area

located on the Main tab of the **Anti-virus / Anti-spyware** panel displays the status of your definition files.

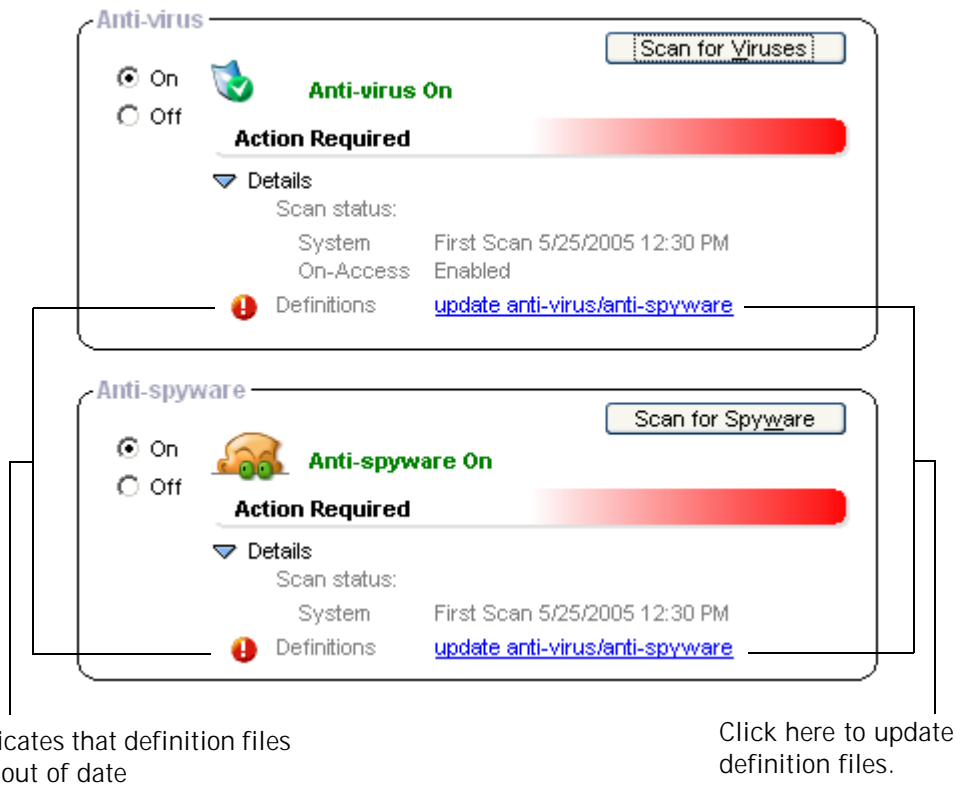


Figure 6-1: Anti-virus and Anti-spyware status

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

To enable automatic updates:

1. Select **Anti-virus / Anti-spyware | Main**.
2. In the Anti-virus area, click **Advanced Options**.
The Advanced Options dialog appears.
3. Select **Updates**, then select the **enable automatic anti-virus updates** check box.
4. Select the **enable automatic anti-spyware updates** check box.
5. Click **OK**.

Customizing virus protection options

In addition to choosing the type of scan you want to perform, you also can specify the method used to detect viruses, and set treatment methods.

Zone Labs security software provides several types of virus scans to keep your computer and data safe: system scans, on-access scans, and e-mail scans.

Specifying scan targets

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

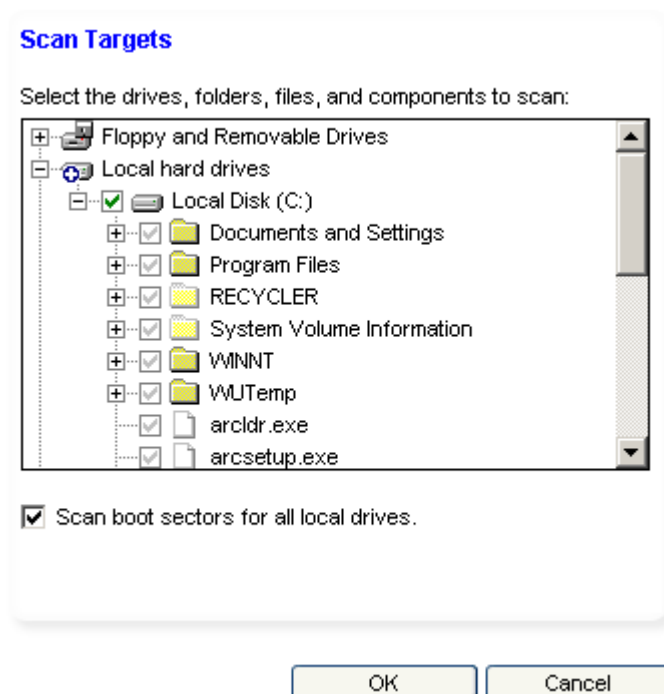


Figure 6-2: Scan targets dialog box

Table 6-2 below provides an explanation of the icons shown in the Scan Targets dialog box.

Icon	Explanation
	The selected disk and all sub-folders and files will be included in the scan.
	The selected disk and all sub-folders and files will be excluded from the scan.

Table 6-2: Icons indicating scan targets







Icon	Explanation
	The selected disk will be included in the scan, but one or more sub-folders or files will be excluded from the scan.
	The selected folder will be excluded from the scan, but one or more sub-folders or files will be included in the scan.
 	The selected folder will be included in the scan. A gray check mark indicates that scanning of the folder or file is enabled because scanning has been enabled for a higher level disk or folder.
 	The selected folder will be excluded from the scan. A gray "x" mark indicates that scanning of the folder or file is disabled because scanning has been disabled for a higher level disk or folder.

Table 6-2: Icons indicating scan targets

To specify scan targets:

1. Select **Anti-virus / Anti-spyware | Main**.

2. Click **Advanced Options**.

The Advanced Options dialog appears.

3. Under Virus Management, select **Scan Targets**.

4. Select the drives, folders, and files to be scanned.

5. Select or clear the **scan boot sectors for all local drives** check box, then click **OK**.

On-Access scanning

On-Access scanning protects your computer from viruses by detecting and treating viruses that may be dormant on your computer. On-Access scanning is enabled by default. On-Access scanning supplies the most active form of virus protection. Files are scanned for viruses as they are moved, opened, executed, or closed, thereby allowing immediate detection and treatment of viruses. (Note that archive files, such as .zip files, are scanned only when you open them.)

To enable on-access scanning:

1. Select **Anti-virus / Anti-spyware | Main**.

2. In the Protection area, click **Advanced Options**.

The Advanced Anti-virus Settings dialog appears.

3. Under Advanced Settings, select **On-Access Scanning**.

4. Select the **Enable On-Access Scanning** check box, then click **OK**.

E-mail Scanning

E-mail scanning builds on the protection offered by MailSafe, by scanning for viruses in the body and attachments of e-mail messages and removing them before they can do damage. Where MailSafe scans for potentially harmful attachments based on file extension, the E-mail scanning feature scans for harmful files by comparing the attachments to the signature files of known viruses. If an infected attachment is detected, the attachment is removed from the e-mail message and replaced with a text file log that provides details about the removed file. For details about performing an e-mail scan, see “Anti-virus protection for e-mail,” on page 133. E-mail scanning is on by default.

To enable or disable E-mail scanning:

1. Select **Anti-virus / Anti-spyware | Main**, then click **Advanced Options**.

The Advanced Options dialog appears.

2. Under Virus Management, select **E-mail Scanning**.
3. Select or clear the **Enable E-mail Scanning** check box, then click **OK**.

Enabling automatic virus treatment

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

To enable automatic virus treatment:

1. Select **Anti-virus / Anti-spyware | Main**, then click **Advanced Options**.

2. Under Virus Management, select **Auto Treatment**.

3. Select the auto treatment option you want:

<input type="checkbox"/>	Alert me - do not treat automatically
<input type="checkbox"/>	Try to repair, and alert me if repair fails
<input type="checkbox"/>	Try to repair, quarantine if repair fails (recommended)

4. Click **OK**.

Specifying virus detection methods

There are two primary methods used to scan files for viruses: Heuristic Analysis and Byte-level scanning. Heuristic Analysis scans files and identifies infections based on a virus' characteristic behavior. Heuristic Analysis is enabled by default. Byte-level filter scans each byte of the file to identify a virus. Byte-level scanning can take considerable

time to perform. As a consequence, it is only recommended after a major virus attack to ensure that there are no infections left behind.



Enabling or disabling Heuristic Analysis has no affect on the scanning of e-mail attachments. Attachments are still scanned using this method. Byte-level scanning does not support On-Access or E-mail scanning.

To specify a detection method:

1. Select **Anti-virus / Anti-spyware | Main, then click **Advanced Options**.**

The Advanced Options dialog appears.

2. Under **Virus Management, select **Detection**.**

3. Select your preferred detection method(s), then click **OK.**

Customizing spyware protection options

In addition to choosing the type of scan you want to perform, you can specify the method used to detect spyware, set treatment methods, and view suspected spy sites that Zone Labs security software has blocked.

Enabling automatic spyware treatment

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

To enable automatic virus treatment:

1. Select **Anti-virus / Anti-spyware** | **Main**, then click **Advanced Options**.
2. Under Spyware Management, select **Auto Treatment**.
3. Select the **Enable automatic spyware treatment** check box, then click **OK**.

Specifying spyware detection methods

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

To specify spyware detection methods:

1. Select **Anti-virus / Anti-spyware** | **Main**, then click **Advanced Options**.
2. Under Spyware Management, select **Detection**.
3. Select the **Scan for tracking cookies** check box.
4. Under Maximum strength detection, select the desired option:

Intelligent quick scan	This option is selected by default.
Full system scan	Scans the local file system. This option can slow down scan performance. Select this option only if you suspect undetected spyware is present on your computer.
Deep-inspection scan.	Scans every byte of data on your computer. This option can slow down scan performance. Select this option only if you suspect undetected spyware is present on your computer.

5. Click **OK**.

Excluding spyware from scans

Although some spyware programs have the potential to harm your computer or to make your data vulnerable to hackers, there are many benign applications that still will be

detected as spyware during a scan. If you are using one of these applications, for example, voice recognition software, you can exclude it from spyware scans by adding it to the exceptions list. You can add spyware to the exceptions list by right-clicking the item in the Scan Results list and choosing Ignore Always from the menu.

Once spyware is on the exceptions list, it no longer will be detected during spyware scans. If spyware was added to the exceptions list accidentally, you can remove it manually.

To remove spyware from the exceptions list:

1. Select **Anti-virus / Anti-spyware | Main**, then click **Advanced Options**.
2. Under Spyware Management, select **Exceptions**.
3. In the Spyware Treatment Exceptions area, select the spyware application you want to remove, then click **Remove from List**.
4. Click **OK**.

Spy Site Blocking

Spy Site Blocking prevents you from accessing Web sites suspected of transmitting spyware. Activated by default, Spy Site Blocking builds up a list of blocked sites, adding suspected spyware sites as you try to access them. If you attempt to access a suspected spyware site, Zone Labs security software blocks the site, displays a warning pop-up, and adds the site to the Blocked Sites list. The warning pop-up includes a link that leads to the Spy Site Blocking tab, where you can turn the feature on or off, review the Blocked Sites list, and change permissions for sites in the list. The Blocked Sites list contains only those sites you have tried to access since last starting Zone Labs security software plus any sites for which you have set access permission to Allow.

To configure Spy Site Blocking:

1. Select **Anti-virus / Anti-spyware | Spy Site Blocking**.
2. In the Spy Site Blocking area, select **On** or **Off** as desired.
3. If you wish to change access permissions for any sites in the Blocked Sites list, click on the Access field for the relevant site and choose **Allow** or **Block** as appropriate.

Preventing spyware attacks

Spy Site Blocking and the Operating System Firewall (OSFirewall) help to prevent spyware from installing itself on your computer.

Spy Site Blocking prevents you from accessing Web sites suspected of transmitting spyware. To see controls for this feature, go to the Spy Site Blocking tab; to read about the feature, see “Spy Site Blocking,” on page 98.

The Operating System Firewall (OSFirewall) prevents spyware from installing itself on your computer. For details about OSFirewall, see “Configuring OSFirewall protection,” on page 68.


Performing a virus scan

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

- You can click **Scan for Viruses** in the Anti-virus area on the Main tab of the **Anti-virus / Anti-spyware** panel.
- You can right-click a file on your computer, then choose **Scan with Zone Labs Anti-virus**.
- You can schedule a system scan to run once or at regular intervals.
- You can open a file (if on-access scanning is enabled).

You may run up to five scans simultaneously. Scans are performed in the order in which they are initiated. System scans provide another level of protection by allowing you to scan the entire contents of your computer at one time. System scans detect viruses that may be dormant on your computer's hard drive, and if run frequently, can ensure that your anti-virus signature files are up to date.

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

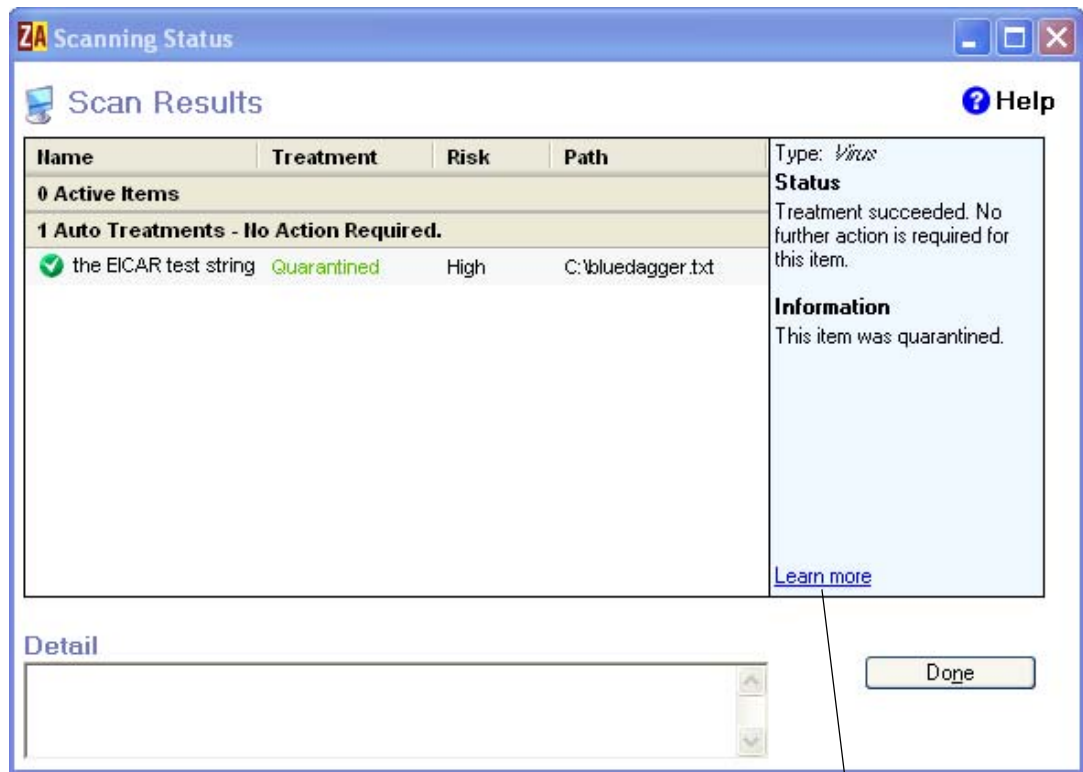
During scans, Zone Labs security software displays a special system tray icon  and provides a system tray menu option for viewing scan status. Right-click the system tray icon and choose **View Scan** to check on scan status.



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

Understanding virus scan results

Regardless of the method used to initiate the scan, the results of the scan are displayed in the Scan Results dialog box as shown in the figure below.



Click here to send virus to SmartDefense Advisor for more information

Figure 6-3: Virus scan results dialog

The Active Items area of the Scan details dialog lists infections found during the scan that could not be treated automatically. To accept the suggested treatments in the Treatment column, click **Apply**. The items listed under Auto Treatment have already been treated, you do not need to take further action.

Name

The name of the virus that caused the infection.

Treatment

Specifies the treatment applied to the infection. Possible values are Quarantined or Deleted.

Security Risk

Indicates the risk level of the infection. All viruses are considered High risk.

Path

The location of the virus that caused the infection.

Type

Specifies whether the infection was caused by a virus, worm, or trojan.

Status

Tells you whether the file has been repaired, deleted, or remains infected. If Zone Labs security software was unable to treat the item, a **What to do next** link may appear here. This link will direct you to further information and instructions.

Information

Provides more detail about the infection. To get more information about a virus or spyware, click the **Learn more** link.

Detail

This field remains empty for virus scans. For information about its use in spyware scans, see “Understanding spyware scan results,” on page 105.

Treating virus files manually

If you do not have automatic treatment enabled, or if a file could not be repaired automatically, you can attempt to treat it manually from the Scan Results dialog.

To treat a file manually:

1. In the Scan Results dialog, select the item you want to treat.
2. In the Treatment column, choose the treatment option you want:

Repair	Tries to repair the selected file.
Delete	Deletes the selected file.
Quarantine	Appends the extension .z16 to the infected file to render it harmless. The file is placed in Quarantine.

3. When you have finished treating files, click **Close**.



If the results of a virus scan contain Error, No treatment available, or Treatment failed, it means that there is not yet a way to automatically remove the virus without risking the integrity of your computer or other files. In some cases, there may be manual treatments available to you. To find out, enter the name of the virus along with the word “removal” into a search engine, such as Google or Yahoo, to locate removal instructions. Otherwise, know that we’re constantly researching viruses and developing safe ways to remove them.

Repairing files in an archive

If the infected file is located in an archive file (such as a .zip file), Zone Labs security software will not be able to treat it (either by repairing, deleting, or placing it in Quarantine) while the file is still included in the archive.

To repair a file in an archive:

1. Select **Anti-virus / Anti-spyware | Main**, then click **Advanced Options**.
2. Select **On-Access Scanning**, then select the **Enable On-Access Scanning** check box.
3. Click **Apply**, then click **OK**.
4. Open the file that was specified in the Scan Results dialog from within an archival utility, such as WinZip.

On-access scanning will scan the file for infections. The Scan Results dialog will appear with the results of the scan. If the file still cannot be repaired, see “Treating virus files manually,” on page 101.

Submitting viruses and spyware to Zone Labs for review

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

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

To submit malware to Zone Labs for review:

1. Place the malware file in a password-protected .zip archive with the password set to *infected*.

For help with creating a password protected archive, refer to the Help for WinZip.

2. Send the .zip file to malware@zonelabs.com

Use this e-mail address only for sending malware to the Zone Labs Security Team.



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

Viewing logged virus events

By default, all Virus events are recorded in the Log Viewer.

To view logged Virus events:

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

2. Select **Virus, from the Alert Type drop-down list.**

Table 6-3 provides an explanation of the log viewer fields available for Virus events.

Field	Information
Date	The date of the infection.
Type	The type of event that occurred. Possible values for this field include: <ul style="list-style-type: none"> • Update • Scan • Treatment • E-mail
Virus name	The common name of the virus. For example, <i>iloveyou.exe</i> .
Filename	The name of the infected file, the name of files being scanned, or the name and version number of update and/or engine.
Action Taken	How the traffic was handled by Zone Labs security software. Possible values include: <ul style="list-style-type: none"> • Updated, Update cancelled, Update Failed • Scanned, Scan cancelled, Scan Failed • File Repaired, File Repair Failed • Quarantined, Quarantine Failed • Deleted, Delete Failed • Restored, Restore Failed • Renamed, Rename Failed
Actor	Whether the action was manual or auto.
E-mail	If the virus was detected in e-mail, the e-mail address of sender of the infected message.

Table 6-3: Virus event log fields

Performing a spyware scan

There are a couple of ways to initiate a spyware scan on your computer.

- You can click **Scan for Spyware** in the Anti-spyware area on the Main tab of the **Anti-virus / Anti-spyware** panel.
- You can schedule a system scan to run once or at regular intervals.

You may run up to five scans simultaneously. Scans are performed in the order in which they are initiated. System scans provide another level of protection by allowing you to scan the entire contents of your computer at one time. System scans detect spyware that may be dormant on your computer's hard drive, and if run frequently, can ensure that your anti-spyware signature files are up to date.

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

During scans, Zone Labs security software displays a special system tray icon (🔍) and provides a system tray menu option for viewing scan status. Right-click the system tray icon and choose **View Scan** to check on scan status.



Clicking **Pause** in the Scan dialog while a scan is being performed will stop the current scan. Click **Pause** again to resume the current scan.

Understanding spyware scan results

The results of a spyware scan are displayed in the Scan Results dialog box as shown in the figure below.

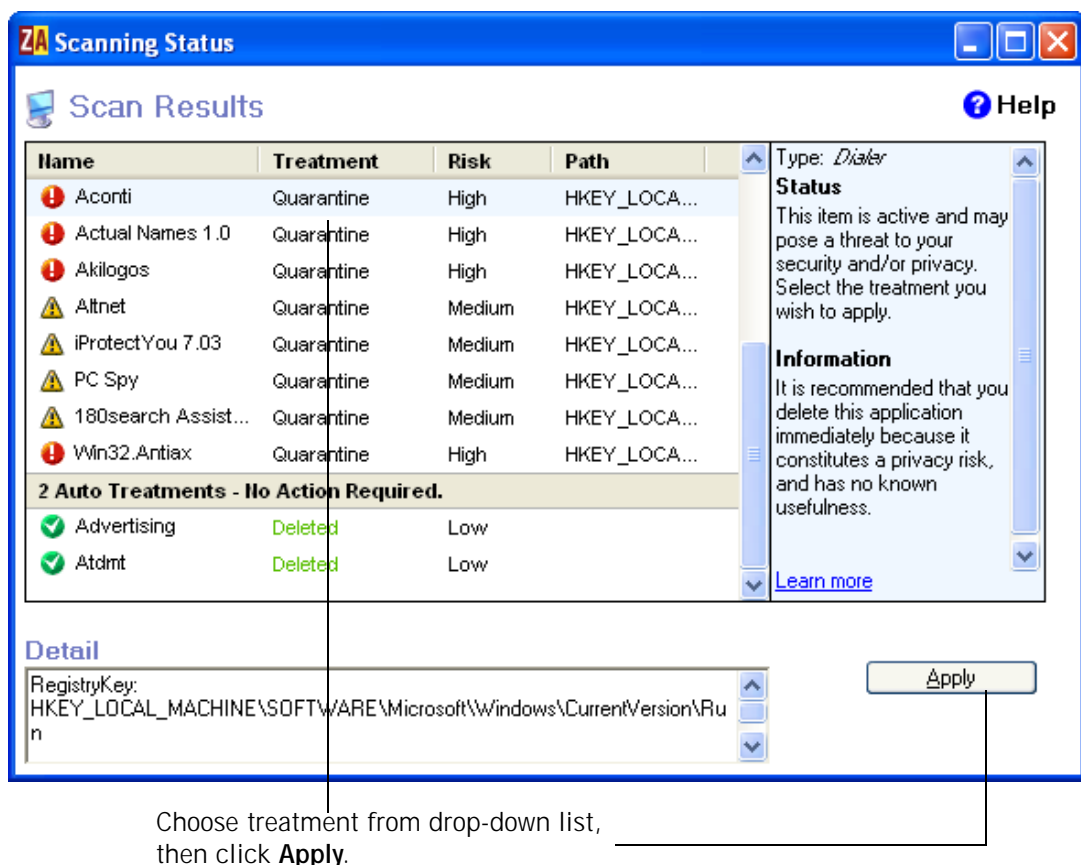


Figure 6-4: Spyware scan results dialog

The Active Items area of the Scan Results dialog lists infections found during the scan that could not be treated automatically. To accept the suggested treatments in the Treatment column, click **Apply**. The items listed under Auto Treatment have already been treated, you do not need to take further action.

Name

The spyware name.

Treatment

Specifies the treatment applied to the infection. Possible values are Quarantined or Deleted.

Security Risk

Indicates the risk level of the infection. Possible values for this column include:

- Low - Adware or other annoying but benign software.

- Med -Potential privacy breach.
- High - Poses a security threat.

Path

The location of the virus or spyware that caused the infection. You can expand the field and scroll right to see the complete path.

Type

The category of spyware detected. Possible values for this field include keylogging software and tracking cookie.

Status

Tells you whether the file has been repaired, deleted, or remains infected. If Zone Labs security software was unable to treat the item, a **What to do next** link may appear here. This link will direct you to further information and instructions.

Information

Provides more detail about the infection. To get more information about a virus or spyware, click the **Learn more** link.

Detail

Lists the full paths of all spyware traces (such as registry keys, cookies, and so on). Advanced users may find this information useful for tracking down spyware programs that cannot be treated automatically.

Errors in spyware scan results

If the results of a spyware scan contain Error, No treatment available, or Treatment failed, it means that there is not yet a way to automatically remove the spyware without risking the integrity of your computer or other files. This is not uncommon, as spyware writers often employ heavy-handed tactics to keep their spyware on your computer with no regard to the damage they could cause.

In most cases, there are manual treatments available to you. To find out, enter the name of the spyware along with the word “removal” into a search engine, such as Google or Yahoo, and see if you can find removal instructions. Otherwise, know that we’re constantly researching spyware such as this and developing safe ways to remove it. Chances are we’ll have a treatment available soon.

Viewing items in quarantine

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

To view viruses in quarantine:

1. Select **Anti-virus / Anti-spyware**.

2. Select the **Quarantine** tab.
3. Choose **Viruses** from the Quarantined View drop-down list.
4. Optionally, select a virus entry in the list and click **Delete** (to delete it from your computer), **Restore** (to restore it to your computer), or **More Info** (to consult SmartDefense Advisor for more information about it).

The virus view in quarantine contains the following columns of information:

Infection

The name of the virus that caused the infection.

Days in Quarantine

The number of days the virus has been in quarantine.

Path

The location of the virus on your computer.

To view spyware in quarantine:

1. Select **Anti-virus / Anti-spyware**.
2. Select the **Quarantine** tab.
3. Choose **Spyware** from the Quarantined View drop-down list.
4. Optionally, select a spyware entry in the list and click **Delete** (to delete it from your computer), **Restore** (to restore it to your computer), or **More Info** (to consult SmartDefense Advisor for more information about it).

The spyware view in quarantine contains the following columns of information:

Type

The name of the virus that caused the infection.

Name

The name of the spyware that was detected.

Risk

The risk level of the infection. Indicates whether the spyware is benign like adware, or a serious threat like keylogging software.

Days in Quarantine

The number of days the spyware has been in quarantine.

Viewing logged spyware events

By default, all Spyware events are recorded in the Log Viewer.

To view logged spyware events:

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

2. Select **Spyware, from the Alert Type drop-down list.**

Table 6-3 provides an explanation the log viewer fields available for spyware events.

Field	Information
Date	The date of the infection.
Type	The type of spyware detected. Possible values for this field include: <ul style="list-style-type: none"> • Adware • Browser Helper Object • Dialer • Keylogger • Screenlogger • Trojan • Worm • Spy Cookie
Spyware name	The common name of the spyware. For example, <i>NavExcel</i> .
Filename	The name of the spyware file, for example <i>gmt.exe</i> .
Action	How the spyware was handled by Zone Labs security software.
Actor	Whether the action was performed by you (manual) or by Zone Labs security software (auto)

Table 6-4: Spyware event log fields

Viewing virus and spyware protection status

There are two places you can view the status of your virus and spyware protection. One is on the **Overview | Status** page, and the other is on the **Anti-virus / Anti-spyware | Main** tab.

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

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

For information on the status information found on the Overview panel, Chapter 2, “Using the Status tab,” starting on page 16. The section that follows describes the status information located on the Main tab of the Anti-virus / Anti-spyware panel.

Monitoring virus protection

One of the most important things you can do to protect your computer against viruses is to install an anti-virus software product. Once installed, however, the anti-virus software must be kept up to date to ensure protection against new viruses as they are created.

No matter which anti-virus software product you use, if you find yourself in either of the following situations, you are putting your computer at risk for virus attack:

- Your trial or subscription period has expired.
- Your virus signature files are out of date.

Anti-virus Monitoring is available in ZoneAlarm, ZoneAlarm Anti-virus, ZoneAlarm Anti-Spyware, ZoneAlarm Pro, and ZoneAlarm Security Suite.

Anti-virus Monitoring is a secondary defense system that tracks anti-virus software you have installed on your computer and lets you know when that anti-virus software is out-of-date or turned off. This secondary alerting system works as a back-up to your anti-virus software's built-in warning and update system. Most anti-virus products include automatic updating, and alert you when your virus definition files become outdated. Note that not all anti-virus products are supported by this feature.

Monitoring Coverage

Anti-virus Monitoring currently detects anti-virus software from these popular manufacturers:

- Symantec
- McAfee
- Computer Associates
- Trend Micro

If you use a different anti-virus product, Anti-virus Monitoring will not recognize it at this time. This does not mean that your ZoneAlarm product is malfunctioning; your security remains as strong as ever. Zone Labs security software will be adding the ability to recognize more products over time. If your anti-virus product is not currently supported, you may simply turn off the Anti-virus Monitoring feature. Do not worry-- Anti-virus Monitoring is monitoring only and has no affect on the firewall and no direct affect on security.

Monitoring in ZoneAlarm, ZoneAlarm Pro, and ZoneAlarm Anti-Spyware

In these products, you will see an Anti-virus Monitoring panel. From this panel you can view the status of your anti-virus product. You can also turn monitoring on or off, or you can turn on or off just the monitoring alerts.

To turn off Monitoring and Monitoring alerts:

1. Select **Anti-virus Monitoring | Main**.
2. In the **Monitoring** area, select **Off**.
3. Clear the check box **Notify me of anti-virus security lapses**.

Monitoring in ZoneAlarm Anti-virus and ZoneAlarm Security Suite

In these products, there is no Anti-virus Monitoring panel because the products are equipped with Zone Labs Anti-virus. Instead, there are monitoring alerts. When Zone Labs Anti-virus is turned off, the Anti-virus Monitoring feature is activated. Monitoring can be turned off from any monitoring alert, or from the Advanced Options dialog.

To turn off Monitoring

1. Select **Alerts & Logs**, then click **Advanced**.
2. Select the **Alerts Events** tab.
3. Clear the following check boxes:

▪	Anti-virus protection not found
▪	Anti-virus Monitoring events

4. Click **OK**.

Enabling and disabling Anti-virus Monitoring

If you do not have Zone Labs Anti-virus installed and are using another anti-virus software product, Anti-virus Monitoring will be enabled by default. In addition, you can choose to enable Monitoring alerts, which will appear whenever a lapse in protection is detected.

To enable or disable Anti-virus Monitoring:

1. Select **Anti-virus Monitoring | Main**.
2. In the Anti-virus Monitoring area, select **On**.

Viewing Status Messages in the Anti-virus Monitoring panel

The Status area of the Anti-virus Monitoring panel displays the current state of your installed Anti-virus products, as well as the state of Anti-virus Monitoring.

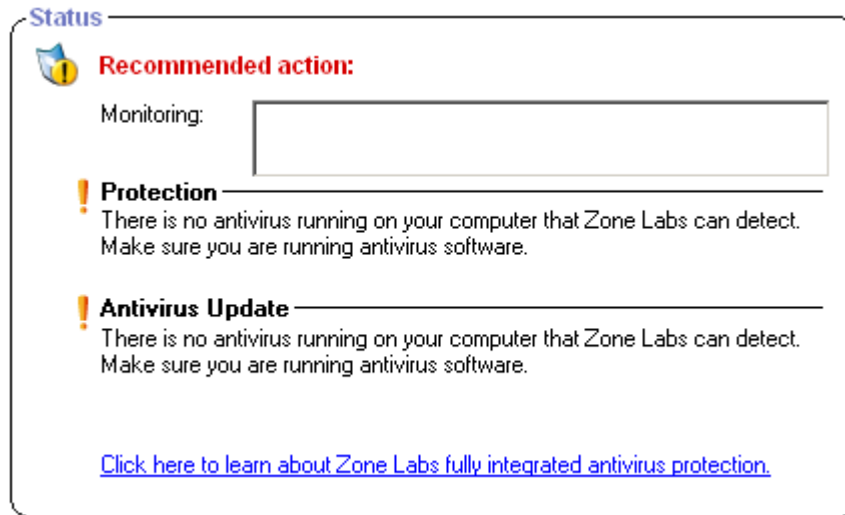


Figure 6-5: Anti-virus Monitoring Status area in ZoneAlarm

Monitoring Anti-virus Product

Zone Labs security software is able to detect most major anti-virus software products. This area includes a drop-down list that displays the anti-virus software products that were detected.

Protection

Displays whether your anti-virus products are active and protecting you.

Anti-virus Update

Displays whether your anti-virus products are up to date, or whether your subscription is current.

Viewing Anti-virus Monitoring alerts

If your anti-virus vendor hasn't sent you the latest virus definitions, if your anti-virus product's notification feature has been disabled, or if you're running an anti-virus product that we have not detected (see "Monitoring Coverage," on page 110) then Anti-virus Monitoring provides you with a warning as a second line of defense.

When a lapse in protection occurs, you will see a Monitoring alert. This alert appears on a slight delay to allow your Anti-virus product to alert you first. When the alert does

appear, it will provide information and instructions for making your Anti-virus product secure.



When running Windows 98, the Anti-virus E-mail scanning feature renames MailSafe to *isafe.exe* rather than the name of the computer's e-mail program.

Chapter

E-mail protection

7

Worms, viruses, and other threats often use e-mail to spread from computer to computer. MailSafe guards your own computer against e-mail-borne threats, while also protecting your friends, co-workers, and others in your e-mail address book.

Topics:

- “Understanding e-mail protection,” on page 116
- “Enabling Inbound MailSafe protection,” on page 117
- “Enabling Outbound MailSafe protection,” on page 117
- “Customizing Inbound MailSafe protection,” on page 118
- “Customizing Outbound MailSafe protection,” on page 121
- “Filtering junk e-mail,” on page 123
- “Anti-virus protection for e-mail,” on page 133

Understanding e-mail protection

Attaching files to e-mail messages is a convenient way of exchanging information. However, it also provides hackers with an easy way of spreading viruses, worms, Trojan horse programs, and other malware.

The inbound and outbound MailSafe features keep suspect attachments quarantined so that they can't infect your computer, and stops worms from mass-mailing themselves to everyone you know.

Inbound MailSafe protection

Potentially dangerous attachments can be identified by their file name extensions—the characters that appear after the “dot” in a file name. They identify the file type so that the appropriate program or system component can open it.

For example:

- .exe (an executable file)
- .js (a JavaScript file)
- .bat (a batch process file)

When an e-mail message with an attachment arrives in your Inbox, MailSafe examines the attachment's file name extension and compares it to the extensions on the attachments list. If the attachment type appears on the list and if attachments of that type are set to quarantine, Zone Labs security software changes the file name extension to “.zl*” (where * is a number or letter).

Changing the filename extension quarantines the attachment by keeping it from running automatically. When you open the e-mail containing the attachment, Zone Labs security software displays a MailSafe alert to let you know that it has quarantined the attachment. If you try to open the attachment, an alert warns you of the potential risk involved. However, you are still able to open the attachment if you are sure that it is safe.

In addition to verifying messages by their file extension, Zone Labs security software scans incoming attachments for potential viruses. If a virus is found, it is removed from the message before it can do damage. For more information about Anti-virus protection and e-mail messages, see “E-mail Scanning,” on page 95.

Inbound MailSafe protection works with any e-mail application that uses POP3 or IMAP protocols.



Inbound MailSafe protection is designed for local access only. If you have configured your POP3 client for remote access, inbound MailSafe protection may not be available.

Outbound MailSafe protection

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

Outbound MailSafe protection works with any e-mail application that uses SMTP.

The Outbound MailSafe protection feature is only available in ZoneAlarm Anti-virus, ZoneAlarm Anti-Spyware, ZoneAlarm Pro, and ZoneAlarm Security Suite.

Enabling Inbound MailSafe protection

Inbound MailSafe protection is enabled by default. When enabled, Inbound MailSafe quarantines attachment types listed on the Attachments tab.

To enable or disable Inbound MailSafe:

1. Select **E-mail Protection | Main**.
2. Select **On** or **Off**.

On	MailSafe quarantines attachment types specified in the attachments tab.
Off	MailSafe allows all attachment types.

Enabling Outbound MailSafe protection

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

To enable or disable Outbound MailSafe Protection

1. Select **E-mail Protection | Main**.
2. In the Outbound MailSafe Protection area, select **On** or **Off**.

Customizing Inbound MailSafe protection

All of the attachment types supported by Inbound MailSafe protection are set to quarantine by default. You can customize Inbound MailSafe protection by changing setting of attachment types to Allow, or by adding new attachment types.

The ability to customize Inbound MailSafe protection settings is not available in ZoneAlarm.

Viewing the Attachments list

Attachment types are listed in alphabetical order. You can sort the list by clicking the column header. The arrow (^) next to the header name indicates the sort order. Click the same header again to reverse the sort order.

To access the attachments list:

 Select E-mail Protection, then select Attachments.










Description [^]	Extension	Quarantine [^]
Application	^.EXE	
Batch File	^.BAT	
Compiled HTML Help File	^.CHM	
Control Panel Extension	^.CPL	
HTML Applications	^.HTA	
Internet Communication Settings	^.IIS	
Internet Communication Settings	^.ISP	
Internet Shortcut (Uniform Resource Locator)	^.URL	
Internet Shortcut (Uniform Resource Locator)	^.URL	

Figure 7-1: Attachments list

Changing the quarantine setting for an attachment type

Zone Labs security software comes configured with more than 45 attachment types that are capable of carrying worms or other harmful code. By default, Zone Labs security software quarantines all of these attachment types. These attachment types are displayed in the attachments list.

To change the quarantine setting for a specific attachment type:

1. Select **E-mail Protection | Attachments**.
2. In the Quarantine column, click an extension type.
3. Select **Quarantine** or **Allow**, then click **Apply**.

Adding and removing attachment types

If you want to quarantine attachments of a type that does not appear on the attachments list, you can add to the list as many unique attachment types as you like.

For your protection, Zone Labs security software prevents you from removing the default attachment types. However, you can remove any attachment types you may have added.

To add an attachment type to the list:

1. Select **E-mail Protection | Attachments**.
2. Click **Add**.
3. Type a description and filename extension (with or without the “.” character), then click **OK**.
4. Click **Apply** to save your changes.

To remove an attachment type from the list:

1. Select **E-mail Protection | Attachments**.
2. In the **Extensions** column, right-click an attachment type.
3. Select **Remove**.

Opening a quarantined attachment

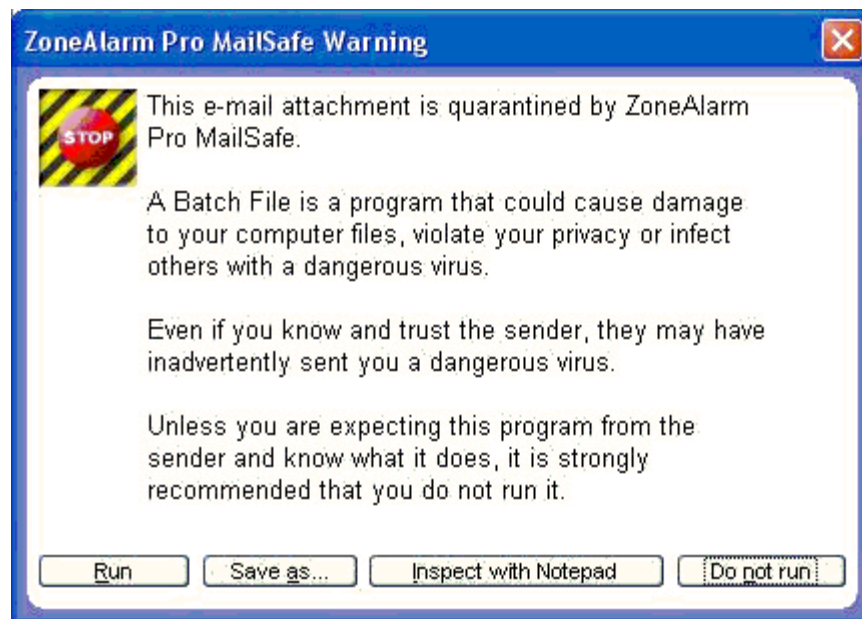
To view the code of the attachment itself, you can open the attachment in Notepad.



For best security, you should never open an e-mail attachment that Zone Labs security software has quarantined unless the sender is someone you know and trust, and you have confirmed the sender sent the message intentionally and the sender is sure that the attachment is harmless.

To open a quarantined attachment:

1. In Windows Explorer, browse to the file you want to open.
2. Double-click the attachment to open it.
3. When you attempt to open an attachment that has been quarantined, Zone Labs security software warns you of the potential risk in opening the attachment.



4. Click **Inspect with Notepad**.

Customizing Outbound MailSafe protection

By default, an Outbound MailSafe protection alert is displayed when your e-mail application attempts to send more than five e-mail messages within two seconds, or if an e-mail message has more than fifty recipients. You can customize these settings to extend the time interval, increase the number of messages and recipients allowed, or specify the e-mail addresses that are allowed to send e-mail from your computer.

Enabling Outbound MailSafe protection by program

When Outbound MailSafe protection is set to On, protection is enabled for all programs that have been granted permission to send e-mail.

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

For information on setting permissions for a program, see “Setting permissions for specific programs,” on page 76.

To enable or disable Outbound MailSafe protection for a program:

1. Select **Program Control | Programs**.
2. In the Programs column, right-click a program name, then select **Options**.
3. Select the **Security** tab.
4. In the Outbound MailSafe Protection area, select the check box labeled **Enable Outbound MailSafe Protection for this program**.

To disable Outbound MailSafe protection, clear this check box.

5. Click **OK**.

Setting Outbound MailSafe protection options

By default, Outbound MailSafe Protection is activated when your computer attempts to send more than five e-mail messages within two seconds, or an e-mail message with more than 50 recipients.

Because even legitimate e-mail messages may have one or both of these characteristics, you may want to customize Outbound MailSafe protection settings to better meet your individual needs.

To customize Outbound MailSafe protection settings:

1. Select **E-mail Protection | Main**, then click **Advanced**.

The Advanced E-mail Protection dialog appears.

2. In the Display Outbound MailSafe Protection Alerts When area, choose your settings.

Too many e-mails are sent at once	An Outbound MailSafe protection alert appears when your computer attempts to send more than the specified number of e-mails within the specified time interval.
A message has too many recipients	An Outbound MailSafe protection alert appears when your computer attempts to send an e-mail message with more than the specified number of recipients.
If the sender's address is not in this list	An Outbound MailSafe protection alert appears when your computer attempts to send an e-mail whose originating address (i.e., the address in the From: field) does not appear on the list. To prevent Zone Labs security software from blocking all outgoing e-mail, make sure that your valid e-mail address appears on this list.

3. Click OK.

Filtering junk e-mail

The Junk E-mail Filter is available in ZoneAlarm Security Suite.

Use the junk e-mail filter to prevent unsolicited junk e-mail (commonly referred to as *spam*) from cluttering your Inbox. The Junk E-mail filter supports Microsoft Outlook and Outlook Express (both referred to in this document simply as “Outlook”).

During installation, Zone Labs security software adds the junk e-mail filter toolbar to your Outlook e-mail program’s toolbar.



Figure 7-2: The junk e-mail filter toolbar



If you have installed Zone Labs security software but the junk e-mail filter toolbar does not appear in your Outlook toolbar, right-click in your Outlook toolbar and choose **ZoneAlarmOutlookAddin**.

The junk e-mail filter also adds three special folders to your Outlook folder list: *ZoneAlarm Challenged Mail*, *ZoneAlarm Junk Mail*, and *ZoneAlarm Fraudulent Mail*. When Zone Labs security software identifies an e-mail message as junk, fraudulent, or challenged, it puts the message in one of these folders. If you are using Outlook to access Hotmail, you must use the junk e-mail filter’s spam blocking features and special folders instead of Hotmail’s.

Allowing or blocking e-mail from specific senders

Each time you send an e-mail to a new person, the junk e-mail filter automatically adds to the Allowed list, the address in the To field. Messages sent to you from those addresses will be put in your Inbox.

When you receive an e-mail from a sender on the Blocked list, the junk e-mail filter automatically moves the message to the Outlook folder named *ZoneAlarm Junk Mail*.

If an unwanted e-mail arrives in your Outlook Inbox, you can easily add the sender of that message to your Blocked People list.

To add e-mail addresses to your Allowed or Blocked list:

1. In your Outlook or Outlook Express e-mail program, select an e-mail.
2. In the junk e-mail filter toolbar, click **ZoneAlarm Options**, then choose **Allow Sender** or **Block Sender**.

Allowing or blocking e-mail from specific companies

The junk e-mail filter allows you to add all e-mail addresses originating from a particular company or network domain to your Companies Allowed or Blocked lists.

To add companies to your Allowed or Blocked list:

1. In your Outlook or Outlook Express e-mail program, select an e-mail.
2. In the junk e-mail filter toolbar, click **ZoneAlarm Options**, then choose **Allow Sender's Company** or **Block Sender's Company**.

The junk e-mail filter adds the domain portion of the sender's address (for example, *example.com*) to the list of allowed or blocked addresses.

Adding contacts to the Allowed List

You can scan the default contacts folder in your e-mail program to add contacts to the list of senders from whom you wish to receive e-mail.

To add contacts to the Allowed List:

1. Open your Outlook or Outlook Express e-mail program.
2. In the junk e-mail filter toolbar, click **ZoneAlarm Options**, then choose **Populate Allowed List**.

Scanning your Inbox

You can scan the contents of your Inbox for fraudulent e-mail and spam. You can use the Scan Inbox option to scan IMAP, POP3, and Hotmail accounts created in Outlook Express, and IMAP, POP3 and Exchange server accounts in Outlook.

To scan your Inbox:

1. Open your Outlook or Outlook Express e-mail program.
2. Select the Inbox you want to scan.
3. In the junk e-mail filter toolbar, click **ZoneAlarm Options**, then choose **Scan selected Inbox**.

Allowing e-mail from distribution lists

If you receive or send e-mail to multiple addressees contained in a distribution list, the junk e-mail filter may block that list name unless it has been added to the Lists tab.

To allow e-mail from mailing lists:

1. Start your Outlook or Outlook Express e-mail program.
2. In the junk e-mail filter toolbar, click **ZoneAlarm Options | Configure Preferences | Lists**.
3. Click **Add**.

4. Type the e-mail address of the distribution list into the text entry area, then click **OK**.

The junk e-mail filter adds the distribution list's e-mail address to the list of allowed addresses.

5. Click **Close** to save your changes and close the Lists tab.

Reporting junk e-mail

The junk e-mail filter allows you to contribute instances of junk e-mail to the Zone Labs Collaborative Filter database.

The junk e-mail filter never sends e-mail of any type from your computer without your permission. When you contribute junk e-mail to the Collaborative Filter database, you can choose to send either the actual e-mail or a digitally processed (sometimes referred to as “hashed”) summary of the e-mail that removes all content, headers, and personally identifiable information from the message. Sending the entire message enables complete analysis of the contents; sending a digitally processed summary of the message ensures complete privacy.



MailFrontier, a trusted Zone Labs partner, manages the Collaborative Filter database for Zone Labs. You can view the full text of MailFrontier's privacy policy at: <http://www.mailfrontier.com/privacy.html>

To report junk e-mail:

1. In your Outlook or Outlook Express e-mail program, select an e-mail.
2. In the junk e-mail filter toolbar:
 - To send the junk e-mail itself, click **ZoneAlarm Options**, then choose **Report Junk E-mail**.
 - To send a digitally processed summary of the junk e-mail, click **Junk**.
3. In the **Contribute E-mail** dialog box, click **OK**.

The junk e-mail filter reports the junk e-mail to the Collaborative Filter database and moves the message to the special Outlook folder **ZoneAlarm Junk Mail**.



To restore e-mail that was incorrectly identified as junk, select the e-mail in the ZoneAlarm Junk Mail folder, and click Unjunk. The e-mail will be restored to your Outlook Inbox.

Reporting fraudulent e-mail

The junk e-mail filter allows you to report instances of fraudulent e-mail (sometimes referred to as *phishing*) to Zone Labs. When fraudulent mail is detected for the first time, a popup appears, asking if you would like to send the fraudulent mail to Zone Labs

for analysis. If you choose Yes, all future fraudulent messages will be sent without prompting you for confirmation. If you choose No, your choice will be reflected in the Configure Preferences dialog box.

The junk e-mail filter never sends e-mail of any type from your computer without your permission. When you report fraudulent e-mail, the junk e-mail filter forwards the complete and original message to Zone Labs.

Zone Labs never divulges your e-mail address, name or other personal information contained in a fraudulent e-mail except as required to investigate and prosecute the originator of the fraudulent message.

Zone Labs forwards selected portions of the reported message to government and law enforcement agencies with jurisdiction over e-mail fraud. These agencies are required by law to protect the confidentiality of the information contained in the message. Zone Labs separately informs individuals or institutions threatened by forwarding to them only the information required to alert them.

To report fraudulent e-mail:

1. In your Outlook or Outlook Express e-mail program, select an e-mail.
2. In the junk e-mail filter toolbar, click **ZoneAlarm Options**, then choose **Report Fraudulent E-mail**.
3. In the **Contribute E-mail** dialog box, click **OK**.

The junk e-mail filter reports the fraudulent e-mail to Zone Labs and moves the message to the special Outlook folder *ZoneAlarm Fraudulent Mail*. If you are using Outlook to access Hotmail, you must use the junk e-mail filter's spam blocking features and special folders instead of Hotmail's.



MailFrontier, a trusted Zone Labs partner, manages the processing of fraudulent e-mail for Zone Labs. You can view the full text of MailFrontier's privacy policy at: <http://www.mailfrontier.com/privacy.html>

Specifying junk e-mail message options

The junk e-mail filter uses three message filtering techniques: *collaborative filter*, *message filters*, and *foreign language filters*. Filter settings determine how messages are treated when received from unknown senders.

Collaborative Filter

Collaborative filtering uses information extracted from junk e-mail reported by you and other Zone Labs security software users to determine whether new messages received from unknown users is spam.

Message Filters

Message filters use heuristic rules to analyze e-mail for characteristics common to various types of junk e-mail.

Foreign language filters

Foreign language filters block e-mail containing non-european languages. (The junk e-mail filter automatically manages e-mail in common european languages such as French, German, or Spanish.)

To customize message filtering options:

1. Start your Outlook or Outlook Express e-mail program.
2. In the junk e-mail filter toolbar, click **ZoneAlarm Options | Configure Preferences | Messages**.

Collaborative Filter	In the area, move the slider to adjust the responsiveness to the characteristics of junk e-mail reported by other Zone Labs security software users.
Message Filters	Move the slider to adjust the responsiveness to common junk e-mail. You can also adjust the responsiveness to specific categories of junk e-mail.
Language Filters	In the area, click Configure then choose which languages to block.

3. Click **Close**.

Challenging e-mail from unknown senders

You can choose to have the junk e-mail filter reply to an e-mail from an unknown sender with a challenge e-mail. Because junk e-mail seldom contains a valid return address, an unanswered challenge confirms that the e-mail is probably junk.

The challenge e-mail instructs the recipient to click a button in the message to validate that he or she was the author of the message. Clicking the button directs the junk e-mail

filter to move the e-mail from the special Outlook folder **ZoneAlarm Challenged Mail** folder to your Outlook Inbox.

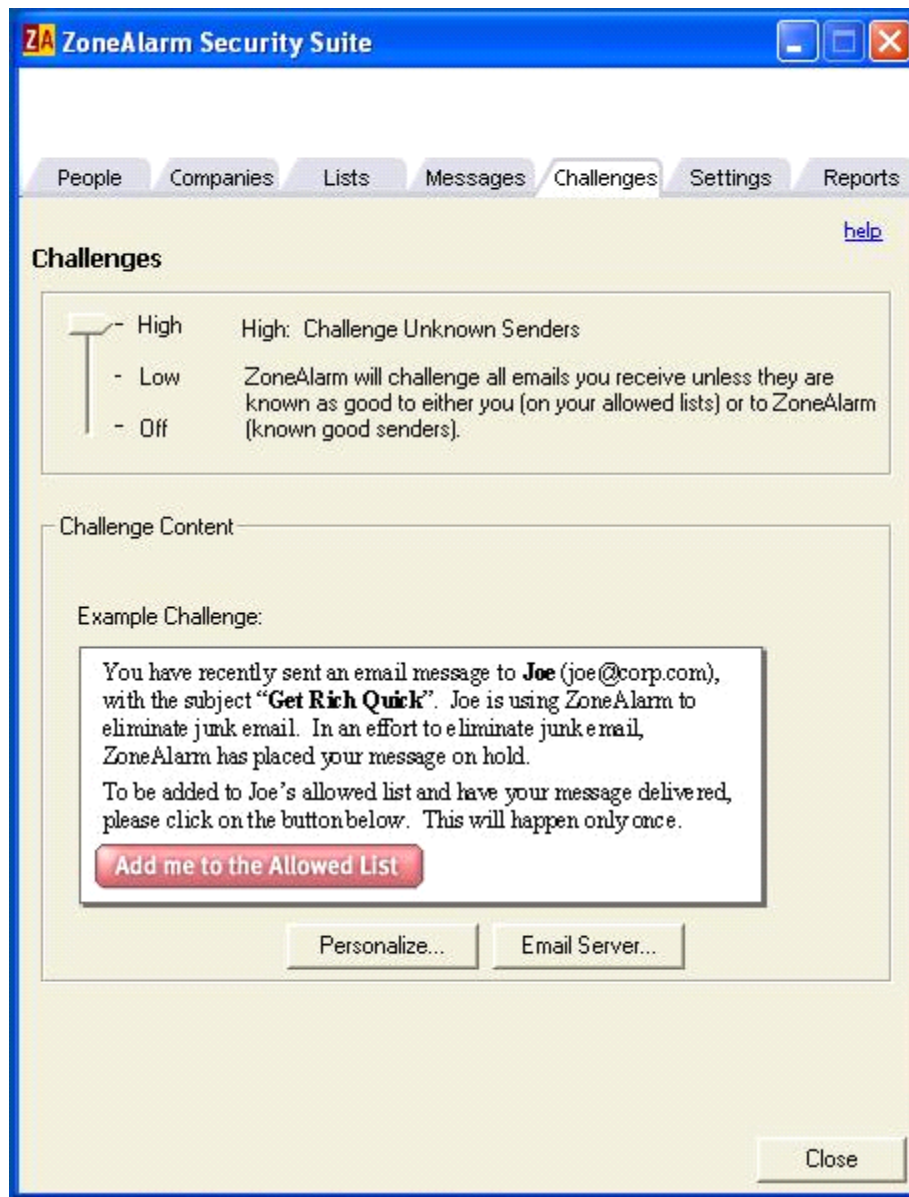


Figure 7-3: Challenge options tab

For messages from an unknown sender, you can choose whether to always send a challenge e-mail, to send a challenge only when the incoming message appears to be junk e-mail, or to never send a challenge. In addition you can customize the challenge e-mail that is sent to users.

To enable challenge e-mails:

1. Start your Outlook or Outlook Express e-mail program.

2. In the junk e-mail filter toolbar, click **ZoneAlarm Options | Configure Preferences | Challenges**.
3. In the Challenges area, use the slider to choose when to send a challenge e-mail.

High	Zone Labs security software will challenge all e-mails that you receive unless they are known as good to either you (on your allowed lists) or to MailFrontier (known good senders). Any e-mail message that is received and can be classified immediately as junk gets sent directly to the ZoneAlarm Mail folder for later deletion and does NOT get a challenge issued.
Low	Zone Labs security software will challenge uncertain e-mail. Zone Labs security software will only challenge e-mails that it cannot determine with certainty are spam or are good. This is typically a small percentage of the e-mail you receive.
Off	Challenge e-mails will not be sent. Zone Labs security software will not send challenge e-mails. Move the slider up to turn on e-mail challenges to eliminate junk e-mail sent by spammer computers.

4. To add a personal message to the standard challenge e-mail, click **Personalize**, type your name and your personal message, then click **OK**.
5. Click **Close**.

The junk e-mail filter moves the message to the **ZoneAlarm Challenged Mail** folder



While waiting for the response to a challenge message, the junk e-mail filter stores your e-mail address. As soon as the challenge has been completely processed, the junk e-mail filter discards the address. If you experience problems sending challenge e-mails, see "Specifying your outbound e-mail server," on page 129.

Specifying your outbound e-mail server

To send challenge e-mails, the junk e-mail filter requires the ability to send e-mail. In most cases the junk e-mail filter uses Outlook's default outbound mail server. If you experience problems sending challenge e-mails, you may need to specify the name of your outbound e-mail server.

To specify the name of an outbound e-mail server:

1. Start your Outlook or Outlook Express e-mail program.
2. In the junk e-mail filter toolbar, click **ZoneAlarm Options | Configure Preferences | Challenges**.
3. In the Challenge Content area, click **E-mail Server**.

4. Type the name of your outbound e-mail server, then click **OK**.
5. Click **Close**.

Customizing junk e-mail filter settings

By default, the junk e-mail filter retains fraudulent e-mail messages in the **ZoneAlarm Fraudulent Mail** folder until you manually delete them. You can specify how long e-mail messages are stored in the **ZoneAlarm Junk Mail** and **ZoneAlarm Challenged Mail** folders, as well as automate fraud e-mail reporting, and configure wireless device forwarding. In addition, if you could like to scan more than one Outlook Inbox, you can specify those settings here.

To specify storage duration for junk e-mail:

1. Start your Outlook or Outlook Express e-mail program.
2. In the junk e-mail filter toolbar, click **ZoneAlarm Options | Configure Preferences | Settings**.
3. In the Junk Folder Settings area, click **Configure**.
4. Type the number of days to retain suspected junk e-mail in the **ZoneAlarm Junk Mail** and **Zone Alarm Challenged Mail** folders.

The junk e-mail filter moves e-mail that has been in the folder for the specified number of days without being validated into Outlook's Deleted Items folder.

5. Click **Close**.

To configure a wireless device:

1. Start your Outlook or Outlook Express e-mail program
2. In the junk e-mail filter toolbar, click **ZoneAlarm Options | Configure Preferences | Settings**.
3. In the Wireless Device Support area, click **Configure**.
4. In the **Zone Alarm Wireless Support** dialog box, type the e-mail address of your wireless device.

You can also choose to forward only e-mail headers, and to specify the number of validate messages forwarded to your wireless device in a 24-hour period.

5. If you need to specify a non-default e-mail server, click **E-mail Server**, type the name of your outbound e-mail server, then click **OK**.

Click **Close** to save your changes and close the Settings tab.

To enable automatic reporting of fraudulent e-mail:

1. Start your Outlook or Outlook Express e-mail program.

2. In the junk e-mail filter toolbar, click **ZoneAlarm Options | Configure Preferences | Settings**.
3. In the Auto Report Fraud E-mail area, select the **Enable auto reporting...** check box.
4. Click **Close**.

To customize confirmation messages:

1. Start your Outlook or Outlook Express e-mail program.
2. In the junk e-mail filter toolbar, click **ZoneAlarm Options | Configure Preferences | Settings**.
3. In the Show Confirmations area, specify the settings you want.

Contribute Junk Email	Displays an alert prior to sending junk e-mail to Zone Labs.
Contribute Fraudulent Email	Displays an alert prior to sending fraudulent e-mail to Zone Labs.

4. Click **Close**.

To configure multiple Outlook inboxes:

1. Start your Outlook or Outlook Express e-mail program.
2. In the junk e-mail filter toolbar, click **ZoneAlarm Options | Configure Preferences | Settings**.
3. In the Outlook Multiple Inbox Support area, select the check box **Support scanning of multiple Inbox in Microsoft Outlook**.



This feature is supported for Outlook 2000, 2002 (XP), and 2003 only and is enabled by default.

Restoring e-mail incorrectly identified as junk

The junk e-mail filter adds three special folders to your Outlook folder list: **ZoneAlarm Challenged Mail**, **Zone Alarm Junk Mail**, and **Zone Alarm Fraudulent Mail**. When Zone Alarm security software identifies an e-mail message as junk, fraudulent, or challenged, it puts the message in one of these special folders.

If you are using Outlook to access Hotmail, you must use the junk e-mail filter's spam blocking features and special folders instead of Hotmail's.

You can restore mail that the junk e-mail filter incorrectly placed in a special folder to your Outlook Inbox.

To restore e-mail incorrectly identified as junk:

1. In your Outlook or Outlook Express e-mail program, in the **ZoneAlarm Challenged Mail**, **Zone Alarm Junk Mail**, or **Zone Alarm Fraudulent Mail** folder, choose an e-mail.
2. In the junk e-mail filter toolbar, click **Unjunk**.

The junk e-mail filter restores the selected message to your Outlook Inbox.

Viewing junk e-mail filter reports

Use the junk e-mail filter's Reports tab to view a summary of mail processing activity.

To view junk e-mail filter reports

1. Start your Outlook or Outlook Express e-mail program
2. In the junk e-mail filter toolbar, click **ZoneAlarm Options | Configure Preferences | Reports**.
3. Choose one of the four report types:

Junk by Day	The total number of legitimate and junk e-mails received by day.
Reasons	The reasons the junk e-mail filter blocked incoming e-mails by day
Total History Junk by Day	The total number of legitimate and junk e-mails received since Zone Labs security software was installed.
Total Reasons	The total number of reasons the junk e-mail filter blocked incoming e-mails since Zone Labs security software was installed.

4. Click **Close** to close the Reports tab.

Anti-virus protection for e-mail

In addition to the protection offered by MailSafe for incoming e-mail, ZoneAlarm Anti-virus and ZoneAlarm - Suite offer the additional protection of scanning incoming e-mail messages for viruses. Unlike MailSafe, E-mail scanning can detect viruses in the body of an e-mail message, as well as in attachments.

🔗 Enabling E-mail scanning

🔗 How e-mail infections are handled

Enabling E-mail scanning

ZoneAlarm Anti-virus and ZoneAlarm Security Suite users have Anti-virus protection for e-mail enabled by default.

To enable or disable E-mail scanning:

1. Select **Anti-virus / Anti-spyware | Main**.
2. In the Protection area, click **Advanced Options**.

The Advanced Options dialog appears.

3. Under Virus Management, select **E-mail Scanning**.
4. Select or clear the **Enable E-mail Scanning** check box, then click **OK**.

How e-mail infections are handled

When Zone Labs security software detects an infection in an e-mail attachment, it removes the infected file and attaches an Infection Report to the e-mail. The Infection report is a text file that contains information about the attachment that was removed from the e-mail, including the filename of the infection.



Figure 7-4: Example of an infection report

Infected attachments are renamed with a .zl6 file extension so that they can no longer be opened.



If you are a Eudora user and you have multiple Infection reports in your inbox, the name of the infection report may contain a numeral before the .txt extension.

When running Windows 98, the E-mail scanning feature renames MailSafe to *isafe.exe* rather than the name of the computer's e-mail program.

For more information about protecting your computer from viruses, see Chapter 6, "Spyware and Virus protection," starting on page 89.

Chapter

Privacy protection

8

Long ago, the World Wide Web contained nothing but harmless text-based pages. Today, Web pages frequently contain elements that can give away private information about you, interrupt your work with annoying pop-ups, or even damage your computer. In addition, the files that get left behind on your computer as you use the Web can slow down your computer's performance. Use privacy protection to guard yourself against the misuse of cookies, advertisements, and dynamic Web content, and to periodically rid your computer of unneeded Internet files.

The Privacy feature is available in ZoneAlarm Pro and ZoneAlarm Pro Security Suite.

Topics:

- “Understanding privacy protection,” on page 136
- “Setting general privacy options,” on page 137
- “Using Privacy Advisor,” on page 139
- “Setting privacy options for specific Web sites,” on page 140
- “Customizing cookie control,” on page 142
- “Customizing ad blocking,” on page 144
- “Customizing mobile code control,” on page 146
- “Understanding Cache cleaner,” on page 147

Understanding privacy protection

Privacy protection helps you manage Web site elements that are commonly used either to display advertising content, or to collect data about you and your Web browsing habits. In addition, privacy settings protect you from the misuse of certain types of dynamic Web content, or mobile code.

Cookie Control keeps advertisers from spying on your Internet habits, and prevents sensitive information (passwords, for example) from being stored in cookies where they can be stolen if a hacker breaks into your computer.

Ad Blocking keeps unwanted advertisements from disrupting your Internet work. With Zone Labs security software you can block all types of ads (*banner ad*, *animated ad*, and so forth) or only specific types.

Mobile Code Control keeps hackers from using active Web page content such as Java applets, *ActiveX controls* controls and plug-ins to compromise your security or damage your computer. Be aware that many legitimate Web sites use mobile code, and that enabling mobile code control may affect the functionality of these Web sites.

Cache Cleaner keeps your computer clutter-free by deleting excess files you collect while you surf the Web and use your computer. It also maintains your privacy by deleting your URL history and browser cache and other files you specify.

The Privacy feature is available in Zone Alarm Pro and ZoneAlarm Security Suite.

Setting general privacy options

Privacy protection is enabled for your browser only if you selected it during setup. If you did not enable privacy during setup, you can enable it manually.

The Privacy group of features that includes the general privacy options is available in Zone Alarm Pro and ZoneAlarm Security Suite.

Setting privacy protection levels

By setting the privacy protection level, you determine whether to allow or block cookies, ads, and mobile code.

To set privacy levels:

1. Select **Privacy | Main**.
2. In the Cookie control area, click the slider and drag it to the desired setting.

High	Blocks all cookies except session cookies. This setting may prevent some Web sites from loading.
Med	Blocks persistent cookies and third party cookies from tracking Web sites. Allows cookies for personalized services.
Off	Allows all cookies.

3. In the Ad Blocking area, click the slider and drag it to the desired setting.

High	Blocks all ads. Blocks all pop-up/pop-under and animated ads.
Med	Blocks all pop-up/pop-under and animated ads. Allows banner ads.
Off	Allows all ads.

4. In the Mobile Code Control area, select **On** or **Off**.
5. Click **OK**.

Applying privacy protection to programs other than browsers

By default, privacy protection is applied only to standard browser programs such as Internet Explorer. You can also enable privacy protection for any other program on your computer.

To apply privacy protection control to a program other than a browser:

1. Select **Program Control | Programs**.
2. In the Programs column, click a program name, then click **Options**.

The Program Options dialog appears.

3. Select the **Security** tab.

4. In the Filter Options area, select the check box labeled **Enable Privacy for this program**.

Using Privacy Advisor

Privacy Advisor is an alert that appears when Zone Labs security software blocks cookies or mobile code, and enables you to allow those elements for a particular page.



Figure 8-1: Privacy Advisor

The Privacy group of features that includes Privacy Advisor is available in Zone Alarm Pro and ZoneAlarm Security Suite. To prevent Privacy Advisor from appearing each time Web page elements are blocked, select the check box labeled **Turn Off Privacy Advisor**.



Although the Site Verification is displayed in the same alert window as the Privacy Advisor, the two are enabled and disabled independently. If you disable Privacy Advisor, the Site Verification alert will appear on its own and vice versa. For more information about Site Verification, see “Licensing, registration, and support,” on page 27.

To enable or disable Privacy Advisor:

1. Select **Privacy | Main**.
2. In the Cookies area, click **Custom**.
The Custom Privacy Settings dialog box appears.
3. In the Privacy Advisor area, clear the **Show Privacy Advisor** check box.
4. Click **Ok**.



To see details or to change privacy settings immediately, click the link labeled **Click here for details**. Zone Labs security software opens to the Privacy panel.

Setting privacy options for specific Web sites

When you browse the Internet, the sites you visit are added to the privacy site list, where you can specify custom privacy options for that site. You also can add a site to the list to customize privacy settings. The Privacy group of features is available in Zone Alarm Pro and ZoneAlarm Security Suite.

Viewing the privacy site list

The list displays sites you have visited in your current Zone Labs security software session, and sites for which you have previously customized settings. If you do not customize settings for a site you've visited, it is dropped from the list when you shut down your computer or shut down Zone Labs security software.



Privacy protection is applied at the domain level, even if a sub-domain appears in the Site List. For example, if you manually add the sub-domain news.google.com to the list, privacy protection will be applied to the entire domain of google.com.

To access the Privacy site list:

Select Privacy|Site List.

Site	Edited	Mobile Code	Cookie Control			Web Bugs	Private Header
			Session	Persistent	3rd Party		
mysite1.com							
mysite2.com							
mysite3.com							
mysite4.com							
mysite5.com							
mysite6.com							
server-us.imrworldwide.com							

Figure 8-2: Privacy site list

A pencil icon in the Edited column indicates that you have customized privacy settings for that site, and that the site will remain in your list.



Using third-party ad blocking software at the same time as Zone Labs security software may prevent the privacy site list from being populated properly.

Adding sites to the privacy site list

To customize privacy settings for a site that does not appear on the site list, you can add the site manually, then edit the privacy options for that site.

To add a site to the privacy site list:

1. Select **Privacy | Site List**.

2. Click **Add**.

The Add Site dialog appears.

3. In the **URL** field, enter the URL of the site you want to add, then click **OK**.

The URL must be a fully qualified host name, for example, `www.yahoo.com`.



If you are using AOL with ZoneAlarm Pro and have enabled Privacy protection, the site `ie3.proxy.aol.com` is added to the Privacy Site List when you visit any site during an AOL session. For example, if during your AOL session you visit the site `www.cnn.com`, only the AOL proxy site, `ie3.proxy.aol.com` is added to the Privacy Site List. The privacy settings for the `ie3.proxy.aol.com` site affect all sites visited within AOL. If you manually add a site to the site list, the privacy settings for that site will be ignored, and only the security settings for the AOL proxy site, `ie3.proxy.aol.com`, are in effect.

Editing sites on the site list

You can customize the behavior of Cookie Control, Ad Blocking, and Mobile Code Control by editing the privacy options for sites on the Site List.

1. Select **Privacy | Site List**.

2. In the Site column, select the site you want to edit, then click **Options**.

The Site Options dialog appears.

3. Select either the Cookies, Ad Blocking, or Mobile Code tab.

For help with selecting custom options, see “Customizing cookie control,” on page 142, “Customizing ad blocking,” on page 144, and “Customizing mobile code control,” on page 146.

4. Specify your options, then click **OK**.

Customizing cookie control

Internet cookies make it possible for e-commerce sites (like Amazon, for example) to recognize you as soon as you arrive and customize the pages you visit. However, cookies can also be used to record information about your Web browsing habits and give that information to marketers and advertisers.

By default, Cookie control is disabled and all types of cookies are allowed. You can instantly block all cookies by choosing the High cookie-control setting, which gives you full protection against all types of cookie abuse—but at the expense of the convenience that cookies make possible.

If you wish, you can instantly block all cookies by choosing the high cookie-control setting, giving you full protection against all types of cookie abuse—but at the expense of the convenience that cookies make possible.

You can customize cookie control by specifying which types of cookies are blocked and if cookies are allowed, when those cookies should expire.

The Privacy group of features that includes cookie control is available in Zone Alarm Pro and ZoneAlarm Security Suite.

Blocking session cookies

Session cookies are stored in your browser's memory cache while you browsing a Web Site and disappear when you close your browser window. Session cookies are the safest type of *cookie* because of their short life span.

To block session cookies:

1. Select **Privacy | Main**.
2. In the Cookies area, click **Custom**.
3. In the Session cookies area, select the **Block session cookies check box**.
4. Click **OK**.

Blocking persistent cookies

Persistent cookies are placed on your hard disk by Web sites you visit so that they can be retrieved by the Web site the next time you visit. While useful, they create a vulnerability by storing information about you, your computer, or your Internet use in a text file.

To block persistent cookies:

1. Select **Privacy | Main**.
2. In the Cookies area, click **Custom**.
3. In the Persistent cookies area, select the **Block persistent cookies check box**.
4. Click **OK**.

Blocking third-party cookies

A third-party cookie is a type of persistent cookie that is placed on your computer, not by the Web site you are visiting, but by an advertiser or other third party. These cookies are commonly used to deliver information about your Internet activity to that third party.

To block third-party cookies:

1. Select **Privacy | Main**.
2. In the Cookies area, click **Custom**.
3. In the 3rd Party Cookies area, specify the cookie type(s) you want to block.

Block 3rd party cookies	Blocks cookies from third-party Web sites.
Disable web bugs	Prevents advertisers from finding out which advertisements and Web pages you have viewed. Blocked web bugs appear as blank boxes.
Remove private header information	Prevents your IP address, your workstation name, login name, or other personal information from being transferred to third-party sources.

Setting an expiration date for cookies

The sites that use persistent cookies may set those cookies to remain active for a few days, several months, or indefinitely. While a cookie is active, the site (or third party) that created it can use the cookie to retrieve information. After the cookie expires, it can no longer be accessed.

If you choose to allow persistent cookies, you can override their expiration dates and specify how long they will remain active before expiring.

To set an expiration date for cookies:

1. Select **Privacy | Main**.
2. In the Cookies area, click **Custom**.
3. In the Cookie Expiration area, select the **Expire cookies** check box.
4. Specify when cookies expire.

Immediately after receipt	Allows persistent cookies to operate only during the session in which they were received.
After n days	Allows persistent cookies to remain active for the number of days you specify. You can choose any number from 1 to 999. The default setting is 1.

5. Click **Apply**, then click **OK**.

Customizing ad blocking

Ad blocking is disabled by default. You can customize ad blocking to block all ads or block only specific types of ads. In addition, you can specify what Zone Labs security software displays in place of blocked ads.

The Privacy group of features that includes ad blocking is available in Zone Alarm Pro and ZoneAlarm Security Suite.

Specifying which ads to block

Privacy protection allows you to specify which types of ads to block or to allow.

To specify which ads to block:

1. Select **Privacy | Main**.

2. In the Ad Blocking area, click **Custom**.

The Custom Privacy settings dialog appears.

3. In the Ads to Block area, select the type of ad you want to block.

Banner/sky-scraper ads	Blocks ads that appear in either a horizontal or vertical banner.
Pop-up/pop-under	Blocks ads that appear in a new browser window in front of or behind the window you are viewing.
Animated ads	Blocks ads that incorporate moving images.

4. Click **OK**.

Setting ad void control options

When Zone Labs security software blocks banner, skyscraper, or animated ads, it leaves a “void” or blank on your screen where the ad was to be displayed. Ad void control lets you specify what will be displayed in that space.

To specify what appears in place of blocked ads:

1. Select **Privacy | Main**.

2. In the Ad Blocking area, click **Custom**.

The Custom Privacy settings dialog appears.

3. In the Ad Void Control area, specify the method for controlling blocked ads.

Nothing	Blocks ads without any indication that the ads were to appear.
A box with the word “[AD]”	Displays a window containing the word AD. This is the default setting.

A box I can mouse over to get the ad to appear	Displays a window containing the ad that appears only when you activate the window using your mouse.
--	--

4. Click OK.

Customizing mobile code control

Mobile code is content on a Web page that is active or executable in nature. Examples of active content include, a *Java applet*, *ActiveX controls*, and *JavaScript*, all of which can be used to make Web pages more interactive and dynamic.

Malicious mobile code, however, can copy files, clear your a hard disk, steal passwords, or command servers. Mobile code control keeps hackers from using active content to compromise your security or damage your computer.

The default setting for mobile code control is Off. When turned to On, all mobile code except JavaScript is blocked. You can customize your mobile code control settings by specifying what types of mobile code are blocked when mobile code control is set to On.

The Privacy group of features that includes mobile code control is available in Zone Alarm Pro and ZoneAlarm Security Suite.

Specifying which types of mobile code to block

You can customize mobile code control by which types of active content to block and which to allow.

To customize mobile code control

1. Select **Privacy | Main**.
2. In the Mobile Code Control area, click **Custom**.

The Custom Privacy settings dialog appears.

3. In the Mobile Code Control area, specify the types of mobile code to block.

Block JavaScript	Blocks JavaScript content, including that required for common uses such as Back and History links, rollover images, and opening and closing browser windows.
Block scripts (vbscript, etc.)	Blocks scripts that execute automatically, including those required for displaying banners, pop-up ads, and dynamic menus.
Block embedded objects (java, ActiveX)	Blocks objects embedded in Web pages, including sound and image files.
Block mime-type integrated objects	Block mime-type integrated objects Blocks objects whose MIME-type indicates that they are applications. Note: This option also blocks legitimate executable files sent through the browser, including downloads that you may want to allow. When this occurs, you'll see the error "This object has been blocked" in the browser. For downloads initiated by you, it is safe to disable the Block mime-type integrated objects feature.

Understanding Cache cleaner

Whenever you open a file, view a Web page, or fill out an online form, copies of the Web pages you view are stored in your browser's cache, enabling pages to load more quickly. If you're working on a shared computer, these files also are available for viewing by anyone who uses that computer.

Similarly, when you open a file, delete a file, or search for files on your computer, these actions leave behind an electronic trail designed to help you retrace your steps, should you need to in the future. Although useful, over time this excess clutter can affect your computer's performance and processing efficiency. And, again, if you are using a shared computer, anyone who uses that computer can find out what Web sites you have viewed.

Use Zone Labs security software's Cache Cleaner to periodically rid your computer of these excess files, free up disk space, and ensure your privacy.

The Privacy group of features that includes cache cleaner is available in Zone Alarm Pro and ZoneAlarm Security Suite.

Using Cache Cleaner

You can run Cache Cleaner manually anytime you want to. If you prefer to schedule cache cleanings, you can configure Cache Cleaner to run automatically at regular intervals: as often as every day, to as infrequently as every 99 days. The default value for automatic cleaning is every 14 days.

To run Cache Cleaner manually:

1. Select **Privacy | Cache Cleaner**.
2. Click **Clean Now**.

A verification message appears.

3. Click **OK**.

You will see a progress meter while Cache Cleaner runs.

To schedule Cache Cleaner to run automatically:

1. Select **Privacy | Cache Cleaner**.
2. Select the **Clean cache automatically every** check box.
3. In the Clean Cache Automatically area, specify a cleaning interval between 1 and 99.

The dates of the last cleaning and the next scheduled cleaning is displayed below the check box.

Customizing hard drive cleaning options

By default, Cache Cleaner cleans the following files from your hard drive:

- Contents of the Recycle Bin
- Contents of the Temp files directory
- Windows Scandisk fragments

You can customize these settings by specifying additional areas to be cleaned, including your Document history, Search history, or Windows Media Player history.

To customize cleaning options for your hard drive:

1. Select **Privacy | Cache Cleaner**, then click **Custom**.
2. Select **Hard Drive**, then specify cleaning options.

Clean Document history	Cleans the list of files that appears at Start Documents . This setting only applies to the document history for the currently logged-in user.
Clean Recycle Bin	Cleans the contents of the Windows Recycle Bin. Selected by default.
Clean temp files directory	Cleans the Windows temp directories. Selected by default.
Clean Windows Find/Search history	Cleans the items in the Windows Find/Search list.
Clean Windows Scandisk fragments	Cleans chunks of lost or damaged data recovered by Windows' ScanDisk program. Selected by default.
Clean Windows Media Player history	Cleans the list of recently played media clips in Windows Media Player.
Run history	Cleans the list that appears in the Open drop-down list at Start Run .

3. Click **Apply**, then click **OK**.

Customizing browser cleaning options

If you use either Internet Explorer or Netscape, you can configure Cache Cleaner to remove cookie files that are stored on your computer while you browse the Web. Cache Cleaner identifies cookies to remove by the cookie source, rather than by the individual cookie file. When you specify a cookie source to remove, Cache Cleaner removes all cookies from that source. If there are cookies on your computer that you do not want to remove, you can configure Cache Cleaner to retain those cookies.

To customize cleaning options for IE/MSN:

1. Select **Privacy | Cache Cleaner**, then click **Custom**.
2. Select the **IE/MSN** tab.

3. In the Internet Explorer/MSN cleaning options area, specify the areas to be cleaned.

Clean cache	Cleans the Internet Explorer browser cache. Selected by default.
Clean URL history	Cleans the URLs list in the Address field.
Clean AutoComplete forms	Cleans the previous entries you've made for Web forms, including passwords. Note: If you do not want your passwords to be cleaned, clear the "Clean AutoComplete forms" check box.
Clean AutoComplete passwords	Cleans passwords for which you selected "Remember password."
Clean locked Index.dat files	Cleans <i>index.dat</i> files that are currently in use by your computer. Selected by default.
Clean typed URL history	Cleans the URLs you have typed into the Address field.

4. To remove cookies, select the **Clean IE/MSN cookies check box, then click **Select**.**

The Select IE/MSN cookies to keep dialog appears. The list on the left shows the sites for which the browser currently has cookies. The list on the right shows the sites whose cookies you do not want to clean.

5. To retain a cookie source, select the cookie source, then click **Keep.**

6. To remove remaining cookies, click **Remove, then click **OK**.**

To customize cleaning options for Netscape:

1. Select **Privacy | Cache Cleaner, then click **Custom**.**

2. Select the **Netscape tab.**

3. In the Netscape cleaning options area, specify the areas to be cleaned.

Clean cache	Cleans the Netscape browser cache. Selected by default.
Clean URL history	Cleans the URLs list in the Location field.
Clean mail trash	Cleans the Netscape Mail Trash folder.
Clean forms data	Cleans the previous entries you've made for Web forms.

4. To remove cookies, select the **Clean Netscape cookies check box and then click **Select**.**

The Select Netscape cookies to keep dialog appears. The list on the left shows the sites for which the browser currently has cookies. The list on the right shows the sites whose cookies you do not want to clean.

5. To retain a cookie source, select the cookie source, then click **Keep**.
6. To remove remaining cookies, click **Remove**, then click **OK**.

Chapter

Alerts and Logs

9

Whether you're the type of person who wants to know everything that happens on your computer—or you only want to know that your computer is secure, Zone Labs security software accommodates you. You can be notified by an alert each time Zone Labs security software acts to protect you; or only when an alert is likely to have resulted from hacker activity. You can also choose to log all alerts, only high-rated alerts, or alerts caused by specific traffic types.

Topics:

- “Understanding alerts and logs,” on page 152
- “Setting basic alert and log options,” on page 160
- “Controlling the number of alerts,” on page 161
- “Game Mode,” on page 162
- “Setting event and program log options,” on page 164
- “Using SmartDefense Advisor and Hacker ID,” on page 170

Understanding alerts and logs

Zone Labs security software alert and logging features keep you aware of what's happening on your computer without being overly intrusive, and enable you to go back at any time to investigate past alerts. Expert rule options let you track not only blocked traffic, but allowed traffic as well, giving advanced users maximum information options when customizing security rules for their environment.

About Zone Labs security software alerts

Zone Labs security software alerts fall into three basic categories: informational, program, and network. Additional alerts that may appear based on the version of Zone Labs security software you are using include ID Lock alerts and OSFirewall alerts.



To learn about the types of alerts that appear and how to respond to them, see Appendix A, "Alert reference," starting on page 203.

Informational alerts

Informational alerts tell you that Zone Labs security software has blocked a communication that did not fit your security settings. The most common type of informational alert is the Firewall alert.

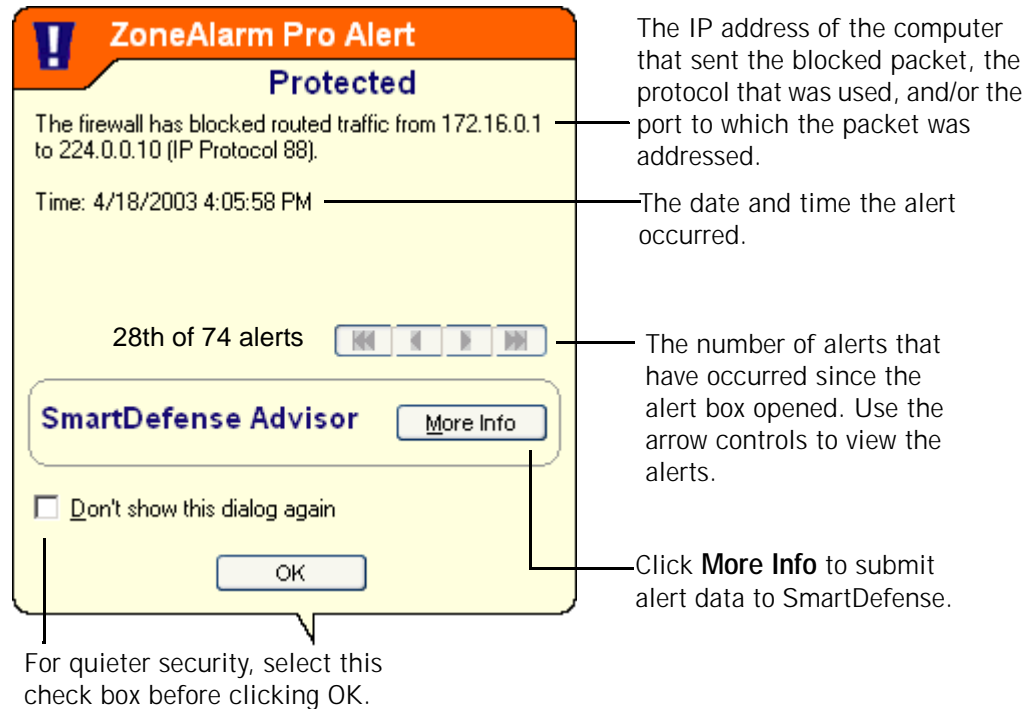


Figure 9-1: Firewall alert

Informational alerts don't require a decision from you. You can close the alert by clicking **OK** at the bottom of the alert. By doing this you are not allowing any traffic to access your computer.

Program alerts

Program alerts ask you if you want to allow a program to access the Internet or local network, or to act as a server. Program alerts require an Allow or Deny response. The

most common types of Program alerts are the New Program alert and Repeat Program alert.

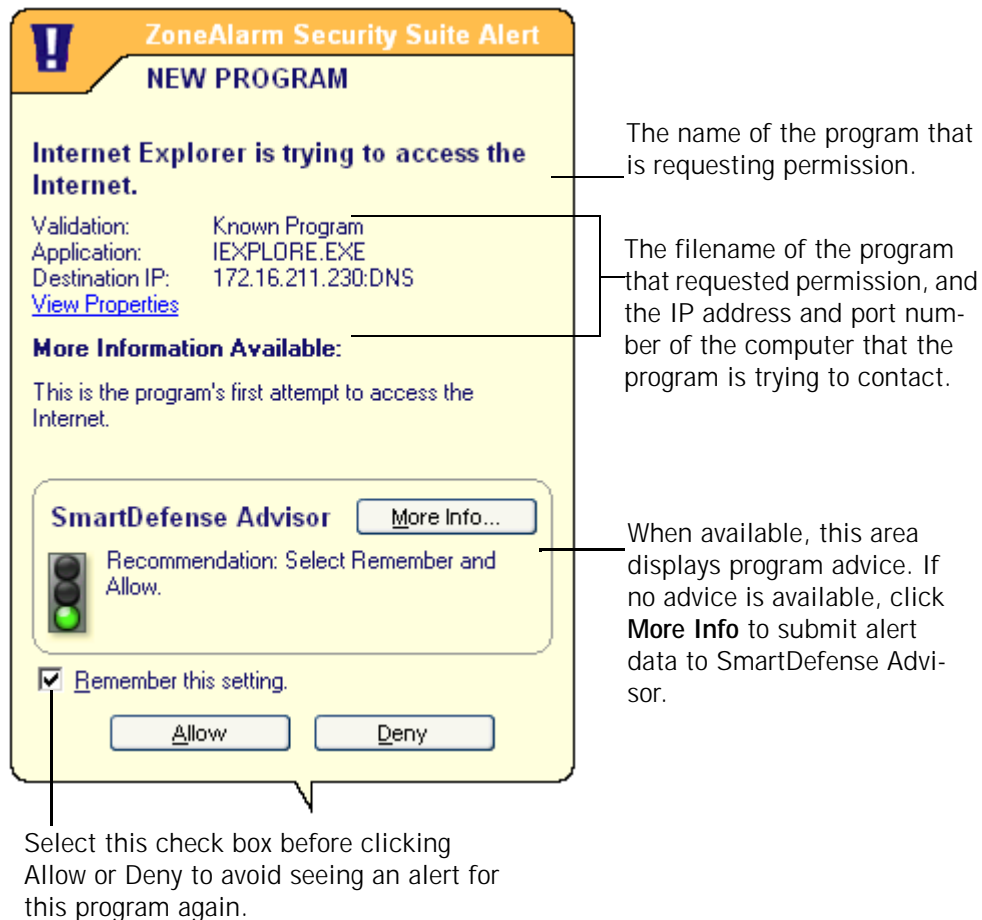


Figure 9-2: New Program alert

By clicking **Allow**, you grant permission to the program. By clicking **Deny**, you deny permission to the program. If SmartDefense Advisor is set to “Auto,” Zone Labs security software issues Program alerts only if no automatic setting is available. If you choose **Remember this setting** in a Program alert when allowing or denying program access, Zone Labs security software keeps your setting unless SmartDefense Advisor comes out with a different setting, or until you change the setting manually in the Programs tab. If you do not choose **Remember this setting**, Zone Labs security software will issue another Program alert the next time the program attempts the same action.

New Network alerts

New Network alerts occur when you connect to any network—be it a wireless home network, a business LAN, or your ISP's network.

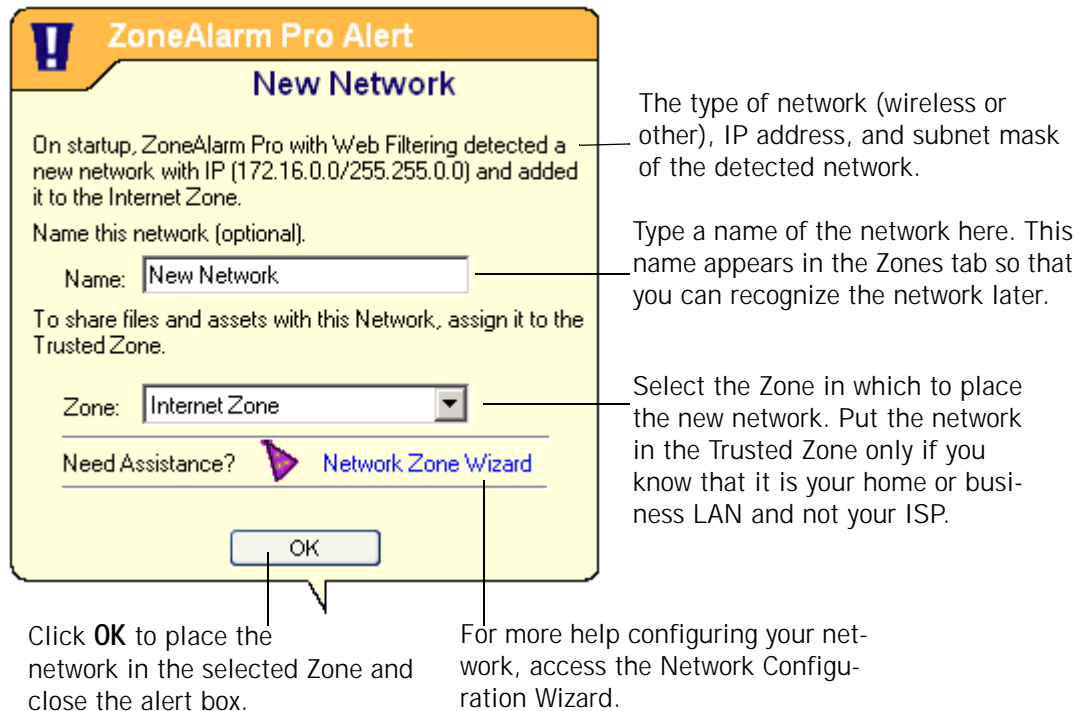


Figure 9-3: New Network alert

ID Lock alerts

If they have enabled the ID Lock feature, users of ZoneAlarm Pro and ZoneAlarm Security Suite may see ID Lock alerts if the personal information stored in myVAULT is sent to a destination that is not listed on their Trusted Sites list.

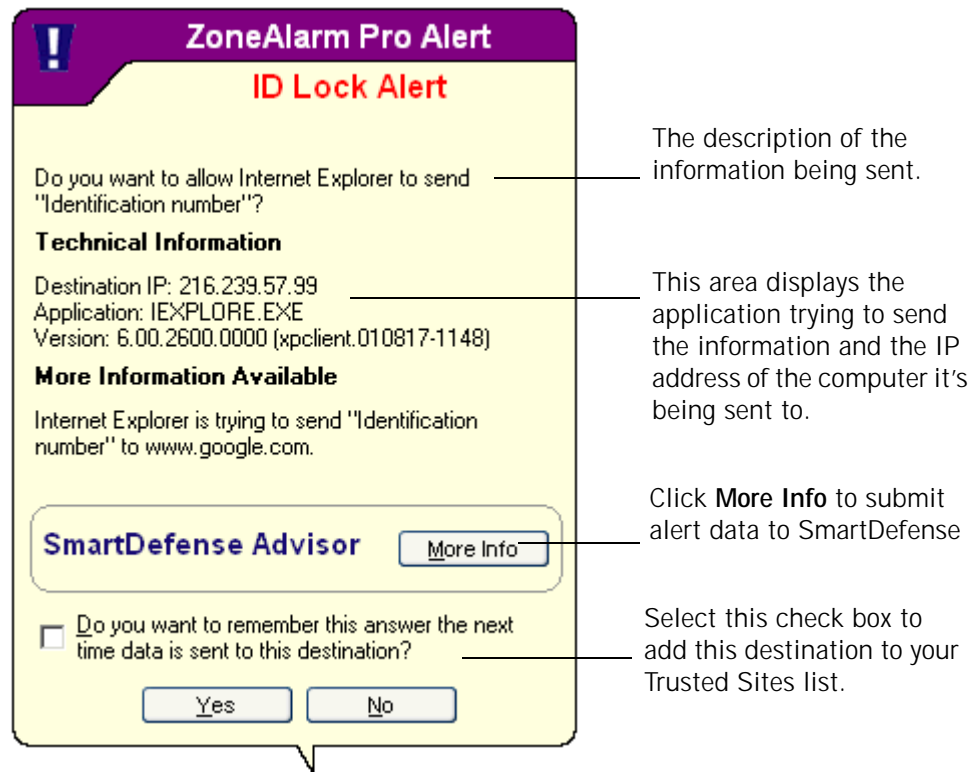


Figure 9-4: ID Lock alert

By clicking the Yes button, you grant permission to send the information to the requesting IP address. If you do not want to be alerted the next time myVAULT data is sent to this destination, select the “**Do you want to remember...**” check box to add the destination to your Trusted Sites list.

OSFirewall alerts

There are three types of OSFirewall alerts that you may see: High-rated Suspicious alert, Medium-rated Suspicious alert, and Malicious alert. These alerts inform you that

ZoneAlarm Security Suite has detected a program on your computer performing an action that could be harmful to your data or computer.

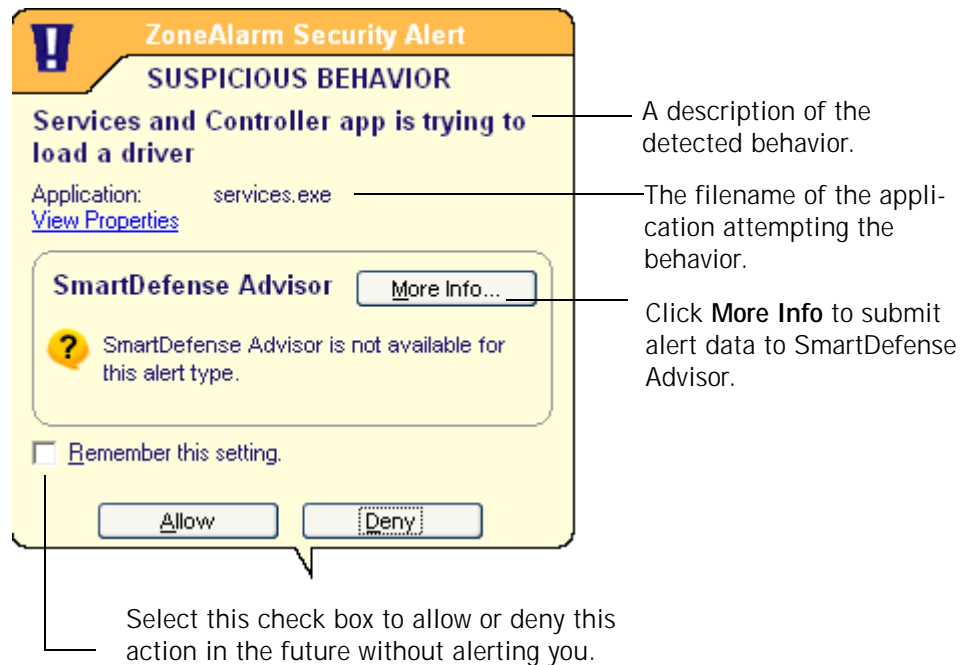


Figure 9-5: Medium-rated Suspicious Behavior alert

Medium-rated Suspicious Behavior alerts inform you that a trusted program is trying to perform an action that may change the default behavior of a program. For example, if a program were to modify your browser's home page, you would see a Medium-rated Suspicious Behavior alert. High-rated Suspicious Behavior alerts, in contrast, inform you that an unknown program is attempting behavior that may cause programs or your operating system to stop functioning normally, or which could be spyware trying to monitor your activity. Because even legitimate programs may sometimes need to perform High-rated Suspicious behavior, you will need to base your decision to allow or deny the action on your knowledge of the program. If the program is one you use frequently, and the action seems reasonable given the functionality of the program, it

may be safe to allow it. If you are unsure, click **More Info**, to submit the program information to SmartDefense Advisor.

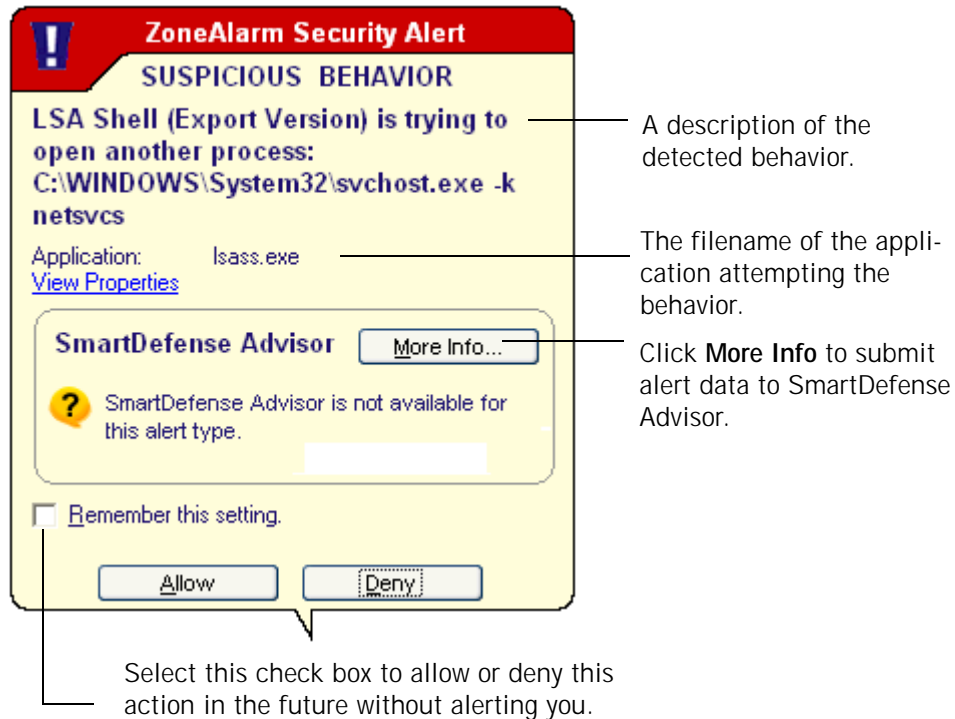


Figure 9-6: High-rated Suspicious Behavior alert

For more information about OSFirewall alerts and the types of behavior detected, see Appendix D, “Program behavior,” starting on page 251.

About event logging

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

You can choose to prevent specific categories of events from being logged—for example, you may want to create log entries only for firewall alerts, or suppress entries for a particular type of Program alert. You can also have Zone Labs security software log specific types of traffic you have decided to allow, by creating expert rules with tracking features enabled.

Setting basic alert and log options

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

Setting the alert event level

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

To set the alert event level:

1. Select **Alerts & Logs | Main**.
2. In the Alert Events Shown area, select the desired setting.

High	Displays an alert for every security event that occurs, both high-rated and medium-rated.
Med	Displays only high-rated alerts, which are most likely a result of hacker activity.
Off	Displays Program and ID Lock alerts only. Informational alerts are not displayed.

Setting event and program logging options

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

To enable or disable event logging and program logging:

1. Select **Alerts & Logs | Main**.
2. In the Event Logging area, select the desired setting.

On	Creates a log entry for all events.
Off	No events are logged.

3. In the Program Logging area, specify the log level.

High	Creates a log entry for all program alerts.
Med.	Creates a log entry for high-rated program alerts only.
Off	No program events are logged.

Controlling the number of alerts

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

If you want to suppress most alerts while playing a computer game, see “Game Mode,” on page 162.

Showing or hiding firewall alerts

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


To show or hide firewall or program alerts:

1. Select **Alerts & Logs | Main**, then click **Advanced**.

The Alert & Log Settings dialog appears.

2. Select the **Alert Events** tab.
3. In the Alert column, select the type of blocked traffic for which Zone Labs security software should display an alert.
4. Click **Apply** to save your changes.

Enabling system tray alerts

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

To enable system tray alerts:

1. Select **Alerts & Logs | Main**.
2. Click **Advanced**, then click the **System Tray Alert** tab.
3. Select the **Enable system tray alert icon** check box.

Game Mode

Game Mode temporarily suppresses most Zone Labs security software scans, product updates, and alerts, so that you can play games on your computer with fewer interruptions. Game Mode lets you temporarily allow or deny all program permission requests, so that Zone Labs security software can answer such requests automatically without displaying alerts. Automatic scans and product updates are postponed until you deactivate Game Mode. Game Mode remains active until you turn it off, or until you turn off Zone Labs security software or your computer.

Game Mode suppresses all Informational alerts and all alerts in which you are prompted to make a decision. This includes alerts caused by Ask settings in the Programs List, such as permission alerts triggered by programs trying to send mail or act as servers. It also includes OSFirewall alerts, which prompt you to allow or deny behavior considered unusual or suspicious. ID Lock alerts and Outbound Mailsafe alerts are also suppressed. Game Mode settings do not override Block or Allow settings in your Programs List. If you have configured Zone Labs security software to always block a specific program, it continues to block that program even if you activate Game Mode with a setting of Allow.

The use of Game Mode may reduce the security of your system. If you choose to allow all permission requests, you may increase the chances of a malicious program harming your computer or gaining access to your data. If, on the other hand, you choose to deny all requests, you may interrupt the functions of a legitimate program. You should therefore activate Game Mode only for the duration of your game.

To turn Game Mode on:

1. Right-click on the system tray icon, and choose **Game Mode...**
2. In the Activate Game Mode dialog that appears, click one of the following:
 - Answer all alerts with “allow”**—Permission requests will be granted.
 - Answer all alerts with “deny”**—Permission requests will be denied.
3. Leave the Activate Game Mode dialog open or minimize it, but do not close it.



If you close the Activate Game Mode dialog, you turn Game Mode off.

While Game Mode is on, Zone Labs security software displays a special icon in the system tray (🚫).

To turn Game Mode off:

➤ Do one of the following:

- Close the Activate Game Mode dialog by clicking either **Cancel** or the Close icon (x) at upper right.
- Click **Stop Game Mode** in the Activate Game Mode dialog.
- Right-click the system tray icon and choose **Stop Game Mode**.

Note that Game Mode is automatically deactivated if you turn off your computer or if you turn off Zone Labs security software.

Setting event and program log options

You can specify whether Zone Labs security software keeps record of security and program events by enabling or disabling logging for each type of alert.

Formatting log appearance

Use these controls to determine the field separator for your text log files.

To format log entries:

1. Select **Alerts & Logs**, then click **Advanced**.

The Advanced Alerts and Log Settings dialog appears.

2. Select the **Log Control** tab.
3. In the Log Archive Appearance area, select the format to be used for logs.

Tab	Select Tab to separate fields with a tab character.
Comma	Select Comma to separate fields with a comma.
Semicolon	Select Semicolon to separate log fields with a semicolon.

Customizing event logging

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

To create or suppress log entries based on event type:

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

2. Click **Advanced**.

The Advanced Alerts and Logs dialog box appears.

3. Select **Alert Events**.
4. In the Log column, select the type of event for which Zone Labs security software should create a log entry.
5. Click **Apply** to save your changes.
6. Click **OK** to close the Alert & Log Settings dialog.

Customizing program logging

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

To create or suppress log entries based on event type:

1. Select **Alerts & Logs | Main**.
2. In the Program Logging area, click **Custom**.
3. In the Program Logs column, select the type of event for which Zone Labs security software should create a log entry.
4. Click **Apply** to save your changes.
5. Click **OK** to close the Alert & Log Settings dialog.

Viewing log entries

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

To view the current log in the Log Viewer:

1. Select **Alerts & Logs | Log Viewer**.
2. Select the number of alerts to display (from 1 to 999) in the alerts list.

You can sort the list by any field by clicking the column header. The arrow (^) next to the header name indicates the sort order. Click the same header again to reverse the sort order.

3. Select the type of alert you want to view:

Anti-spyware	Displays the Date, Type, Spyware name, Filename, Action, and Actor columns.
Anti-virus	Displays the Date/Time, Type, Virus Name, File Name, Action Taken, Mode, and E-mail Info columns.
Firewall	Displays the Rating, Date/Time, Type, Protocol, Program, Source IP, Destination IP, Direction, Action Taken, Count, Source DNS, and Destination DNS columns.
IM Security	Displays the Date/Time, Type, Source, Program, Local User, Remote User, and Action columns.
OSFirewall	Displays the Rating, Date/Time, Type, Subtype, Data, Program, Direction, Action Taken, and Count columns.
Program	Displays the Rating, Date/Time, Type, Program, Source IP, Destination IP, Direction, Action Taken, Count, Source DNS, and Destination DNS columns.
Spy Site Blocking	Displays the Date/Time and the site that was blocked.



The Log Viewer shows security events that have been recorded in the Zone Labs security software log. To view details of Log Viewer fields for each alert type, refer to the Firewall, Program Control, Anti-virus, and IM Security chapters.

Field	Information
Description	A description of the event.
Direction	The direction of the blocked traffic. "Incoming" means the traffic was sent to your computer. "Outgoing" means the traffic was sent from your computer.
Type	The type of alert: Firewall, Program, ID Lock, or Lock Enabled.
Source DNS	The domain name of the computer that sent the traffic that caused the alert.
Source IP	The IP address of the computer that sent the traffic that Zone Labs security software blocked.
Rating	Each alert is high-rated or medium-rated. High-rated alerts are those likely to have been caused by hacker activity. Medium-rated alerts are likely to have been caused by unwanted but harmless network traffic.
Protocol	The communications protocol used by the traffic that caused the alert.
Action Taken	How the traffic was handled by Zone Labs security software.
Destination DNS	The domain name of the intended addressee of the traffic that caused the alert.
Destination IP	The address of the computer the blocked traffic was sent to.
Count	The number of times an alert of the same type, with the same source, destination, and protocol, occurred during a single session.
Date/Time	The date and time the alert occurred.
Program	The name of the program attempting to send or receive data. (Applies only to Program and ID Lock alerts).

Table 9-6: Log viewer fields

Viewing the text log

By default, alerts generated by Zone Labs security software are logged in the file, *ZALog.txt*. If you are using Windows95, Windows98 or Windows Me, the file is located in the following folder: (x):\Windows\Internet Logs. If you are using WindowsNT or Windows2000, the file is located in the following folder: (x):\Winnt\Internet Logs.

To view the current log as a text file:

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

2. Click **Advanced**.

The Advanced Alerts & Log Settings dialog box opens.

3. Select the **Log Control** tab.

In the Log Archive Location area, click **View Log**.

Text log fields

Log entries contain some combination of the fields described in the table below.

Field	Description	Example
Type	The type of event recorded.	FWIN
Date	The date of the alert, in format yyyy/mm/dd	2001/12/31 (December 31, 2001)
Time	The local time of the alert. This field also displays the hours difference between local and Greenwich Mean Time (GMT).	17:48:00 -8:00GMT (5:48 PM, eight hours earlier than Greenwich Mean Time. GMT would be 01:48.)
Virus Name	The name of the virus that caused the event. This field only appears for anti-virus events.	iloveyou
File name	The name of the file that caused the event. This field only appears for Anti-virus events.	iloveyou.exe
Action	How the event was handled. The value for this field will depend on the type of event that occurred.	Anti-virus: Renamed IM Security: Encrypted MailSafe: Quarantined ID Lock: Blocked
Category	The ID Lock category of information that was detected in the event. This field only appears for ID Lock events.	Access PIN
Program	The program sending or receiving the e-mail that contains the ID Lock information. This field only appears for ID Lock events.	Outlook.exe
Source	The IP address of the computer that sent the blocked packet, and the port used; OR the program on your computer that requested access permission.	192.168.1.1:7138 Outlook.exe
Destination	The IP address and port of the computer the blocked packet was addressed to.	192.168.1.101:0

Field	Description	Example
Transport	The protocol (packet type) involved.	UDP

Archiving log entries

At regular intervals, the contents of ZALog.txt are archived to a date-stamped file, for example, ZALog2004.06.04.txt (for June 4, 2004). This prevents ZALog.txt from becoming too large.

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

To set archive frequency:

1. Select **Alerts & Logs | Main**, then click **Advanced**.
2. Select the **Log Control** tab.
3. Select the **Log Archive Frequency** check box.



If the Log Archive Frequency check box is not selected, Zone Labs security software continues to log events for display in the Log Viewer tab, but does not archive them to the ZALog.txt file.

4. In the Log Frequency area, specify the log frequency (between 1 and 60 days), then click **Apply**.

Specifying the archive location

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

To change the log and archive location:

1. Select **Alerts & Logs | Main**.
2. Click **Advanced**.

The Advanced Alerts & Log Settings dialog box opens.

3. Select the **Log Control** tab.
4. In the Log Archive Location area, click **Browse**.
Select a location for the log and archive files.

Using SmartDefense Advisor and Hacker ID

Zone Labs SmartDefense Advisor is a service that enables you to instantly analyze the possible causes of an alert, and helps you decide how to respond. When available, SmartDefense Advisor provides advice as to how to respond to Program alerts. If no advice is available, click **More Info** in the alert to receive more information about the alert. SmartDefense Advisor returns an article that explains the alert and gives you advice on what, if anything, you need to do to ensure your security.

To determine the physical location and other information about the source IP address or destination IP address in an alert, click the Hacker ID tab. This tab displays available information about the IP address that was submitted.



If you are a frequent visitor to eBay, and you have received an ID Lock alert blocking your eBay password, you can use SmartDefense Advisor to submit a fraud report to eBay. To learn more about how Zone Labs security software protects your eBay identity, see “Creating an online fraud protection profile,” on page 26.

To submit an alert to SmartDefense Advisor:

1. Select **Alerts & Logs | Log Viewer**.
2. Right-click anywhere in the alert record you want to submit.
3. Select **More Info** from the shortcut menu.



One or two years of access to updates, support, and services is included with the purchase of ZoneAlarm Anti-virus, ZoneAlarm Pro, or ZoneAlarm Security Suite; annual maintenance contract required for subsequent access. Zone Labs reserves the right to remove the features and services available through ZoneAlarm at any time.

Chapter

Identity protection

10

With the rise of e-commerce, electronic record keeping, and mass financial mailings, the incidence of identity theft has increased in recent years. Hackers can use malware to intercept your personal information online, while thieves can steal CDs and laptops containing customer information, or they can intercept sensitive mail items (such as pre-approved credit card offers) that include personal data.

Zone Labs security software helps protect your personal data online and out in the everyday world. ID Lock keeps your personal information safe from hackers and identity thieves. The Zone Labs Identity Protection Center offers resources that help you prevent, detect, and, if necessary, recover from identity theft.

Identity Protection features are only available in ZoneAlarm Pro and ZoneAlarm Security Suite.

Topics:

- “Understanding the ID Lock feature,” on page 172
- “About myVAULT,” on page 175
- “Using the Trusted Sites list,” on page 178
- “Identity Protection Center,” on page 180

Understanding the ID Lock feature

Every time you or someone else using your computer enters personal information into an e-mail message or Web form—such as your credit card number, address, or social security number—it is possible that the information could be stolen. To help prevent that from happening, the ID Lock ensures that your personal information is only sent to sites you trust.

The ID Lock feature provides a secure area called myVAULT, where you can store personal information that you want to protect. The contents of myVAULT are blocked from being transmitted to unauthorized destinations, whether by you, someone else using your computer, or by a Trojan horse attempting to transmit your personal information.

The ID Lock feature is available in ZoneAlarm Pro and ZoneAlarm Security Suite.

How your personal information is protected

Zone Labs security software prevents your personal information from being transmitted without your authorization, whether in e-mail or on the Web.

E-mail transmission

When you or someone using your computer attempts to send myVAULT data in an e-mail message, Zone Labs security software displays an alert asking you whether to allow the information to be sent. If you want to always allow or always block the information from being sent to this destination, before clicking Yes or No select the check box labeled “**Do you want to remember this answer...**” to add the destination to your Trusted Sites list with the corresponding permission set automatically. For example, if you were to select the “Do you want to remember this answer...” check box and then click **Yes**, the destination would be added to the Trusted Sites list with the permission set to **Allow**. Conversely, if you were to click **No**, the permission would be set to **Block**.



When responding to an ID Lock alert that is the result of an e-mail transmission, clicking the “**Do you want to remember this answer...**” check box adds the domain of the intended recipient's e-mail server—not the e-mail recipient—to the Trusted Sites list. For example, if you were to allow myVAULT data to be transmitted to your contact john@example.com, and you chose to remember that answer, the next time myVAULT data is sent to ANY contact on example.com's e-mail server, the transmission would be allowed and you would not see an alert.

Web transmission

When transmitting myVAULT data on the Web, Zone Labs security software allows or blocks the transmission according to the permission for the domain in the Trusted Sites list. As with e-mail transmission of myVAULT contents, if you choose to remember

your response to an ID Lock alert for a particular Web site, that Web site will be added to the Trusted Sites list automatically with the permission set accordingly.

IM transmission

When transmitting myVAULT data in an Instant Messaging conversation, Zone Labs security software prevents the information from being received.

Figure 10-1 shows an instant messaging conversation in which information that is stored in myVAULT is transmitted. The description of the item stored in myVAULT (in this example, My Visa Card) appears in brackets.

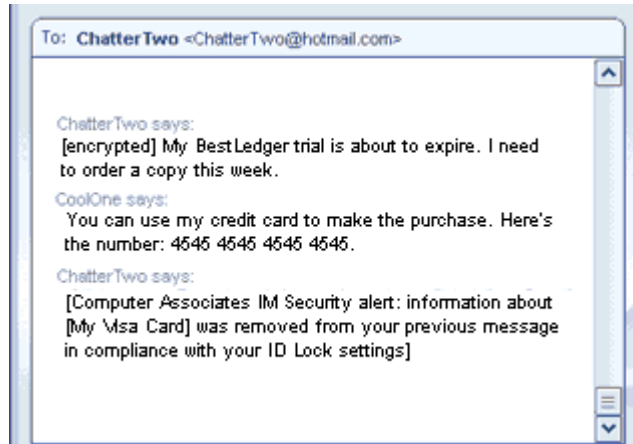


Figure 10-1: Transmission of myVAULT contents

Figure 10-2 shows how the transmitted information is displayed to the recipient. The protected information is replaced with asterisks so that it is unreadable.



Figure 10-2: Receipt of myVAULT contents

Setting the ID Lock protection level

The ID Lock is disabled by default. By enabling the ID Lock, you ensure that the data entered in myVAULT will be protected.

Zone Labs security software keeps track of the number of items stored in myVAULT and displays the number of times your information was protected.

To set the ID Lock protection level:

1. Select **Identity Protection | Main**.
2. In the Identity Lock area, specify the desired protection level.

High	Prevents the contents of myVAULT from being sent to unauthorized destinations. Zone Labs security software will block transmission of your data silently. If you are using a shared computer, this setting is recommended for maximum security.
Medium	Alerts you when your identity information is about to be sent to destinations not listed on the Trusted Sites list. This is the default setting.
Off	Identity protection is disabled. The contents of myVAULT can be sent to any destination, whether or not it appears on the Trusted Sites list.

About myVAULT

The myVAULT feature provides a secure area for entering your critical personal data—data that you want to protect from hackers and identity thieves. When it detects an attempt to send data stored in myVAULT to a destination, Zone Labs security software determines whether the information should be blocked or allowed. By default, Zone Labs security software encrypts myVAULT data as it is entered, storing only the hash value of the data rather than the data itself. Encrypting the data keeps your information secure, as data cannot be retrieved using the hash value.

Adding data to myVAULT

While you can store any type of information in myVAULT, it is a good idea only to store information that you wish to keep secure, such as credit card numbers and identification information. If you were to store information such as your country of residence (for example, Canada) in myVAULT separately from the rest of your address, any time you typed “Canada” into an online Web form, Zone Labs security software would block transmission of the data.



If you're unsure of the type of information that should be entered into myVAULT, refer to the pre-defined categories for guidance. To access the list of categories, select **Identity Protection | myVAULT**, then click **Add**.

To add information to myVAULT:

1. Select **Identity Protection | myVAULT**.
2. Click **Add**.

The Add information to myVAULT dialog box will appear.

For maximum protection, Zone Labs security software encrypts myVAULT data by default. If you do not want to encrypt the data as you enter it, clear the **Use one-way encryption...** check box.

3. Type a description of the item you are adding.



Zone Labs security software displays the item description in ID Lock alerts. Be sure that the description you enter is different from the value of the item to be protected. If the information to be protected and the description contain some or all of the data, you may receive multiple ID Lock alerts.

4. Select a category from the drop-down list.

Access PIN	Personal access code or other ID number. Maximum of 6 characters. For added security, Access PINs are always encrypted.
Address	Maximum 30 characters.

American Express card	For added security, Zone Labs security software does not record the last 5 digits of your American Express card number.
Bank account	Maximum 14 characters.
Credit card	For added security, Zone Labs security software does not record the last 4 digits of your credit card number.
Driver's license	Maximum 15 characters.
eBay password	The password you use to access the eBay Web site. Your eBay password can only be sent to eBay. Maximum 20 characters.
E-mail Address	Maximum 60 characters.
International tax ID	Maximum 15 characters.
Mother's maiden name	Maximum 30 characters.
Name	Maximum 30 characters.
Passport number	US passport number or other International ID number. Maximum 30 characters.
Password	Enter the password to be protected. Maximum 20 characters.
Phone	Separators such as parentheses and dashes are not allowed. Maximum 13 characters.
US Social Security number	Requires 9 digits.
Other	Use this field to enter items that either do not correspond to any of the pre-configured categories, or which exceed the character limit for the corresponding category. Maximum 30 characters.

5. Type the data to be protected.



Data encryption is enabled by default. If you do not want to encrypt your data, clear the **Use one-way encryption...** check box. Because of the sensitive nature of the data, PIN numbers, passwords, the last four digits of your social security number, and the last four digits of your credit card numbers will always be displayed as asterisks, whether or not you choose to encrypt them.

To disable the encryption confirmation that appears by default, select **Identity Protection | myVAULT**, then click **Options**. Clear the **Show encryption confirmation** check box.

Asterisks will appear in place of the data you entered and an encrypted form of your data will be stored in myVAULT. Zone Labs security software will compare the encrypted data with your outgoing messages.

6. Specify whether you want the information to be protected when using Web, E-mail, and Instant Messengers (ZoneAlarm Security Suite only).

7. Click **OK** to save your changes.

Editing and removing myVAULT contents

In the myVAULT tab you can modify the encryption setting, remove myVAULT contents, and edit unencrypted data. Because encrypted data is displayed in asterisks, it is unreadable and therefore cannot be edited.


To edit myVAULT contents:

1. Select **Identity Protection | myVAULT**.
2. Select the item you want to edit, then click **Edit**.

The Edit information from myVAULT dialog appears.

3. Modify data as necessary, then click **OK** to save your changes.

To remove myVAULT contents:

1.  Select the item you want to remove, then click **Remove**.



If you remove the last item in myVAULT, the ID Lock protection level will be set to Off. If you later add items to myVAULT, the protection level will be reset to the default Medium setting.

Using the Trusted Sites list

The myVAULT feature provides a secure area for entering your critical personal data—data that could be used by hackers and identity thieves. When it detects an attempt to send data stored in myVAULT to a destination, Zone Labs security software determines whether the information should be blocked or allowed, by making sure the destination is one you trust.

There are two kinds of sites that can appear on the Trusted Sites list: Security Alliance and Custom. Security Alliance sites are sites that Zone Labs, Inc. has authenticated to ensure they are not fraudulent. Custom sites are sites you add to the list.

Viewing the Trusted Sites list

In addition to listing sites you trust with your personal information, you can add sites to the list that you explicitly do *not* want to trust, such as known spam or chat sites, and prevent information from being sent to them.

The Trusted Sites list also lets you specify which sites are allowed to send your password as *clear text*. Because clear-text passwords are unencrypted, they can easily be viewed by others if intercepted during transmission.

Access	Site	Type	
✓	eBay	Security Alliance	✓
✓	msn.com	Custom	?
✗	shopping.msn.com	Custom	✗

Figure 10-3: Trusted Sites list

Access permission

Specifies whether Zone Labs security software will allow, block, or alert you before sending myVAULT contents to the listed destinations. To modify the permission for a site, click beside the site in the Access column and choose **Allow**, **Block**, or **Ask**.

Site

Displays the domain of the site.

Type

Specifies whether the site is a Security Alliance partner or a Custom site.

Clear Text password

Specifies whether Zone Labs security software will allow, block, or alert you before sending your password as clear text to the listed destinations. To modify the permission

for a site, click beside the site in the Clear Text password column and choose **Allow**, **Block**, or **Ask**.

Site Entry Details

In addition to the site name and type, the Entry Details box displays the site IP Address and the date and time you last accessed the site.

Adding to the Trusted Sites list

There are two types of sites that appear on the Trusted Sites list: Custom and Security Alliance. Custom sites are sites that you add to the list. Security Alliance partner sites are sites that Zone Labs has verified are legitimate and has added automatically.

Custom sites are trusted at the domain level, therefore each sub-domain you want to trust must be added separately. For example, www.msn.com and shopping.msn.com would need to be added separately. Security Alliance sites explicitly trust all sub-domains, so you do not need to create an entry for each sub-domain you want to trust.

To add a site to the Trusted Sites list:

1. Select **Identity Protection | Trusted Sites**, then click **Add**.

The Add Trusted Site dialog appears.

2. Type the URL of the site (omit <http://www>), then click **OK**.

After you click OK, Zone Labs security software verifies the site address and records the IP address. This process can take several seconds.

3. Modify the site permissions as desired.

By default, access and clear text password permissions for Custom sites are set to Ask.

Editing and removing trusted sites

In the Trusted Sites tab, you can modify the access permission for a site, and edit or remove Custom sites. Although you can modify the permissions for Security Alliance partner sites, you cannot edit or remove the site entry.

To edit a Custom site:

1. Double-click the site you want to edit.

The Edit trusted site dialog appears.

2. Edit the site as necessary, then click **OK** to save your changes.

To remove a custom site:

1.  Right-click the site you want to remove, then click **Remove**.

Identity Protection Center

The ZoneAlarm Identity Protection Center is a Web site that helps you prevent, detect, and, if necessary, recover from identity theft. (Identity theft is a crime in which someone exploits your personal information for their own gain.) The Identity Protection Center includes identity protection tips as well as resources for monitoring the use of your personal information and for recovering from identity theft.

Access to the Identity Protection Center is available in ZoneAlarm Pro and ZoneAlarm Security Suite.

To visit the Identity Protection Center:

1. Go to **Identity Protection | Main**.
2. In the Identity Protection Center area, click **Go to ZoneAlarm Identity Protection Center**.

Chapter

Parental Control

11

Parental Control protects your family from Web sites containing violence, pornography, or other undesirable content. You can choose which categories of Web sites to block, and use Smart Filtering to instantly categorize and filter previously un-rated sites.

The Parental Control feature is only available in ZoneAlarm Security Suite.

Topics:

- “Understanding Parental Control,” on page 182
- “Enabling parental control and smart filtering,” on page 183
- “Choosing which content categories to block,” on page 185

Understanding Parental Control

When your browser is pointed to a Web site or other Web-based content, ZoneAlarm Security Suite contacts *Blue Coat*[™] Parental Control servers to see how that site or content has been categorized. If the site your browser is trying to reach has been placed by Blue Coat [™] in a category you have decided to block, access to the site is denied. This process normally takes less than a second. A Parental Control Violation page is displayed, explaining why the site was blocked. If you disagree with a site categorization, you can request a reevaluation of the site by clicking a link in the Filtering Violation page that appears when the site is blocked.

The Parental Control feature is only available in ZoneAlarm Security Suite.

Enabling parental control and smart filtering

When you enable parental control (Parental Control), you immediately block Web sites that Blue Coat has determined contain nudity, pornography, information on illegal drugs, racist text or images, and other content you might not want your children exposed to. If you enable Smart Filtering, new and nonrated sites will instantly be categorized and filtered, enhancing your protection.



To prevent your children from changing your Parental Control settings, set a Zone Labs security software password. See "Setting your password," on page 22.

The Parental Control feature is only available in ZoneAlarm Security Suite.

Enabling or disabling parental control

Parental Control lets you block sites that are set to Block in the Categories List. If Parental Control is disabled, Category and Smart Filtering settings are ignored.

To enable or disable parental control:

1. Select **Parental Control | Main**.
2. In the Parental Control area, select **On** or **Off**.

Enabling or disabling Smart Filtering

Smart Filtering (Dynamic Real-Time Rating) lets you block undesirable sites even if they are brand-new and have not yet been categorized. When this feature is enabled, and your computer points to uncategorized content, Blue Coat™ instantly analyzes the content of the Web site and places it in a category. The site is then blocked or allowed based on your Parental Control settings. This process normally takes two to four seconds.

To enable or disable Smart Filtering:

1. Select **Parental Control | Main**.
2. In the Smart Filtering area, select **On** or **Off**.

To access this option, Parental Control must be enabled.

Setting timeout options

Timeout options determine how long Zone Labs security software will try to obtain a rating for a Web site, and what it do if it is unable to obtain one.

To set timeout options:

1. Select **Parental Control | Main**, then click **Advanced**.

The Parental Control Options dialog appears.

2. Specify your timeout preferences.

Parental Control timeout (sec)	The interval, in seconds, for which Zone Labs security software will try to obtain a rating when Smart Filtering is disabled.
Timeout when DRTR enabled (sec)	The interval, in seconds, for which Zone Labs security software will try to obtain a rating when Smart Filtering is enabled.
When rating unavailable	Specifies whether Zone Labs security software should allow or block sites for which a rating is unavailable.

3. Click **OK**.



If **When rating unavailable** is set to **allow the site**, setting the timeout options to very low numbers might cause undesirable sites to be allowed. We recommend keeping the default timeout options.

Choosing which content categories to block

The Parental Control feature is only available in ZoneAlarm Security Suite.

Parental Control provides numerous categories for filtering Web content. Table 11-1 below provides a description of each category, along with its default setting.

To change the setting for a category:

1. Select **Parental Control | Categories**.
2. In the Site Categories to block column, select or clear the check box beside the category.

A red check mark indicates that content belonging to that category will be blocked. An empty check box indicates that content belonging to that category will be allowed.



To block all site categories, click **Check All**. To allow all site categories, click **Clear All**. To revert to default settings, click the **Reset to Defaults** link.

Category	Definition	Default Setting
Abortion	Site which provide information or arguments in favor of or against abortion; describes abortion procedures; offers help in obtaining or avoiding abortion; provides information on the physical, social, mental, moral, or emotional effects, or the lack thereof, of abortion.	Allowed
Adult: Intimate Apparel/Swimsuit	Sites offering pictures of models in lingerie, swim wear or other types of suggestive clothing. This does not include sites selling undergarments as a sub-section of the other products offered.	Allowed
Adult: Nudity	Sites containing nude or semi nude depictions or pictures of the human body. These depictions are not necessarily sexual in intent or effect but may include sites containing nude paintings or photo galleries of artistic nature. It also includes nudist or naturist sites that contain pictures of nude individuals.	Blocked
Adult: Pornography	Sites containing sexually explicit material for the purpose of arousing a sexual or prurient interest.	Blocked

Table 11-1: Parental Control categories

Category	Definition	Default Setting
Adult: Sex Education	Sites that provide information on reproduction, sexual development, sexually transmitted disease, contraception, safe sex practices, sexuality and sexual orientation. This does not include sites offering suggestions or tips on how to have better sex.	Allowed
Alcohol/Tobacco	Sites that promote or offer for sale alcohol/tobacco products or provide the means to create them. Also may include sites that glorify, tout or otherwise encourage the consumption of alcohol/tobacco.	Blocked
Chat Room / Instant Messenger	Sites that provide chat and Instant Messaging capability.	Allowed
Criminal Skills / Illegal Skills / Cheating	Sites that advocate or give advice on performing illegal acts such as service theft, evading law enforcement, fraud, burglary techniques and plagiarism. Sites that provide instructions about or promote crime, unethical/dishonest behavior or evasion of prosecution thereof.	Blocked
Cult / Occult	Prominent organized modern religious groups that are identified as "cults" by three or more authoritative sources. Sites that promote or offer methods, means of instruction, or other resources to affect or influence real events through the use of spells, curses, magic powers or supernatural beings.	Allowed
Dating and Personals	Sites that promote interpersonal relationships. Does not include those pertaining to gay or lesbian appeal.	Allowed
Drugs: Illegal Drugs	Sites that promote, offer, sell, supply, encourage or otherwise advocate the illegal use, cultivation, manufacture, or distribution of drugs, pharmaceuticals, intoxicating plants or chemicals and their related paraphernalia.	Blocked
E-mail	Sites offering Web-based E-mail services.	Allowed
Freeware / Software Downloads	Sites that promote or offer free software or products for general download or trial purposes.	Allowed
Gambling	Sites where a user can place a bet or participate in a betting pool (including lotteries) online; obtain information, assistance or recommendations for placing a bet; receive instructions, assistance or training on participating in games of chance. Does not include sites that sell gambling related products or machines.	Blocked

Table 11-1: Parental Control categories

Category	Definition	Default Setting
Gay and Lesbian	Sites that provide information on or cater to gay and lesbian lifestyles. Does not include sites that are sexually oriented.	Allowed
Glamour / Life-style	Sites that emphasize or provide information or news on how the user can achieve physical attractiveness, allure, charm, beauty, or style with respect to personal appearance.	Allowed
Government: Military	Sites that promote or provide information on military branches or armed services.	Allowed
Hacking / Proxy Avoidance Systems	Sites providing information on illegal or questionable access to or the use of communications equipment/software, or provide information on how to bypass proxy server features or gain access to URLs in any way that bypasses the proxy server.	Blocked
Humor / Jokes	Sites that primarily focus on comedy, jokes, fun, etc. Does not include sites containing jokes of adult or mature nature.	Allowed
Internet Auctions	Sites that support the offering and purchasing of goods between individuals.	Allowed
MP3 / Streaming	Sites that support and or allow users to download music and media files such as MP3, MPG, MOV, etc. Also includes sites that provide streaming media (radio, movie, TV).	Allowed
News Groups	Sites that offer access to Usenet New Groups or other like sites.	Allowed
News and Media	Sites that primarily report, information, or comments, on current events or contemporary issues of the day. Items like weather, editorials, and human interest are considered target within the context of major news sites.	Allowed
Online Games	Sites that provide information and support game playing or downloading, video games, computer games, electronic games, tips and advice on games or how to obtain cheat codes, journals and magazines dedicated to game playing, online games, as well as sites that support or host online games including sweepstakes and giveaways.	Allowed
Pay to Surf Sites	Sites that pay users money for clicking on specific links or locations.	Blocked

Table 11-1: Parental Control categories

Category	Definition	Default Setting
Political /Activist / Advocacy	Sites that are sponsored by and contain information about specific political parties or groups. Sites that are sponsored by or devoted to organizations that promote change or reform in public policy, public opinion, social practice, economic activities and relationships. Excludes commercially sponsored sites dedicated to electoral politics or legislation.	Allowed
Religion	Sites that promote and provide information on Buddhism, Baha'i, Christianity, Christian Science, Hinduism, Islam, Judaism, Mormonism, Shinto, Sikhism, Atheism, other conventional or unconventional religious or quasi-religious subjects, as well as churches, synagogues, other houses of worship, any faith or religious beliefs including "alternative" religions such as Wicca and witchcraft.	Allowed
Search Engines / Portals	Sites that support searching the Web, indices and directories.	Allowed
Shopping	Sites that provide the means to obtain products and services that satisfy human wants and or needs. This does not include products or services that are principally marketed to satisfy industrial or commercial needs.	Allowed
Sports / Recreation / Hobbies	Sites that promote or provide information about spectator sports.	Allowed
Violence / Hate / Racism	Sites which advocate or provide instructions for causing physical harm to people or property through use of weapons, explosives, pranks, or other types of violence. Sites that advocate hostility or aggression toward an individual or group on the basis of race, religion, gender, nationality, ethnic origin, or other involuntary characteristics; a site which denigrates others on the basis of those characteristics or justifies inequality on the basis of those characteristics; a site which purports to use scientific or other commonly accredited methods to justify said aggression, hostility or denigration.	Blocked
Weapons	Sites that sell, review, or describe weapons such as guns, knives, or martial arts devices, or provide information on their use, accessories, or other modifications.	Blocked
Web Communication / Message Boards	Sites that allow or offer Web based communication using any of the following mediums: E-mail (Web based), Chat, Instant Messaging, Message Boards, etc.	Allowed

Table 11-1: Parental Control categories

Category	Definition	Default Setting
Web Hosting / Personal Web Pages	<p>Sites of organizations that provide top-level domain pages of Web communities or hosting services. Sites that host Web Chat services, on-IRC chat rooms, Chat sites via HTTP, home pages devoted to IRC, as well as sites that offer forums or discussion groups. Sites that promote or provide the means to practice illegal or unauthorized acts using computer-programming skills (hacking).</p> <p>Also sites containing ALL types of content such as GEO Cities.</p>	Allowed

Table 11-1: Parental Control categories



If you are using ZoneAlarm Security Suite and you choose to block new categories, you may want to clean your browser cache to remove pages from newly blocked sites that may be stored there. Otherwise, anyone using your computer will have access to blocked content that has been stored in your browser's cache.

Chapter

Instant Messaging Security

12

Zone Labs IM Security is your front line of defense against instant messaging threats. IM Security's default security levels give you immediate protection against hackers, spam, and provides controls that prevent inappropriate Web content from being sent to your instant messaging client.

The IM Security feature is only available in ZoneAlarm Security Suite.

Topics:

- "IM Security Overview," on page 192
- "Setting IM Security options," on page 199

IM Security Overview

Zone Labs security software provides comprehensive instant messaging (IM) security for the most popular instant messaging services, including MSN Messenger, Yahoo! Messenger, AOL Instant Messenger, and ICQ. IM Security also supports third-party programs that run on these services, such as Trillian. IM Security keeps instant messaging conversations private and protects computers from IM spammers, identity thieves, hackers and predators who exploit vulnerable IM connections.

IM Security includes the following features:

- **Access Control** - Controls which IM services can be accessed using your computer.
- **Spam Blocker**- Blocks messages sent by people not on your contact lists.
- **Feature Control** - Determines which IM features are allowed on your computer.
- **Inbound threat protection** - Guards your computer against attacks by filtering invalid messages, dangerous scripts, and executable URLs.
- **Message Encryption** - Protects your IM traffic from being intercepted and read by others.



The protection features described above apply only to one-on-one conversations. Zone Labs security software does not protect conversations with more than one participant (for example, chat room conversations).

Access

Access control lets you allow or block traffic for a particular instant messaging service.

To block or allow IM traffic for a particular service:

1. Select **Security | Settings**.
2. In the **Access** column, click beside the instant messaging for which you want to block or allow traffic.
3. Select **Allow** or **Block**.

Blocking spam

Spam Blocker filters out unsolicited communications from senders who are not on your contact list. By default, Spam Blocker is enabled only when the IM Security level is set to

High. However, you can customize your settings to enable Spam Blocker for a particular service regardless of the protection level.



You will not see visual confirmation that Zone Labs security software blocked an incoming message, however, you can refer to the log to determine the sender's identity. If you want to receive future messages from the sender, be sure to add the sender's ID to the contact list for each of your instant messaging programs. Blocked messages appear in the Log Viewer with "A message from someone not on your contact list was blocked" in the Type column.

To enable or disable Spam Blocker for a particular service:

1. Select **Security | Settings**.
2. Locate the instant messaging service you want to customize, then click in the **Spam Blocker** column.
3. Choose **On** or **Off**.

Feature Control

Feature Control settings allow you to restrict the types of media that you can receive during an instant messaging session. Because inappropriate content can be sent in many forms, Zone Labs security software allows parents to protect their children by blocking specific types of media from instant messaging sessions, including audio, video, and voice transmissions.

When a message is blocked, the sender is notified, as shown in Figure 12-1.

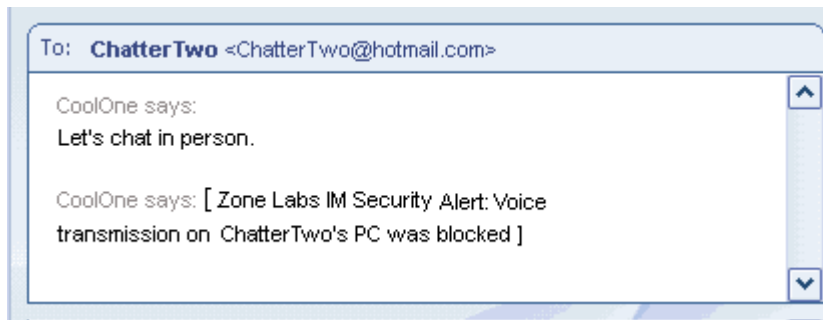


Figure 12-1: Sending a voice transmission that is blocked

The recipient is also notified as shown in Figure 12-2.

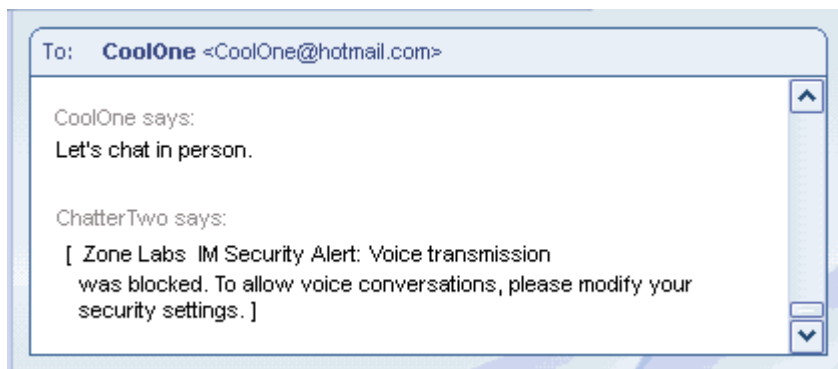


Figure 12-2: Blocking an incoming voice transmission

To customize Feature Control settings:

1. Select **Security | Settings**.
2. Locate the instant messaging service you want to customize, then click in the **Feature Controls** column.
3. Click in the **Audio, Video, or Files**, then choose **Allow** or **Block**.

Inbound protection

Inbound protection settings let you specify which instant messaging services are allowed to transmit active links and formatting tags, such as JavaScript, in incoming messages.

Active links and formatting tags can contain viruses that can attack your computer when you click on a link in a message.

The Inbound “Tags” setting removes extra formatting that could contain scripts and other potentially harmful code. The Tags setting also removes innocuous formatting, such as bold, underline, italic, etc.

The “Active” setting blocks links that, if clicked, could execute code or download dangerous files onto your computer.

When you send an active link to a contact, it appears as shown in Figure 12-3.

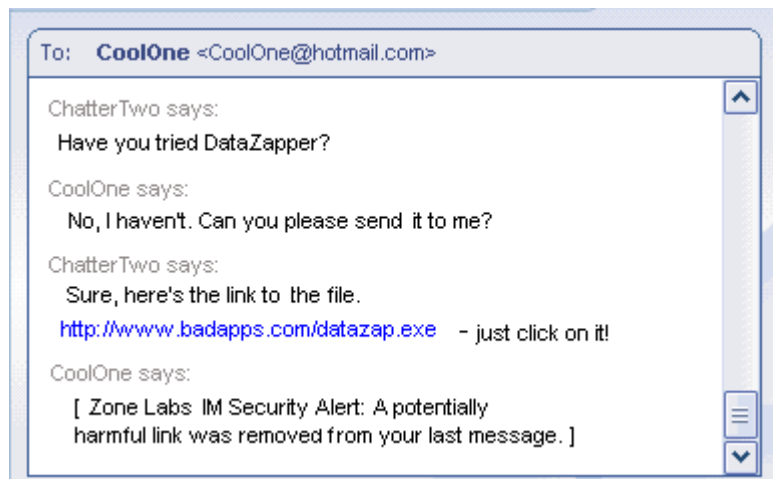


Figure 12-3: Sending an executable URL to a contact

When an active link is filtered from a message, the receiver is notified as shown in Figure 12-4 shows.



Figure 12-4: Potentially harmful link removed

To customize inbound protection settings:

1. Select **Security | Settings**.
2. Locate the instant messaging service you want to customize, then click in the **Inbound** column.
3. Click below **Tags** or **Active**, then choose **Allow** or **Block**.

Encrypting instant messaging traffic

Encryption keeps others from intercepting and reading your instant message conversations. To encrypt instant messaging conversations, both parties must have ZoneAlarm Security Suite installed, have an account on the same IM service. Conversations will not be encrypted if the parties are not on each other's contact list, even if each has ZoneAlarm Security Suite installed.

When you initiate a conversation with another ZoneAlarm Security Suite user, and you both have encryption enabled for the IM service you're connected to, the word **encryption** appears in brackets after your contact's instant messaging ID. If you initiate a conversation with a contact who is not using ZoneAlarm Security Suite, or who does

not have encryption enabled, you will see the word **unencrypted** after the contact's instant messaging ID.

Figure 12-5 shows an encrypted conversation.

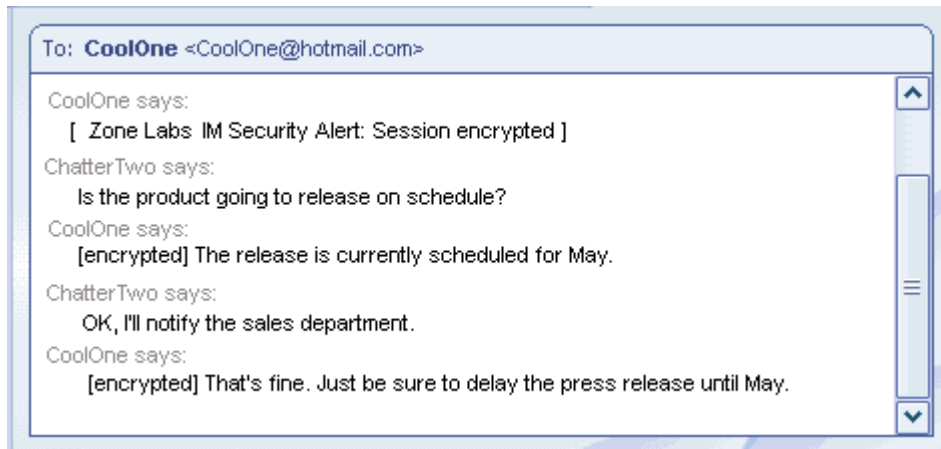


Figure 12-5: Example of an encrypted conversation.

Here is the same conversation as shown in Figure 12-5, but in unencrypted mode.

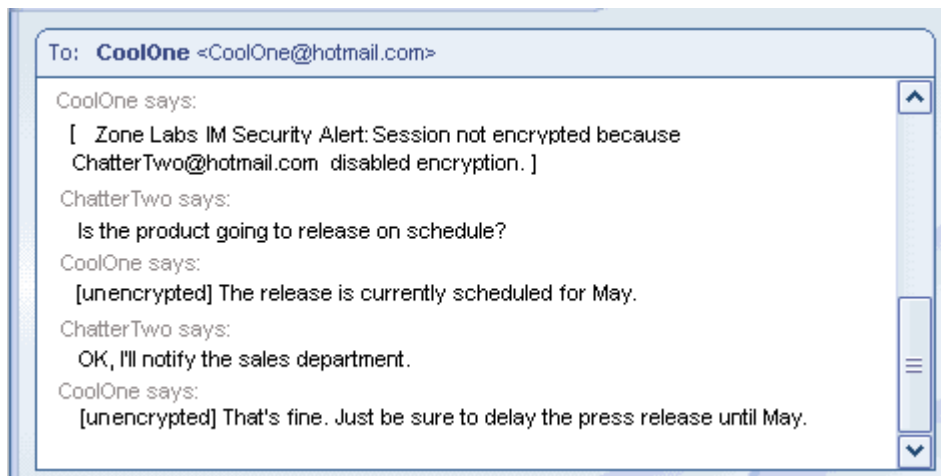


Figure 12-6: Example of an unencrypted conversation

To enable or disable encryption for a particular IM service:

1. Select **Security | Settings**.
2. In the Encrypt column, click beside the service whose traffic you want to encrypt.
3. Select **Allow** or **Block**.

How instant messages are encrypted

ZoneAlarm Security Suite relies on the *OpenSSL* library for cryptographic services. The text of each message in a secure session is encrypted with a 168-bit key cipher.

ZoneAlarm Security Suite automatically and transparently creates a *self-signed certificate* for each of the user's IM accounts upon the first login. At the beginning of the first IM conversation between two ZoneAlarm Security Suite users after installing ZoneAlarm Security Suite, the certificates are transparently exchanged between the users and stored on their computers. The public key from one of the certificates is used to encrypt the session key to be used for the duration of the session.

Setting IM Security options

Zone Labs security software protects you by applying restrictions to instant messaging software, filtering spam, and encrypting Instant Message traffic. In combination with the ID Lock feature, Zone Labs security software prevents your personal data from being transmitted during an instant messaging session without your authorization. You can specify your desired level of protection by using pre-defined options, or by manually customizing individual security settings.

- 🔗 Setting the protection level
- 🔗 Viewing IM Security protection status
- 🔗 Customizing protection settings
- 🔗 Setting advanced IM Security options
- 🔗 Viewing logged IM Security events

Setting the protection level

The default Medium protection level balances security with convenience by allowing instant messaging functions, while ensuring that your instant messaging communications are secure.

To set the global protection level:

1. Select **IM Security | Main**.
2. In the **Protection Level** area, click the slider and drag it to the desired setting.

High	Prevents your instant messaging programs from sending media files of all types, filters spam messages, executable URLs, and encrypts instant messaging traffic.
Medium	This is the default setting. Encrypts instant messaging traffic and filters executable URLs.
Off	Instant messaging protection disabled.

Viewing IM Security protection status

You can view the status of IM Security protection from the Main tab. The Protection status area provides statistics for the number of messages that were blocked that violated the security settings for Inbound, Spam Blocker, and Feature Control options.

The Program History log lists all active IM programs and displays the last date and time the programs were used.



If you start an IM program before starting Zone Labs security software, the IM program will not appear in the History log. To accurately reflect all IM program activity, start IM programs after starting Zone Labs security software.

Customizing protection settings

By setting the protection level to High, Med, or Off, you specify globally whether instant messaging programs can send files, JavaScript, and links to your instant messaging client. In some cases, you may want to specify settings for an individual service that are different than these global settings allow.

To customize protection settings:

1. Select **IM Security | Settings**.
2. Locate the service you want to modify, then right-click in the column for the content you want to customize.

Access	If set to Block, instant messaging traffic from any program that uses the selected service, is stopped.
Spam Blocker	If set to On, blocks messages from messages sent from people who are not in your contact list.
Feature Control	If set to Block, transmission of Audio, Video, or Files is allowed blocked.
Inbound	Specifies whether formatting tags, such as JavaScript or executable links, can be contained in inbound messages.
Encrypt	Specifies whether instant messaging traffic is encrypted.



To return to the default Medium protection level, select **IM Security|Main**, then click **Reset to Defaults**.

Setting advanced IM Security options

By default, Zone Labs security software alerts you when harmful content is filtered from an IM conversation, and tells you whether or not your sessions are encrypted. Using the Advanced dialog, you can modify these and other settings.

To set advanced IM Security options:

1. Select **IM Security | Settings**, then click **Advanced**.
2. Specify your settings.

Notify my contacts that I am protected by Zone Labs IM Security	When you initiate a conversation with a contact after installing Zone Labs security software, your contact will receive notification that you are protected. Note: This notification occurs only during the first session after installation. Your contacts will not be notified during subsequent sessions.
---	--

Notify me about encryption status of each IM session	Zone Labs security software marks the beginning of each IM session with the default "encrypted" or "unencrypted" label.
Label encrypted messages with	Attaches the specified label to encrypted incoming messages. The default label is "encrypted."
Label unencrypted messages with	Attaches the specified label to unencrypted incoming messages. The default label is "unencrypted."
Notify me when harmful content is filtered	Zone Labs security software will display a message in your IM window when potentially harmful content is filtered from an IM conversation.
Block IRC	In the event your computer becomes compromised, this feature blocks attempts to establish a connection with IRC channels. This prevents infected computers from establishing malicious connections. If you are an IRC user and require use of IRC applications, clear this option.
Block all links	Filters all URLs, which can be used to spread worms.

3. Click **OK to save your changes.**

Viewing logged IM Security events

By default, all IM Security events are recorded in the Log Viewer. Although you will not receive notification when Zone Labs security software blocks Spam, you will be able to view the details of any blocked message in the Log viewer.

To view logged IM Security events:

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

2. Select **IM Security, from the Alert Type drop-down list.**

Table 12-6 provides an explanation the log viewer fields available for IM Security.

Field	Explanation
Rating	Event rating based on the Protection Level of the security option.
Date/Time	Date and time the event occurred
Type	Brief description of the event. Depending upon the security settings that were violated (for example, Spam Blocker, ID Lock, etc.), this field may contain any of the following descriptions: <ul style="list-style-type: none"> • Connection blocked • A message from someone not on your contact list was blocked • Media transmissions • Potentially harmful content removed • A link to active content removed • Encrypted session established • Session not encrypted • Sensitive data removed
Service	The service on which the event occurred.
Program	The instant messaging program (displayed as the application file) that was connected when the event occurred.
Local user	The user ID of the instant messaging contact who received the message.
Remote user	The user ID of the instant messaging contact who triggered the event.
Action	Describes the action taken. Common values for this column are encrypted, encryption deactivated, blocked audio/video/file, blocked script.

Table 12-6: Log Viewer field explanations

Appendix

Alert reference



This chapter provides detailed information about the various types of alerts you may see while using Zone Labs security software. Use this chapter to find out why alerts happen, what they mean, and what to do about them.

Throughout this chapter, there are tips for reducing the number of alerts Zone Labs security software displays. For information about suppressing most alerts while playing games on your computer, see “Game Mode,” on page 162.

Topics:

- “Informational alerts,” on page 204
- “Program alerts,” on page 209
- “OSFirewall alerts,” on page 218
- “ID Lock alert,” on page 220
- “New Network alert,” on page 221
- “Instant Messaging alerts,” on page 223

Informational alerts

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

Firewall alerts/Protected

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

Why these alerts occur

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

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

What you should do

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

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

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

How to see fewer of these alerts

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

- Determine if the source of the alerts should be trusted.
 - Submit repeated alerts to SmartDefense Advisor to determine the source IP address that caused the alerts.
 - If the alerts were caused by a source you want to trust, add it to the Trusted Zone.
- Determine if your Internet Service Provider is sending you "heartbeat" messages.
 - Try the procedures suggested for managing ISP heartbeat. See "Allowing ISP Heartbeat messages," on page 239.

MailSafe alert

MailSafe alerts let you know that Zone Labs security software has quarantined a potentially dangerous attachment to an incoming e-mail message. By clicking OK, you're not letting anything into your computer.

Why these alerts occur

MailSafe alerts can occur due to violations of Inbound or Outbound MailSafe protection settings. For example, an Inbound violation occurs when you open an e-mail that has an attachment whose filename extension is on the list of extensions to be quarantined in the Attachments tab of the E-mail Protection panel. In such a case, the alert informs you that Zone Labs security software has changed the extension to prevent the attachment from being opened without warning. A violation of Outbound MailSafe protection settings, such as an e-mail that has too many recipients, or too many e-mails within a short time, can cause a MailSafe alert to occur.

What you should do

How you respond to MailSafe alerts depends upon whether the alert was caused by a violation of Inbound or Outbound MailSafe protection settings.

If the alert was caused by an Inbound MailSafe violation, do the following:

- Examine the e-mail message carefully. Are you sure it's from someone you know and trust? Remember, hackers can fake e-mail messages so that they look like they are from a friend. Also, if a friend has accidentally opened a file containing an e-mail worm, that worm may have sent itself to you, using your friend's e-mail program.
- Contact the sender by telephone or e-mail before opening the attachment to make sure the message is genuine.
- Open the attachment only if you are certain the attachment is harmless. You can open the attachment by clicking the quarantine icon (which replaces the normal file icon).



When you try to open a quarantined attachment, Zone Labs security software will display a warning dialog box to remind you that the attachment is potentially dangerous.

If the alert was caused by an Outbound MailSafe violation, do the following:

- Examine the alert carefully. Does the activity noted describe actions you were recently performing? If so, you may want to modify your Outbound MailSafe settings to better accommodate your needs. See “Outbound MailSafe protection,” on page 117. If not, the alert may be the result of a virus on your computer. In this case deny the outbound e-mails, then scan your computer with an anti-virus program.
- Verify that your e-mail address is listed on the approved sender’s list. If you selected the **if the sender’s e-mail is not in this list** option, and if your e-mail either is not on that list or is misspelled, add your valid e-mail address to the list.

How to see fewer of these alerts

Outbound MailSafe Protection is an important part of your Internet security system, and we recommend leaving it on. However, if you are getting a lot of these messages in error, you may want to adjust the sensitivity of the feature or turn it off. See “Outbound MailSafe protection,” on page 117.

Blocked Program alert

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

Why these alerts occur

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

What you should do

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

How to see fewer of these alerts

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

- When you see a Blocked Program alert, select **Do not show this dialog again** before clicking **OK**. From then on, all Blocked Program alerts will be hidden. Note that this will not affect New Program, Repeat Program, or Server Program alerts.
- In the Program Control panel, click **Advanced** to access the Alerts & Functionality tab, then clear the check box labeled **Show alert when Internet access is denied**.



Turning off Blocked Program alerts does not affect your level of security.

Internet Lock alert

Internet Lock alerts let you know that Zone Labs security software has blocked incoming or outgoing traffic because the Internet Lock (or the Stop button) is engaged. By clicking OK, you're not opening the lock; you're just acknowledging that you've seen the alert.

If the Internet Lock has been engaged automatically (or accidentally), open it to prevent further alerts. See "Understanding Zones," on page 18.

Why these alerts occur

These alerts occur only when the Internet Lock is engaged.

What you should do

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

If the Internet Lock has been engaged automatically (or accidentally), open it to prevent further alerts. See "Understanding Zones," on page 18.

You may want to give certain programs (for example, your browser) permission to bypass the Internet Lock, so that you can continue to perform some basic functions under the lock's higher security. See "Setting passlock permission for a program," on page 84.

How to see fewer of these alerts

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

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

- Turn off the Automatic Internet Lock.
- Increase the interval of inactivity required to engage the Automatic Internet Lock to engage. For more information, see "Enabling the automatic lock," on page 70.

Remote alert

Remote alerts are displayed on an ICS client machine when Zone Labs security software blocked traffic at the ICS gateway. If you are not on a machine that is a client in an ICS network, you will never see this alert.

Why these alerts occur

Remote alerts occur when:

- Zone Labs security software starts up on the ICS gateway. The alert displays the message “The remote firewall has started.”
- Zone Labs security software shuts down on the ICS gateway. The alert displays the message “The remote firewall has stopped.”
- The Internet Lock has engaged on the ICS gateway. This may prevent the client machine from performing some tasks. The alert displays the message “The remote firewall has engaged the Internet Lock.”
- The Internet Lock is opened on the ICS gateway. The alert displays the message “The remote firewall has disengaged the Internet Lock.”

What you should do

Click **OK** to close the alert box. You do not have to do anything else to ensure your security.

How to see fewer of these alerts

If you do not want to see Remote alerts on the ICS client machine:

1. Select **Firewall | Main**, then click **Advanced**.
2. In the Internet Connection Sharing area, clear the check box labeled **Forward alerts from gateway to this computer**.

Program alerts

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

New Program alert

New Program alerts enable you to set access permission for program that has not asked for Internet Zone or Trusted Zone access before. If you click **Allow**, the program is allowed access. If you click **Deny**, the program is denied access.

Why these alerts occur

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

As you begin to work with Zone Labs security software, you will probably see one or more New Program Alerts.

What you should do

Click **Allow** or **Deny** in the alert pop-up after answering these questions:

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



If your browser does not have permission to access the Internet, you will be re-routed to this help file. To access SmartDefense Advisor, give your browser permission to access the Internet.

- If you're really not sure what to do, it's best to click **Deny**. You can always grant permission later by going to the Programs tab. "Setting access permissions for new programs," on page 74.

How to see fewer of these alerts

It's normal to see several New Program alerts soon after installing Zone Labs security software. As you assign permissions to each new program, the number of alerts you see will decrease. To keep from seeing Repeat Program alerts, select **Remember this setting** before clicking **Allow** or **Deny**.

If SmartDefense Advisor is set to "Auto," Zone Labs security software issues Program alerts only if no automatic setting is available. If you choose **Remember this setting** in a Program alert when allowing or denying program access, Zone Labs security software

keeps your setting unless SmartDefense Advisor comes out with a different setting, or until you change the setting manually in the Programs tab.

Repeat Program alert

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

Why these alerts occur

If you respond Allow or Deny to a New Program alert without checking **Remember this answer**, you'll see a Repeat Program alert the next time the program asks for access permission.

What you should do

You should respond to Repeat Program alerts in the same way you would to New Program alerts. See "New Program alert," on page 210.

How to see fewer of these alerts

To keep from seeing Repeat Program alerts, select **Remember this setting** before clicking Allow or Deny in any New Program or Repeat Program alert. This sets the permission for the program to Allow or Block in the Programs tab.

If SmartDefense Advisor is set to "Auto," Zone Labs security software issues Program alerts only if no automatic setting is available. If you choose **Remember this setting** in a Program alert when allowing or denying program access, Zone Labs security software keeps your setting unless SmartDefense Advisor comes out with a different setting, or until you change the setting manually in the Programs tab.

Changed Program alert

Changed Program alerts warn you that a program that has asked for access permission or server permission before has changed somehow. If you click Allow, the changed program is allowed access. If you click Deny, the program is denied access.

Why these alerts occur

Changed Program alerts can occur if you have updated a program since the last time it accessed the Internet. However, they can also occur if a hacker has somehow managed to tamper with the program.

Remember, some programs are configured to access the Internet regularly to look for available updates. Consult the documentation for your programs, or refer to the support Web sites of their vendors, to find out if they have automatic update functionality.

What you should do

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

- Did you (or, if you're in a business environment, your systems administrator) recently upgrade the program that is asking for permission?

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

If you can answer “yes” to both questions, it’s probably safe to click **Allow**.



If you're not sure, it's safest to click **Deny**. You can always grant permission later by going to the Programs tab. See “Setting permissions for specific programs,” on page 76.

How to see fewer of these alerts

Changed Program alerts are always displayed because they require a Allow or Deny response from you. If you are using a program whose checksum changes frequently, you can avoid seeing numerous alerts by having Zone Labs security software check the program’s file name only. “Adding a program to the programs list,” on page 79.

Program Component alert

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

By clicking Allow, you allow the program to access the Internet while using the new or changed components. By clicking Deny, you prevent the program from accessing the Internet while using those components.

Why these alerts occur

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

Zone Labs security software automatically secures the components that a program is using at the time you grant it access permission. This prevents you from seeing a Component alert for every component loaded by your browser. To learn how Zone Labs security software secures program components, see “Managing program components,” on page 85.

What you should do

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

- Are any of the following true?
 - You just installed or reinstalled Zone Labs security software.
 - You recently updated the application that is loading the component (For the application name, look under Technical Information in the alert pop-up.)
 - The application that is loading the component has an automatic update function.

- Someone else (for example, a systems administrator at your workplace) may have updated a program on your computer without your knowledge.
- Are you actively using the application that loaded the component?

If you can answer “yes” to both questions, it is likely that Zone Labs security software has detected legitimate components that your browser or other programs need to use. It is probably safe to answer Allow to the Program Component alert.

By clicking Allow, you allow the program to access the Internet while using the new or changed components. If you cannot answer yes both questions, or if you feel unsure about the component for any reason, it is safest to click Deny.

By clicking Deny, you prevent the program from accessing the Internet while using those components.



If you're not sure what to do, or if you decide to click **Deny**, investigate the component to determine if it is safe.

How to see fewer of these alerts

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

To reduce the number of alerts, lower the authentication level to medium for the first few days after installing Zone Labs security software.

If you have been using Zone Labs security software for more than a few days, it is very rare to see large numbers of program alerts.

Server Program alert

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

Why these alerts occur

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

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

- Chat
- Internet Call Waiting

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

If you are using the types of programs described above that require server permission to operate properly, grant permission before you start using the program. See “Granting a program permission to act as a server,” on page 81.



If your browser does not have permission to access the Internet, you will be re-routed to the online help. To access SmartDefense Advisor, give your browser permission to access the Internet. See “Granting a program permission to access the Internet,” on page 80.

What you should do

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

- Did you just launch a program or process that would reasonably require permission? If so, it’s probably safe to click Allow. If not, continue.
- Do you recognize the name of the program in the alert pop-up, and if so, does it make sense for the program to need permission? If so, it’s probably safe to click Allow.
- Click the **More Info** button in the alert box. This submits your alert information (for example, the name of the program and the address it was trying to reach) to SmartDefense Advisor, which then displays a Web page with information about the alert and the program. Use the SmartDefense Advisor information to help you decide if it’s safe to answer Allow. For more information, see “Using SmartDefense Advisor and Hacker ID,” on page 170.
- If you are still not certain that the program is legitimate and needs server permission, it is safest to click Deny. If it becomes necessary, you can give the program server permission later by using the Programs tab. See “Granting a program permission to act as a server,” on page 81.

How to see fewer of these alerts

If you are using the types of programs described above that require server permission to operate properly, use the Programs tab in Zone Labs security software to grant permission before you start using the program. If you’re seeing many server program alerts, you may want to download and run an anti-virus or anti-spyware tool as an added precaution.

Advanced Program alert

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

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

Why these alerts occur

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

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

What you should do

How you should respond to an Advanced Program alert depends upon the cause of the alert. If the Advanced Program alert was caused by the OpenProcess function being called, you should determine whether the function was called by a legitimate program or by a malicious one. Verify that the program cited in the alert is one you trust to carry out this function. For example, if you were attempting to shut down a program using Windows Task Manager when you received the Advanced Program alert, it is probably safe to answer **Allow**. Similarly, if the alert was caused by a program using another program to access the Internet and that program routinely requests such permission, is probably safe to answer **Allow**. If you are unsure as to the cause of the alert or the expected behavior of the program initiating the request, it is safest to click **Deny**. After denying advanced permission to the program, perform an Internet search on the program's file name. If the program is malicious, it is likely that information about it is available, including how to remove it from your computer.

How to see fewer of these alerts

It is unusual to see a large number of Advanced Program alerts. If you receive repeated alerts, research the program name or names and consider either removing the program from your computer or providing the program with the necessary access rights.

Automatic VPN Configuration alert

Automatic VPN Configuration alerts occur when Zone Labs security software detects VPN activity. Depending upon the type of VPN activity detected, and whether Zone Labs security software was able to configure your VPN connection automatically, you may see one of three Automatic VPN Configuration alerts.

Why these alerts occur

Automatic VPN Configuration alerts occur when Zone Labs security software detects VPN activity that it is not configured to allow.

What you should do

How you should respond to an Automatic VPN Configuration alert depends upon which Automatic VPN Configuration alert you encounter, whether you are running VPN software or not, and whether you want to configure Zone Labs security software to allow your VPN connection.



If you have created an expert firewall rule that blocks VPN traffic, you will need to modify the expert rule to allow VPN traffic. See “Creating expert firewall rules,” on page 55.

- If you are running VPN software on your computer and you want to configure the connection, select either:

Configure Zone Labs security software to support this VPN connection, or

I am running VPN software and would like to configure Zone Labs security software to support it

- If are running VPN software but do not want Zone Labs security software to configure your connection, select **Do not configure Zone Labs security software to support this VPN connection.**
- If you are not running VPN software, select **I am not running VPN software.**

How to see fewer of these alerts

If you are running VPN software, the only way to see fewer of these alerts is to properly configure your Zone Labs security software to allow your VPN software and its required resources. See “Configuring your VPN connection manually,” on page 36.

Manual Action Required alert

A Manual Action Required alert informs you that further steps must be taken before Zone Labs security software is properly configured to support your VPN connection.

Why these alerts occur

A Manual Action Required alert occurs when Zone Labs security software is unable to configure your VPN connection automatically, or if further manual changes are required before automatic configuration can be completed.

What you should do

Manual Action Required alerts do not require a response from you. To configure VPN connection manually, see “Configuring your VPN connection manually,” on page 36 and follow the instructions for manual configuration.

How to see fewer of these alerts

It is unusual for you to see many Manual Action Required alerts. If you do see multiple alerts, either perform the required steps to properly configure your Zone Labs security software to support your VPN connection, or remove the VPN software from your computer.

OSFirewall alerts

OSFirewall alerts are alerts that appear when programs or processes on your computer are attempting to modify your computer's settings or programs.

There are three types of OSFirewall alerts, two of which require a response from you: Medium-rated Suspicious and High-rated Suspicious. Malicious alerts do not require a response from you.

OSFirewall protection is not available in ZoneAlarm.

Medium-rated Suspicious Behavior alert

A Medium-rated Suspicious Behavior alert informs you that a program on your computer is attempting activity that is uncommon or unexpected. If you click Allow, the program is allowed to perform the activity. If you click Deny, the program is prevented from performing the activity and is given Restricted access, which means that all future suspicious behavior will be denied.

Why these alerts occur

Hackers often use trusted programs to modify other programs, such as your browser settings or to compromise your computer's operating system.

What you should do

Click **Allow** or **Deny** to respond. If you are not sure whether to allow or deny the action, click the **More Info** button in the alert box. This submits your alert information (for example, the name of the program and the activity it was trying to perform) to SmartDefense Advisor, which then displays a Web page with information about the alert and the behavior. Use the SmartDefense Advisor information to help you decide whether to allow or deny the action. For more information on the causes of suspicious behavior alerts, see "Medium-rated suspicious behavior," on page 252.



Selecting **Remember this setting** before clicking Allow or Deny causes Zone Labs security software to remember your setting and apply it automatically when the program attempts another similar action. If SmartDefense Advisor is set to Auto, and you select **Remember this setting** in an OSFirewall alert, your setting will remain effective unless SmartDefense Advisor comes out with a different setting, or until you change the setting manually in the Programs tab.

High-rated Suspicious Behavior alert

A High-rated Suspicious Behavior alert informs you that a program on your computer is attempting activity that could be dangerous. If you click Allow, the program is allowed to perform the activity. If you click Deny, the program is prevented from performing the activity and is given Restricted access, which means that all future suspicious behavior will be denied.

Why these alerts occur

These alerts occur when a program or component on your computer was detected trying to hijack a process or program on your computer, or to alter default settings on your computer or one of its programs.

What you should do

Because of the nature of the actions that cause a High-rated Suspicious Behavior alert to appear, it's safest to click Deny in the alert pop-up. If you're not sure, click the **More Info** button in the alert box. This submits your alert information (for example, the name of the program and the activity it was trying to perform) to SmartDefense Advisor, which then displays a Web page with information about the alert and the behavior. Use the SmartDefense Advisor information to help you decide whether to allow or deny the action. Be aware, however, that some legitimate programs perform behavior of this kind as part of normal program functioning. If you trust the program requesting permission, then it may be safe to allow this behavior. In such cases, denying the behavior may result in interrupted program activity. For more information on the causes of suspicious behavior alerts, see "Program behavior," on page 251.



Selecting **Remember this setting** before clicking Allow or Deny causes Zone Labs security software to remember your setting and apply it automatically when the program attempts another similar action. If SmartDefense Advisor is set to Auto, and you select **Remember this setting** in an OSFirewall alert, your setting will remain effective unless SmartDefense Advisor comes out with a different setting, or until you change the setting manually in the Programs tab.

Malicious behavior alert

A Malicious Behavior alert informs you that a malicious program is attempting to run on your computer. Programs that are designated by Zone Labs security experts tend to be known worms, viruses, trojans, or other such malware.

Why these alerts occur

These alerts inform you that a program on your computer will be killed (shut down).

What you should do

Malicious alerts do not require a response from you. They merely inform you of an action that is taking place. If a trustworthy program is mistakenly killed, you can enable the program from the Programs List.

ID Lock alert

An ID Lock alert informs you that information stored in myVAULT is about to be sent to a destination that is not on the Trusted Sites list.

Why these alerts occur

An ID lock alert occurs when information stored in myVAULT is either entered into a Web page or e-mail message, or when your password is being sent to a destination in clear text (unencrypted) form without your authorization.

What you should do

You should determine whether the site requesting the information is one that you trust. Whether you should allow or block the information depends upon the sensitivity of the information, the legitimacy of the request, and the authenticity of the site. If you are in the process of making an online purchase with a trustworthy vendor when you see the alert, it's probably safe to let the information go through. If you see an alert requesting your information when you are not performing such a transaction, it's safest to block the transmission.

Additionally, a few sites transmit passwords in clear text format. If you were to block clear text passwords for a site, then visit that site and enter your password, you would see an ID Lock alert.

How to see fewer of these alerts

You may see frequent ID lock alerts if you frequently submit myVAULT contents to sites that you have not entered on the Trusted Sites list, or if you have blocked clear text passwords for a site that uses clear text passwords. You can minimize the number of ID Lock alerts by adding sites to the Trusted Sites list with which you frequently share your personal information, and by allowing clear text passwords for those sites that use them.

New Network alert

A New Network alert appears when Zone Labs security software detects that you're connected to a network you haven't seen before—be it a wireless home network, a business LAN, or your ISP's network. You can use the alert pop-up to enable file and printer sharing with that network.

The first time you use Zone Labs security software, you will almost certainly see a New Network alert. Don't worry! This alert is a convenience tool designed to help you configure Zone Labs security software.

Why these alerts occur

New Network alerts occur when you connect to any network—be it a wireless home network, a business LAN, or your ISP's network.

What you should do

How you respond to a New Network alert depends on your particular network situation.

If you are connected to a home or business local network and you want to share resources with the other computers on the network, put the network in the Trusted Zone.

To add the new network to the Trusted Zone:

1. In the New Network alert pop-up, type a name for the network (for example "Home NW") in the Name box.
2. Select **Trusted Zone** from the Zone drop-down list.
3. Click **OK**.



If you are not certain what network Zone Labs security software has detected, write down the IP address displayed in the alert box. Then consult your home network documentation, systems administrator, or ISP to determine what network it is.

Use caution if Zone Labs security software detects a wireless network. It is possible for your wireless network adapter to pick up a network other than your own. Be sure that the IP address displayed in the New Network alert is your network's IP address before you add it to the Trusted Zone.

If you are connected to the Internet through a standard modem and dial-up connection, a Digital Subscriber Line (DSL), or a cable modem, click **OK** in the New Network alert pop-up.



If you click Cancel, Zone Labs security software will block your Internet connection. Do not add your ISP network to the Trusted Zone.

How to see fewer of these alerts

It is unusual to receive a lot of New Network alerts.

Instant Messaging alerts

This section provides an explanation of the types of alert messages that may appear during an instant messaging session that is protected by Zone Labs security software.

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

Alert text	Explanation
Session not encrypted because [contact's IM ID] disabled encryption	This alert appears when you have encryption enabled, but your contact has disabled encryption.
Session not encrypted because [contact's IM ID] is not protected by ZoneAlarm Security Suite	This alert appears in your instant messaging window when you are having a conversation with a contact who is not using ZoneAlarm Security Suite
Information about [description] was removed from your previous message in compliance with your ID Lock settings	This alert appears when you attempt to transmit information that is stored in myVAULT. The description of the item as it appears in myVAULT is displayed between brackets.
Link removed	This alert appears in the message recipients's window in place of a removed link.
Session encrypted	This alert appears at the beginning of an encrypted instant messaging conversation.
Potentially harmful content was removed from this message	This alert is appended to the filtered message.
Your message was blocked because you are not on [contact's IM ID]'s contact list	This alert appears when you attempt to send a message to someone who has Spam Blocker enabled, but who does not have you on his or her contact list.
A file transfer on [contact's IM ID]'s PC was blocked	This alert appears when you attempt to send a file to a contact, but the contact has blocked file transfers in ZoneAlarm Security Suite.
Video transmission on [contact's IM ID]'s PC was blocked	This alert appears when a you attempt to transmit video to a contact, but the contact has blocked video transmission.

Table A-1: IM alert messages

Alert text	Explanation
Potentially harmful formatting or scripting was removed from your last message	This alert appears when your contact set the Inbound protection option for Tags to Block, and you attempt to send a message to a contact that includes formatting or scripting.
A potentially harmful link was removed from your last message	This alert appears when your contact set the Inbound protection option for Active to Block, and you attempt to send a message to a contact that includes an executable link.

Table A-1: IM alert messages

Appendix

Keyboard shortcuts

B

Many features of Zone Labs security software are accessible using keyboard shortcuts.

- “Navigation shortcuts,” on page 226
- “Global function shortcuts,” on page 227
- “Dialog box commands,” on page 229
- “Button shortcuts,” on page 230

Navigation shortcuts

Use these keystrokes to navigate through Zone Labs security software's panels, Tabs, and dialog boxes. Use F6 to reach the navigation element you want. Then use UP, DOWN, LEFT, and RIGHT arrows to reach the selection you want within that group.

For example:

To reach the Zones tab of the Firewall panel:

1. Press **F6** until the left menu bar is selected.
2. Press the **DOWN** arrow until the Firewall panel is selected
3. Press **F6** until the tabs are selected.
4. Press **UP, DOWN, LEFT, or RIGHT** until the Zones tab is selected.

Keystroke	Function
F1	Opens online help for the current panel.
F6	Navigates through interface areas in the following order: panel selection, TAB selection, panel area, Stop/Lock controls.
TAB	Navigates through the interface areas in the same order as F6. However, pressing Tab when the panel area is active also navigates through the groups of controls within the panel.
UP and DOWN arrows	Navigates through individual controls within a group of controls.
LEFT and RIGHT arrows	Also navigate through individual controls within a group of controls. In list views, controls horizontal scrolling.
ALT+SPACEBAR	Opens the Windows control menu (maximize, minimize, close).

Table B-1: Navigation shortcuts

Global function shortcuts

Use the following keystrokes to activate functions from multiple locations in the interface. Note that some keystrokes may have other functions in specific panels. Those cases are listed under Button Shortcuts, below.

Keystroke	Function
CTRL+S	Engages and disengages the Stop button (Emergency Lock).
CTRL+L	Engages and disengages the Internet Lock.
ALT+T	Hides and displays explanatory text.
ALT+D	Restores defaults settings.
ALT+C	Opens a Custom dialog box, where one is available.
ALT+U	Opens a second Custom dialog box, where two Custom buttons are available (for example, in the Main tab of the Program Control panel).
ALT+A	Opens an advanced dialog box, where one is available.
ALT+DOWN ARROW	Opens the active drop-down list box. In list views, opens the left-click shortcut menu if one is available.
SHIFT+F10	In list views, opens the right-click shortcut menu if one is available.
ESC	Equivalent to clicking a Cancel button.
ENTER	Equivalent to clicking the active button.
ALT+P	Equivalent to clicking an Apply button.
Delete	Removes a selected item from a list view.
ALT+F4	Shuts down Zone Labs security software.

Table B-2: Global shortcuts

Keystroke	Function
ALT+K	Hides everything except the Dashboard.
ALT+A	Equivalent to clicking an Add button, where one is available.
ALT+R	Equivalent to clicking a Remove button
ALT+E	Equivalent to clicking an Edit button.
ALT+M	Equivalent to clicking a More Info button, where one is available.

Table B-2: Global shortcuts

Dialog box commands

Use the keystrokes below when a dialog box is open.

Keystroke	Function
Tab	Activates the next control in the dialog box.
SHIFT+TAB	Activates the previous control in the dialog box.
CTRL+TAB	Opens the next TAB in a multiple-TAB dialog box.
CTRL+SHIFT+TAB	Opens the previous TAB in a multiple-TAB dialog box.
ALT+DOWN ARROW	Opens the active drop-down list box.
SPACEBAR	Clicks an active button. Selects/clears an active check box.
ENTER	Same as clicking the active button
ESC	Same as clicking the Cancel button.

Table B-3: Dialog box shortcuts

Button shortcuts

Use the keystrokes below to click available buttons in an active window.

Panel	Tab	Keystroke	Equivalent to clicking
Overview	Status Tab	Alt + R	Tutorial
Overview	Status Tab	Alt + M	What's New at Zone Labs?
Overview	Product Info	Alt + I	Change License
Overview	Product Info	Alt + B	Buy Now
Overview	Product Info	Alt + N	Renew
Overview	Product Info	Alt + R	Change Reg.
Overview	Preferences	Alt + P	Set Password
Overview	Preferences	Alt + B	Backup
Overview	Preferences	Alt + R	Restore
Overview	Preferences	Alt + O	Log In/Log Out
Overview	Preferences	Alt + U	Check for Update
Firewall	Main	Alt + C	Internet Zone Custom
Firewall	Main	Alt + U	Trusted Zone Custom
Firewall	Main	Alt + A	Advanced
Firewall	Zones	Alt + A	Add
Firewall	Zones	Alt + R	Remove
Firewall	Zones	Alt + E	Edit
Firewall	Zones	Alt + P	Apply
Firewall	Expert	Alt + A	Add
Firewall	Expert	Alt + R	Remove
Firewall	Expert	Alt + E	Edit
Firewall	Expert	Alt + P	Apply
Firewall	Expert	Alt + G	Groups
Program Control	Main	Alt + C	Program Control Custom
Program Control	Main	Alt + U	Automatic Lock Custom
Program Control	Main	Alt + A	Advanced
Program Control	Programs	Alt + A	Add
Program Control	Programs	Alt + O	Options
Program Control	Components	Alt + M	More info

Table B-4: Keystrokes for activating buttons

Panel	Tab	Keystroke	Equivalent to clicking
Anti-virus / Anti-spyware	Main	ALT + S	Scan for Viruses/Spyware
Anti-virus / Anti-spyware	Main	ALT + U	Update Now
Anti-virus / Anti-spyware	Main	ALT + A	Advanced Options
Anti-virus / Anti-spyware	Main	ALT + V	Scan for Viruses
Anti-virus / Anti-spyware	Main	ALT + W	Scan for Spyware
Anti-virus / Anti-spyware	Quarantine	ALT + D	Delete
Anti-virus / Anti-spyware	Quarantine	ALT + E	Restore
Anti-virus / Anti-spyware	Quarantine	ALT + M	More Info
E-mail Protection	Main	ALT + A	Advanced
E-mail Protection	Attachments	ALT + C	Check All
E-mail Protection	Attachments	ALT + R	Clear All
E-mail Protection	Attachments	ALT + A	Add
E-mail Protection	Attachments	ALT + P	Apply
Privacy	Main	Alt + C	Cookie Control Custom
Privacy	Main	Alt + U	Ad Blocking Custom
Privacy	Main	Alt + S	Mobile Code Control Custom
Privacy	Site List	Alt + A	Add
Privacy	Site List	Alt + O	Options
Privacy	Cache Cleaner	Alt + N	Clean Now
Privacy	Cache Cleaner	Alt + U	Custom
Privacy	Hard Drive IE/MSN Netscape	Alt + D	Reset to Default
Privacy	Hard Drive IE/MSN Netscape	Alt + P	Apply
Privacy	IE/MSN Netscape	Alt + S	Select
ID Lock	myVAULT	Alt + A	Add
ID Lock	myVAULT	Alt + O	Options
ID Lock	myVAULT	Alt + N	Encrypt
ID Lock	myVAULT	Alt + E	Edit
ID Lock	myVAULT	Alt + R	Remove
ID Lock	Trusted Sites	Alt + A	Add

Table B-4: Keystrokes for activating buttons

Panel	Tab	Keystroke	Equivalent to clicking
ID Lock	Trusted Sites	Alt + R	Remove
Parental Control	Main	Alt + A	Advanced
Parental Control	Categories	Alt + C	Check All
Parental Control	Categories	Alt + R	Clear All
Alerts & Logs	Main	Alt + D	Reset to Default
Alerts & Logs	Main	Alt + C	Custom
Alerts & Logs	Main	Alt + A	Advanced
Alerts & Logs	Log Viewer	Alt + M	More Info
Alerts & Logs	Log Viewer	Alt + D	Clear List
Alerts & Logs	Log Viewer	Alt + A	Add to Zone
Alerts & Logs	Log Control	Alt + B	Browse
Alerts & Logs	Log Control	Alt + E	Delete Log

Table B-4: Keystrokes for activating buttons

Appendix

Troubleshooting

C

This chapter provides guidance for troubleshooting issues you may encounter while using Zone Labs security software.

Topics:

- “VPN,” on page 234
- “Networking,” on page 236
- “Internet Connection,” on page 238
- “IM Security,” on page 241
- “Anti-virus,” on page 242
- “Third-party software,” on page 244

VPN

If you are having difficulty using VPN software with Zone Labs security software, refer to the table for troubleshooting tips provided in this section.

If...	See...
You can't connect to your Virtual Private Network (VPN)	"Configuring Zone Labs security software for VPN traffic," on page 234
You have created expert firewall rules	"VPN auto-configuration and expert rules," on page 234
You are using a supported VPN client and Zone Labs security software does not detect it automatically the first time you connect	"Automatic VPN detection delay," on page 234

Table C-1: Troubleshooting VPN problems

Configuring Zone Labs security software for VPN traffic

If you cannot connect to your VPN, you may need to configure Zone Labs security software to accept traffic coming from your VPN.

To configure Zone Labs security software to allow VPN traffic:

1. Add VPN-related network resources to the Trusted Zone.

See "Adding to the Trusted Zone," on page 47.

2. Grant access permission to the VPN client and any other VPN-related programs on your computer.

See "Setting permissions for specific programs," on page 76.

3. Allow VPN protocols.

See "Adding a VPN gateway and other resources to the Trusted Zone," on page 37.

VPN auto-configuration and expert rules

If you have created expert firewall rules that block VPN protocols, Zone Labs security software will not be able to automatically detect your VPN when you initiate a connection. To configure your VPN connection, you will need to make sure that your VPN client and VPN-related components are in the Trusted Zone, and that they have permission to access the Internet. See "Configuring your VPN connection," on page 35.

Automatic VPN detection delay

Zone Labs security software periodically polls your computer to determine if supported VPN protocols are engaged. Upon detection, Zone Labs security software prompts you to configure your connection automatically. If you have recently install a VPN client and have tried to connect, Zone Labs security software may not have detected your VPN configuration. If you prefer Zone Labs security software to configure your connection

automatically, you can wait ten minutes then, try connecting again. If you prefer to connect right away, you can configure your connection manually. See “Configuring your VPN connection,” on page 35.

Networking

If you are having difficulty connecting to your network or using networking services, refer to the table for troubleshooting tips provided in this section.

If ...	See...
You can't see the other computers in your Network Neighborhood, or if they can't see you	"Making your computer visible on your local network," on page 236
You can't share files or printers over your home or local network	"Sharing files and printers across a local network," on page 236
Your computer is on a Local Area Network (LAN) and takes a long time to start up when Zone Labs security software is installed	"Resolving a slow start up," on page 237

Table C-2: Troubleshooting network problems

Making your computer visible on your local network

If you can't see the other computers on your local network, or if they can't see your computer, it is possible that Zone Labs security software is blocking the NetBIOS traffic necessary for Windows network visibility.

To make your computer visible on the local network:

1. Add the network subnet (or, in a small network, the IP address of each computer you're sharing with) to your Trusted Zone. See "Adding to the Trusted Zone," on page 47.
2. Set the Trusted Zone security level to Medium, and the Internet Zone security level to High. This allows trusted computers to access your shared files, but blocks all other machines from accessing them. See "Setting advanced security options," on page 42.



Zone Labs security software will detect your network automatically and display the New Network alert. You can use the alert to add your network subnet to the Trusted Zone. For more information, see "New Network alert," on page 221.

Sharing files and printers across a local network

Zone Labs security software enables you to quickly and easily share your computer so that the trusted computers you're networked with can access your shared resources, but Internet intruders can't use your shares to compromise your system.

To configure Zone Labs security software for secure sharing:

1. Add the network subnet (or, in a small network, the IP address of each computer you're sharing with) to your Trusted Zone. See "Adding to the Trusted Zone," on page 47.
2. Set the Trusted Zone security level to Medium. This allows trusted computers to access your shared files. See "Choosing security levels," on page 41.
3. Set the Internet Zone security level to High. This makes your computer invisible to non-trusted computers. See "Setting the security level for a Zone," on page 41.

Resolving a slow start up

If Zone Labs security software is configured to load at startup, some users connected to the LAN may find that it takes several minutes for the startup process to finish.

In most cases, this is because your computer needs access to your network's Domain Controller to complete its startup and login process, and Zone Labs security software is blocking access because the Controller has not been added to the Trusted Zone.

To solve this problem, add the host name or IP address of your network's Domain Controller to the Trusted Zone.

Internet Connection

If you are having difficulty connecting to the Internet, refer to the table for troubleshooting tips provided in this section.

If...	See...
You cannot connect to the Internet	"Connecting to the Internet fails after installation," on page 238
You can connect to the Internet but are disconnected after a short time	"Allowing ISP Heartbeat messages," on page 239
Your computer is an Internet Connection Sharing (ICS) client and you can't connect to the Internet	"Connecting through an ICS client," on page 239
Your computer uses a proxy server to connect to the Internet and you can't connect to the Internet	"Connecting through a proxy server," on page 240
You see the message "Could not contact automatic program server" in a program alert.	"Unable to connect to program advice server," on page 240

Table C-3: Troubleshooting Internet connection problems

Connecting to the Internet fails after installation

If you are unable to connect to the Internet after installing Zone Labs security software, the first troubleshooting step is to determine whether Zone Labs security software is the cause. If you are unable to follow the steps below, for example, if you can't clear the **Load Zone Labs security software at startup** check box, contact Zone Labs technical support.

To determine if Zone Labs security software is the cause of connection problems:

1. Select **Overview | Preferences**.
2. In the General area, clear the check box **Load Zone Labs security software at startup**.
A warning dialog labeled Zone Labs TrueVector Service opens.
3. Click **Allow**.
4. Restart your computer, then try to connect to the Internet.

If you can connect	Your Zone Labs security software settings may be the cause of your connection problems. Make sure that your browser has access permission.
If you cannot connect	Your Zone Labs security software settings are not the cause of your connection problems.

Allowing ISP Heartbeat messages

Internet Service Providers (ISPs) periodically send heartbeat messages to their connected dial-up customers to make sure they are still there. If the ISP cannot determine that the customer is there, it might disconnect the customer so that the user's IP address can be given to someone else.

By default, Zone Labs security software blocks the protocols most commonly used for these heartbeat messages, which may cause you to be disconnected from the Internet. To prevent this from happening, you can identify the server sending the messages and add it to your Trusted Zone or you can configure the Internet Zone to allow ping messages.

Identifying the source of the heartbeat messages

This is the preferred solution because it will work whether your ISP uses NetBIOS or *ICMP (Internet Control Message Protocol)* to check your connection, and it allows you to maintain high security for the Internet Zone.

To identify the server your ISP uses to check your connection:

1. When your ISP disconnects you, click **Alerts & Logs | Log Viewer**.
2. In the alerts list, find the alert that occurred at the time you were disconnected.
3. In the Entry Detail area, note the Source DNS detected.

If you're not able to identify the server this way, contact your ISP to determine which servers need access permission.

4. After you have identified the server, add it to the Trusted Zone.

See "Adding to the Trusted Zone," on page 47.

Configuring Zone Labs security software to allow ping messages

If your ISP uses ICMP echo (or ping) messages for connectivity checks, configure Zone Labs security software to allow ping messages from the Internet Zone.

To configure Zone Labs security software to allow ping messages:

1. Select **Firewall | Main**.
2. In the Internet Zone area, click **Custom**.
3. Select check box labeled **Allow incoming ping (ICMP echo)**.
4. Click **OK**.
5. Set the security level for the Internet Zone to Medium.

See "Choosing security levels," on page 41.

Connecting through an ICS client

If you are using Windows' Internet Connection Sharing (ICS) option, or a third-party connection sharing program, and you are unable to connect to the Internet, make sure

that Zone Labs security software is properly configured for the client and gateway machines. See “Enabling Internet Connection Sharing,” on page 34.

Do not configure Zone Labs security software for Internet Connection Sharing if you use hardware such as a server or router, rather than a host PC.

Connecting through a proxy server

If you connect to the Internet through a proxy server and you are unable to connect to the Internet, make sure that the IP address of your proxy server is in your Trusted Zone. See “Adding to the Trusted Zone,” on page 47.

Unable to connect to program advice server

If you receive a Program alert with the message “Could not contact automatic program server,” in the SmartDefense Advisor area, make sure that your Internet Connection is working properly.

- Verify that your computer is connected to the network or modem properly.
- If you are connected to the Internet via cable modem or DSL, you may have encountered a temporary service interruption.
- Many times it is just a matter of trying again later if the user has a working configuration.
- Launch your browser. If you are unable to connect to any site on the Internet, you may have Zone Labs security software configured to block Internet access. Providing the correct permission to your browser may resolve the problem.

If none of these scenarios apply, it's possible that the server is temporarily unavailable.

IM Security

If you are having difficulty with the IM Security feature, refer to the table for troubleshooting tips provided in this section.

If...	See...
An active IM program does not appear in the Protection Status table	"IM programs not appearing in status," on page 241

Table C-4: Troubleshooting IM Security problems

IM programs not appearing in status

If you currently have an instant messaging program running but it does not appear in the Protection Status table on the IM Security panel, exit the instant messaging program and restart it.

This can occur if your instant messaging programs and Zone Labs security software are set to launch on startup. To prevent this from recurring, modify the settings for your instant messaging programs to allow a manual launch.

Anti-virus

If you are having difficulty connecting using anti-virus software refer to the table for troubleshooting tips provided in this section.

If...	See...
Anti-virus feature is unavailable	"Anti-virus feature installation problem," on page 242
Anti-virus Monitoring feature is unavailable	"Anti-virus Monitoring alert," on page 242
You receive an alert about conflicting products	"Resolving conflicts with anti-virus products," on page 242
You are unable to turn on the Anti-virus or IM security features	"E-mail scanning or IM Security is unavailable," on page 243

Table C-5: Troubleshooting Zone Labs Anti-virus problems

Anti-virus feature installation problem

In some cases, the Anti-virus feature will be unavailable after installation if there were problems with the installation. This can occur if the `av.dll` file is not registered properly during installation, or if an error occurs during an AV Update operation. In such cases, you will see "Action Required: Re-install ZoneAlarm Security Suite (or ZoneAlarm Anti-virus)".

To resolve this issue, exit Zone Labs security software and run the installation program again. When prompted during installation, choose **Upgrade** rather than **Clean Install**. If after reinstalling the product the Anti-virus panel still does not function properly, you may try uninstalling the product and performing a clean install. If you cannot resolve this problem using these measures, please contact Zone Labs customer support.

Anti-virus Monitoring alert

The Anti-virus Monitoring alert lets you know when the anti-virus protection on your computer is not fully protecting you from viruses. You may receive this alert when your anti-virus is turned off, when your anti-virus signatures are not up-to-date, or when you are not running any anti-virus software at all.

Note that not all anti-virus products are monitored, so the absence of an alert does not necessarily mean you are protected. To ensure your protection, open your anti-virus software (if it is installed) and perform an update or renew your subscription, if it has expired.

Resolving conflicts with anti-virus products

If you are using ZoneAlarm Security Suite and you also have another anti-virus product installed, you may receive a conflict alert that states you must uninstall that product before using Zone Labs anti-virus. The alert will list the anti-virus software products that were detected and specify whether ZoneAlarm Security Suite is able to uninstall

them automatically, or if they must be uninstalled manually. If the products listed cannot be uninstalled automatically, refer to the individual vendor's documentation for instructions for uninstalling the products.

E-mail scanning or IM Security is unavailable

If you are attempting to enable the e-mail scanning option of Zone Labs anti-virus software or the IM Security feature and are unable to do so, you may have a product installed that uses Layered Service Provider (LSP) technology that is incompatible with ZoneAlarm Security Suite. To remedy this situation, you will need to uninstall the conflicting product(s).

When a conflict occurs, a file called `lspconflict.txt` is created and placed in the `C:/Windows/Internet Logs` directory. This file contains the name of the product(s) that caused the conflict. You can remove the product(s) manually or send e-mail to lspsupport@zonelabs.com and attach the file. Refer to the individual vendors' documentation for instructions for uninstalling the product(s).

Third-party software

Many of your most commonly used programs can be configured automatically for Internet access. Although, in some cases, Internet access can be configured automatically, many programs also require server access rights.

If you are using programs that Zone Labs security software is unable to recognize and configure automatically, you may need to configure permissions manually. Refer to the sections that follow to learn how to configure your programs for use with Zone Labs security software.

Anti-virus

In order for your anti-virus software to receive updates it must have access permission for the Trusted Zone.

Automatic updates

In order to receive automatic updates from your anti-virus software vendor, add the domain that contains the updates (e.g., update.avupdate.com) to your Trusted Zone. See “Adding to the Trusted Zone,” on page 47.

E-mail protection

In some cases, Zone Labs security software’s MailSafe feature may conflict with the e-mail protection features of anti-virus software. If this occurs, you can adjust Zone Labs security software and anti-virus settings so that you benefit from both anti-virus and Zone Labs security software protection.

To configure your anti-virus software:

1. Set your anti-virus program to scan all files on access, and disable the e-mail scanning option.
2. In Zone Labs security software, enable Inbound MailSafe protection.
See “Enabling Inbound MailSafe protection,” on page 117.
3. Disable alert display for quarantined MailSafe attachments.
See “Controlling the number of alerts,” on page 161.



With this configuration, MailSafe will still quarantine suspect e-mail attachments and warn you when you try to open them. If you elect to open an attachment anyway, your anti-virus software will still scan it.

Browsers

In order for your browser to work properly, it must have access permission for the Internet Zone and Trusted Zone. Before granting permission, make sure that you

understand how to configure your browser's security for optimal protection and have the latest service packs installed for the browser you are using.

To grant your browser access permission, do any of the following:

- Grant access to the program directly. See “Granting a program permission to access the Internet,” on page 80.
- Select **Allow** when a Program alert for the browser appears.

Internet Explorer

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

To grant Internet access permission to the Services and Controller App:

1. Select **Program Control | Programs**.
2. In the Programs column, locate **Services and Controller App**.
3. In the Access column, select **Allow** from the shortcut menu.

Netscape

Netscape Navigator versions above 4.73 will typically experience no problems running concurrently with Zone Labs security software. If you are using Navigator version 4.73 or higher and are still experiencing difficulty accessing the Web with Zone Labs security software active, check the browser preferences to make sure you are not configured for proxy access.

Chat and instant messaging programs

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

To grant server permission to your chat program:

- Answer Allow to the Server Program alert caused by the program.
- Grant server permission to the program.

See “Granting a program permission to act as a server,” on page 81.



We strongly recommend that you set your chat software to refuse file transfers without prompting first. File transfer within chat programs is a means to distribute malware such as worms, viruses, and Trojan horses. Refer to your chat software vendor's help files to learn how to configure your program for maximum security. If you are using ZoneAlarm Security Suite, set the IM Security level to High to block file transfers.

E-mail programs

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

While you can give your e-mail program access to the Internet Zone, and leave the mail server there, it's safer to place the mail server in the Trusted Zone, and limit the program's access to that Zone only. Once your e-mail client has access to the Trusted Zone, add the remote mail server (host) to the Trusted Zone.

To learn how to give a program permission to access or act as a server to the Trusted Zone, see "Setting program permissions manually," on page 65.

To learn how to add a host to the Trusted Zone, see "Managing traffic sources," on page 46.

Internet answering machine programs

To use Internet answering machine programs (such as CallWave) with Zone Labs security software, do the following:

- Give the program server permission and access permission for the Internet Zone.
- Add the IP address of the vendor's servers to the Trusted Zone.



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

- Set the security level for the Internet Zone to Med.

File sharing programs

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

FTP programs

To use FTP (File Transfer Protocol) programs, you may need to make the following settings adjustments in your FTP client program and in Zone Labs security software:

- Enable passive or PASV mode in your FTP client

This tells the client to use the same port for communication in both directions. If PASV is not enabled, Zone Labs security software may block the FTP server's attempt to contact a new port for data transfer.

- Add the FTP sites you use to the Trusted Zone
- Give Trusted Zone access permission to your FTP client program.

To learn how to add to the Trusted Zone and give access permission to a program, see “Setting advanced security options,” on page 42.

Games

In order to play games over the Internet while using Zone Labs security software, you may have to adjust the settings listed below.



Note that you can configure Zone Labs security software to suppress most alerts while you are playing a game. For details, see “Game Mode,” on page 162.

Program permission

In order to function, many Internet games require access permission and/or server permission for the Internet Zone.

The easiest way to grant access is to answer “Allow” to the program alert caused by the game program. However, many games run in “exclusive” full screen mode, which will prevent you from seeing the alert. Use any of the methods below to solve this problem.

- Set the game to run in a window

This will allow you to see the alert, if the game is running at a resolution lower than that of your desktop. If the alert appears but you cannot respond to it because your mouse is locked to the game, press the Windows logo key on your keyboard.

After granting the game program Internet access, reset the game to run full-screen.

- Use software rendering mode

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

- Use Alt+Tab

Press **Alt+Tab** to toggle back into Windows. This leaves the game running, but allows you to respond to the alert. Once you have allowed Internet access, press **Alt+Tab** again to restore your game.



The last method may cause some applications to crash, especially if you are using Glide or OpenGL; however, the problem should be corrected the next time you run the game. Sometimes you can use Alt-Enter in the place of Alt-Tab.

Security level/Zone

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

- Change your Internet Zone security level to Medium, or
- Add the IP address of the game server you’re connecting to the Trusted Zone. The game manufacturer’s documentation should indicate the IP address or host name of the server.

To learn how to add a host or IP address to the Trusted Zone, see “Adding to the Trusted Zone,” on page 47.



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

Remote control programs

If your computer is either the host or the client of a remote access system such as PCAnywhere or Timbuktu:

- Add the IP address(es) of the hosts or clients to which you connect to your Trusted Zone. See “Adding to the Trusted Zone,” on page 47.
- Add the subnet of the network you are accessing remotely to your Trusted Zone. See “Adding to the Trusted Zone,” on page 47.
- If a dynamic IP address is assigned to the remote machine, add the DHCP server address or range of addresses to the Trusted Zone.



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

VNC programs

In order for VNC and Zone Labs security software to work together, follow the steps below.

1. On both the server and viewer (client) machine, do one of the following:
 - If you know the IP address or subnet of the viewer (client) you will be using for remote access, and it will always be the same, add that IP or subnet to the Trusted Zone. See “Adding to the Trusted Zone,” on page 47.

If you do not know the IP address of the viewer, or if it will change, then give the program access permission and server permission for the Trusted and Internet Zones. See “Setting access permissions for new programs,” on page 74.

When prompted by VNC Viewer on the viewer machine, enter the name or IP address of the server machine, followed by the password when prompted. You should be able to connect.



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

2. On the viewer (client) machine, run VNC Viewer to connect to the server machine. Do not run in “listen mode.”

Telnet

To access a remote server via Telnet, add the IP address of that server to your Trusted Zone.

Streaming media programs

Applications that stream audio and video, such as RealPlayer, Windows Media Player, QuickTime, etc., must have server permission for the Internet Zone in order to work with Zone Labs security software.

To learn how to give server permission to a program, see “Granting a program permission to act as a server,” on page 81.

Voice over IP programs

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

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

Web conferencing programs

If you experience problems using a Web conferencing program such as Microsoft NetMeeting, try the following:

1. Add the domain or IP address that you connect to in order to hold the conference to the Trusted Zone. See “Adding to the Trusted Zone,” on page 47.

- 2. Disable the conferencing program's "Remote Desktop Sharing" option.**

Appendix

Program behavior

D

This appendix provides guidance for determining whether to allow or deny programs to perform suspicious behavior.

- “Medium-rated suspicious behavior,” on page 252
- “High-rated suspicious behavior,” on page 253

Medium-rated suspicious behavior

The table below provides some information you can use to determine how to respond to Medium-rated Suspicious Behavior alerts when they appear. The information listed here is for your reference only. Bear in mind that some legitimate programs need to perform the actions listed below. Whether to allow or deny suspicious program behavior should be determined by your individual situation. (Note that you can configure Zone Labs security software to prevent several of these behaviors automatically. For details, see “Configuring OSFirewall protection,” on page 68.)

Detected Behavior	What this means	What to do
Modifications of the startup directory	A program is setting itself to run each time your computer is started.	Unless you are installing a program, you should deny this action, as it could be spyware.
Modification of browser search defaults	Your default browser search is being modified.	Unless you are currently modifying your browser's search function, you should deny this action.
Modification of browser page defaults	Your default browser home page is being modified.	Unless you are changing your home page, you should deny this action.
Unloading of driver	A program is trying to trying to unload another program's driver.	There are no legitimate reasons for this behavior. You should deny this action.

Table D-1: Medium-rated suspicious behavior guide

High-rated suspicious behavior

The table below provides some information you can use to determine how to respond to High-rated Suspicious Behavior alerts when they appear. The information listed here is for your reference only. Bear in mind that few legitimate programs need to perform the actions listed below.

Detected Behavior	What this means	What to do
Transmission of DDE (Dynamic Data Exchange) input	Program is trying to send DDE input to another program, which could allow the program to gain Internet access or to leak information.	This behavior is often used to open URLs in Internet Explorer. If the application performing the behavior is known and trusted, it is probably safe to allow the behavior. Otherwise, click Deny.
Sending Windows messages	A program is trying to send a message to another program.	A program could be trying to force the another program to perform certain functions. Unless you are installing software that needs to communicate with another program, you should deny this action.
A program is trying to kill another program.	A program is trying to terminate another program	A program could be trying to kill a trusted program. Unless you have just used Task Manager to end a program or process, or have just installed software that requires a reboot of your computer, you should deny this action.
Invoking open process/thread	A program is trying to control another program. It is legitimate for system applications to do this.	Unless the program performing the behavior is trusted, you should deny this action.
Monitoring keyboard and mouse input	A program is attempting to monitor your keyboard strokes and mouse input.	Unless you are running a specialized program that needs to monitor this activity in order to function, such as narration software, you should deny this action.

Table D-2: High-rated suspicious behavior guide

Detected Behavior	What this means	What to do
Remote control of keyboard and mouse input	A program is attempting to remotely control your keyboard and mouse.	Unless you are running remote-access software, such as PC Anywhere or VNC, you should deny this action.
Installation of driver	A program is attempting to load a <i>driver</i> . Loading a driver allows a program to do anything it wants on your computer.	Unless you are installing anti-virus, anti-spyware, firewall, VPN, or other system tools, you should deny this action.
Modification of <i>physical memory</i>	A program may be attempting to modify or read information owned by another program.	Unless you are running gaming, video, or system utility software, you should deny this action.
Injection of code into a program or system service	A program is attempting to inject code into another program, which can be used to disable the program or service.	Unless you are running highly specialized software to change the appearance or behavior of a program, you should deny this action.
Modifying network parameters	A program is attempting to change your network settings, possibly to re-route you to dangerous Web sites and monitor your Web traffic.	Unless you are running TCP/IP tuning software, you should deny this action.
Launching an unknown or bad program from a good one	A program is attempting to modify another program.	Unless a program you are using has a reason to open another program (such as a Word document with a link to a browser, or an IM program with links to other programs) you should deny this action.
Accessing system registry	The process is trying to modify registry settings.	This behavior is usually blocked automatically. If you have program control set to Manual mode, deny this action.
Deletion of a run key	A program was trying to delete a run key entry.	If the program was set to launch on start-up but was cancelled, it will delete the run key. In other cases, you should deny this action.

Table D-2: High-rated suspicious behavior guide

Detected Behavior	What this means	What to do
Modification of ZoneAlarm program	A program is trying to modify the ZoneAlarm program, possibly to prevent it from running, or performing product updates.	Unless you are upgrading the ZoneAlarm client, deny this action.

Table D-2: High-rated suspicious behavior guide

Glossary

1394

A very fast external bus standard that supports data transfer rates of up to 400Mbps (in 1394a) and 800Mbps (in 1394b). Products supporting the 1394 standard go under different names, depending on the company. Apple, which originally developed the technology, uses the trademarked name FireWire.

3DES

Short for Triple Data Encryption Standard, a standards-based symmetric-key encryption method using a 168-bit key. 3DES is a more robust variation of the older 56-bit DES encryption standard.

ACCESS PERMISSION

Access permission allows a program on your computer to initiate communications with another computer. This is distinct from server permission, which allows a program to “listen” for connection requests from other computers. You can give a program access permission for the Trusted Zone, the Internet Zone, or both.

ACT AS A SERVER

A program acts as a server when it “listens” for connection requests from other computers. Several common types of applications, such as chat programs, e-mail clients, and Internet Call Waiting programs, may need to act as servers to operate properly. However, some hacker programs act as servers to listen for instructions from their creators. Zone Labs security software prevents programs on your computer from acting as servers unless you grant server permission.

ACTIVE X CONTROLS

A set of technologies developed by Microsoft that can be automatically downloaded and executed by a Web browser. Because ActiveX controls have full access to the Windows operating system, they have the potential to damage software or data on a user’s machine.

AD BLOCKING

A Zone Labs security software feature that enables you to block banner, pop-up and other types of advertisements.

ADVANCED PROGRAM CONTROL

Advanced Program Control is an advanced security feature that tightens your security by preventing unknown programs from using trusted programs to

access the Internet.

ANIMATED AD

An advertisement that incorporates moving images.

BANNER AD

An ad that appears in a horizontal banner across a Web page.

BLOCKED ZONE

The Blocked Zone contains computers you want no contact with. Zone Labs security software prevents any communication between your computer and the machines in this Zone.

BLUE COAT

Blue Coat is a software development and application services company that filters, monitors and reports on Internet use and activity. ZoneAlarm Pro's Parental Control feature uses Blue Coat content categories to determine whether access to Web sites you visit will be allowed or blocked.

BOOT SECTOR VIRUS

Type of computer virus that infects the first or first few sectors of a computer hard drive or diskette drive allowing the virus to activate as the drive or diskette boots.

CACHE CLEANER

Privacy feature that enables you to remove unwanted files and cookies from your computer on demand, or on a scheduled basis.

CLEAR TEXT

Clear text, also referred to as "plain text," is data that is being transmitted in textual form and is not encrypted. Because the data is not encrypted, it could be intercepted and read by others during transmission.

COLLABORATIVE FILTER

A feature of Zone Labs security software's junk e-mail filter. Collaborative filtering uses information extracted from junk e-mail reported by you and other Zone Labs security software users to determine the probability that new messages from unknown senders are spam.

COMPONENT

A small program or set of functions that larger programs call on to perform specific tasks. Some components may be used by several different programs simultaneously. Windows operating systems provide many component DLLs (Dynamic Link Libraries) for use by a variety of Windows applications.

COMPONENT LEARNING MODE

The period after installation when program control is set to Medium. When in component learning mode, Zone Labs security software can quickly learn the MD5 signatures of many frequently used components without interrupting

your work with multiple alerts.

COOKIE

A small data file used by a Web site to customize content, remember you from one visit to the next, and/or track your Internet activity. While there are many benign uses of cookies, some cookies can be used to divulge information about you without your consent.

COOKIE CONTROL

Privacy feature that allows you to prevent cookies from being stored on your computer.

DES

Short for Data Encryption Standard, a popular symmetric-key encryption method using a 56-bit key. DES has been supplanted by 3DES, a more robust variation of DES.

DESTRUCTIVENESS

Refers to the extent of the damage caused by a virus. The Destructiveness rating refers to the degree to which the damage can be reversed. A low Destructiveness rating would indicate that the scale of the interruption was small, and that any damage done could be reversed. A Medium or High Destructiveness rating would indicate that the damage caused may be irreversible, or that it caused a widespread interruption.

DHCP (DYNAMIC HOST CONFIGURATION PROTOCOL)

A protocol used to support dynamic IP addressing. Rather than giving you a static IP address, your ISP may assign a different IP address to you each time you log on. This allows the provider to serve a large number of customers with a relatively small number of IP addresses.

DHCP (DYNAMIC HOST CONFIGURATION PROTOCOL) BROADCAST/MULTICAST

A type of message used by a client computer on a network that uses dynamic IP addressing. When the computer comes online, if it needs an IP address, it issues a broadcast message to any DHCP servers which are on the network. When a DHCP server receives the broadcast, it assigns an IP address to the computer.

DIAL-UP CONNECTION

Connection to the Internet using a modem and an analog telephone line. The modem connects to the Internet by dialing a telephone number at the Internet Service Provider's site. This is in distinction to other connection methods, such as Digital Subscriber Lines, that do not use analog modems and do not dial telephone numbers.

DLL (DYNAMIC LINK LIBRARY)

A library of functions that can be accessed dynamically (that is, as needed) by

a Windows application.

DNS (DOMAIN NAME SERVER)

A data query service generally used on the Internet for translating host names or domain names (like www.yoursite.com) into Internet addresses (like 123.456.789.0).

DRIVER

A program that controls a device. In Windows environments, drivers often have a.DRV extension. A driver acts like a translator between the device and programs that use the device. Each device has its own set of specialized commands that only its driver knows. In contrast, most programs access devices by using generic commands. The driver accepts generic commands from a program and then translates them into specialized commands for the device.

EMBEDDED OBJECT

An object such as a sound file or an image file that is embedded in a Web page.

ENCRYPTION

The process of transmitting scrambled data so that only authorized recipients can unscramble it. For instance, encryption is used to scramble credit card information when purchases are made over the Internet.

FOREIGN LANGUAGE FILTERS

A feature of Zone Labs security software's junk e-mail filter. Foreign language filters block e-mail containing non-European languages.

GAME MODE

Game Mode temporarily suppresses most Zone Labs security software scans, product updates, and alerts, so that you can play games on your computer with fewer interruptions. Game Mode lets you temporarily allow or deny all program permission requests, so that Zone Labs security software can answer such requests automatically without displaying alerts.

GATEWAY

In networking, a combination of hardware and software that links two different types of networks. For example, if you are on a home or business Local Area Network (LAN), a gateway enables the computers on your network to communicate with the Internet.

HASH

A hash is a number generated by a formula from a string of text in such a way that it is unlikely that some other text would produce the same value. Hashes are used to ensure that transmitted messages have not been tampered with.

HEARTBEAT MESSAGES

Messages sent by an Internet Service Provider (ISP) to make sure that a dial-up connection is still in use. If it appears a customer is not there, the ISP might

disconnect her so that her IP address can be given to someone else.

HIGH-RATED ALERTS

An alert that is likely to have been caused by hacker activity. High-rated Firewall alerts display a red band at the top of the alert pop-up. In the Log Viewer, you can see if an alert was high-rated by looking in the Rating column.

HTTP REFERRER HEADER FIELD

An optional field in the message that opens a Web page, containing information about the “referring document.” Properly used, this field helps Web masters administer their sites. Improperly used, it can divulge your IP address, your workstation name, login name, or even (in a poorly-implemented e-commerce site) your credit card number. By selecting Remove Private Header information in the Cookies tab, you prevent this header field from transferring any information about you.

ICMP (INTERNET CONTROL MESSAGE PROTOCOL)

An extension of the Internet Protocol that supports error control and informational messages. The “ping” message is a common ICMP message used to test an Internet connection.

ICS (INTERNET CONNECTION SHARING)

ICS is a service provided by the Windows operating system that enables networked computers to share a single connection to the Internet.

INDEX.DAT

Index.dat files keep copies of everything that was in your Temporary Internet, Cookies, and History folders even AFTER these files have been deleted.

INFORMATIONAL ALERTS

The type of alerts that appear when Zone Labs security software blocks a communication that did not match your security settings. Informational alerts do not require a response from you.

INTERNET ZONE

The Internet Zone contains all the computers in the world—except those you have added to the Trusted Zone or Blocked Zone.

Zone Labs security software applies the strictest security to the Internet Zone, keeping you safe from hackers. Meanwhile, the medium security settings of the Trusted Zone enable you to communicate easily with the computers or networks you know and trust—for example, your home network PCs, or your business network.

IP ADDRESS

The number that identifies your computer on the Internet, as a telephone number identifies your phone on a telephone network. It is a numeric address, usually displayed as four numbers between 0 and 255, separated by periods.

For example, 172.16.100.100 could be an IP address.

Your IP address may always be the same. However, your Internet Service Provider (ISPs) may use Dynamic Host Configuration Protocol (DHCP) to assign your computer a different IP address each time you connect to the Internet.

ISP (INTERNET SERVICE PROVIDER)

A company that provides access to the Internet. ISPs provide many kinds of Internet connections to consumers and business, including dial-up (connection over a regular telephone line with a modem), high-speed Digital Subscriber Lines (DSL), and cable modem.

JAVA APPLET

A small Internet-based program written in Java that is usually embedded in an HTML page on a Web site and can be executed from within a browser.

JAVASCRIPT

A popular scripting language that enables some of the most common interactive content on Web sites. Some of the most frequently used JavaScript functions include Back and History links, changing images on mouse-over, and opening and closing browser windows. Zone Labs security software default settings allow JavaScript because it is so common and because most of its uses are harmless.

KEYLOGGER

A form of spyware that records keystrokes on your computer, often sending the data to a remote server. Any text input using the keyboard, including credit card numbers or other sensitive personal information could be gathered by a keylogging program and used to commit identity theft.

MAIL SERVER

The remote computer from which the e-mail program on your computer retrieves e-mail messages sent to you.

MD5 SIGNATURE

A digital “fingerprint” used to verify the integrity of a file. If a file has been changed in any way (for example, if a program has been compromised by a hacker), its MD5 signature will change as well.

MEDIUM-RATED ALERT

An alert that was probably caused by harmless network activity, rather than by a hacker attack.

MESSAGE FILTERS

A feature of Zone Labs security software’s junk e-mail filter. Message Filters use heuristic rules to analyze e-mail for characteristics common to various

types of junk e-mail.

MIME-TYPE INTEGRATED OBJECT

An object such as an image, sound file, or video file that is integrated into an e-mail message. MIME stands for Multipurpose Internet Mail Extensions.

MOBILE CODE

Executable content that can be embedded in Web pages or HTML e-mail. Mobile code helps make Web sites interactive, but malicious mobile code can be used to modify or steal data, and for other malevolent purposes.

MOBILE CODE CONTROL

A Zone Labs security software feature that enables you to block active controls and scripts on the Web sites you visit. While mobile code is common on the Internet and has many benign uses, hackers can sometimes use it for malevolent purposes.

NETBIOS (NETWORK BASIC INPUT/OUTPUT SYSTEM)

A program that allows applications on different computers to communicate within a local network. By default, Zone Labs security software allows NetBIOS traffic in the Trusted Zone, but blocks it in the Internet Zone. This enables file sharing on local networks, while protecting you from NetBIOS vulnerabilities on the Internet.

OPENSSL

OpenSSL is an open source security protocol based on the SSL library developed by Eric A. Young and Tim J. Hudson.

PACKET

A single unit of network traffic. On “packet-switched” networks like the Internet, outgoing messages are divided into small units, sent and routed to their destinations, then reassembled on the other end. Each packet includes the IP address of the sender, and the destination IP address and port number.

PASS-LOCK

When the Internet Lock is engaged, programs given pass-lock permission can continue accessing the Internet. Access permission and server permission for all other programs is revoked until the lock is opened.

PERSISTENT COOKIE

A cookie put on your hard drive by a Web site you visit. These cookies can be retrieved by the Web site the next time you visit. While useful, they create a vulnerability by storing information about you, your computer, or your Internet use in a text file.

PERVASIVENESS

Pervasiveness refers to a virus' potential to spread. A boot sector virus that spreads through the manual sharing of floppy disks is given a low Pervasiveness rating, while a worm that has the ability to send itself out to a

large number of victims is given a high pervasiveness rating.

PHISHING

The act of sending a deceptive e-mail that falsely claims to be from a legitimate business or agency. A phishing e-mail attempts to deceive recipients into providing personal information that can then be used for fraudulent purposes.

PHYSICAL MEMORY

The memory hardware (normally RAM) installed in a computer.

PING

A type of ICMP message (formally “ICMP echo”) used to determine whether a specific computer is connected to the Internet. A small utility program sends a simple “echo request” message to the destination IP address, and then waits for a response. If a computer at that address receives the message, it sends an “echo” back. Some Internet providers regularly “ping” their customers to see if they are still connected.

POP-UNDER AD

An ad that appears in a new browser window that opens under the window you're looking at, so you don't see the ad until you close the original browser window.

POP-UP AD

An ad that appears in a new browser window that 'pops up' in front of the window you're looking at.

PORT

A channel associated with the use of TCP or UDP. Some ports are associated with standard network protocols; for example, HTTP (Hypertext Transfer Protocol) is traditionally addressed to port 80. Port numbers range from 0 to 65535.

PORT SCAN

A technique hackers use to find unprotected computers on the Internet. Using automated tools, the hacker systematically scans the ports on all the computers in a range of IP addresses, looking for unprotected or “open” ports. Once an open port is located, the hacker can use it as an access point to break in to the unprotected computer.

PRIVACY ADVISOR

A small display that shows you when Zone Labs security software blocks cookies or mobile code, and enables you to un-block those elements for a particular page.

PRIVATE NETWORK

A home or business Local Area Network (LAN). Private networks are placed

in the *Trusted Zone* by default.

PRODUCT UPDATE SERVICE

Zone Labs subscription service that provides free updates to Zone Labs security software. When you purchase Zone Labs security software, you automatically receive a year's subscription to product update service.

PROGRAMS LIST

The list of programs to which you can assign Internet access and server permissions. The list is shown in the Programs tab of the Program Control panel. You can add programs to the list, or remove programs from it.

PROTOCOL

A standardized format for sending and receiving data. Different protocols serve different purposes; for example SMTP (Simple Mail Transfer Protocol) is used for sending e-mail messages; while FTP (File Transfer Protocol) is used to send large files of different types. Each protocol is associated with a specific port, for example, FTP messages are addressed to port 21.

PUBLIC NETWORK

A large network, such as that associated with an ISP. Public networks are placed in the *Internet Zone* by default.

QUARANTINE

A method used to render harmless suspicious attachments, viruses, or spyware.

SCRIPT

A series of commands that execute automatically, without the user intervening. These usually take the form of banners, menus that change when you move your mouse over them, and pop-up ads.

SECURITY LEVELS

The High, Med., and Off settings that dictate the type of traffic allowed into or out of your computer.

SELF-SIGNED CERTIFICATE

A public-key certificate for which the public key bound by the certificate and the private key used to sign the certificate are components of the same key pair, which belongs to the signer.

SERVER PERMISSION

Server permission allows a program on your computer to “listen” for connection requests from other computers, in effect giving those computers the power to initiate communications with yours. This is distinct from access permission, which allows a program to initiate a communications session with another computer.

SESSION COOKIE

A cookie stored in your browser's memory cache that disappears as soon as you close your browser window. These are the safest cookies because of their

short life-span.

SHA1

An algorithm used for creating a hash of data.

SKYSCRAPER AD

An ad that appears in a vertical column along the side of a Web page.

SMARTDEFENSE ADVISOR

Zone Labs SmartDefense Advisor is an online utility that enables you to instantly analyze the possible causes of an alert, and helps you decide whether to respond Allow or Deny to a Program alert. To use SmartDefense Advisor, click the More Info button in an alert pop-up. Zone Labs security software sends information about your alert to SmartDefense Advisor. SmartDefense Advisor returns an article that explains the alert and gives you advice on what, if anything, you need to do to ensure your security.

SPAM

An inappropriate attempt to use a mailing list or USENET or other networked communications facility as if it were a broadcast medium by sending unsolicited messages to a large number of people.

STEALTH MODE

When Zone Labs security software puts your computer in stealth mode, any uninvited traffic receives no response--not even an acknowledgement that your computer exists. This renders your computer invisible to other computers on the Internet, until permitted program on your computer initiates contact.

TCP (TRANSMISSION CONTROL PROTOCOL)

One of the main protocols in TCP/IP networks, which guarantees delivery of data, and that packets are delivered in the same order in which they were sent.

THIRD PARTY COOKIE

A persistent cookie that is placed on your computer, not by the Web site you are visiting, but by an advertiser or other "third party." These cookies are commonly used to deliver information about your Internet activity to that third party. Also known as tracking cookies.

TROJAN HORSE

A malicious program that masquerades as something useful or harmless, such as a screen saver. Some Trojan horses operate by setting themselves up as servers on your computer, listening for connections from the outside. If a hacker succeeds in contacting the program, he can effectively take control of your computer. This is why it's important to only give server permission to programs you know and trust. Other Trojan horses attempt to contact a remote address automatically.

TRUEVECTOR SECURITY ENGINE

The primary component of Zone Labs security software security. It is the

TrueVector engine that examines Internet traffic and enforces security rules.

TRUSTED ZONE

The Trusted Zone contains computers you trust and want to share resources with.

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

UDP (USER DATAGRAM PROTOCOL)

A connection-less protocol that runs on top of IP networks and is used primarily for broadcasting messages over a network.

WEB BUG

An image file, often 1x1 pixel, designed to monitor visits to the page (or HTML e-mail) containing it. Web bugs are used to find out what advertisements and Web pages you have viewed. If you have blocked web bugs using Privacy control, blank boxes will appear in place of the web bugs.

WILD

Refers to a virus that is spreading as a result of normal day-to-day operations on and between the computers of unsuspecting users. The Wild rating refers to the number of customer reports about this virus. A low Wild rating will reflect a low number of customer reports, whereas a Medium or High Wild rating will reflect a more substantial number of customer reports.

Index

SYMBOLS

.z16 file extension 133

A

Access control

- about 192
- setting options for 200

access permission

- and anti-virus software 244
- browser software and 244
- configuring for programs 7
- e-mail programs and 246
- for Trusted Zone 19
- FTP programs and 247
- games and 247
- granting to programs 38, 65
- password and 74
- setting for ports 51

act as server 19

- defined 257

Action

- in expert rule 55, 61
- in Log Viewer 49, 166

Active Programs area 14

activist sites, blocking 188

ad blocking

- about 136

adding

- custom ports 51
- expert rules to programs 87
- networks to the Trusted Zone 44
- programs to the programs list 79
- to the Blocked Zone 48
- to the Trusted Zone 47
- wireless networks to the Internet Zone 45

Address 59

Address Mask Reply and Request 59

Address Resolution Protocol, enabling 43

adult content, blocking 185

Advanced Program alert 215

adware 108

alerts

- high-rated 204
- ID Lock 220
- Informational 204
- Internet Lock 207
- logging of 159
- medium-rated 204
- New Network 221
- OSFirewall 218
- preferences for 75
- Program
 - Advanced Program alert 215
 - Automatic VPN Configuration alert 35, 215
 - Blocked Program 206
 - Changed Program alert 211
 - MailSafe 116
 - Manual Action Required alert 216
 - New Program 210, 218, 219
 - Repeat Program alert 164
 - Server Program alert 65, 164, 207, 245
- reference 203–222
- responding to 20, 35
- stopping them while gaming 162–163

Alt 59

Amazon protection profile, creating 26

animated ads

- blocking 137
- filling void left by 144

answering machine programs 246

antivirus protection

- status, viewing 109

antivirus protection feature 89–113

anti-virus software

- e-mail protection and 244

antivirus software

- e-mail protection and 244

AOL

- in expert rules 58
- Instant Messenger, using 245
- Privacy Site List and 141

AOL Instant Messenger 192

Application Interaction 82

Application Interaction Control 68

archive files

- viruses and 101

asterisks, use of 176

Attachments List

- accessing 118
- editing 118

- audio transmission, blocking 200
- Authenticating Header (AH) Protocol 35
- AutoComplete forms, clearing data *see* Cache Cleaner
- automatic lock
 - enabling 70
 - setting options for 71
- Automatic VPN Configuration alert 215

B

- backing up and restoring security settings 23
- banner ads
 - blocking 137
 - filling void left by 144
- Blocked Intrusions area 16
- Blocked Program alert 206
- Blocked Zone
 - about 18
 - adding to 48
- blocking
 - ads 144–145
 - cookies 142–143
 - e-mail attachments 116
 - embedded objects 146
 - executable URLs 223
 - file transfers 223
 - inappropriate Web content 185–189
 - packet fragments 43
 - ports 50–52
 - programs 43
 - scripts 146
 - video transmission 223
 - Web content by category 183–189
- Blue Coat 182, 183
- Blue Coat, mentioned 183
- browser cache, cleaning 149, 189
- browser defaults, modifying 252
- browser help object 108
- browser software, using 244

C

- Cache Cleaner 147–150
 - about 136, 147
 - browser cleaning options, setting 148–150
 - hard drive cleaning options, setting 148
 - running manually 147
- categories
 - allowing and blocking 183, 185–189
- Cerberian, mentioned 182
- Challenged Mail 129
- Changed Program alert 211
- Changes Frequently 80
- chat conversations, protection of 192
- chat programs
 - Server Program alert and 245
 - using 245
- check for update settings 22

- clear text password 220
- closing the Zone Labs security software application 15
- code injection *see suspicious behavior*
 - types of 254
- collaborative filter 126
- color-scheme, changing 24, 25
- components
 - managing 85
 - VPN-related 35
- Components List 85
- contributing fraudulent e-mail 126
- contributing junk e-mail 125
- Control Center 12
- Control Center, overview 12–14
- cookie control
 - about 136
- cookies 108
 - blocking 136, 142–143
 - keeping and removing 148
 - setting an expiration date for 143
- CreateProcess 82
- custom ports, adding 51

D

- dashboard
 - keyboard shortcut for 228
 - using 13
- Date/Time
 - in Log Viewer 166
- Day/Time
 - adding to expert rule 56
 - ranges, creating group of 60
- deep-inspection scan 97
- default security settings 199, 200
- DefenseNet 7
- destination
 - in expert rules 53, 55, 56
- dialer 108
- dial-up connection
 - configuring 222
- disabling
 - Windows Firewall 43
- display preferences, setting 24
- Domain Name Server (DNS)
 - defined 260
 - in expert rules 59
 - incoming messages
 - determining source of 166
 - outgoing messages
 - default port permissions for 50
 - determining destination of 49, 166
 - required VPN resources 37
 - troubleshooting Internet connection 239
- Driver event 73
- drivers, loading 254

Dynamic Host Configuration Protocol (DHCP) messages
 default port permissions for 50
 in Day/Time group 59
 remote control programs and 248
Dynamic Real-time rating (DRTR) 184

E

eBay protection profile, creating 26
EBay, blocking 187
echo request
 in expert rules 59
e-mail
 fraudulent, reporting 126
 junk, reporting 125
E-mail Filter toolbar 123
e-mail protection 115–122
 about 116
 Attachments List 118
 inbound 116, 117
 outbound 117
 status of 244
embedded objects, blocking 146
Encapsulating Security Payload (ESP) protocol
 VPN protocols and 35, 43
Encryption 192
 about 196
 enabling and disabling 197
 examples 196–197
 setting options for 200
Eudora, infected e-mail and 133
event logging
 about 159
 customizing 164
 turning on and off 160
Execution event 73
expert firewall rules
 about 53
 creating 55–56
 editing 62
 enforcement of 53–54
 for programs 87
 managing 61–62
 ranking 61
 tracking options for 62
expiration date
 setting for cookies 143
 subscription services and 17

F

Feature Control
 about 194
 mentioned 192
 setting options for 200

file and printer sharing
 enabling 33, 221
 network security and 44
 server access and 214
 troubleshooting 246
File event 73
file fragments, removing *see* Cache Cleaner 148
file transfer, blocking 223
filter options, setting 83
filtering Web content 185
Firewall alert 153
 determining source of 204
 logging of 164
 responding to 204
firewall protection 39–62
 about 40
 advanced security options 42–48
 blocking and unblocking ports 50
 expert rules and 53–54
 keeping current 17
 setting security level for 41
FireWire 43
foreign language filters 126
formatting log file 164
forms data, removing from cache *see* Cache Cleaner
fragments, blocking 43
fraudulent e-mail, *see* junk e-mail filter
Fraudulent Mail folder 126
FTP
 programs, using 246
 protocols, adding to expert rules 58
full system scan 97

G

Game Mode 162–163
games
 online, blocking access to 186
 stopping alerts while playing 162–163
 using with Zone Labs security software 247–248
gaming software
 suspicious behavior and 254
gateway
 adding to the Trusted Zone 47
 as Location type 57
 forwarding or suppressing alerts 42
 Internet Connection Sharing (ICS) and 34
 default port permissions 50
 security enforcement of 42
Generic Routing Encapsulation (GRE) protocol
 mentioned 43
 VPN protocols and 35, 38
glamour and lifestyle sites, blocking 187
government sites, blocking 187
groups
 adding to expert rules 57–60

H

- Hacker ID
 - about 170
- hard drive, cleaning 148
- harmful links, removing 223
- heartbeat messages
 - allowing 239
 - defined 260
 - dial-up connection, troubleshooting 239
- High security setting
 - about 18
 - ad blocking and 137
 - alert events shown in 160
 - allowing uncommon protocols 38
 - cookie control 137
 - default port permissions in 50–51
 - file and printer sharing 33
 - firewall protection and 41
 - for ID Lock 174
 - for Internet Zone 41
 - for Trusted Zone 41
 - logging options and 160
 - privacy protection and 137
 - program control and 67
- high-rated alerts 204
- High-rated Suspicious Behavior alert 218
- home network
 - Firewall alerts and 204
- host file, locking 43
- host name
 - adding to Trusted Zone 237
 - in list of traffic sources 46
 - in Privacy Site list 141
- Hotmail, special folders 123, 131
- humor sites, blocking 187
- Hypertext Transfer Protocol (HTTP)
 - in expert firewall rules 59
- I**
- ID Lock 171–179
 - overview 172
 - see also* myVAULT
- ID Lock alert 220
- Identity Protection Center 171, 180
- identity theft
 - protection from 171, 180
- ie3.proxy.aol.com 141
- IGMP
 - default port permissions for 50
 - in expert rules 53, 87
- IM Security
 - overview 192–198
- IMAP4
 - in expert rules 58
- Inbound Protection
 - about 194–196
 - mentioned 192
 - setting options for 200
- Inbound/Outbound traffic indicator 13
- index.dat files, removing *see* Cache Cleaner
- infected files
 - risk assessment of 100, 105
- Information reply 59
- Information request 59
- Informational alerts 153, 204
- installing
 - ZoneAlarm 4
- installing Zone Labs security software 1–5
- Instant Messaging services
 - blocking access to 192
 - encrypting traffic 196
- Intelligent quick scan 97
- Internet auction sites, blocking 187
- Internet Connection Sharing (ICS)
 - alert options for 208
 - enabling 34
 - setting security options for 42
- Internet Control Messaging Protocol (ICMP)
 - default port permissions for 50
 - in expert firewall rules 53
 - message types 59
 - troubleshooting Internet connection 239
- Internet Explorer
 - cache, cleaning 149
 - granting access permission to 245
 - privacy protection and 137
 - setting cleaning options for 148
- Internet Key Exchange (IKE) protocol
 - VPN protocols and 35
- Internet Lock 14, 15
 - icon 15
- Internet Lock alerts 207
- Internet Relay Chat, blocking 201
- Internet Service Provider (ISP)
 - heartbeat messages from 13, 239
 - in alert details 155
 - in list of traffic sources 46
- Internet Zone 14
 - adding networks to automatically 44, 45
 - networks, adding to automatically 30
 - permissions and 19
- IP address
 - adding to the Trusted Zone 33, 47
 - determining network type from 30, 31
 - hiding in submissions to Zone Labs 25
 - in expert rules 53
 - in list of traffic sources 46
- IP Security (IPSec) protocol
 - VPN protocols and 35
- isafe.exe 134

J

- Java applets, blocking 146
- JavaScript
 - e-mail protection and 116
- junk e-mail filter
 - and privacy 129
 - automatic reporting option 130
 - blocking company names 124
 - blocking mailing lists 124
 - blocking senders 123
 - Challenged Mail folder 129
 - collaborative filter 126
 - contributing junk e-mail 125
 - foreign language filters 126
 - Fraudulent Mail folder 126
 - Hotmail, and 123, 131
 - Junk Mail folder 125
 - message filtering options 126
 - message filters 126
 - protecting privacy 125, 126
 - reporting fraudulent e-mail 125, 126, 130
 - reporting junk e-mail 125
 - reports 132
 - special Outlook folders 123–132
 - toolbar 123
 - wireless device support 130
- Junk E-mail Filter, *see* junk e-mail filter 123
- Junk Mail folder 125

K

- keeping cookies 149
- keyboard and mouse
 - monitoring 253
- keyboard shortcuts 225–232
- keylogger 108
- killing a program 79

L

- Layer 2 Tunneling protocol (L2TP)
 - VPN protocols and 35
- license key
 - updating 27
- Lightweight Directory Access protocol (LDAP)
 - VPN protocols and 35
- local servers, blocking 43
- Location 57
- locations
 - adding to expert firewall rules 56
 - creating groups of 57
- lock icon
 - in System Tray 15
- lock mode, specifying 71

- log entries
 - about 159
 - archiving 169
 - expert rules and 87
 - fields in 168
 - for Program alerts 164
 - for programs 164
 - formatting 164
 - options for 164
 - viewing 165, 167
- Log Viewer
 - accessing 165
 - using 201–202
- Lookup button 57
- loopback adaptor
 - adding to the Trusted Zone 35
- Low security setting
 - Changes Frequently option 80
 - default port permissions for 50–51
 - file and printer sharing and 41
 - program control and 67
 - Zones and 41
- lsass.exe 20

M

- mail servers, connecting to 33
- mail trash, cleaning *see* Cache Cleaner
- MailFrontier 125
- MailSafe
 - outbound protection
 - sender's address, verifying 27
- MailSafe alert 116, 205
- MD5 Signature 80
 - defined 262
- Medium security setting
 - about 18
 - ad blocking and 137
 - alert events 160
 - alerts and 204, 213
 - customizing 19
 - default port permissions for 50–51
 - file and printer sharing and 33
 - ID Lock and 174
 - Internet Zone and 41, 239, 246
 - logging options and 160
 - networking and 33
 - port access and 51
 - privacy protection and 137
 - program control and 67, 246
 - resource sharing and 237
 - Trusted Zone and 41, 47, 236
 - uncommon protocols and 43
- Medium security setting, defined 199
- medium-rated alerts 204
- message encryption 192
- Message event 73
- message filters 126
- military sites, blocking 187

- mime-type integrated objects
 - blocking 146
 - defined 263
- mobile code control
 - about 136
 - customizing 141, 146
- Module event 73
- More Info button 153, 154, 156, 157, 158, 214
 - keyboard shortcut for 228, 232
- MP3 sites, blocking 187
- MSN Messenger 192
- My Computer 55
- myVAULT 175–177
 - adding data to 175
 - editing and removing data 177

N

- NetBIOS
 - default port permissions for 50
 - defined 263
 - firewall alerts and 204
 - heartbeat messages and 239
 - High security setting and 41
 - in expert firewall rules 58
 - network visibility and 236
- Netscape
 - cache, cleaning 149
 - removing cookies 149
 - setting cleaning options for 148
 - version 4.73 245
- Network Configuration Wizard
 - about 30
 - disabling 31
- Network News Transfer Protocol (NNTP) 58
- network resources, sharing 30
- network security options, setting 44
- network settings
 - setting 44
- Networks indicator 13, 14
- New Network alert 221
- New Program alert 210, 218, 219
- news and media sites, blocking 187

O

- OpenGL
 - and system crash 247
- OpenProcess 82
- OSFirewall
 - configuration 68–69
- OSFirewall events
 - types of 73
- Outbound MailSafe protection
 - customizing 121–122
 - enabling 117
 - sender's address, verifying 27
- Outbound Protection area 17

- Outlook, and junk e-mail filter 123

P

- packet
 - defined 263
 - expert firewall rules 53
 - in alerts 153
 - source of
 - determining 168
 - types, blocking 43
- parameter problem
 - in expert rules 59
- Parental Control 181–189
 - about 182
 - allowing and blocking categories 185–189
 - enabling 183
 - setting preferences for 184
 - setting timeout options for 183
 - Smart Filtering and 183
- pass-lock permission
 - granting to a program 84
- passwords
 - clearing from cache 149
 - creating 22
 - Program Control and 74
 - VNCviewer and 249
- pay-to-surf sites, blocking 187
- PC Anywhere
 - suspicious behavior and 254
- PCAnywhere *see* remote control programs, using
- pencil icon 140
- permission
 - pass-lock 14, 70
 - passwords and 22
 - server 19
- persistent cookies 137
 - setting an expiration date for 143
- phishing 125
- Physical Memory event 73
- physical memory, changes to *see suspicious*
- types of 254
- ping messages
 - allowing in Internet Zone 239
 - and alerts 204
 - default port permissions for 50
- Point-to-Point Tunneling Protocol (PPTP)
 - VPN protocols and 35
- policy 69
- POP3
 - in expert firewall rules 58
- ports
 - 1394 43
 - adding 51
 - blocking and unblocking 50–51
 - default permissions for 50
 - firewall protection and 40
 - High security setting and 41
 - in expert firewall rules 53

- preferences
 - for firewall protection 42
 - for Parental Control 184
 - for Program Control 75
 - keyboard shortcut 230
 - load at startup 238
- preferences, setting 24
- printers *see* network resources, sharing
- Privacy Advisor
 - using 139
- Privacy Protection
 - ad blocking
 - customizing 144–145
 - setting level for 137
 - Cache Cleaner 147–150
 - running manually 147
 - cookie control 142–143
 - customizing 142–143
 - setting level for 137
 - enabling per program 137
 - mobile code control
 - customizing 146
 - enabling and disabling 137
 - setting levels for 137
- Privacy Site List
 - accessing 140
 - ad blocking software and 140
 - adding Web sites to 141
 - AOL and 141
- Privacy Site list 140
- private network
 - defined 264
 - Network Configuration Wizard and 30
 - virtual *see* Virtual Private Network (VPN)
- Process event 73
- Program alerts 209–215
 - responding to 69
- Program Component alert 212
- program components
 - managing 85–86
- Program Control 63–248
 - about 64
 - Internet Lock and 70
 - setting level for 67
 - Zones and 19
- program permissions 78
- programs
 - adding to the programs List 79
 - creating expert rules for 87
 - stopping 79
 - trust level of 79
- programs list
 - accessing 76
 - adding and removing programs 79
- protection level
 - customizing 200
 - setting 199

- protocols
 - creating group of 57
 - default permissions for 50
 - firewall protection and 43
 - in expert firewall rules 53
 - in expert rules 43
 - mail 33
 - VPN 35, 38
- proxy server
 - avoidance systems, blocking access to 187
 - troubleshooting Internet Connection 238
- public network
 - defined 265
 - Network Configuration Wizard and 30

Q

- quarantine
 - icon 205
 - Inbound MailSafe protection and 116
 - opening attachments 120, 244
 - setting for attachment types, changing 118

R

- range of IP addresses
 - adding to the Trusted Zone 47
 - in expert firewall rules 55
- ranking expert firewall rules 54, 61
- Real Networks
 - in expert firewall rules 58
- redirect 59
- Registry event 73
- remote access programs
 - troubleshooting 24
- remote control programs, using 248
- remote host computers
 - VPN configuration and 37
- Repeat Program alert 211
 - logging options and 164
- reporting
 - fraudulent e-mail 126
 - junk e-mail 125
- responding to alerts 20, 35, 152
- restoring default settings 200
- restoring security settings 23
- restricting program access 79
- risk assessment of infections 100, 105
- router advertisement 59
- router solicitation 59
- RTSP 58

S

- scanning for viruses 99–102
- schedule scans 90
- screenlogger 108
- scripts, blocking 146

- Secure Hypertext Transfer Protocol (HTTPS) 58
 - secured wireless network
 - Wireless Network Configuration Wizard and 31
 - security components
 - customizing 200
 - managing 199
 - security events, logging 201–202
 - security settings
 - backing up and restoring 23
 - sharing with Zone Labs *see* DefenseNet
 - self-signed certificate 198
 - send mail permission 81
 - Outbound MailSafe protection and 117
 - server permission
 - alerts and 213
 - chat programs and 245
 - column in programs list 79
 - default for traffic types 50
 - e-mail programs and 246
 - expert rules and 87
 - file sharing programs and 246
 - games and 247
 - granting to programs 80
 - streaming media programs and 249
 - Voice Over Internet programs and 249
 - Zones and 19
 - Server Program alert 65, 74, 207, 245
 - logging options and 164
 - services.exe 20
 - session cookies
 - blocking 142
 - High security setting and 137
 - shortcut menu 15
 - SKIP 35
 - skyscraper ads
 - filling void left by 144
 - Smart Filtering
 - about 182
 - enabling 183
 - setting timeout options for 183
 - SmartDefense 78
 - SmartDefense Advisor 204
 - about 170
 - browser permission and 214
 - defined 266
 - setting level for 69
 - submitting alerts to 154, 156
 - SMTP
 - in expert firewall rules 59
 - software rendering mode 247
 - source
 - in expert firewall rules 53
 - keeping cookies from a 148
 - of traffic, determining 46, 159
 - Spam Blocker
 - about 192–193
 - mentioned 192
 - setting options for 200
 - spoolsv.exe 20
 - spy cookie 108
 - Spy Site Blocking 98
 - spyware
 - blocking spyware sites 98
 - preventing 76
 - scanning for 97
 - types of 108
 - Status tab 16
 - stealth mode
 - defined 266
 - High security setting and 41
 - Stop button 15
 - about 13
 - keyboard shortcut for 227
 - system tray icon 15
 - when to click 13
 - subnet
 - adding to the Trusted Zone 47
 - entry type 46
 - VPN configuration and 37
 - Super access 79
 - Suspicious Behavior alert 218
 - suspicious program behavior
 - types of 252
 - suspicious behavior
 - types of 253
 - svchost.exe 20
 - System area 14
- ## T
- Telnet 58, 249
 - TFTP 59
 - third-party cookies, blocking 143
 - Timbuktu *see* remote control programs, using
 - time exceeded 59
 - Timestamp, Timestamp reply 59
 - toolbar, E-mail Filter 123
 - traceroute 59
 - tracking options
 - for expert firewall rules 55, 62
 - traffic sources
 - default port permissions for 50
 - list of 46
 - managing 46
 - Transmission Control Protocol (TCP)
 - default port permission for 50
 - in expert firewall rules 53
 - treating viruses 95
 - Trojan 65
 - Trojan horse 65, 108
 - e-mail protection and 116
 - Program Control and 81
 - protecting Zone Labs security software from 74
 - Troubleshooting 233–240
 - TrueVector security engine 74, 238
 - Trust Levels 78, 79
 - Trusted access 79
 - Trusted Sites list 178–179

Trusted Zone
adding networks to automatically 44
adding to 47
Internet Connection Sharing (ICS) and 34
Networks indicator 14
networks, adding to automatically 30
permissions and 19
VPN resources, adding to 35

U

UDP
default port permissions for 50
in expert firewall rules 53
unsecured wireless network
Wireless Network Configuration Wizard and 31
updating software 22
URL history, cleaning *see* Cache Cleaner
URLs, blocking 201

V

video software
suspicious behavior and 254
video transmission, blocking 200, 223
violent content, blocking 188
Virtual Private Network (VPN)
alerts 35, 215
Automatic Configuration alert 215
configuring connection 35–38, 234
Manual Action Required alert 216
troubleshooting connection 234
viruses
and archive files 101
scanning for 99–102
treating 95, 101
updating signature files 91
VNC
suspicious behavior and 254
VNC programs, using 248
voice transmission
blocking 194
example 194
VoIP programs, using 249

W

Web conferencing programs, using 249
web content, filtering 83
Who Is tab *see* Hacker ID
Windows 98 134
Windows Firewall, disabling 43
Windows Media
clearing history 148
in expert rules 58
winlogon.exe 20
wireless network security options, setting 45

wireless network settings
setting 45
worm 108

Y

Yahoo! Messenger 192

Z

Zone Alarm Fraudulent Mail, *see* junk e-mail filter
Zone Alarm Junk Mail, *see* junk e-mail filter, special Outlook folders
Zone Labs security software 4
about 15
closing the application 15
file sharing programs and 246
FTP programs and 246
installing 1–5
loading at startup 24
updating 17, 22
ZoneAlarm Challenged Mail, *see* junk e-mail filter
ZoneAlarm, installing 4
Zones
about 18
adding to 47–48
firewall protection and 46
keyboard shortcuts 226

