ZoneAlarm ZoneAlarm Help Contents

Getting started

How ZoneAlarm protects you

Troubleshooting

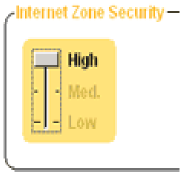
Contact Zone Labs

Setting up

Your setup is already complete!

If ZoneAlarm is running on your computer, you're already protected. You don't have to perform any setup tasks, unless you have special networking or security needs.

Should I change the default security settings?



ZoneAlarm's default settings are appropriate for most Internet users. To learn about the default settings and to find out if they are right for you, see the related topic *Choosing security settings.*

Should I engage the Internet Lock?

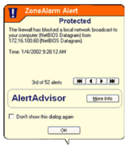
No! You don't need to close the Internet Lock except in emergency situations. For more information, see the related topic *Using the Internet Lock and Stop button.*

How do I know ZoneAlarm is working?

The ZA icon in the lower right corner of your screen tells you ZoneAlarm is protecting you. The icon becomes a red and green traffic indicator whenever network traffic leaves or enters your computer.

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

What do alerts mean?



Protected

The firewall has blocked a local network broadcast to your computer (NetBIOS Datagram) from 172.16.100.60 (NetBIOS Datagram).

Time: 1/4/2002 9:28:12 AM

□ Don't show this dialog again

If you see alerts, don't panic! Alerts help you configure your Program Control settings, and let you know that ZoneAlarm is protecting you. To find out about the different types of alerts, and to learn how to respond to them, see the related topic *Responding to alerts.*

How do I set up for my network?

If you're on a home or business local network, see the related topic *Setting up ZoneAlarm for your network.*

ZoneAlarm Choosing security settings

You don't have to make any settings choices to be protected by ZoneAlarm! Read below to learn how the default settings protect you from hacker threats.

Security and convenience

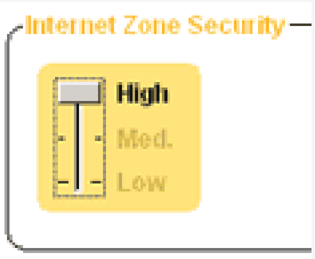
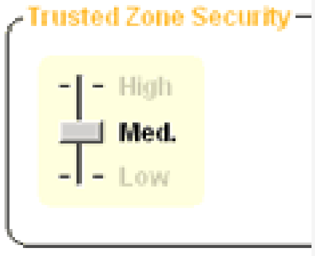
In choosing Internet security settings, your goal is to ensure the highest possible security with the least loss of Internet convenience.

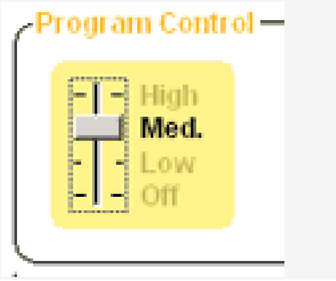
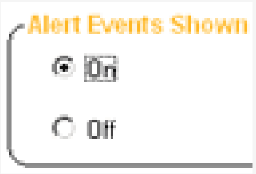
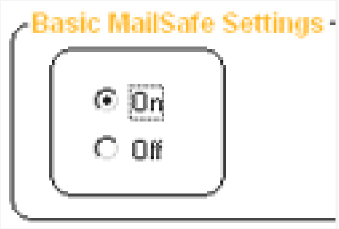
Our security professionals have chosen ZoneAlarm's default security settings with this double goal in mind. They protect your computer from harm and safeguard your information, while keeping your Internet experience convenient.

---

1 ZoneAlarm default settings

For most people, the default settings chosen by the security professionals at Zone Labs provide strong security without sacrificing too much convenience and interactivity.

Control	Default	What the default setting does
Firewall-Internet Zone	 Internet Zone Security High Med. Low	Makes your computer invisible to hackers. Traffic to or from the Internet Zone is blocked, unless it is initiated by a program on your computer that you've given permission to communicate with the Internet Zone.
Firewall- Trusted Zone	 Trusted Zone Security High Med. Low	Enables you to share files and printers with computers on your home or local network.

Program Control-Authentication	 Program Control High Med. Low Off	Programs must ask for permission and be authenticated before communicating with the Internet.
Alerts & Logs	 Alert Events Shown ● On ○ Off	All alerts are shown.
E-mail Protection	 Basic MailSafe Settings ● On ○ Off	Quarantines potentially dangerous e-mail attachments bearing the filename extension .vbs.

Related Topics

Program authentication

ZoneAlarm Using the Internet Lock and Stop button

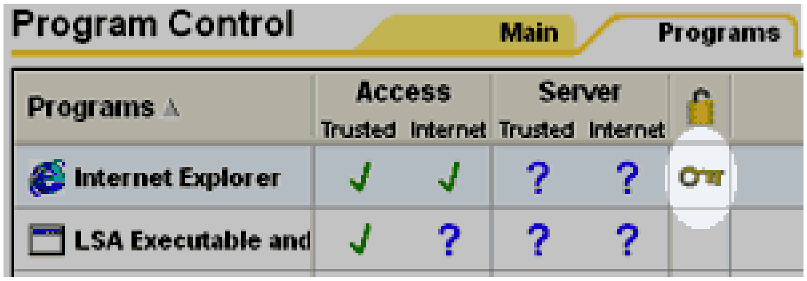
Use the Stop button to instantly "shut the doors" to your computer if you think your under attack. Use the Internet Lock for extra protection when you leave your computer unattended for a time.

Note: The Internet Lock and Stop button can prevent DHCP and ICP heartbeat functions from operating properly, causing problems with your Internet connection.

What's the difference between 'Stop' and 'Lock'?

The **Stop** button stops ALL traffic to and from your computer--no exceptions!

The **Internet Lock** stops all traffic to and from your computer, except traffic initiated by programs to which you have given pass-lock permission.



Program Control

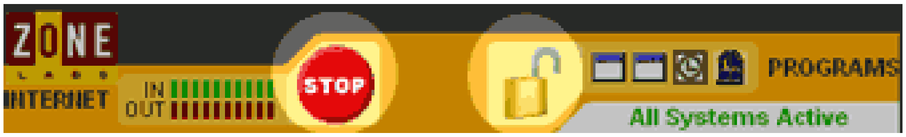
Main | Programs

Programs	Access		Server		
	Trusted	Internet	Trusted	Internet	
Internet Explorer	✓	✓	?	?	O⊤
LSA Executable and	✓	?	?	?	

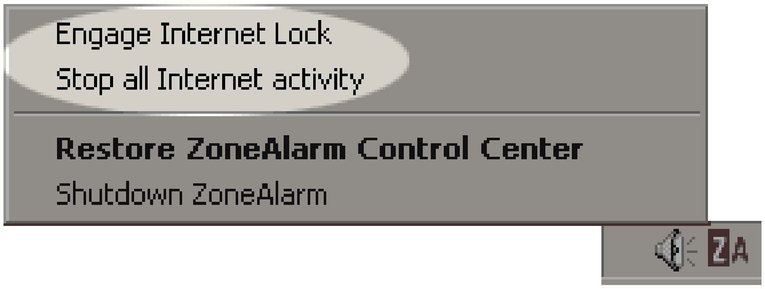
Tip In the Programs tab, a lock icon indicates that the program has pass-lock permission. Click the icon to remove permission.

Turning the lock on and off

There are two ways to manually activate or deactivate the Internet Lock and Stop functions:



Click the **Stop** button or the **Lock** icon on the dashboard at the top of the Control Center.

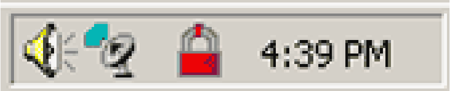


Right-click the ZoneAlarm system tray icon, then select from the shortcut menu.

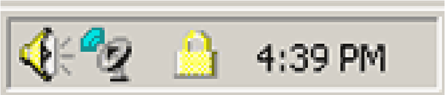
In addition, the Internet Lock can be activated automatically.

How do I know the lock is on?

If the **Stop** button has been clicked, you'll see a red lock icon in the system tray. You may also begin to see a lot of alerts.



If the **Internet Lock** has been clicked, you'll see a yellow lock icon.



To turn either function off, just click the icon again.

Using the Automatic Internet 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.

You can set the automatic lock to engage:

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

You can turn the automatic lock on or off in the Programs panel. For more information about customizing automatic lock settings, see the related topic *Auto-Lock tab.*

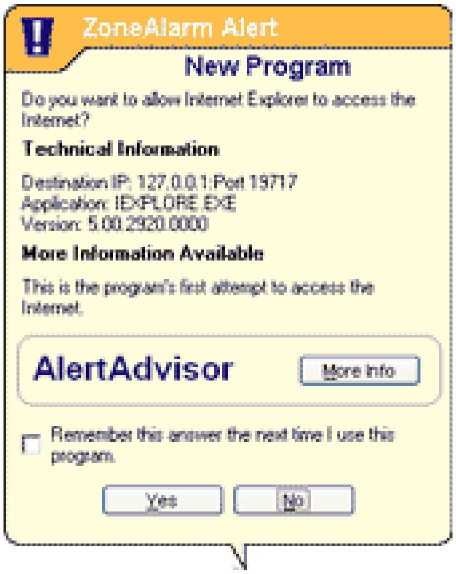
Related Topics

Auto-Lock tab

ZoneAlarm Responding to alerts

When you start using ZoneAlarm, you are likely to see two types of alerts: New Program alerts, and Firewall alerts. Read below to learn what these alerts mean and how to respond to them. For information about all types of alerts, see the related topic *ZoneAlarm alerts*.

New Program alert



Do you want to allow Internet Explorer to access the Internet?

Technical Information

Destination IP: 127.0.0.1:Port 19717
Application: IEXPLORE.EXE
Version: 5.00.2920.0000

More Information Available

This is the program's first attempt to access the Internet.

□ Remember this answer the next time I use this program.

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

Again, don't worry! New Program alerts help you to give access permission to programs that need it—like your browser and e-mail program. They also let you deny permission to programs that you don't want to access the Internet.

New Program alerts occur when ask for Internet or local network access for the first time.

What you should do

To decide how to respond, consider these questions:

• Do you recognize the Program Name? (For example, "Microsoft Outlook")

• Does it makes sense that this program would need Internet access? (For example, am I actively using this program?)

If you can answer "yes" to both these questions, it's probably safe to answer **Yes** to the alert.

If you you cannot answer "yes" to both questions, click the **More Info** button. This will open a browser window and take you to Zone Labs' Alert Advisor, which will analyze information about the alert and give you the most likely explanation for it.

Tip if you're still not sure how to respond, click **No**, and then see if any of your trusted programs are unable to function properly. If so, you can change the program's permission to Yes in the Programs tab. How?

What is a Zone?

Zones are how ZoneAlarm keeps track of the **good**, the **bad**, and the **unknown** out on the Internet.

Zones are virtual spaces

Zones are virtual spaces—ways of classifying the computers and networks that your computer communicates with.

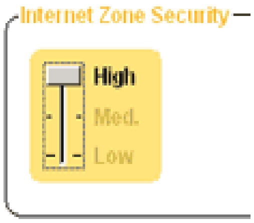
- The **Internet Zone** is the "unknown." All the computers and networks in the world belong to this Zone—until you move them to one of the other Zones.
- The **Trusted Zone** is the "good." It contains all the computers and networks you trust and want to share resources with—for example, the other machines on your local or home network.
- **Blocked Zone** is the "bad." It contains computers and networks you distrust. **(Note:** The **Blocked Zone** is available only in ZoneAlarm Pro and ZoneAlarm Plus).

When another computer wants to communicate with your computer...

ZoneAlarm looks at the Zone it is in—that is, whether it is **good** or **unknown**—to help decide what to do.

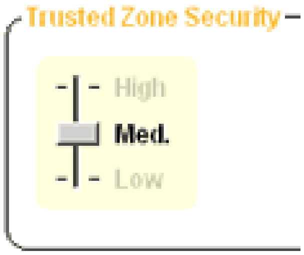
Tip To learn how to put a computer or network in the Trusted Zone, see the related topic *Adding to the Trusted Zone.*

Zones organize firewall security



By default, ZoneAlarm applies **High** security to the Internet Zone and **Medium** security to the Trusted Zone. You are safe from hackers out on the Internet, but you can share resources with the computers and networks you trust.

Using controls in the Firewall panel, you can adjust the security level for each Zone.

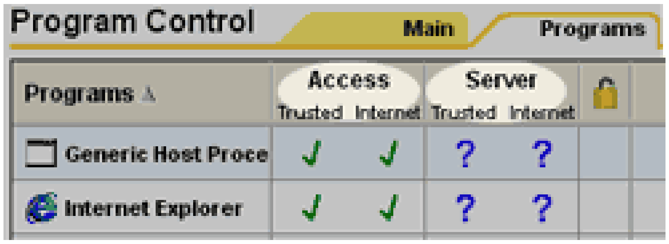

Trusted Zone Security

- High
- Med.
- Low

For more information on security levels, see the related topic *Security levels.*

Zones organize program control

Whenever a program wants access permission or server permission, ZoneAlarm checks in the programs list. Each program has the following permission settings:



Program Control

Programs	Access		Server		
	Trusted	Internet	Trusted	Internet	
Generic Host Proce	✓	✓	?	?	
Internet Explorer	✓	✓	?	?	

• **Access** permission for the **Trusted** Zone/**Internet** Zone

• **Server** permission for the **Trusted** Zone/**Internet** Zone

As you use your computer, ZoneAlarm will display a New Program alert whenever a new program wants access or server permission.

To find out how to change access and server permissions for a program, see the related topic *Changing program permissions.*

Related Topics Back to top

Related Topics

Adding to the Trusted Zone
Changing program permissions
Zones tab
Security levels

Note ZoneAlarm resolves the host name you enter to its IP address(es) when you click **OK**. To see the IP addresses before adding the site, click the **Lookup** button. If the IP addresses associated with the host name are changed after you place the host in the Trusted Zone, those IP addresses are not added to the Trusted Zone.

Adding to the Trusted Zone

Adding IP addresses, ranges and subnets

To add a single IP address:

1. Go to the Zones tab in the Firewall panel.
2. Click the **Add** button, and select **IP address** from the shortcut menu. This will open the Add IP Address dialog box.
3. Type the IP address and a description in the boxes provided, then click **OK** or **Apply.**

To add an IP range:

1. Go to the Zones tab in the Firewall panel.
2. Click the **Add** button, and select **IP range** from the shortcut menu. This will open the Add IP Range dialog box.
3. Type the beginning IP address in the first box, and the ending IP address in the second box.
4. Type a description in the box provided, then click **OK**.

To add a subnet:

1. Go to the Zones tab in the Firewall panel.
2. Click the **Add** button, and select **Subnet** from the shortcut menu. This will open the Add Subnet dialog box.
3. Type the IP address in the first box, and the subnet mask in the second box.
4. Type a description in the box provided, then click **OK**.

Adding hosts/sites

To add a host or site:

1. Go to the Zones tab in the Firewall panel.
2. Click the **Add** button, and select **Host/Site** from the shortcut menu. This will open the Add Host/Site dialog box.
3. Type the host name in the box provided.
4. Type a description in the box provided, then click **OK**.

ZoneAlarm® Firewall protection

ZoneAlarm's firewall protection guards the "doors" into your computer to keep you safe from "fires" out on the Internet.

What is a firewall?

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" there out on the Internet—hacker activity, viruses, worms, and so forth. A firewall is a system that stops the fire from spreading to your computer.

A firewall guards the "doors" to your computer—that is, the ports through which Internet traffic comes in and goes out. The firewall only lets traffic through the ports that you have specified can be used. This has two security benefits:

- No one can sneak into your computer through an unguarded port.
- Programs on your computer can't use unguarded ports to contact the outside world without your permission.

What are ports?

Ports are logical channels through which traffic enters or leaves your computer. Your computer has thousands of ports, each identified by a number.

Whenever a another computer sends a message to your computer, it addresses that message to a specific port. For example, a server delivering a Web page to your browser, using the Hypertext Transfer Protocol (HTTP), traditionally sends to port 80.

What is a protocol?

A protocol is a bit like a language—it is an agreed-on way of transmitting information. The Internet uses many protocols, and each of them is normally associated with a particular port or ports. For example, the NetBIOS protocol, which is used by Windows systems to enable resource sharing on a local network, traditionally uses ports 135, 137-39, and 445.

How does it work?

All Internet traffic—Web pages, e-mail, audio files, and so on—are transmitted in bite-sized chunks called "packets." Each packet is addressed to a particular computer, and to a particular port on that computer.

ZoneAlarm examines every packet that arrives at your computer and asks three questions:

1. What Zone did the message come from? Trusted or Internet?
2. What port is it addressed to?
3. Do the rules for that Zone allow traffic through that port?

If the answer to number three is yes, the packet is allowed in.

If the answer is no, the packet is blocked.

Note This describes the treatment of unsolicited traffic—that is, packets that arrive from the Internet or a local network unexpectedly. Port scans are a good example of unsolicited traffic that ZoneAlarm protects you from. When a permitted program on your computer has established a communications session with another computer, those permissions override the firewall rules.

How does the firewall use Zones and security levels?

The answer to question number three above ("Do the rules for that Zone allow traffic through that port?") depends on the security level that is applied to each Zone.

To choose a security level for a Zone, use the slider controls in the Main tab of the Firewall panel..

The meaning of each security level (that is, the ports that are blocked or allowed at that level) is described in the related topic *Security levels*. use the Internet Zone tab and Trusted Zone tab in the Custom Securities dialog box (see the right column in the table below).

Related Topics

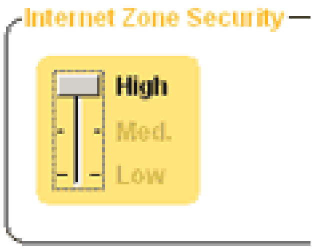
What's a Zone?

ZoneAlarm Security levels

ZoneAlarm's preconfigured security levels make it easy to configure your firewall settings.

Tip to be able to customize security levels by blocking or unblocking specific ports, upgrade to ZoneAlarm Pro.

High security



High security for both the Internet Zone and Trusted Zone places your computer is in stealth mode. 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

Medium security enables file and printer sharing, 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.

Low Security

Low security defaults allow all types of traffic.

High security defaults

Traffic Type	**High Security**	**Medium Security**	**Low Security**
DNS outgoing	allow	allow	allow
DHCP outgoing	allow	allow	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	block	block	allow
outgoing	block	allow	allow
UDP ports not in used by a permitted program			
incoming	block	allow	allow
outgoing	block	allow	allow
TCP ports not in use by a permitted program			
incoming	block	allow	allow
outgoing	block	allow	allow

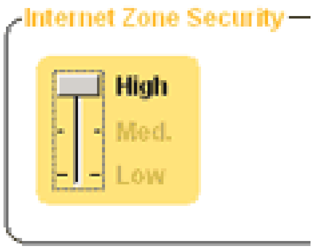
Medium security defaults

Traffic Type	**High Security**	**Medium Security**	**Low Security**
DNS outgoing	allow	allow	allow
DHCP outgoing	allow	allow	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	block	allow (Trusted Zone) block (Internet Zone)	allow
outgoing	block	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			
incoming	block	allow	allow
outgoing	block	allow	allow

Low security defaults

Traffic Type	**High Security**	**Medium Security**	**Low Security**
DNS outgoing	allow	allow	allow
DHCP outgoing	allow	allow	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	block	allow (Trusted Zone) block (Internet Zone)	allow
outgoing	block	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			
incoming	block	allow	allow
outgoing	block	allow	allow

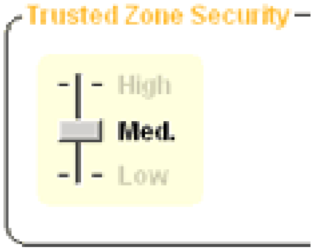
ZoneAlarm® Setting the Internet Zone security level



To set the security level for the Internet Zone:

1. In the Main tab of the Firewall panel, move the slider to **High**, **Medium**, or **Low**.

ZoneAlarm® Setting the Trusted Zone security level



To set the Trusted Zone security level:

1. In the Main tab of the Firewall panel, move the slider to **High**, **Medium**, or **Low**.

ZoneAlarm Program Control

Program control protects you from Trojan horses and other hacker malware by making sure only programs with your permission can access the Internet.

Why do I need program control?

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

Hackers exploit this fact by planting "malware"—literally, evil programs—on your computer. Sometimes they send out malware as e-mail attachments with innocent names like "screensaver.exe." If you open the attachment, you install the malware on you computer without even knowing it. Other times, they convince you to download the the malware from a server by making it masquerade as an update to a legitimate program.

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

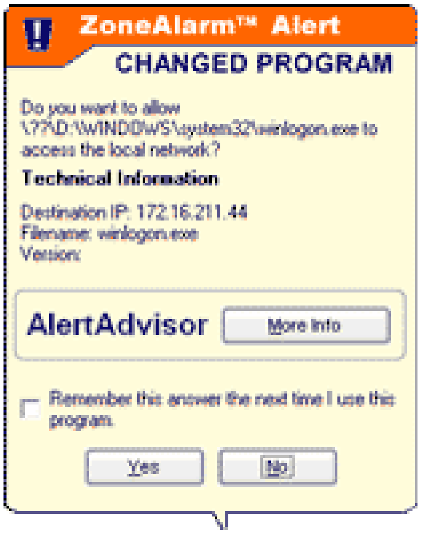
ZoneAlarm protects you from malware attacks

ZoneAlarm's program control features use the following methods to protect you from malware attacks:

- **Program authentication.** ZoneAlarm makes sure your programs haven't been tampered with.
- **Program access control**. ZoneAlarm gives programs access permission or server permission only if you tell it to.

Program Authentication

Whenever a program on your computer wants to access the Internet, ZoneAlarm authenticates it via its MD5 signature.



Do you want to allow \??\D:\WINDOWS\system32\winlogon.exe to access the local network?

Technical Information

Destination IP: 172.16.211.44
Filename: winlogon.exe
Version:

□ Remember this answer the next time I use this program.

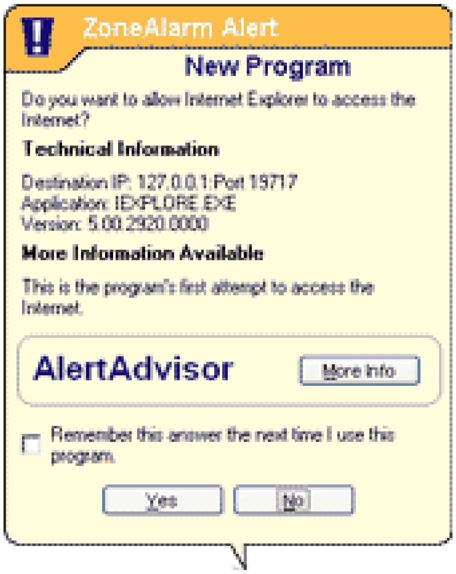
If the program has been altered since the last time it accessed the Internet, ZoneAlarm displays a Changed Program alert (shown at left). YOU decide whether the program should be allowed access or not.

For more information about program authentication or about alerts, see Related Topics.

Program Access Control

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

When a program requests access for the first time...



Do you want to allow Internet Explorer to access the Internet?

Technical Information

Destination IP: 127.0.0.1:Port 19717
Application: IEXPLORE.EXE
Version: 5.00.2920.0000

More Information Available

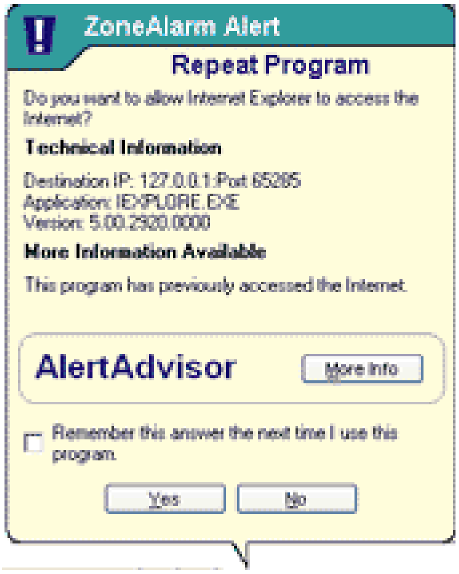
This is the program's first attempt to access the Internet.

□ Remember this answer the next time I use this program.

A New Program alert (shown at left) asks you if you want to grant the program access permission.

If you're not sure whether to click **Yes** or **No**, you can click the **More Info** to have Zone Labs' Alert Advisor help you decide what to do.

If the same program requests access again...



ZoneAlarm Alert

Repeat Program

Do you want to allow Internet Explorer to access the Internet?

Technical Information

Destination IP: 127.0.0.1:Port 65285
Application: IEXPLORE.EXE
Version: 5.00.2920.0000

More Information Available

This program has previously accessed the Internet.

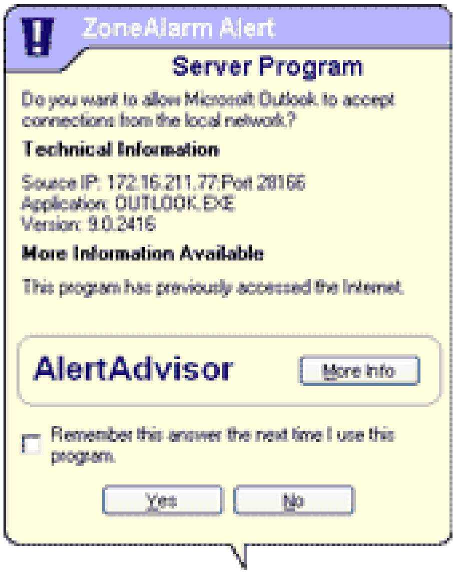
AlertAdvisor

□ Remember this answer the next time I use this program.

A Repeat Program alert (shown at left) asks you if you want to grant (or deny) access permission to a program that has requested it before.

Tip To avoid seeing repeat program alerts, select the **Remember this answer** check box near the bottom of the alert before clicking **Yes** or **No**. After that, ZoneAlarm will silently block or allow the program.

When a program asks for server permission...



ZoneAlarm Alert

Server Program

Do you want to allow Microsoft Outlook to accept connections from the local network?

Technical Information

Souce IP: 172.16.211.77:Port 28166
Application: OUTLOOK.EXE
Version: 9.0.2416

More Information Available

This program has previously accessed the Internet.

AlertAdvisor

□ Remember this answer the next time I use this program.

A Server Program alert (shown at left) asks you if you want grant server permission to a program.

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

Related Topics

Program authentication
ZoneAlarm alerts

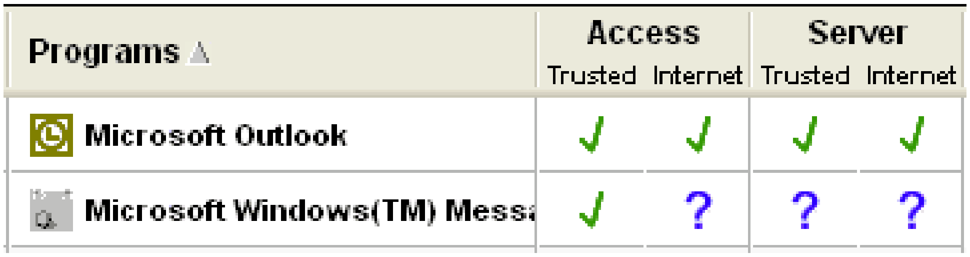
ZoneAlarm Program Authentication

ZoneAlarm's program authentication feature makes sure that only legitimate programs on your computer can access the Internet.

How ZoneAlarm authenticates programs

ZoneAlarm authenticates your programs by recording their MD5 signatures the first time the program requests network or Internet access, then checking those signatures when the program requests access again.

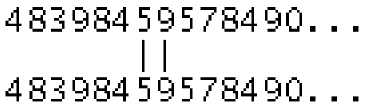
The first time a program requests access or server permission...



Programs ▲	Access		Server	
	Trusted	Internet	Trusted	Internet
Microsoft Outlook	✓	✓	✓	✓
Microsoft Windows(TM) Mess	✓	?	?	?

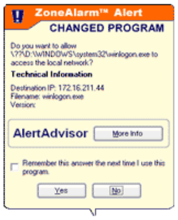
ZoneAlarm adds the program to the Programs tab and records the MD5 signature of the program.

The next time the same program requests access or server permission...



```
483984 59578490...
        ||
483984 59578490...
```

ZoneAlarm compares the recorded MD5 signature of the program with its current signature.



ZoneAlarm™ Alert

CHANGED PROGRAM

Do you want to allow \??\D:\WINDOWS\system32\winlogon.exe to access the local network?

Technical Information

Destination IP: 172.16.211.44
Filename: winlogon.exe
Version:

If the program signatures don't match, it means the program has changed somehow since it first requested access, and a Changed Program alert is displayed. By clicking **No**, you can deny access to the changed program.

Related Topics

Main tab (Program Control panel)

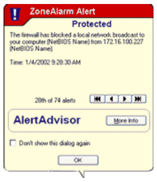
Changed Program alert

ZoneAlarm Alerts & Logging

ZoneAlarm's alert and logging features keep you aware of what's happening on your computer without being overly intrusive.

Controlling the display of alerts

You may be the type of person who wants to know everything that happens on your computer—or you may not want to be bothered, as long as you know your computer is secure.



The firewall has blocked a local network broadcast to your computer (NetBIOS Name) from 172.16.100.227 (NetBIOS Name).

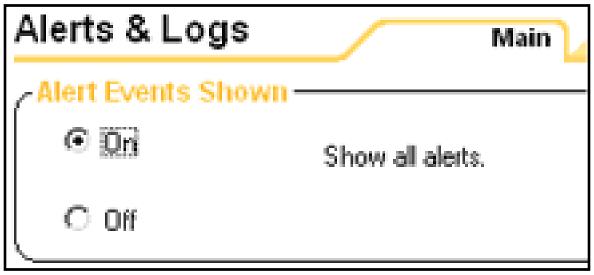
Time: 1/4/2002 9:28:30 AM

28th of 74 alerts

□ Don't show this dialog again

ZoneAlarm accommodates you, no matter which kind of person you are. You can be notified by an alert box (shown in reduced size at left) each time ZoneAlarm acts to protect you; or you can opt for quieter protection.

Alert display settings



Alert Events Shown

● On — Show all alerts.

○ Off

The default **On** alert display setting displays an alert pop-up whenever ZoneAlarm blocks Internet traffic.

If you don't want to be bothered by firewall alerts or Blocked Program alerts, just select **Off**.

Note If you select Off, some program alerts (New Program, Repeat Program, Server Program, and Changed Program) will still be displayed. This is because those alerts require you to make a Yes/No choice.

Logging security events

ZoneAlarm logs its activity to a text file on your computer, automatically providing you with a a complete record of security activity.

ZoneAlarm gives you easy access to alert log records via the Log Viewer tab, so you can quickly retrieve the details on any individual alert. ZoneAlarm also provides easy tools for formatting and archiving text logs.

Related Topics

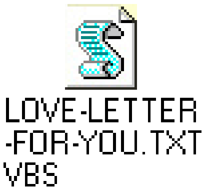
Showing and hiding firewall alerts
Viewing the ZoneAlarm log

ZoneAlarm E-mail protection

ZoneAlarm's MailSafe™ feature protects you from new viruses, worms, and other malware distributed in e-mail attachments. It also protects you from any old, known threats.

The problem with attachments

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. For example, the infamous "Love Bug" worm was distributed as a Visual Basic Script (.VBS) file

Fortunately, only certain types of attachments can contain potentially dangerous code. These attachments types can be identified by their filename extensions.

About filename extensions

Filename extensions are the characters that appear after the "dot" in a file name. They identify the file type so that the appropriate program can open it.

Tip It's a good idea never to open an e-mail attachment unless you know the person it came from, and have confirmed (by phone or separate e-mail message) that that person actually sent it to you. Remember hackers can alter an e-mail message to look like it came from a friend!

The MailSafe quarantine

ZoneAlarm's MailSafe protects you by 'quarantining' e-mail attachments that may contain malicious code.

When an e-mail with an attachment arrives...

MailSafe examines the attachment's filename extension.

If that extension is .VBS (one of the most common file types used to distribute worms and viruses), ZoneAlarm changes the filename extension to ".zl*" (where * is a number or letter.)

Note Basic MailSafe quarantines .VBS attachments only. To obtain protection against additonal attachment types, and to be able to edit the quarantine list, upgrade to ZoneAlarm Pro.

Changing the filename extension 'quarantines' the attachment by keeping it from running automatically.

When you try to open the attachment...

ZoneAlarm warns you of the potential risk in opening the attachment. If you're sure the file is harmless and you want to open it, click the **Run** button. You can also save the file for later.

Tip Users who know how to read code can click **Inspect with Notepad** to examine the code of attachment itself.

Related Topics

Main tab (E-mail panel)

ZoneAlarm Using Web meeting software with ZoneAlarm

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

- Add the domain or IP address that you connect to in order to hold the conference to the Trusted Zone
- Turn off the conferencing program's "Remote Desktop Sharing" option

To learn how to add elements to the Trusted Zone, see Related Topics.

Related Topics

Adding to the Trusted Zone.

ZoneAlarm Using browsers with ZoneAlarm

In order for your browser to work properly, it must have access permission for the Internet Zone and Trusted Zone. You can grant access in any of the following ways:

- Run the Program Wizard from the Main tab of the Program Control panel. ZoneAlarm will automatically detect your default browser and prompt you to grant it Internet Zone access.
- Go to the Program tab in the Program Control panel, and use the controls there to grant access.
- Answer **Yes** when a Program alert for the browser appears.

To learn how use the Program tab to grant Zone access to a program, see the related topic *Changing program permissions.*

Windows 2000

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 do this:

1. Open the Programs tab in the Program Control panel.
2. Locate Services and Controller App in the program list.
3. Click the buttons in the Access field, and select **Allow** from the shortcut menu.

Netscape

Netscape Navigator versions above 4.73 will typically experience no problems running concurrently with ZoneAlarm . If you are using Navigator version 4.73 or higher are still experiencing difficulty accessing the web with ZoneAlarm active, check the browser Preferences to make sure you are not configured for proxy access.

Tip 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.

Related Topics

Changing program permissions

ZoneAlarm Using chat programs with ZoneAlarm

Chat and instant messaging programs (for example, AOL Instant Messenger and ICQ) may require server permission in order to operate properly. You can grant server permission by:

- Answering "Yes" to the Server Program alert caused by the program, or
- Using the Programs tab.

To learn how to grant server permission by using the Programs tab, see the related topic *Changing program permissions.*

For more information on Server Program alerts, see the related topic *Server Program alert.*

⚠ **Caution** 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 maximize security.

💡 **Tip** For best security, we suggest that mIRC users disable the IDENT function in the mIRC interface.

Related Topics

Changing program permissions
Server Program alert

ZoneAlarm Using e-mail programs with ZoneAlarm

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, MS Outlook requires 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 the related topic *Changing program permission.*

To learn how to add a host to the Trusted Zone, see the related topic *Adding to the Trusted Zone*.

Related Topics

Changing program permission
Adding to the Trusted Zone

ZoneAlarm Using file sharing with ZoneAlarm

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 ZoneAlarm.

To learn how to give server permission to a program, see Related Topics.

Related Topics

Giving server permission to a program

ZoneAlarm Using FTP programs with ZoneAlarm

To use FTP (File Transfer Protocol) programs, you may need to make the following settings adjustments in your FTP client program and in ZoneAlarm.

- Enable passive or PASV mode in your FTP client

  This tells the client to use the same port for communication both directions. If PASV is not enabled, ZoneAlarm 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 Related Topics.

Related Topics

Adding to the Trusted Zone
Giving access permission to a program

ZoneAlarm Using games with ZoneAlarm

In order to play games over the Internet while using ZoneAlarm, you may have to adjust the following settings.

Program permission

Internet games to function require access permission and/or server permission for the Internet Zone.

The easiest way to grant access is to answer "Yes" 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 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 ZoneAlarm 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.

Note 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.

To learn how to grant access or server permission by using the Programs tab, see the related topic *Changing program permission.*

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 game server you're connecting to to your Trusted Zone. The game documentation or from the game manufacturer's Web site 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 the relate topic *Adding to the Trusted Zone.*

Caution Trusting game servers means trusting the other players in the game. ZoneAlarm 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.

Firewall settings

ZoneAlarm dynamically opens and closes ports as needed when you're gaming, so no adjustments to firewall configuration need to be made.

Related Topics

Changing program permission
Adding computers to the Trusted Zone

ZoneAlarm Using Internet answering machine/Internet call waiting programs with ZoneAlarm

To use Internet answering machine programs (such as CallWave) with ZoneAlarm, do the following:

1. Give the program server permission and access permission for the Internet Zone. How?
2. Add the IP address of the vendor's servers to the Trusted Zone. How?

   Tip To find the server IP address, contact the vendor's technical support.

3. Set the security level for the Internet Zone to medium. How?

Related Topics

Giving server permission to a program
Setting the Internet Zone security level

ZoneAlarm Using remote control/display software

PCAnywhere and Timbuktu

If your computer is either the host or the client of a remote access system such as PCAnywhere or Timbuktu:

1. Add the IP address(es) of the hosts or clients to which you connect to your Trusted Zone. How?
2. Add the subnet of the network you are accessing remotely to your Trusted Zone.
3. If a dynamic IP address is assigned to the remote machine, add the DHCP server address or range of addresses to the Trusted Zone.

Note 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

In order for VNC and ZoneAlarm to work together, follow the steps below.

1. On the server 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. This is the preferred option.
   - If you **do not know** the IP address of the viewer, or it will change, then give the program access permission and server permission for the Trusted and Internet Zones.
2. On the viewer (client) machine, run VNCviewer to connect to the server machine. Do not run in "listen mode."
3. On the viewer (client) machine, do one of the following:
   - If you **know** the IP address or subnet of the server, and it will always be the same, add that address or subnet to the Trusted Zone. This is the preferred option.
   - If you **do not know** the IP of the Server, or it will change, then give the program access permission and server permission for both the Trusted Zone and Internet Zone.
4. When prompted by VNCviewer 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.

Caution 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.

Tip Leave the Trusted Zone security level on medium. If you raise it to high, you may have access problems.

To learn how to add IP addresses, subnets, or ranges to the Trusted Zone, or give access and server permissions to programs, see Related Topics.

Telnet

To access a remote server via Telnet, add the IP address of that server to your Trusted Zone.

Related Topics

Adding to the Trusted Zone
Giving access permission to a program
Giving server permission to to a program

ZoneAlarm Using streaming media applications with ZoneAlarm

Applications that stream audio and video, such as RealPlayer, Windows Media Player, QuickTime, and so forth, etc. must have server permission for the Internet Zone in order to work with ZoneAlarm.

To learn how to give server permission to a program, see Related Topics.

Related Topics

Giving server permission to a program

ZoneAlarm Using Voice over IP (VoIP) programs with ZoneAlarm

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

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

Related Topics

Adding to the Trusted Zone
Giving server permission to a program
Giving access permission to a program

ZoneAlarm Using anti-virus software with ZoneAlarm

Automatic updates

In order to receive automatic updates from your anti-virus software vendor, add the domain that contains the updates (e.g. update.avsupdate.com) to your Trusted Zone.

To learn how to add a domain to the Trusted Zone, see Related Topics.

E-mail protection

In some cases, ZoneAlarm's MailSafe feature may conflict with the e-mail protection features of anti-virus software. If this occurs, you can adjust ZoneAlarm and anti-virus settings so that you benefit from both anti-virus and ZoneAlarm protection. Follow these steps:

1. Set your anti-virus program to scan all files on access, and disable the e-mail scanning option.
2. In ZoneAlarm, enable MailSafe. How?

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.

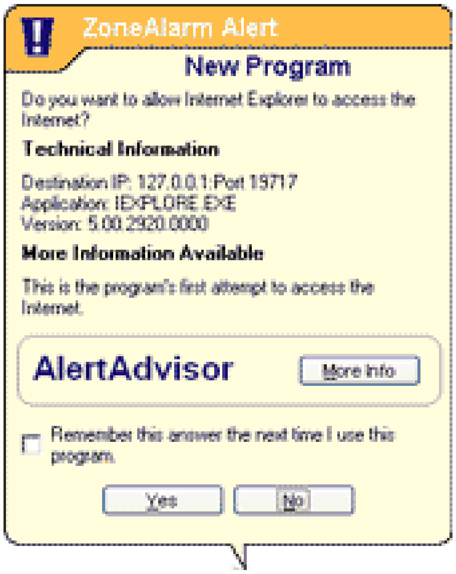
To learn how to disable MailSafe, or to learn more about the MailSafe feature, see Related Topics.

Related Topics

Giving server permission to a program
E-mail protection

ZoneAlarm Giving access permission to a program

Using alerts to give access permission


ZoneAlarm Alert

New Program

Do you want to allow Internet Explorer to access the Internet?

Technical Information

Destination IP: 127.0.0.1:Port 19717
Application: IEXPLORE.EXE
Version: 5.00.2920.0000

More Information Available

This is the program's first attempt to access the Internet.

□ Remember this answer the next time I use this program.

By default, ZoneAlarm displays a program alert when a new, repeat, or changed program tries to access the Internet or local network resources. You can use the alert itself to give the program one-time or permanent access permission for the Zone the program is trying to access.

Giving one-time access

Click the **Yes** button in a New Program alert, Repeat Program alert, or Changed Program alert appears.
The next time the program wants access, you'll be alerted again.

Note One time access is granted to the existing program instance. If you shut down the program, but its underlying process continues to run, that process will continue to have access permission until it is ended.

Giving permanent access

Select the **"Remember this answer..."** check box at the bottom of the alert, then click **Yes**.
The next time the program wants access, it will be allowed.

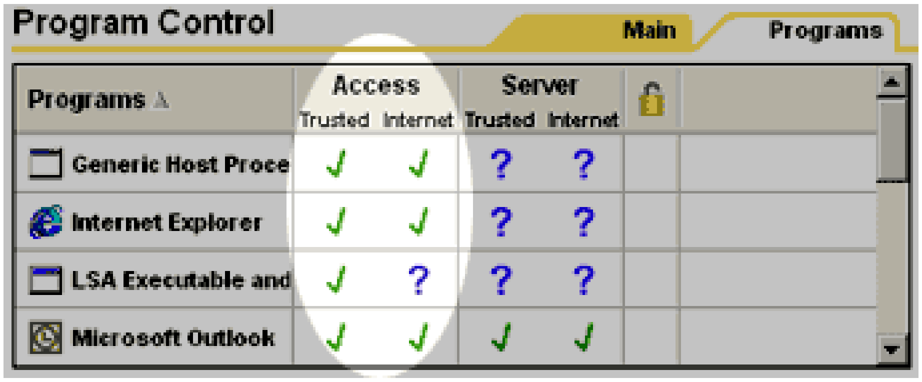
Using the Programs tab to give access permission

ZoneAlarm adds programs to the Programs list automatically when they request network or Internet access, even if you answer "No" to the resulting Program alert.

To give permanent access permission to a program in the Programs List:

1. Go to the Programs tab in the Program Control panel

2. Click the permission symbol you want to change, then select **Allow** from the shortcut menu.



Program Control

Programs	Access		Server		🔓
	Trusted	Internet	Trusted	Internet	
Generic Host Proce	✓	✓	?	?	
Internet Explorer	✓	✓	?	?	
LSA Executable and	✓	?	?	?	
Microsoft Outlook	✓	✓	✓	✓	

Tip If the program you want to give permission to is not yet in the Programs list, click the **Add** button, then use the Windows interface to browse to the program location.

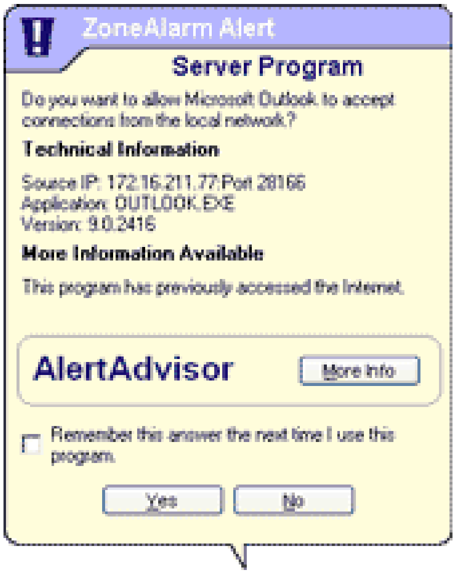
✓ = **Allow** access.

? = **Ask** for access permission by displaying a Repeat Program alert.

✗ = **Block** access for this program.

Giving server permission to a program

Using alerts to give server permission



Server Program

Do you want to allow Microsoft Outlook to accept connections from the local network?

Technical Information

Source IP: 172.16.211.77:Port 28166
Application: OUTLOOK.EXE
Version: 9.0.2416

More Information Available

This program has previously accessed the Internet.

□ Remember this answer the next time I use this program.

By default, ZoneAlarm displays a Server Program alert when a program wants to act as a server to machines in either the Internet or Trusted Zone. You can use the alert itself to give the program one-time or permanent server permission for the Zone the program is trying to access.

Giving one-time permission

To give one-time server permission, click the **Yes** button. The next time the program wants to accept incoming connections, you'll be alerted again.

Note One time server permission is granted to the existing program instance. If you shut down the program, but its underlying process continues to run, that process will continue to have server permission until it is ended.

Giving permanent permission

To give permanent server permission, select the the **Remember this answer...** check box at the bottom of the alert, then click **Yes**. The next time the program wants to act as a server, it will be allowed.

Tip Use the Programs tab to revoke server permission.

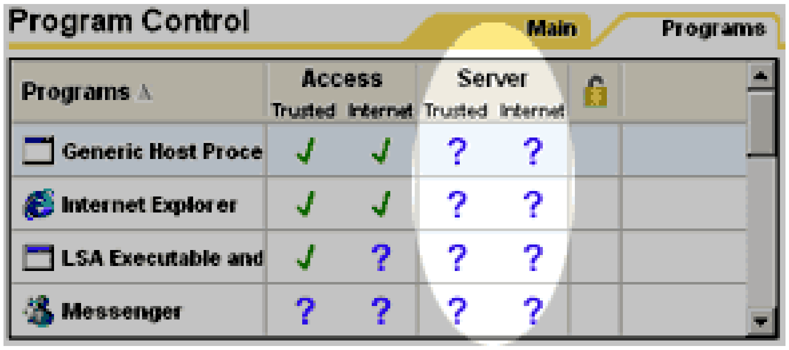
Using the Programs tab to give server permission

ZoneAlarm adds programs to the Programs list automatically when they request network or Internet access or server rights, even if you answer "No" to the resulting alert.

To give server permission to a program in the Programs List:

1. Go to the Programs tab in the Program Control panel

2. Click the permission symbol you want to change, then select **Allow** from the shortcut menu.



Program Control

Programs	Access		Server		
	Trusted	Internet	Trusted	Internet	
Generic Host Proce	✓	✓	?	?	
Internet Explorer	✓	✓	?	?	
LSA Executable and	✓	?	?	?	
Messenger	?	?	?	?	

Tip If the program you want to give permission to is not yet in the Programs list, click the **Add** button, then use the Windows interface to browse to the program location.

✓ = **Allow** the program to act as a server.

? = **Ask** for server permission by displaying a Server Program alert.

✗ = **Block** server permission for this program.

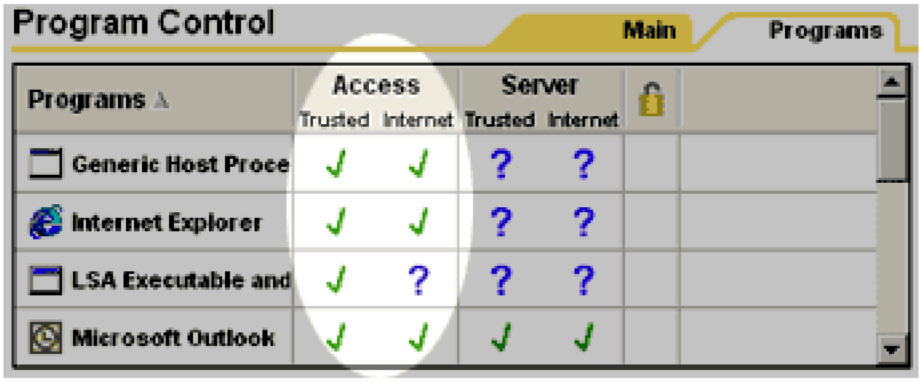
Changing program permission

Changing access permission

To change access permission for program in the Programs List:

1. Go to the Programs tab in the Program Control panel

2. Click the permission symbol you want to change, then select the option you want from the shortcut menu.



Programs	Access Trusted	Access Internet	Server Trusted	Server Internet
Generic Host Proce	✓	✓	?	?
Internet Explorer	✓	✓	?	?
LSA Executable and	✓	?	?	?
Microsoft Outlook	✓	✓	✓	✓

Access permission symbols

✓ = **Allow** access.

? = **Ask** for access permission by displaying a program alert.

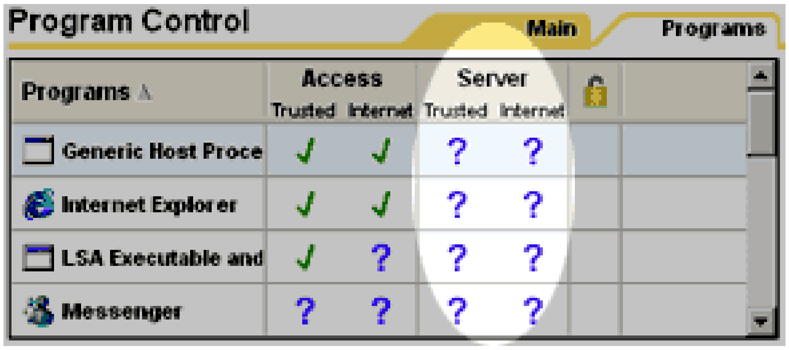
✗ = **Block** access.

Changing server permission

To server permission for a program in the Programs List:

1. Go to the Programs tab in the Program Control panel

2. Click the permission symbol you want to change, then select the option you want from the shortcut menu



Programs	Access Trusted	Access Internet	Server Trusted	Server Internet
Generic Host Proce	✓	✓	?	?
Internet Explorer	✓	✓	?	?
LSA Executable and	✓	?	?	?
Messenger	?	?	?	?

Server permission symbols

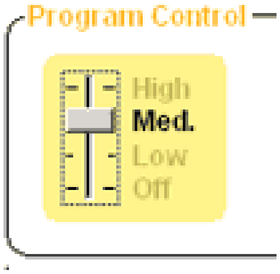
✓	= **Allow** program to act as a server.
?	= **Ask** for server permission by displaying a Server Program alert.
✗	= **Block** server permission.

Giving pass-lock permission to a program

To give pass-lock permission to a program:

1. In the Program Control panel, open the Programs tab.
2. Locate the program you want to give pass-lock permission to, and click in the lock column 🔒.
3. Select pass-lock from the shortcut menu.

ZoneAlarm Setting the Program Control level



To set the program control level:

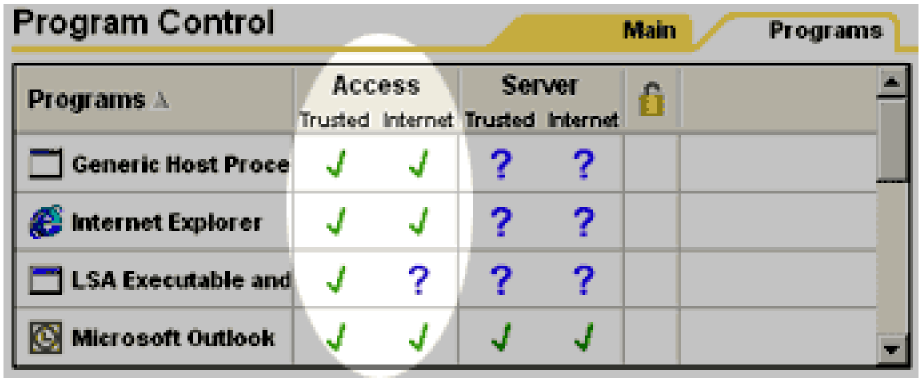
In the Main tab of the Program Control panel, move the slider to High, Medium, or Low.

ZoneAlarm Blocking program access permission / server permission

Blocking access permission for a program

To prevent a program on your computer from accessing resources in the Internet Zone or Trusted Zone:

1. Go to the Programs tab of the Program Control panel.
2. Locate the program to which you want to deny access.
3. Click the Allow ✓ or Ask ? permission symbol in the Access column for the Zone you want to deny program access to.
4. Choose Block ✗ from the shortcut menu.



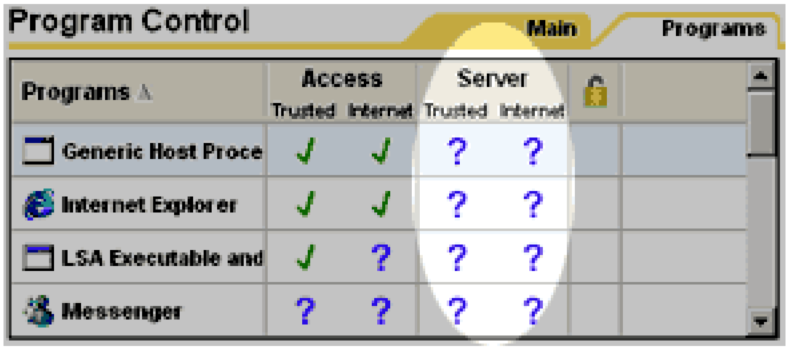
Programs	Access		Server		🔓
	Trusted	Internet	Trusted	Internet	
Generic Host Proce	✓	✓	?	?	
Internet Explorer	✓	✓	?	?	
LSA Executable and	✓	?	?	?	
Microsoft Outlook	✓	✓	✓	✓	

If the program is not displayed in the Programs list, click the **Add** button to locate it and add it to the list.

Blocking server permission for a program

To prevent a program on your computer from accessing resources in the Internet Zone or Trusted Zone:

1. Go to the Programs tab of the Program Control panel.
2. Locate the program to which you want to deny server rights.
3. Click the Allow ✓ or Ask ? permission symbol in the Server column for the Zone you want to deny server rights to.
4. Choose Block ✗ from the shortcut menu.

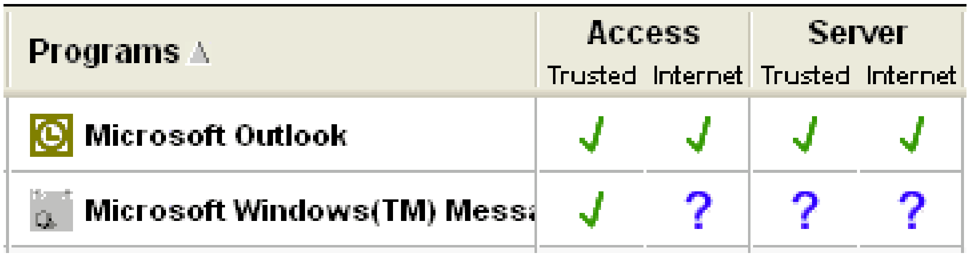


Programs	Access		Server	
	Trusted	Internet	Trusted	Internet
Generic Host Proce	✓	✓	?	?
Internet Explorer	✓	✓	?	?
LSA Executable and	✓	?	?	?
Messenger	?	?	?	?

If the program is not displayed in the Programs list, click the **Add** button to locate it and add it to the list.

Adding programs to the program list

Adding programs automatically



Programs ▲	Access		Server	
	Trusted	Internet	Trusted	Internet
Microsoft Outlook	✓	✓	✓	✓
Microsoft Windows(TM) Mess	✓	?	?	?

ZoneAlarm automatically adds a program to the list in the Programs tab the first time it requests network access. Access permission and server permission are set according to the response you gave to the initial New Program alert or Server Program alert.

To add a program such as your browser to the list, use the program to access the Internet. A New Program alert will appear.

Adding programs manually

To add a program to the list:

1. Go to the Programs tab in the Program Control panel.
2. Click the **Add** button.
3. Select the program you want to add, and click **Open**.

Tip ZoneAlarm automatically sets the access permission and server permission for the program to Ask (?). To change a permission, click the ? symbol and select **Allow** or **Block** from the shortcut menu.

ZoneAlarm Deleting programs from the program list

To prevent a program on your computer from accessing resources in the Internet Zone or Trusted Zone:

1. Go to the Programs tab of the Program Control panel.
2. Select the program you want to remove by right-clicking it.
3. Choose **Remove** from the shortcut menu.

Note Removing a program from the ZoneAlarm programs list does not remove the program from your computer, or deny it Internet access permission or server rights. If you remove a program, it will generate a New Program alert the next time it tries to access the Internet, or a Server Program alert the next time it tries to act as a server. To learn how to remove a program from your computer, see Microsoft Windows help.

ZoneAlarm Investigating changed programs

When you receive a Changed Program alert, you may want to investigate to see if there is a known hacker exploit or other problem associated with the program that caused the alert.

Investigating changed programs

Use virus scanning/Trojan scanning software and technical support resources to determine if a changed program is dangerous or not.

Tip In order to investigate the program, you will need the file name, version number, and location of the file on your computer. You can get this information from the Changed Program alert box.

Follow these steps to investigate the program:

1. Make sure your virus scanner/Trojan scanner is up to date
2. Scan the program file.
3. If your scanner does not indicate a virus or other problem, contact the technical support staff of the manufacturer of the changed program. They may be able to give a reason why the program changed, such as an automatic update.

ZoneAlarm Networking with ZoneAlarm

File and printer sharing

Place your home or local network in the Trusted Zone to allow secure sharing of resources over a local network. How?

ZoneAlarm Making your computer visible on your local network

If you can't see the other computers on your local network, or they can't see you, it is possible that ZoneAlarm is blocking the NetBIOS traffic necessary for Windows network visibility.

To make your computer visible to the others on your 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. How?
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.

Note: ZoneAlarm automatically detects your network adapter subnet and places it in the Internet Zone. We recommend that you leave the adapter subnet in the Internet Zone, and add to your Trusted Zone any specific networks you want to trust. If you place your adapter subnet in the Trusted Zone, you are in effect trusting every network you connect to.

Related Topics

Adding to the Trusted Zone

ZoneAlarm Sharing files and printers across a local network

ZoneAlarm enables you to quickly and easily secure your computer so that the trusted machines you're networked with can access your shared resources, but Internet intruders can't use your shares to compromise your system.

To configure ZoneAlarm 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. How?
2. Set the Trusted Zone security level to medium. How? This allows trusted computers to access your shared files.
3. Set Internet Zone security level to high. How? This makes your computer invisible to non-trusted machines.

Note: ZoneAlarm automatically detects your network adapter subnet and places it in the Internet Zone. We recommend that you leave the adapter subnet in the Internet Zone, and add to your Trusted Zone any specific networks you want to trust. If you place your adapter subnet in the Trusted Zone, you are in effect trusting every network you connect to.

Related Topics

Adding to the Trusted Zone

ZoneAlarm Connecting to mail servers on a network

ZoneAlarm is configured to work with Internet-based mail servers using POP3 and IMAP4 protocols, when you give your e-mail client privileges 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 features to work.

To configure ZoneAlarm for mail servers with collaboration and synchronization features:

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

Connecting through a proxy server

To enable your computer to connect to the Internet through a proxy server, add the proxy to your Trusted Zone. How?

ZoneAlarm ISP heartbeat

Most ISPs periodically send "heartbeat" messages to their connected dial-up customers to make sure they are still there. If it appears a customer is not there, the ISP might disconnect her so that her IP address can be given to someone else.

By default, ZoneAlarm blocks the protocols most commonly used for these heartbeat messages, which may cause you to be disconnected from the Internet.

If this happens you can solve the problem in either of the two ways described below.

Identify the server sending the message and add it to your Trusted Zone.

This is the preferred solution, because it will work whether your ISP uses NetBIOS or ICMP to check your connection, and it allows you to maintain high security for the Internet Zone. To identify the server your ISP uses to check your connection, follow these steps:

1. Wait until your ISP disconnects you.
2. Go to the Alert Log tab (Alerts & Logs panel).
3. In the alerts list, find the alert that corresponds to the time you were disconnected.

If you're not able to identify the server this way, contact your ISP. They should be able to tell you what servers your need to allow.

After you have identified the server, add it to the Trusted Zone. How?

Set the security level for the Internet Zone to medium.

The quickest but least secure solution is to reduce the security level for the Internet Zone to medium. How?

To learn more about the medium security setting and how it protects you, see the related topic, *Security levels.*

Related Topics

Security levels

Setting Internet Zone security to medium

ZoneAlarm DHCP

If you are using dial-up or a broadband connection with a non-static IP address, your ISP may use DHCP to allocate and periodically renew your IP address. To configure ZoneAlarm to allow DHCP renewal, do the following:

1. Add your ISP's DHCP servers to the Trusted Zone, or (if the DHCP server is in a different subnet from your computer) add your gateway to the Trusted Zone.(If you get your DHCP from your own local network (e.g. from a Linksys router), make sure the DHCP source is included in the Trusted Zone. If you you have added your local network to the Trusted Zone, this is already done).

   Tip If your ISP uses multiple DHCP servers, it may be easiest to add them to the Trusted Zone by host name rather than by IP address.

2. Make sure the security level for the Trusted Zone is medium.

Tip If necessary, you can also configure ZoneAlarm to allow DNS and DHCP traffic at high security. Use the Security tab to do this.

To learn how to set the security level, add elements to the Trusted Zone, and allow protocols, see Related Topics.

If you are still having connection problems after following the steps above, contact your ISP's customer support staff.

Related Topics

Setting the Trusted Zone security level
Adding to the Trusted Zone
Security tab

ZoneAlarm Internet Connection Sharing (ICS)

ZoneAlarm does not support configuration for Windows' Internet Connection Sharing (ICS) option.

If you are using ICS or a third-party connection sharing program, upgrade to ZoneAlarm Pro to protect all of the computers that share the connection from inbound threats.

ZoneAlarm Troubleshooting Internet connection

What sort of trouble are you having?

- I have ZoneAlarm Pro installed, and I can't connect to the Internet.
- I can connect, but am disconnected after a short time
- I have uninstalled ZoneAlarm Pro, and I still can't connect to the Internet.

ZoneAlarm Troubleshooting your Internet connection

If you're having trouble connecting to the Internet or viewing Web pages after installing ZoneAlarm, try these troubleshooting steps.

1. Determine whether the problem involves ZoneAlarm. How?
2. Make sure your browser has access permission and server permission. How?
3. Make sure ZoneAlarm isn't blocking all servers. How?
4. Make sure ZoneAlarm isn't blocking your ISP's servers. How?
5. If you're connecting through a proxy server, add the proxy server to the Trusted Zone. How?
6. If you still cannot connect after doing all of the above, click here.

ZoneAlarm Determining if your connection problem involves ZoneAlarm

If you are having Internet connection trouble after installing ZoneAlarm, the first troubleshooting step is to determine whether ZoneAlarm is really the cause. Follow these steps:

1. Go to the Preferences tab in the Overview panel.
2. Under General, clear the check box labeled **Load ZoneAlarm at startup.** A warning dialog labeled Zone Labs TrueVector Service opens.
3. Click the **Yes** button in the Zone Labs TrueVector Service dialog.
4. Restart your computer, then try to connect to the Internet.

If you are still not able to connect to the Internet after restarting your computer, the problem does not lie with your ZoneAlarm settings.

If you are able to connect to the Internet, and remain connected, after following the steps above, the problem may lie with your ZoneAlarm browser settings. The next step is to make sure your browser has access permission. How?

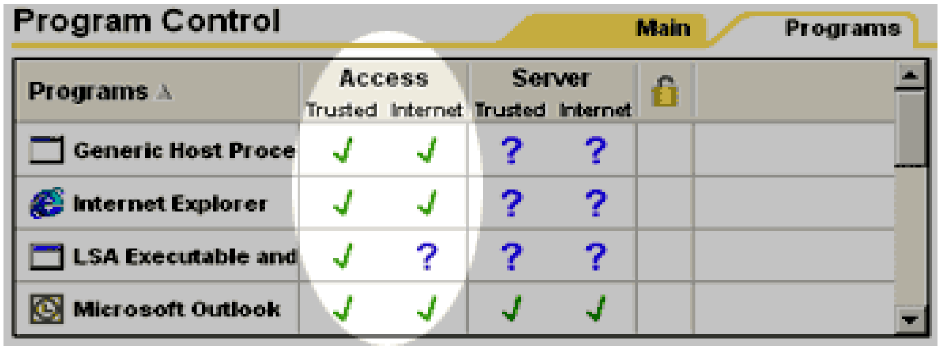
If you are unable to follow the steps above (for example, if you can't clear the Load ZoneAlarm at startup box), contact Zone Labs technical support.

Making sure your browser has access permission

In order for your browser to retrieve Web pages, it must have access permission for both Zones.

To see whether your browser has access permission:

1. Go to the Programs tab in the Program Control panel.
2. Under Access, make sure green check marks appear in the row for the browser in both the Internet Zone column and the Trusted Zone column.
3. If the browser doesn't have permission, click the symbols in the Access column, then select **Allow** from the shortcut menu.



Program Control

Programs	Access		Server		🔓
	Trusted	Internet	Trusted	Internet	
Generic Host Proce	✓	✓	?	?	
Internet Explorer	✓	✓	?	?	
LSA Executable and	✓	?	?	?	
Microsoft Outlook	✓	✓	✓	✓	

If your browser has access permission, but you still cannot view Web pages, the next step is to make sure ZoneAlarm is not blocking all servers. How?

ZoneAlarm Making sure ZoneAlarm isn't blocking all servers

ZoneAlarm has a global setting that will block all Internet or local servers, regardless of program permissions. Make sure this setting isn't causing the problem by following these steps:

1. Go to the Main tab of the Firewall panel.
2. Click the **Advanced** button. This opens the Advanced Settings dialog box.
3. In the dialog box, locate the General section.
4. Confirm that **Block Trusted Zone servers** and **Block Internet Zone servers** are not checked.

After completing all the steps above, try connecting to the Internet again. If you can't, the next step is to make sure ZoneAlarm isn't blocking your ISP's servers. How?

ZoneAlarm Making sure ZoneAlarm isn't blocking your ISP's servers

You may need to configure ZoneAlarm to allow DNS, DHCP, or other servers at your ISP that are needed to establish or maintain your Internet connection. Follow the steps below to find out.

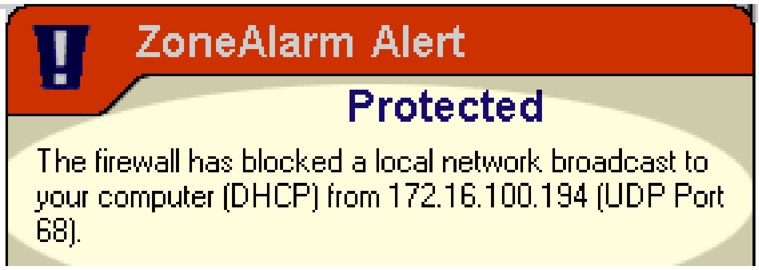
1. Enable alerts.

Make sure ZoneAlarm will show you all relevant alerts. To do this:

1. Go to the Main tab of the Alerts & Logs panel.
2. Click **On** under Internet Zone Security.

2. Use the alerts to find out what IP addresses and applications ZoneAlarm is blocking.

Try to access the Internet. If any **firewall alerts** appear:



ZoneAlarm Alert

Protected

The firewall has blocked a local network broadcast to your computer (DHCP) from 172.16.100.194 (UDP Port 68).

1. Note the IP addresses displayed near the top of the alert box. If any applications are mentioned in the alert (for example"svchost.exe" or "services.exe"), note those file names as well.

2. Call your ISP to confirm that these IP addresses belong to their server; and that the applications mentioned are used by your ISP to establish your Internet connection.

Note Your ISP's site may resolve to one of several IP addresses, depending on when you connect. In this case, your ISP can provide you with a range, rather than a single IP address.

3. If the blocked IP addresses belong to your ISP, add them to your Trusted Zone. How?

4. Make sure any programs that were mentioned in the alert (for

example"svchost.exe" or "services.exe") have server permission for the Trusted Zone. How?

If you have checked the settings described above, and you still can't connect to the Internet, please contact Zone Labs technical support.

ZoneAlarm Troubleshooting connection problems after uninstall

If you have uninstalled ZoneAlarm and are still experiencing connection problems, it is possible that the TrueVector engine is in a locked-down state because:

- Someone unauthorized tried to shut down your firewall, or
- An event occurred on your computer that made ZoneAlarm believe someone unauthorized tried to shut down your firewall.

In a locked-down state, ZoneAlarm protects you from data theft or malicious activity by locking down Internet access so no one can access your computer.

To solve this problem and restore your Internet connection, try the following steps.

Step 1: Reinstall and then uninstall ZoneAlarm

Note When installing or uninstalling ZoneAlarm on Windows NT/2000/XP systems, always use an account with administrator rights. This can be and administrator account, or a user account that is in the administrator group. For more information, see Windows help.

1. Reinstall ZoneAlarm by running the installer you downloaded from the Zone Labs Web site.
2. In the ZoneAlarm Control Center, go to the Preferences tab of the Overview panel.
3. Clear the check box labeled **Load ZoneAlarm at startup.**
4. Restart your computer. **IMPORTANT**: Make sure you are not connected to the Internet before proceeding to step 5.
5. In the Windows Start menu, go to Programs | Zone Labs.
6. Click **Uninstall ZoneAlarm.**
7. Answer **Yes** to all dialogs during the uninstallation process.

If you are still unable to connect after following the steps above, manually unininstall ZoneAlarm Pro. How?

ZoneAlarm Troubleshooting your Internet connection: Locked-down state

If you're having trouble connecting to the Internet or viewing Web pages even though you have tried all the troubleshooting steps, it is possible that ZoneAlarm is in a locked-down state. To resolve this problem, try the following additional steps:

Step 1: Uninstall then reinstall ZoneAlarm

Note When installing or uninstalling ZoneAlarm on Windows NT/2000/XP systems, always use an account with administrator rights. This can be and administrator account, or a user account that is in the administrator group. For more information, see Windows help.

1. In the ZoneAlarm Control Center, go to the Preferences tab of the Overview panel.
2. Clear the check box labeled **Load ZoneAlarm at startup.**
3. Restart your computer.
4. Check your Internet connection. If you can connect, start ZoneAlarm, return to the Preferences tab, check **Load ZoneAlarm at startup**, then click here to continue troubleshooting.
   If you can't connect, continue with step 5 below.
5. In the Windows Start menu, go to Programs | Zone Labs.
6. Click **Uninstall ZoneAlarm.**
7. Answer **Yes** to all dialogs during the uninstallation process.
8. Check your Internet connection.

- If you can connect, reinstall ZoneAlarm by running the installer you downloaded from the Zone Labs Web site.
- If you cannot connect, perform a manual uninstallation of ZoneAlarm. How?

ZoneAlarm Troubleshooting your local network

What sort of trouble are you having?

- I can't see the other computers in my Network Neighborhood, or they can't see me.
- I can't share files or printers over my home or local network.
- My machine is an Internet Connection Sharing (ICS) client, and can't connect.
- My computer uses a proxy server to connect to the Internet, and can't connect.

ZoneAlarm Troubleshooting your programs

What type of program are you having trouble with?

- Anti-Virus
- Browser
- Chat/Instant messaging
- E-mail
- FTP
- Games
- Internet Call Waiting
- File sharing
- Remote control/display
- Streaming audio/video
- Voice over Internet
- Web conferencing/Web cam

Shutting down ZoneAlarm

To shut down ZoneAlarm:

1. Right-click the system tray icon ZA.
2. Choose **Shutdown ZoneAlarm** from the shortcut menu.

ZoneAlarm Uninstalling ZoneAlarm

Basic uninstall

To uninistall ZoneAlarm:

1. In the ZoneAlarm Control Center, go to the Preferences tab of the Overview panel.
2. Clear the check box labeled **Load ZoneAlarm at startup.**
3. Restart your computer.
4. In the Windows start menu, go to Start | Programs | Zone Labs.
5. Click **Uninstall ZoneAlarm.**
6. During the uninstallation process, you will see a dialog box titled **This is a security check from the Zone Labs security engine.** Click **Yes** in this dialog box.

Manually uninstalling ZoneAlarm

If you are having persistent connection problems even after running the ZoneAlarm uninstaller, manually uninstall ZoneAlarm by following the steps below. Note that the steps differ depending on your operating system.

Windows 98/2K/XP

To manually uninstall ZoneAlarm from a Windows , 98, 2000, or XP system, follow the steps below.

Step 1: Start your computer in Safe Mode.

Enter Safe Mode with administrative account without networking. To learn how to start in Safe Mode refer to Windows help. Go to Start | Help, click the Search tab, then type 'Safe Mode' in the search box and click List Topics.

Important Do not start ZA/ZAP, or run the uninstaller, while in Safe Mode.

Step 2: Remove VSDATA registry entry (Windows 98/ME only--not required for NT/2K/XP)

Important Deleting registry entries incorrectly may require reinstalling your operating system. Always make a backup copy of the registry before editing. Perform the steps below with extreme care, or seek help from someone familiar with registry editing. For further information about registry editing, see Windows help.

1. In the Windows Start menu, click **Run...**
2. In the Open box, type **regedit**.
3. In the Registry Editor window, use the left-hand navigation to locate the following key:
   W95/98/Me/XP
   HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\VxD\VSDATA95.
4. In the right pane of the window, right-click the key, then choose **Delete** from the popup menu.
5. Choose File | Exit to finish.

Note After editing the registry in safe mode, you may get a VXD error when restarting your computer. This means Windows did not allow editing of the registry in Safe Mode. If this occurs, press **Enter**. Restart your computer in normal (not Safe) mode, then repeat Step 2.

Step 3: Delete selected files

1. Using the Windows search function, locate and delete the files VSDATA95 and/or VSDATANT.
2. If you want to keep a record of previous alerts, copy the ZALog files from the Internet Logs folder to a safe location).
3. Using the Windows search function, locate and delete the Internet Logs folder.

Step 4: Cleanup

1. Empty your Recycle Bin.
2. Restart your computer.

Step 5: Complete Uninstallation

At this point, your Internet connection should function normally. To complete the manual uninstall, you will follow steps posted on the ZoneAlarm Web site.

1. Go to http://www.zonelabs.com/store/content/support/zapInstallFAQ.jsp.
2. Under **How do I unininstall, then reinstall ZoneAlarm**, click the link for your operating system.
3. Under **Uninstallation step 1**, begin with substep **A**, then follow all the remaining uninstallation steps.

Windows NT

To manually uninstall ZoneAlarm from a Windows NT system, follow the steps below.

Step 1: Log on to your computer as an administrator

- To learn how to do this, see Windows help.

Step 2: Show hidden files

1. In Windows folder options, set Windows to show hidden files. To learn how to do this, see Windows help.

Step 3: Rename vsmon.exe

1. Using the Windows search function, locate the program vsmon.exe.
2. Change the name of the file, and write down the new file name. You will need to locate this file again later.
3. Shut down ZoneAlarm and restart your computer.

Step 4: Delete selected files

1. Using the Windows search function, locate and delete the files VSDATA95 and/or VSDATANT.
2. If you want to keep a record of previous alerts, copy the ZALog files from the Internet Logs folder to a safe location.
3. Using the Windows search function, locate and delete the Internet Logs folder.

Step 5: Restore vsmon

1. Locate the renamed file from step 3 above, and rename it vsmon.exe.
2. Restart your computer.

Step 6: Cleanup

1. Empty your Recycle Bin.
2. Restart your computer.

Step 7: Complete Uninstallation

At this point, your Internet connection should function normally. To complete the manual uninstall, you will follow steps posted on the ZoneAlarm Web site.

1. Go to http://www.zonelabs.com/store/content/support/zapInstallFAQ.jsp.
2. Under **How do I unininstall, then reinstall ZoneAlarm**, click the link for your operating system.
3. Under **Uninstallation step 1**, begin with substep **A**, then follow all the remaining uninstallation steps.

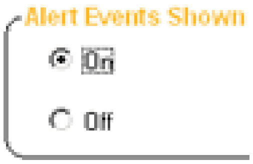
ZoneAlarm Showing and hiding firewall alerts

Hiding all informational alerts

To suppress all Firewall alerts, Internet Lock alerts, and other informational alerts:

1. Go to the Main tab in the Alerts & Logs panel.
2. Under Alert Events Shown, choose **Off**.

Setting the alert level



Alert Events Shown

● On

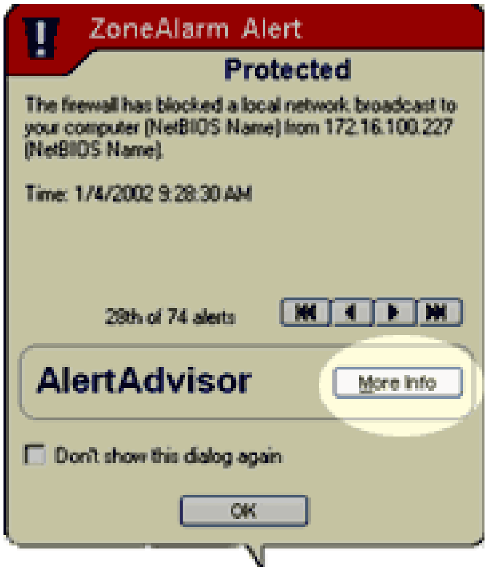
○ Off

To turn the display of informational alerts on or off:

In the Main tab of the Alerts and Logs panel, select **On** or **Off**.

ZoneAlarm Submitting alerts to AlertAdvisor

Submitting new alerts



The firewall has blocked a local network broadcast to your computer (NetBIOS Name) from 172.16.100.227 (NetBIOS Name).

Time: 1/4/2002 9:28:30 AM

28th of 74 alerts

□ Don't show this dialog again

To submit a new alert to AlertAdvisor, click the **More Info** button in the alert box.

Submitting logged alerts

To submit logged alerts to AlertAdvisor for analysis:

1. In the Alerts & Logs panel, open the Log Viewer tab.
2. Locate the alert you want to submit, and right-click it.

   Tip Sort the alerts by clicking any field header.

3. Choose More Info from the shortcut menu.

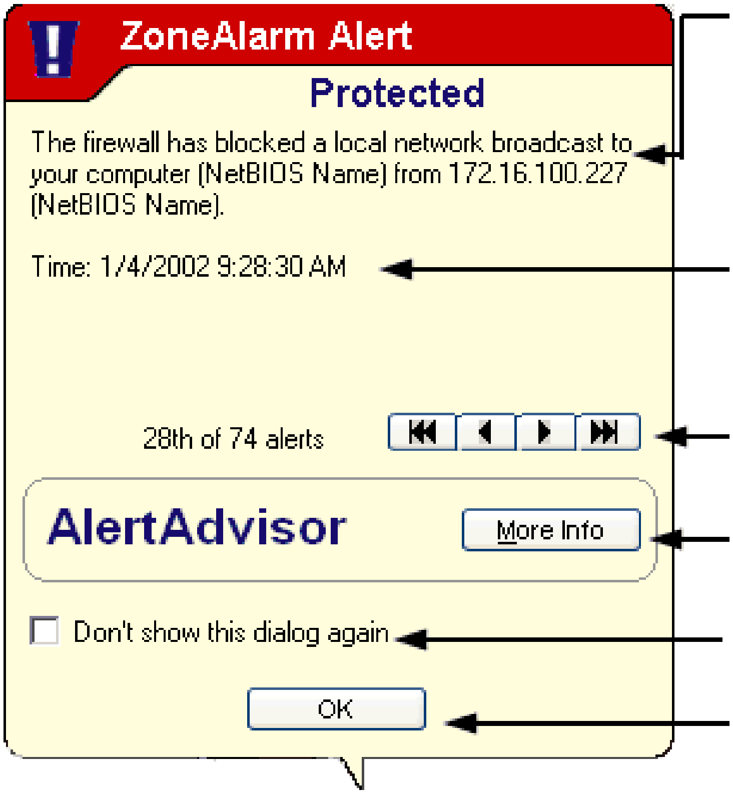
ZoneAlarm Researching a source IP address

AlertAdvisor and Who Is can help you determine the physical location and other information about the source IP address or destination IP address in an alert. Follow these steps:

1. Submit an alert to AlertAdvisor. How?
2. In AlertAdvisor, open the **Who Is** tab. This tab will display available information about the IP address that was submitted.

ZoneAlarm® Alert details

Firewall alerts



ZoneAlarm Alert

Protected

The firewall has blocked a local network broadcast to your computer (NetBIOS Name) from 172.16.100.227 (NetBIOS Name).

Time: 1/4/2002 9:28:30 AM

28th of 74 alerts

□ Don't show this dialog again

The top of the alert contains the IP address of the computer that sent the blocked packet, the protocol that was used, and/or the port the packet was addressed to.

The date and local time at which the alert occurred.

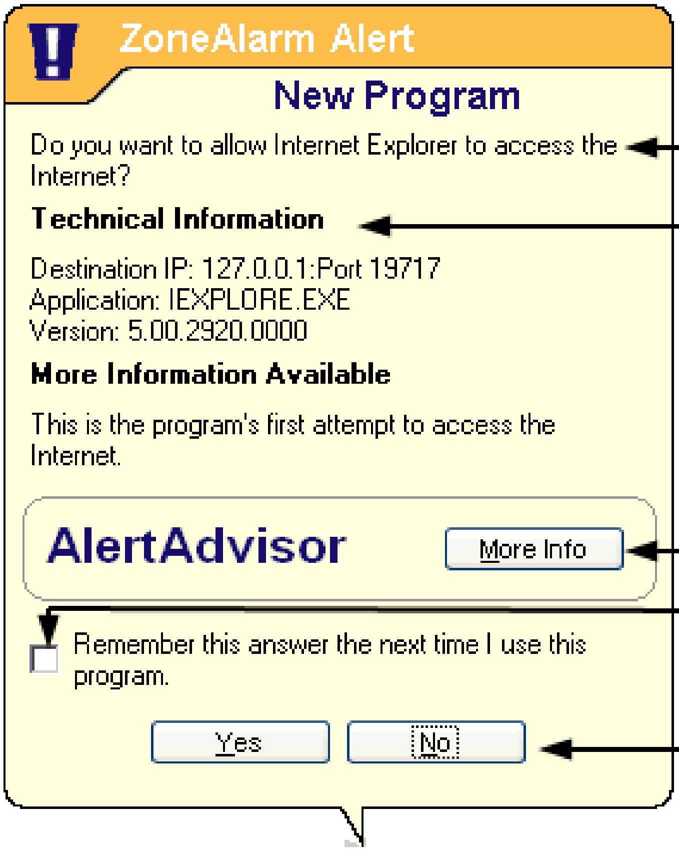
The number of alerts that have occurred since the alert bo opened. Use the arrow controls to scroll through alerts.

Click **More Info** to submit alert data to AlertAdvisor, which Web page with an analysis.

For quieter security, select this check box before clicking **OK.** Alerts are still logged, but the alert box is hidden.

Click this button to close the alert box.

Program alerts



ZoneAlarm Alert

New Program

Do you want to allow Internet Explorer to access the Internet?

Technical Information

Destination IP: 127.0.0.1:Port 19717
Application: IEXPLORE.EXE
Version: 5.00.2920.0000

More Information Available

This is the program's first attempt to access the Internet.

AlertAdvisor

☐ Remember this answer the next time I use this program.

The top of the program alert tells you the name of the program that requested access permission or server permission.

Technical information includes the file name and version number of the program that requested permission, and the IP address and port number of the computer that the program is trying to contact.

Click the **More Info** button to submit data from the alert to Zone Labs' AlertAdvisor, which displays a Web page with an analysis. AlertAdvisor can help you decide whether to answer **Yes** or **No** to a program alert.

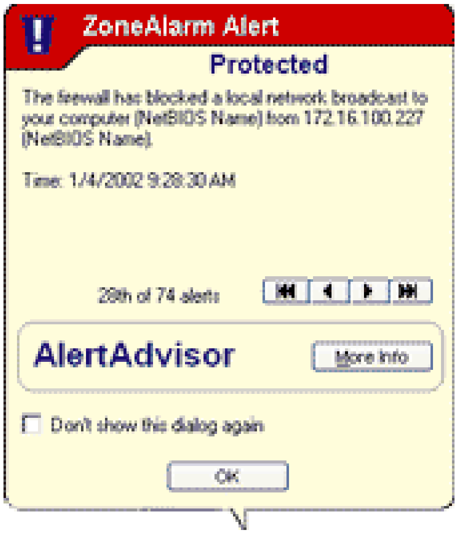
Select this check box before clicking **Yes** or **No** to avoid seeing an alert about the same program again. The next time the program asks for permission, your answer is applied silently.

Click **Yes** to grant access permission/server permission to the program. Click **No** to deny permission.

ZoneAlarm alerts

With the exception of the New Network alert, ZoneAlarm alerts fall into two basic categories: informational and program.

Informational alerts



ZoneAlarm Alert

Protected

The firewall has blocked a local network broadcast to your computer (NetBIOS Name) from 172.16.100.227 (NetBIOS Name).

Time: 1/4/2002 9:28:30 AM

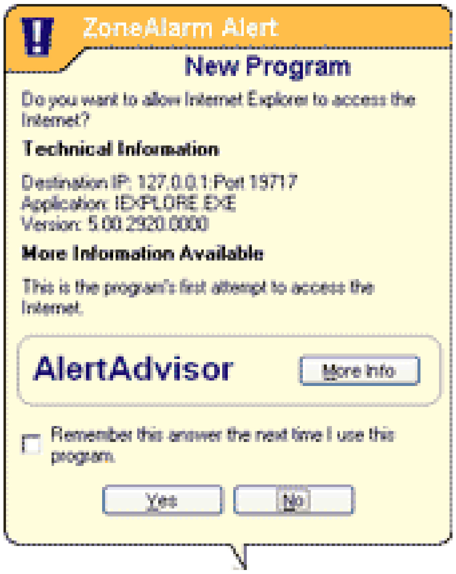
28th of 74 alerts

Informational alerts tell you that ZoneAlarm has blocked a communication that didn't fit your security settings.

They don't require a decision from you. By clicking the **OK** button at the bottom of the alert pop-up, you close the alert box, but you don't allow anything into or out of your computer.

The most common type of informational alert is the Firewall alert.

Program alerts



ZoneAlarm Alert

New Program

Do you want to allow Internet Explorer to access the Internet?

Technical Information

Destination IP: 127.0.0.1:Port 19717
Application: IEXPLORE.EXE
Version: 5.00.2920.0000

More Information Available

This is the program's first attempt to access the Internet.

Program alerts ask you if you want to allow a program to access the Internet or local network, or to act as a server. They offer you a **Yes** or **No** choice.

By clicking the **Yes** button, you are granting permission to the program. By clicking the **No** button, you deny permission to the program.

The most common type of Program alert is the New Pr

Alert types

Firewall Alerts

Firewall alerts inform you that the ZoneAlarm firewall has blocked traffic based on port and protocol restrictions. More info

Program Alerts

There are several types of Program alert:

- **New Program** alerts occur when a program requests access permission for the first time. You can answer Yes or No. More info
- **Repeat Program** alerts occur when the program requests access permission again. You can answer Yes or No. More info
- **Server Program** alerts occur when a program requests server permission. You can answer Yes or No. More info
- **Changed Program** alerts occur when a program that is requesting access permission or server permission has changed since its last request. More info
- **Blocked Program** alerts occur when a program requests access or server permission, and you have already configured ZoneAlarm to block it. More info

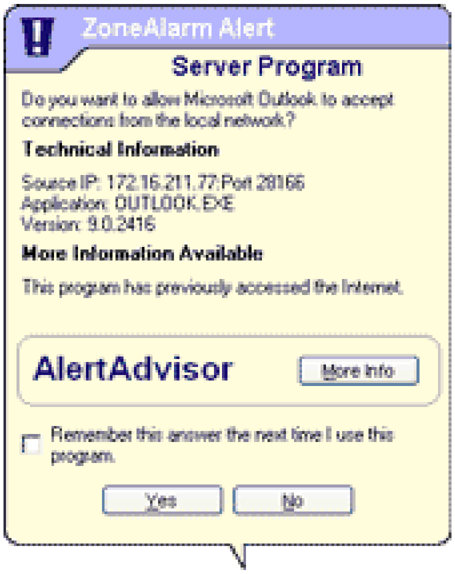
Internet Lock alerts

Internet Lock alerts occur when ZoneAlarm blocks traffic because the Internet Lock is engaged. More info

Related Topics

Responding to alerts

ZoneAlarm® Server Program alert



Server Program

Do you want to allow Microsoft Outlook to accept connections from the local network?

Technical Information

Source IP: 172.16.211.77:Port 28166
Application: OUTLOOK.EXE
Version: 9.0.2416

More Information Available

This program has previously accessed the Internet.

□ Remember this answer the next time I use this program.

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

For detailed information about the contents of the alert box, see the related topic *Alert details.*

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

What you should do

Click **Yes** or **No** in the alert pop-up after following these steps:

1. Did you just launch a program or process that would reasonably require permission? If so, it's probably safe to click Yes. If not, continue with step 2.

2. Do you recognize the name of the program in the Alert pop-up, and if so, does it make sense for the program to need permission? If so, it's probably safe to click Yes. If not, or if you're not sure, continue with step 3.
3. Click the More Info button in the alert box. This submits your alert information (for example, the name of the program and the address it was trying to reach) to AlertAdvisor, which then displays a Web page with information about the alert and the program. Use the AlertAdvisor information to help you decide if it's safe to answer Yes.

Caution If you are still not certain that the program is legitimate and needs server permission, it is safest to anwser **No**. If it becomes necessary, you can give the program server permission later by using the Programs tab. How?

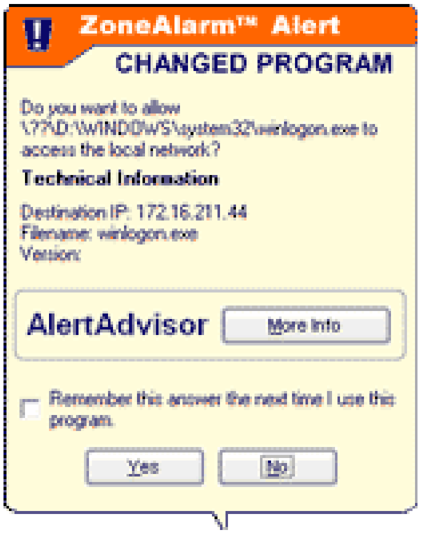
How you can see fewer of these alerts

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

Related Topics

Alert details
What's a Zone?

ZoneAlarm Changed Program alert



ZoneAlarm™ Alert

CHANGED PROGRAM

Do you want to allow \??\D:\WINDOWS\system32\winlogon.exe to access the local network?

Technical Information

Destination IP: 172.16.211.44
Filename: winlogon.exe
Version:

□ Remember this answer the next time I use this program.

Changed Program alerts warn you that a program that has asked for access permission or server permission before has changed somehow. If you click Yes, the changed program is allowed access. If you click No, the program is denied access.

For detailed information about the contents of the alert box, see the related topic *Alert details.*

Why these alerts occur

Changed Program alerts can occur if you have updated a program since the last time it access the Internet. (Some programs update themselves automatically. See the program documentation to find out.) However, they can also occur if a hacker has somehow managed to tamper with the program.

What you should do

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

1. Did you (or, if you're in a business environment, your systems administrator) recently upgrade the program that is asking for permission?
2. Does it make sense for the program to need permission?

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

Tip If you're not sure, it's safest to answer **No**. You can always grant permission later by going to the Programs tab. How?

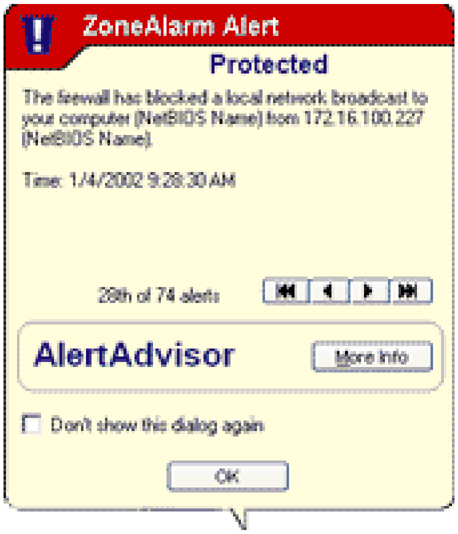
How you can see fewer of these alerts

Changed Program alerts are always displayed because they require a Yes or No response from you. To avoid a large number of Changed Program alerts, avoid unnecessary or repeated program updates.

Related Topics

Alert details

ZoneAlarm Firewall alert



The firewall has blocked a local network broadcast to your computer (NetBIOS Name) from 172.16.100.227 (NetBIOS Name).

Time: 1/4/2002 9:28:30 AM

□ Don't show this dialog again

When you see a Firewall alert, it means that ZoneAlarm has protected you by blocking traffic not allowed by your Firewall settings. By clicking **OK**, you are not letting anything into your computer—you are only saying "Yes, I've seen the alert."

For detailed information about the contents of the alert box, see the related topic *Alert details.*

Why these alerts occur

Firewall alerts occur when ZoneAlarm blocks an incoming or outgoing packet because of the port and protocol restrictions set in the Firewall panel.

Firewall alerts can be caused by harmless network traffic, for example, if your ISP is using ping to verify that you're still connected. However, they can also be caused by a hacker trying to find unprotected ports on your computer.

If the alert was probably caused by harmless network traffic, the alert has an orange band at the top. If the alert was probably caused by hacker activity, the pop-up has a red band at the top

What you should do

When you see a Firewall alert, there's nothing you have to do to ensure your security.

To dismiss the alert box, click **OK**. By doing this, you're not allowing any traffic in or out of your computer.

If you're interested in learning more about the alert, for example, the common uses of the port it was addressed to, or the likelihood that it stemmed from hacker activity, click the **More Info** button. This submits your alert information to Zone Labs' AlertAdvisor, which analyzes the information and provides the most likely explanation.

How you can see fewer of these alerts

To have ZoneAlarm enforce firewall security without alerting you, turn off the display of informational alerts. How?

If you are receiving a lot of firewall alerts, but you don't suspect you're under attack, try the following troubleshooting steps:

1. Make sure your Trusted Zone security is set to medium

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

2. Determine if the source of the alerts should be trusted

Repeated alerts may indicate that a resource you want to trust is trying repeatedly to contact you.

1. Submit repeated alerts to AlertAdvisor. How?
2. Use AlertAdvisor to determine who the source IP address that caused the alerts belongs to. How?
3. If the alerts were caused by a source you want to trust, add it to the Trusted Zone. How?

3. Determine if your Internet Service Provider is sending you "heartbeat" messages

Try the procedures suggested for managing ISP heartbeat.

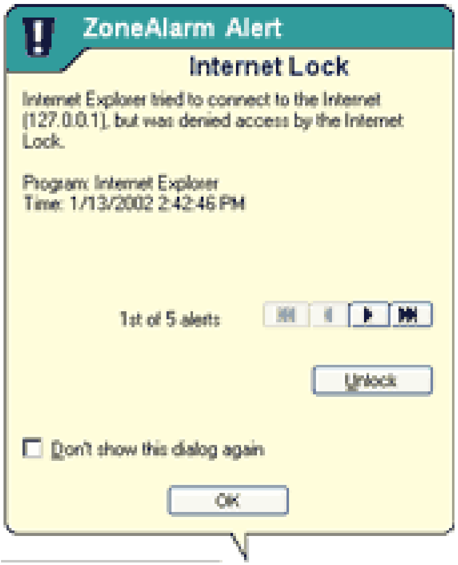
4. Set your alert display controls to medium

By default, ZoneAlarm 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. How?

Related Topics

Firewall protection

ZoneAlarm® Internet Lock alert


ZoneAlarm Alert

Internet Lock

Internet Explorer tried to connect to the Internet [127.0.0.1], but was denied access by the Internet Lock.

Program: Internet Explorer
Time: 1/13/2002 2:42:46 PM

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

For detailed information about the contents of the alert box, see the related topic *Alert details.*

Why these alerts occur

These alerts occur only when the Internet Lock is engaged.

To learn more about the Internet Lock, see the related topic *Using the Internet Lock and Stop button*.

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. How?

Tip 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. How?

How you can 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:

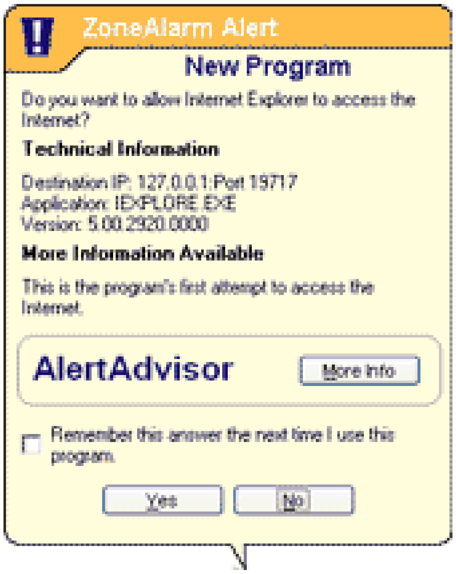
- In the Programs tab, turn the Automatic Internet Lock off.
- In the Auto-Lock tab, Increase the number of minutes of inactivity required for the Automatic Lock to engage.

For more information, see the related topics *Programs tab* and *Auto-Lock tab.*

Related Topics

Using the Internet Lock and Stop button
Programs tab
Auto-Lock tab

New Program alert



ZoneAlarm Alert

New Program

Do you want to allow Internet Explorer to access the Internet?

Technical Information

Destination IP: 127.0.0.1:Port 19717
Application: IEXPLORE.EXE
Version: 5.00.2920.0000

More Information Available

This is the program's first attempt to access the Internet.

AlertAdvisor

□ Remember this answer the next time I use this program.

New Program alerts are central to your Internet security. They ensure that no program on your computer can use your Internet connection without your permission, preventing hackers from communicating with Trojan horses or other malware they may have distributed. They enable you to set access permission for program that has not asked for Internet Zone or Trusted Zone access before. If you click Yes, the program is allowed access. If you click No, the program is denied access.

For detailed information about the contents of the alert box, see the related topic *Alert details.*

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.

There are many programs and program components that require access permission as part of their normal function. Browsers and e-mail client applications, for example, must connect to remote servers to retrieve Web pages and send or receive e-mail.

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 ZoneAlarm, 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.

What you should do

Click **Yes** or **No** in the alert pop-up after following these steps:

1. Did you just launch a program or process that would reasonably require permission? If so, it's probably safe to click Yes. If not, continue with step 2.
2. Do you recognize the name of the program in the Alert pop-up, and if so, does it make sense

for the program to need permission? If so, it's probably safe to click Yes. If not, or if you're not sure, continue with step 3.

3. Click the More Info button in the alert box. This submits your alert information (for example, the name of the program and the address it was trying to reach) to AlertAdvisor, which then displays a Web page with information about the alert and the program. Use the AlertAdvisor information to help you decide if it's safe to answer Yes.

Tip If you're really not sure what to do, it's best to answer **No**. You can always grant permission later by going to the Programs tab. How?

How you can see fewer of these alerts

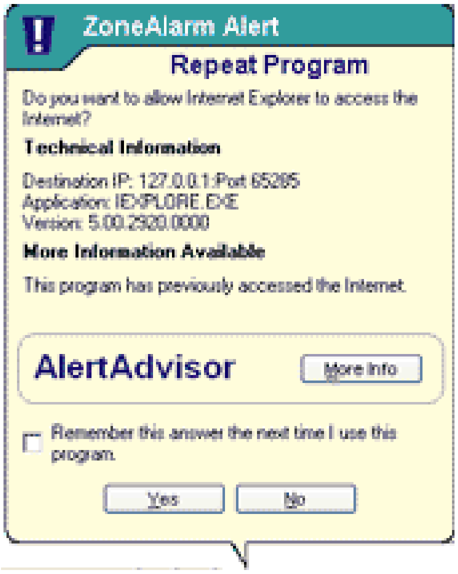
It's normal to see several New Program alerts soon after installing ZoneAlarm. As you assign permissions to each new program, the number of alerts you see will decrease.

Tip To keep from seeing Repeat Program alerts, select **Remember this answer the next time I use this program** before clicking Yes or No.

Related Topics

Alert details
What's a Zone?
Program Control

ZoneAlarm Repeat Program alert



ZoneAlarm Alert

Repeat Program

Do you want to allow Internet Explorer to access the Internet?

Technical Information

Destination IP: 127.0.0.1:Port 65285
Application: IEXPLORE.EXE
Version: 5.00.2920.0000

More Information Available

This program has previously accessed the Internet.

□ Remember this answer the next time I use this program.

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

For detailed information about the contents of the alert box, see the related topic *Alert details.*

Why these alerts occur

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.

There are many programs and program components that require access permission as part of their normal function. Browsers and e-mail client applications, for example, must connect to remote servers to retrieve Web pages and send or receive e-mail.

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 ZoneAlarm, 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.

What you should do

Click **Yes** or **No** in the alert pop-up after following these steps:

1. Did you just launch a program or process that would reasonably require permission? If so, it's probably safe to click Yes. If not, continue with step 2.
2. Do you recognize the name of the program in the Alert pop-up, and if so, does it make sense for the program to need permission? If so, it's probably safe to click Yes. If not, or if you're

not sure, continue with step 3.

3. Click the More Info button in the alert box. This submits your alert information (for example, the name of the program and the address it was trying to reach) to AlertAdvisor, which then displays a Web page with information about the alert and the program. Use the AlertAdvisor information to help you decide if it's safe to answer Yes.

Tip If you're really not sure what to do, it's best to answer **No**. You can always grant permission later by going to the Programs tab. How?

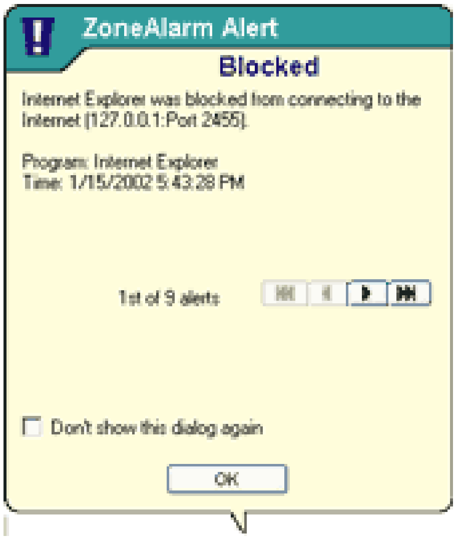
How you can see fewer of these alerts

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

Related Topics

Alert details
What's a Zone?

ZoneAlarm Blocked Program alert



Internet Explorer was blocked from connecting to the Internet [127.0.0.1:Port 2455].

Program: Internet Explorer
Time: 1/15/2002 5:43:28 PM

1st of 9 alerts

□ Don't show this dialog again

Blocked Program alerts tell you that ZoneAlarm 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.

For detailed information about the contents of the alert box, see the related topic *Alert details.*

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. Because you've already configured ZoneAlarm to block the program, the alert displays only an OK button, rather than the Yes and No options that appear in other Program alerts.

What you should do

Click OK to close the alert box. There's nothing further you have to do to ensure your security.

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?

How you can 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**.

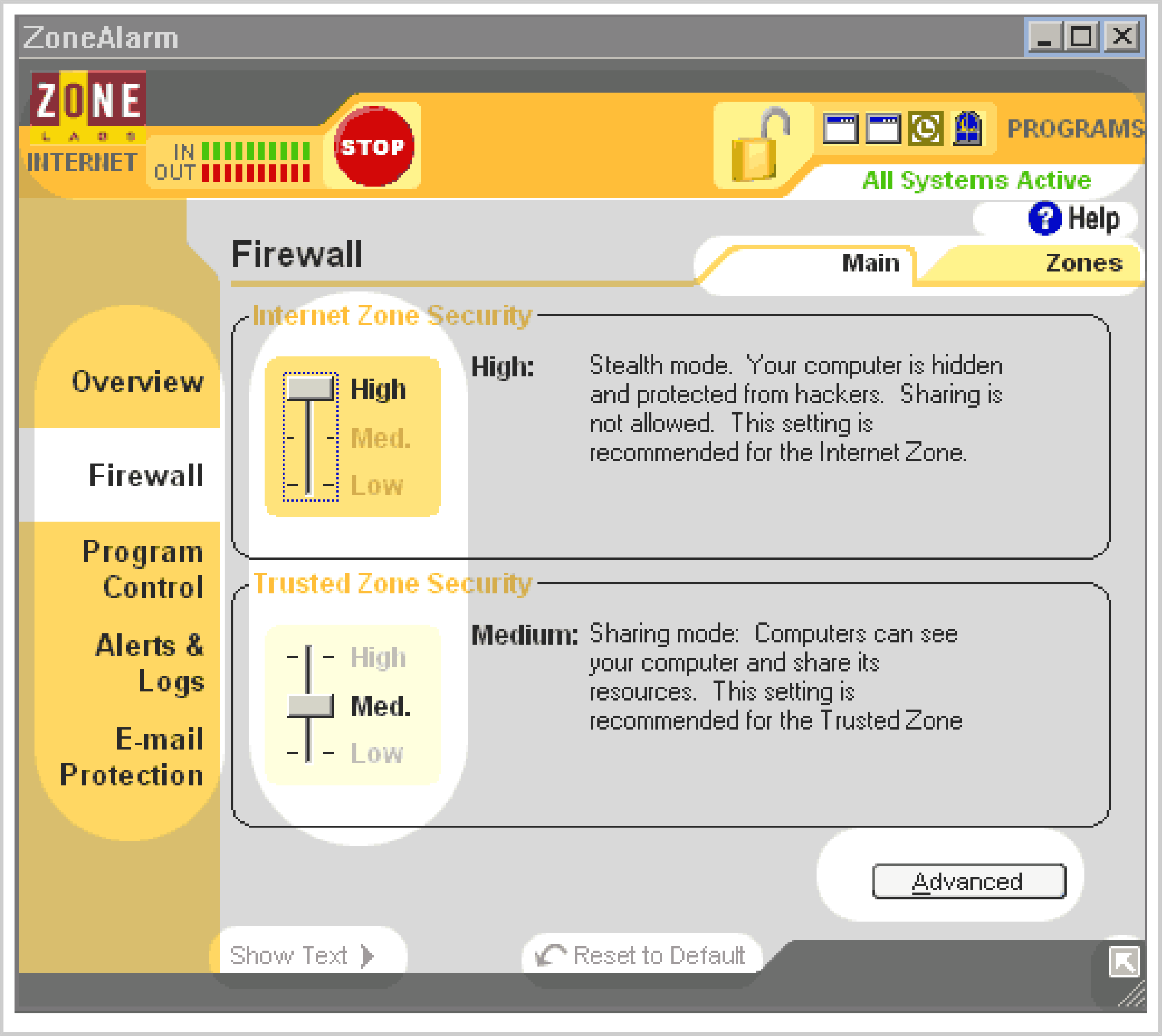
Note Turning off Blocked Program alerts does not affect your level of security.

Related Topics

Program control

ZoneAlarm Control Center

The ZoneAlarm Control Center has a simple menu and tab structure that gives you instant access to all your security features. You can use standard mouse-clicks or keyboard access.

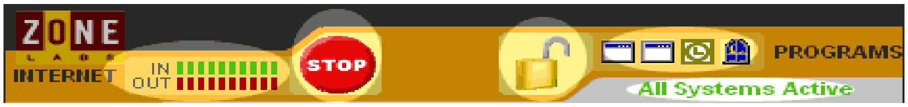


High: Stealth mode. Your computer is hidden and protected from hackers. Sharing is not allowed. This setting is recommended for the Internet Zone.

Medium: Sharing mode: Computers can see your computer and share its resources. This setting is recommended for the Trusted Zone

Click the highlighted areas to learn about specific parts of the Control Center.

Dashboard

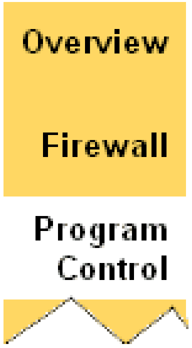


The dashboard appears at the top of every panel. It gives you constant access to basic security indicators and functions. See dashboard details.

Help button

To get help with the controls on any panel, click the Help link in the upper-right corner. ZoneAlarm's online help system goes immediately to the help topic for the tab you are looking at.

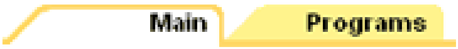
Menu bar



Use the menu on the left side of the Control Center to select the panel you want to work in. In this example, the Program Control panel is selected.

The tools in each panel are arranged in two or more tabs. Use the tab selectors to choose the tab you want to work in.

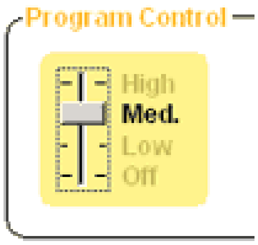
Tab selectors



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.

Global Controls



The Main tabs of most panels contain global controls for each of ZoneAlarm's security features. By adjusting the global controls, you can instantly adjust your security to meet your needs.

Tip For most users, the default settings of the global controls provide the optimum balance of security and convenience. For more information, see the related topic *Choosing security settings.*

Custom and Advanced buttons

Custom and Advanced buttons give you access to dialog boxes that contain detailed security settings. If you have an unusual computer configuration, or very specific security needs, these dialog boxes give you granular control over your firewall, application control, and other security features.

Show/Hide Text

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

Reset to Default

Click this link to set controls on the selected panel to their Zone Labs defaults.

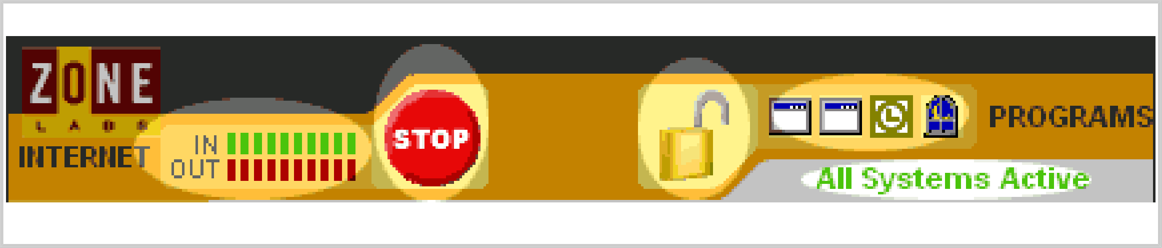
Resize

Use the resize handle to customize the size of the Control Center. Click the arrow to hide all but the dashboard.

Related Topics

Choosing security settings
Keyboard access
Dashboard

ZoneAlarm The ZoneAlarm dashboard

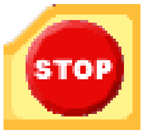


Inbound/Outbound traffic indicator

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

Note 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 (Emergency Panic Lock)

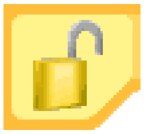


Click the **Stop** button to immediately stop all inbound and outbound traffic. Click again to disengage.

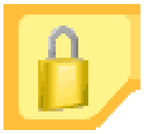
Tip Use the Stop button only in emergencies. For more information, see the related topic *Using the Internet Lock and Stop button*

Internet Lock

Click the lock icon to close the Internet lock. Click again to disengage.



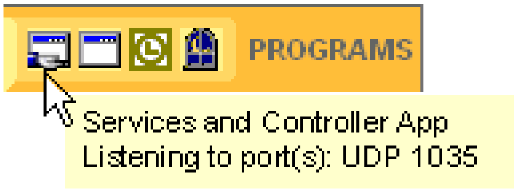
This view indicates the lock is **open**.



This view indicates the lock is **closed**.

Note Use the Internet Lock to protect your computer if you leave it connected to the Internet but inactive for long periods. For more information , see the related topic *Using the Internet Lock and Stop button*

Active programs



Services and Controller App
Listening to port(s): UDP 1035

The active programs area displays the icons of programs that are currently open and that have accessed the Internet in your current session.

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.

To see information about a program displayed here, hover your mouse pointer over the icon.

Related Topics Back to top

All systems active

This area can display two messages.

- The message **All Systems Active** indicates that ZoneAlarm is functioning normally.
- The message **Error. Please Reboot** indicates that you are not protected by ZoneAlarm because the underlying security process is not running. Restart your computer to allow ZoneAlarm to reset.

Related Topics

Using the Internet Lock and Stop button

ZoneAlarm Keyboard access

All ZoneAlarm functions are available through the keystrokes described below.

Navigation

Use these keystrokes to navigate through ZoneAlarm's panels, TABs, and dialog boxes.

Tip 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.

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).

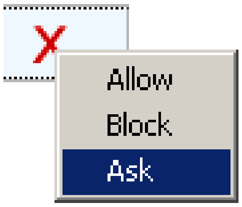
Global functions

Use the following keystrokes to activate functions from anywhere in the interface.

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+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 ZoneAlarm.

Shortcut menu items



You can use the keystrokes below to choose from the options on a shortcut menu.

Programs Tab/—Access and Server fields

Keystroke	Chooses in left-click shortcut menu
A	Allow
B	Block
K	Ask

Keystroke	Chooses in right-click shortcut menu

O	Options
R	Remove
P	Properties
A	Add Program

Programs Tab—Lock field

Keystroke	Chooses in left-click shortcut menu
N	Normal
P	Pass lock

Zones Tab

Keystroke	Chooses in left-click shortcut menu
I	Internet
T	Trusted
B	Blocked

Button shortcuts

Use the keystrokes below to click available buttons in an active window.

Product Info Tab

Keystroke	Equivalent to clicking this button
ALT+R	Change Reg

Zones Tab

Keystroke	Equivalent to clicking this button
ALT+A	Add

Overview Tab (Program Control panel)

Keystroke	Equivalent to clicking this button
ALT+W	Program Wizard

Log Viewer Tab

Keystroke	Equivalent to clicking this button
ALT+M	More Info

Log Control Tab

Keystroke	Equivalent to clicking this button
ALT+B	Browse
ALT+E	Delete Log

Dialog box commands

Use the keystrokes below when a dialog box is open.

Keystroke	Function
Tab	Activates the next control in the dialog box.
SHIFTt+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

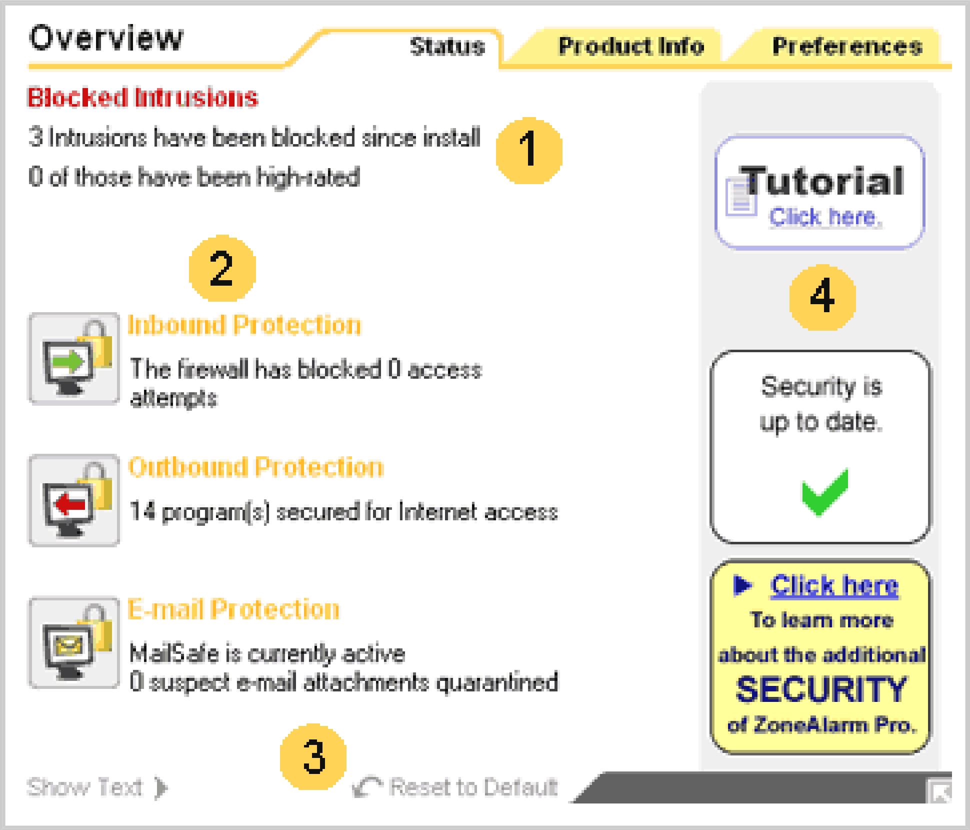
ESC	Same as clicking the Cancel button.

Hiding the ZoneAlarm Control Center

To keep the ZoneAlarm Control Center from opening automatically:

1. In the Overview panel, choose the Preferences tab.
2. Under General, clear the check box labeled **Show ZoneAlarm on top during Internet activity**.

ZoneAlarm® Status tab



Overview

Blocked Intrusions

3 Intrusions have been blocked since install

0 of those have been high-rated

Inbound Protection

The firewall has blocked 0 access attempts

Outbound Protection

14 program(s) secured for Internet access

E-mail Protection

MailSafe is currently active

0 suspect e-mail attachments quarantined

Click the numbers to learn about specific controls, or read an introduction.

Status tab

Use the Status tab to:

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

1 Blocked intrusions

Blocked Intrusions shows you how many times the ZoneAlarm firewall and MailSafe have acted to protect you , and how many of the alerts were high-rated.

2 Inbound, outbound, and e-mail protection

The protection area tells you at a glance whether your firewall, program, and e-mail security settings are safe. It also summarizes security activity of each type.

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

Inbound Protection

Use this area to see:

- If your firewall is configured safely. ZoneAlarm will warn you if firewall security is set too low.
- How many Firewall alerts have occurred since the last reset.

Outbound Protection

Use this area to see:

- If program control is configured safely. ZoneAlarm will warn you if program security is turned off.
- How many Program alerts have occured since the last reset.

E-mail Protection

Use this area to see MailSafe is ON. The text message shows you how many attachments have been quarantined since the last reset.

Tip Click the underlined text of any warning (for example, "Program control is off") to go immediately to the panel where you can change that setting.

3 Reset to Default

Clicking the **Reset to Default** link returns the event counters in the Inbound Protection, Outbound Protection, and E-mail protection areas to 0. These counters are also reset if uninstall and reinstall ZoneAlarm.

4 Update and tutorial information

Click the **Tutorial** link to learn the basics of how ZoneAlarm works.

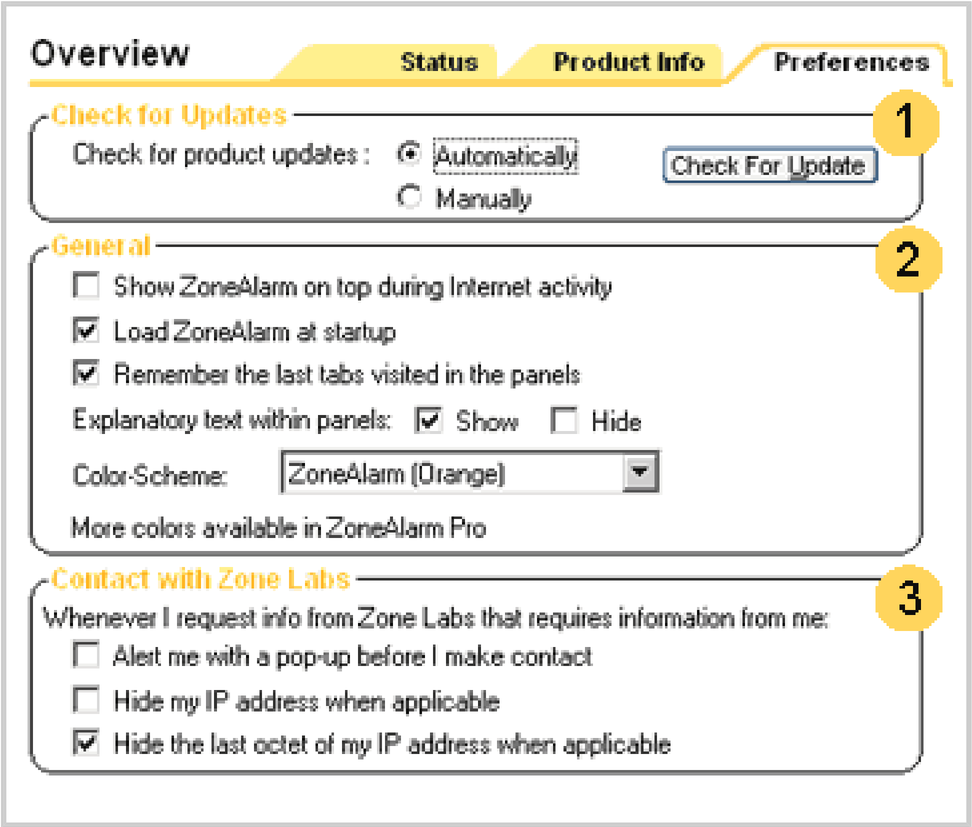
Use the **Update** box to make sure you're running the latest version of ZoneAlarm , and gives you quick access to product updates when they arrive.

To download a free trial version of ZoneAlarm Pro, click the download link.

Related Topics

Firewall protection
Getting Updates to ZoneAlarm
Program control
E-mail protection

ZoneAlarm® Preferences tab



Check for Updates

Check for product updates : ● Automatically ○ Manually

General

□ Show ZoneAlarm on top during Internet activity

☑ Load ZoneAlarm at startup

☑ Remember the last tabs visited in the panels

Explanatory text within panels: ☑ Show □ Hide

Color-Scheme: ZoneAlarm (Orange)

More colors available in ZoneAlarm Pro

Contact with Zone Labs

Whenever I request info from Zone Labs that requires information from me:

□ Alert me with a pop-up before I make contact

□ Hide my IP address when applicable

☑ Hide the last octet of my IP address when applicable

Click the numbers to learn about specific controls, or read an introduction.

Preferences tab

Use the Preferences tab to:

- Configure ZoneAlarm to automatically notify you of product updates.
- Set general options for the display of the ZoneAlarm Control Center.
- Configure privacy settings for communications with Zone Labs.

---

1 Check for updates

Select **Automatically** to have ZoneAlarm automatically notify you of available updates.

If you would rather check for upgrades yourself by looking in the Status tab of the Overview panel, select **Manually**.

2 General

Select **Show ZoneAlarm on top during Internet activity** to have the ZoneAlarm window come to the top of all other open windows whenever Internet activity occurs.

Select **Load ZoneAlarm at startup** to have ZoneAlarm start automatically whenever you turn your computer on.

Select **Remember the last tabs visited in the panels** to have ZoneAlarm start on the tab you had open the last time you closed the Control Center.

Select **Show** or **Hide** to show or hide the explanatory text that appears to the left of each ZoneAlarm tab. If you select **Hide**, you can still display the text for any panel by clicking the **Show Text** link at the bottom.

3 Contact with Zone Labs

These controls enable you to protect your privacy when ZoneAlarm communicates with Zone Labs.

Select **Alert me with a pop-up before I make contact** to have ZoneAlarm warn you before it contacts Zone Labs to deliver registration information, get product updates, or find more information about an alert.

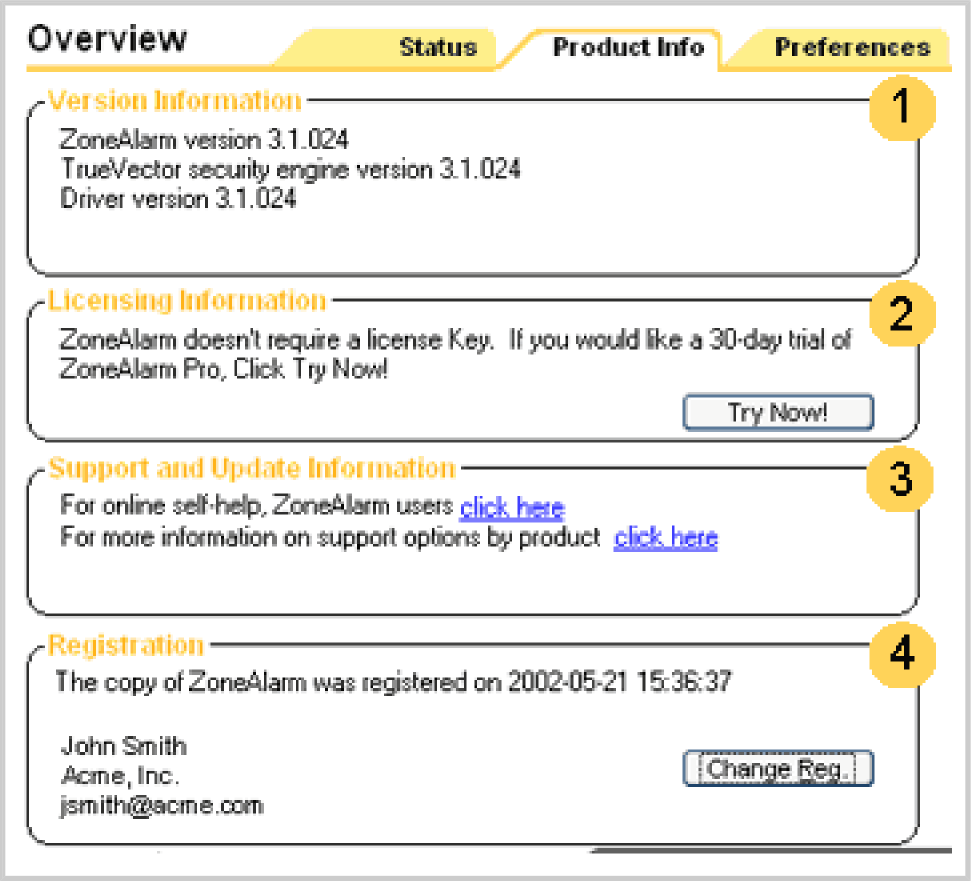
Select **Hide my IP address when applicable** to not include your IP address when you submit an alert to Zone Labs AlertAdvisor. This prevents Zone Labs, as well as anyone else who might intercept the message, from identifying your computer.

Select **Hide the last octet of my IP address** to not include the last three digits (for example, 123.456.789.XXX) of your IP address when you access AlertAdvisor.

Related Topics

Getting updates to ZoneAlarm

ZoneAlarm Product Info tab



Version Information

ZoneAlarm version 3.1.024
TrueVector security engine version 3.1.024
Driver version 3.1.024

Licensing Information

ZoneAlarm doesn't require a license Key. If you would like a 30-day trial of ZoneAlarm Pro, Click Try Now!

Support and Update Information

For online self-help, ZoneAlarm users click here
For more information on support options by product click here

Registration

The copy of ZoneAlarm was registered on 2002-05-21 15:36:37

John Smith
Acme, Inc.
jsmith@acme.com

Click the numbers to learn about specific controls, or read an introduction.

Product Info tab

The Product Info tab gives you quick access to information about your version of ZoneAlarm.

Use this tab to:

- See what version of ZoneAlarm you have. How?
- Access a 30-day trial of ZoneAlarm Pro How?
- Access the Technical Support area of the Zone Labs Web site. How?
- Change your registration. How?

1 Version Information

This area shows what version of ZoneAlarm, and what version of the TrueVector security engine, are running on your computer.

Tip To see if there is a new version available, go to the Status tab in the Overview panel, and check the update information on the right side of the screen.

2 Licensing Information

ZoneAlarm does not require a license key.

Click **Try Now!** to download a 30-day trial version of ZoneAlarm Pro.

3 Support and Update Information

Follow the technical support link to access FAQ, troubleshooting, and other technical information on the Zone Labs Web site.

Tip Before contacting Zone Labs technical support, try the troubleshooting steps provided in this help system. Start at the help welcome page.

4 Registration

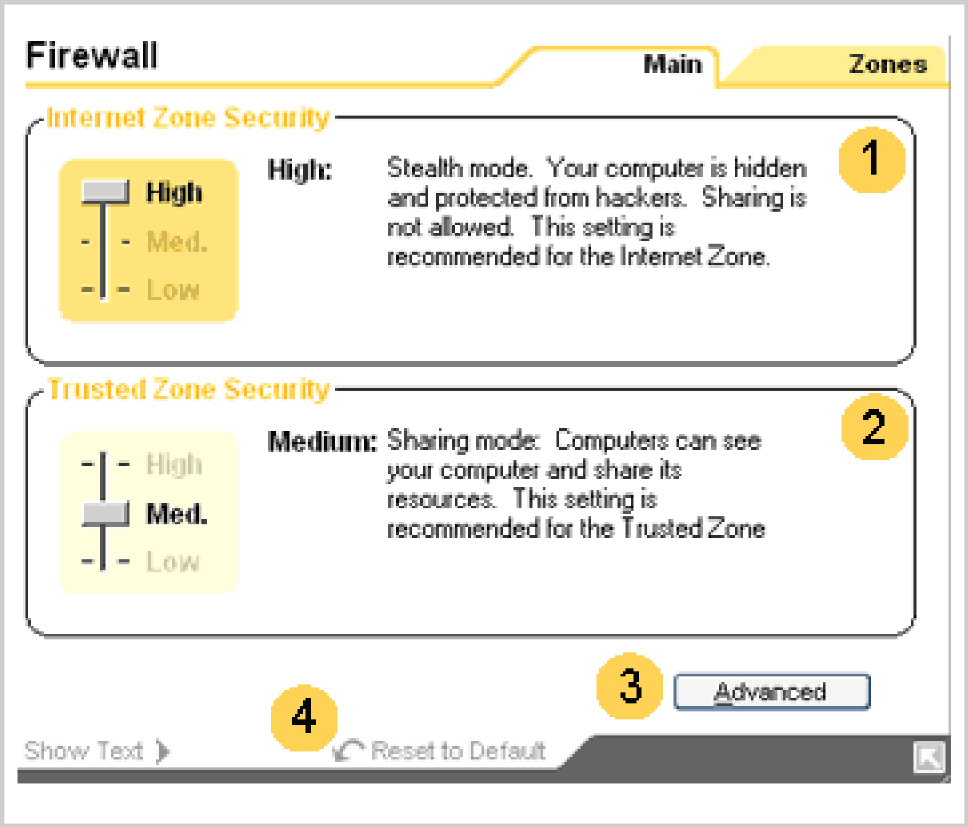
This area shows whether you have registered your copy of ZoneAlarm. If your registration is "pending", you have submitted registration information, but ZoneAlarm has not yet received confirmation of registration from Zone Labs.

Click **Change Reg.** to edit your registration information (name, company, or e-mail).

Click **Register** to register online. Registration only takes a few seconds.

Related Topics

ZoneAlarm Main tab (Firewall panel)



High: Stealth mode. Your computer is hidden and protected from hackers. Sharing is not allowed. This setting is recommended for the Internet Zone.

Medium: Sharing mode: Computers can see your computer and share its resources. This setting is recommended for the Trusted Zone

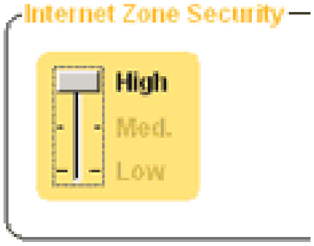
Click the numbers to learn about specific controls, or read an introduction.

Main tab (Firewall panel)

Use this tab to choose the basic level of security ZoneAlarm will apply to traffic from computers you know and trust (the Trusted Zone) and computers you don't know (the Internet Zone).

To learn about Zones and security levels and see the related topics *Security levels* and *What is a Zone?*

1 Internet Zone Security

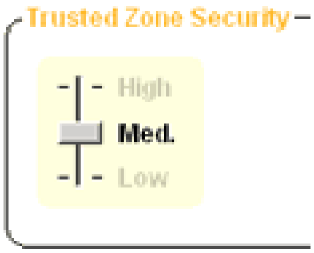


Use the slider to set the security level for the Internet Zone. The recommended security level for the Internet Zone is **High**.

About Internet Zone security levels

- **High** security puts your computer in stealth mode. Windows (NetBIOS) services and file and printer shares are blocked. Ports are opened only when a program to which you have given permission needs them.
- **Medium** security takes your computer out of stealth mode, making it visible to other computers on the Internet. Windows services are still blocked. Program permissions are still enforced.
- **Low** security enables Windows services. Your computer is visible to others, and file sharing is allowed. Program controls is still enforced.

2 Trusted Zone Security



Use the slider to set the security level for the Trusted Zone. The recommended security level for the Trusted Zone is **Medium**.

About Trusted Zone security levels

- **High security** puts your computer in stealth mode. Windows (NetBIOS) services and file and printer shares are blocked. Ports are opened only when a program you have given access permission or server permission needs them. Programs must have your permission in order to access the Internet or local network.
- **Medium security** takes your computer out of stealth mode, making it visible to other computers on the Internet. File and printer sharing, as well as Windows services (NetBIOS), are enabled. Programs must still have permission to access the Internet or local network.
- **Low security** enables Windows services. Your computer is visible to others, and file sharing is allowed. Program controls is still enforced.

3 Advanced

Click the Advanced button to access the Security tab.

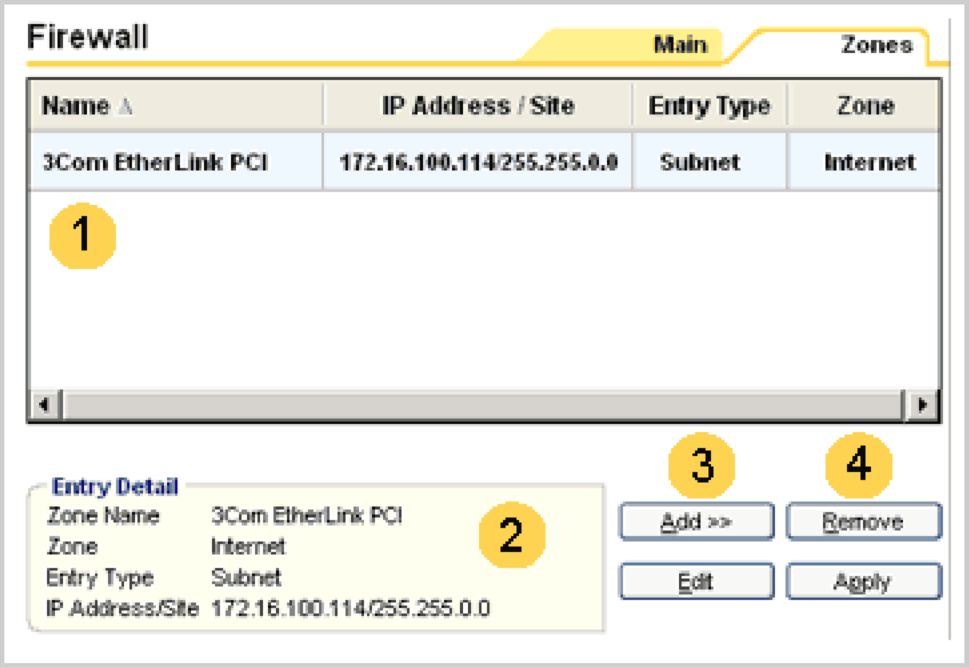
4 Reset to Default

Click to reset the security levels for the Internet and Trusted Zones to their defaults (high and medium, respectively).

Related Topics

Choosing security settings
Security levels
What is a Zone?

ZoneAlarm Zones tab



Name △	IP Address / Site	Entry Type	Zone
3Com EtherLink PCI	172.16.100.114/255.255.0.0	Subnet	Internet

Entry Detail

Zone Name	3Com EtherLink PCI
Zone	Internet
Entry Type	Subnet
IP Address/Site	172.16.100.114/255.255.0.0

Click the numbers to learn about specific controls, or read an introduction.

Zones tab

The Zones tab contains the traffic sources (computers, networks, or subnets, or sites) you have added to the Trusted Zone. It also contains any networks that ZoneAlarm has detected. Use this tab to:

- Move your detected network adapter subnet to a different Zone.
- Move an existing computer, host, site, or subnet to a different Zone.
- Manually add a computer, host, site, or subnet to the Trusted Zone.

Note: ZoneAlarm automatically detects your network adapter subnet and places it in the Internet Zone. We recommend that you leave the adapter subnet in the Internet Zone, and add to your Trusted Zone any specific networks you want to trust. If you place your adapter subnet in the Trusted Zone, you are in effect trusting every network you connect to.

1 Traffic source list

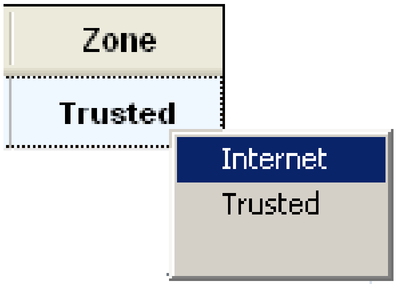
The list displays the traffic sources and the Zones they belong to. You can sort the list by any field by clicking the column header. The arrow (△) next to the header name indicates the sort order.

Click the same header again to reverse the sort order.

Traffic source list fields

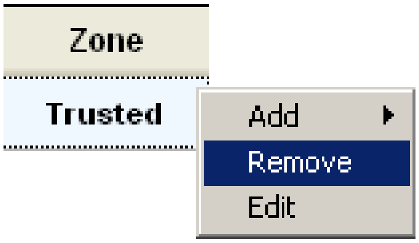
Field	Information
Name	The name you assigned to this computer, site, or network
IP Address/Site	The IP address or host name of the traffic source
Entry Type	The type of traffic source this is: Network, Host, IP, Site, or Subnet
Zone	The Zone the traffic source is assigned to: Internet, Trusted, or Blocked.

Changing the Zone of a traffic source



To change the Zone of a traffic source, left-click click in the Zones column for the source, then select from the shortcut menu.

Adding, removing, or editing a traffic source



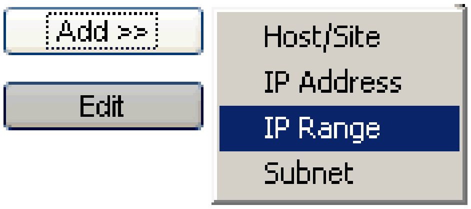
To add, remove, or edit a traffic source, right-click in the Zones column for the source, then select from the shortcut menu.

Tip You must click the **Apply** button to save your changes.

2 Entry Detail window

The entry detail window displays information about the traffic source currently selected in the traffic source list. The fields are the same as those in the traffic source list.

3 Add/Edit buttons



To add a traffic source to the list, click the **Add** button and select the type of traffic source you want to add from the shortcut menu. The Add dialog box will appear.

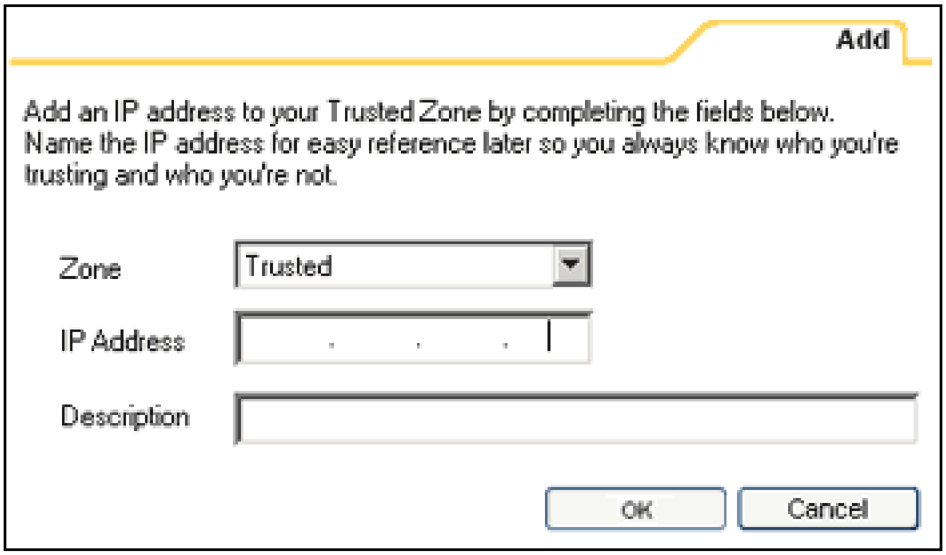
To change the Zone or any other information about a traffic source already in the list, select the traffic source, then click the **Edit** button. The Edit dialog box opens.

4 Remove/Apply buttons

To remove a traffic source from the list, select it, then click the **Remove** button.

To save any changes you have made in this tab, click the **Apply** button.

Add/Edit dialog box



Add an IP address to your Trusted Zone by completing the fields below. Name the IP address for easy reference later so you always know who you're trusting and who you're not.

Zone: Trusted

IP Address: . . .

Description:

Use the Add and Edit dialogs to provide or change the Zone, address, and description for a traffic source. The fields available will vary depending on the type of source involved (host/site, IP address, IP range, or subnet).

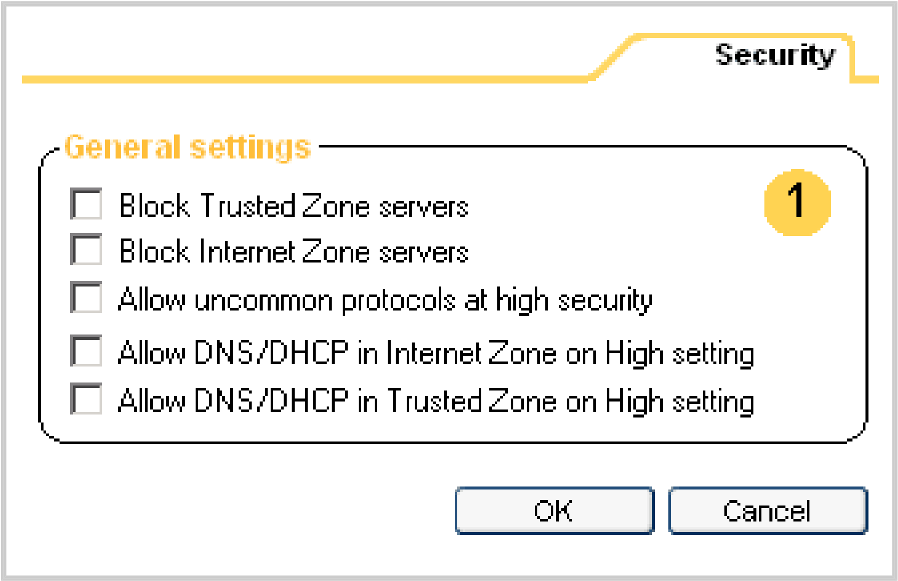
Access the Edit dialog by selecting a traffic source from the list, and clicking the **Edit** button.

Access the Add dialog by clicking the **Add** button.

Related Topics

What is a Zone?

Security tab



□ Block Trusted Zone servers
□ Block Internet Zone servers
□ Allow uncommon protocols at high security
□ Allow DNS/DHCP in Internet Zone on High setting
□ Allow DNS/DHCP in Trusted Zone on High setting

Click the numbers to learn about specific controls, or read an introduction.

To reach this tab:

1. Go to Firewall / Main tab
2. Click the Advanced button.

Security tab (Advanced Settings dialog box)

Use the Advanced Settings dialog box to establish global network and security settings.

1 General Settings

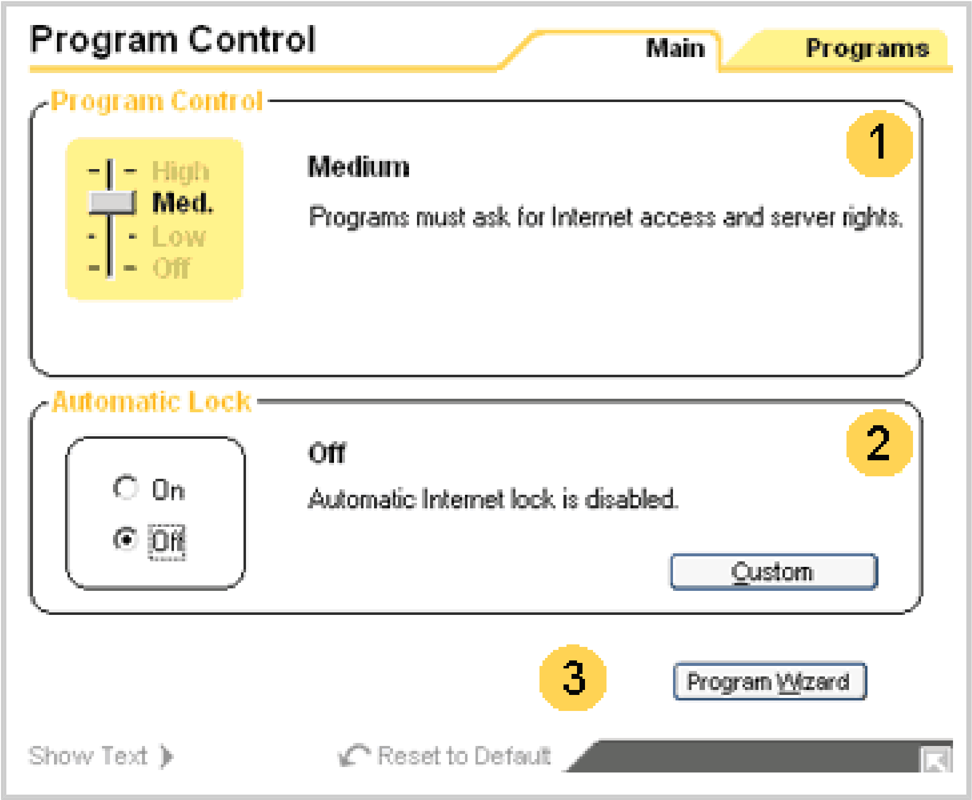
These controls apply global rules regarding certain protocols, packet types and other forms of traffic (such as server traffic) to both the Trusted Zone and the Internet Zone.

Control	Function when selected
Block Trusted Zone 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 Zone 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.

Allow uncommon protocols at high security	Allows the use of uncommon protocols. When this control is not selected, these protocols are allowed only at medium security.
Allow DNS/DHCP in Internet Zone on High Setting	Allows traffic from the Internet Zone through well-known DNS and DHCP ports even if the security level is set to high.
Allow DNS/DHCP in Trusted Zone on High Setting	Allows traffic from the Trusted Zone through well-known DNS and DHCP ports even if the security level is set to high.

Related Topics

ZoneAlarm Main tab (Program Control panel)



Medium

Programs must ask for Internet access and server rights.

Off

Automatic Internet lock is disabled.

Click the numbers to learn about specific controls, or read an introduction.

Main tab (Program Control panel)

Use this panel to choose a program control level, and to turn the Automatic Internet Lock on or off.

1 Program Control

Use the slider to choose a global setting for program control.

High

The added protection of the high program control setting is available only in ZoneAlarm Pro.

- Programs and their components are authenticated. More Info.
- Program permissions are enforced.

- Possible alerts:
    - New/Repeat/Changed Program
    - Server Program
    - Program Component / Component Loading

Medium

- Programs are authenticated.
- Program permissions are enforced.
- Possible alerts:
    - New/Repeat/Changed Program
    - Server Program

Low

- Programs are learned.
- No program alerts are shown.

Off

- No programs are authenticated or learned.
- No program permissions are enforced.
- All programs are allowed access/server rights. No program alerts can occur.

---

2 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 using network resources.

If you turn the Automatic Lock **on**, the Internet Lock will engage when your screen saver engages OR after a specific number of minutes of network inactivity, depending on settings in the Auto Lock tab.

For more information about the Internet Lock, see the related topic, *Using the Internet Lock and Stop button*.

---

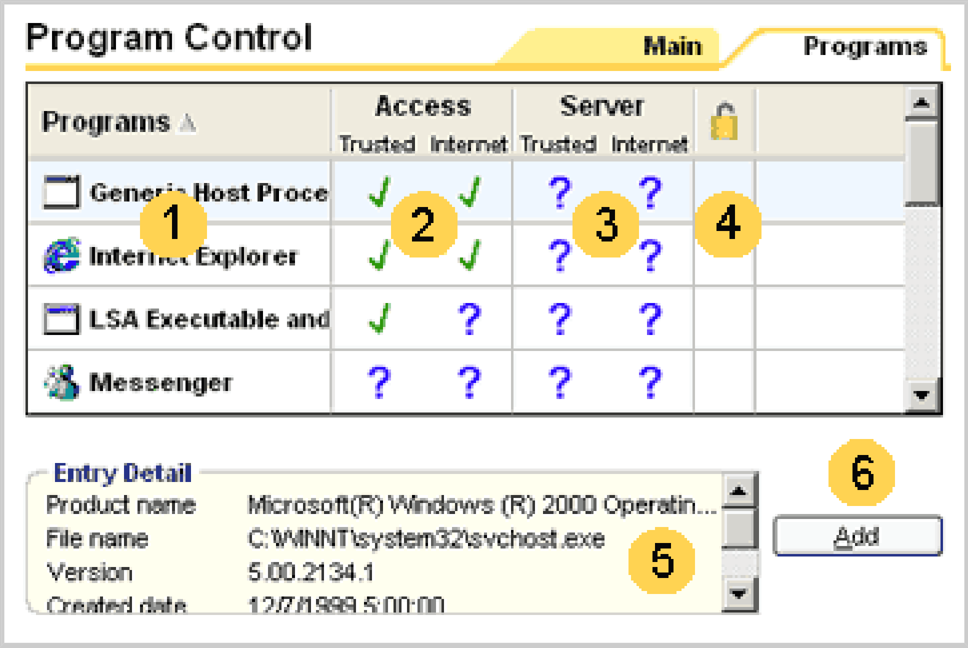
3 Program Wizard

Click the **Program Wizard** button to have the ZoneAlarm program wizard help you set up your programs for Internet access.

Related Topics

Changed Program alert
Program authentication
Using the Internet Lock and Stop button

ZoneAlarm Programs tab



Program Control

Programs ▲	Access Trusted	Access Internet	Server Trusted	Server Internet	🔒
Generic Host Proce	✓	✓	?	?	
Internet Explorer	✓	✓	?	?	
LSA Executable and	✓	?	?	?	
Messenger	?	?	?	?	

Entry Detail

Product name	Microsoft(R) Windows (R) 2000 Operatin...
File name	C:\WINNT\system32\svchost.exe
Version	5.00.2134.1
Created date	12/7/1999 5:00:00

Click the numbers to learn about specific controls, or read an introduction.

Programs tab

Use this tab to:

1. Grant or deny access permission and server permission to your programs
2. Add programs to the list and establish their permissions
3. Review your settings

Program permission symbols

✓ A green check means the program is allowed access/server rights.

✗ A red X means the program is denied access/server rights.

? A blue question mark means ZoneAlarm will display a Program alert when the program asks for access/server rights.

Tip You can sort the programs in the list by any field. Click on the field header to sort. The arrow icon ▲ indicates the sort order.

1 Program name and status

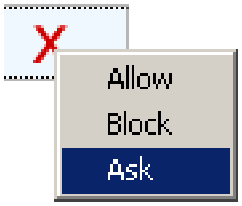
As you use your computer, ZoneAlarm detects every program that requests network access and adds it to this list. It also records the answer you gave to the Program alert for that program. A green bullet in the Active column means the program listed is currently accessing network resources. The program column displays the program name and associated icon.

Tip For more information about a program, click the program name, then look in the Entry Details box at the bottom of the screen.

2–3 Access permission / Server permission

Use these fields to establish access permission and server permission for a program.

Left-click menu



To change a permission setting, click the symbol, then select from the shortcut menu.

Right-click menu

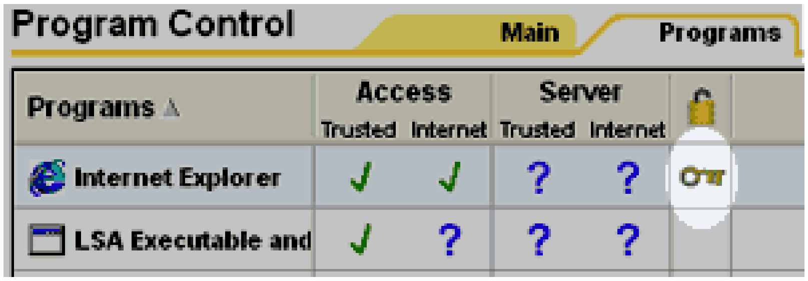
Right-click anywhere in the program's row to access a shortcut menu with the add and remove options described in the table below.

Menu item	Description
Remove	Deletes the program from the list.

Add program	Opens an explorer window so you can browse to a program on your computer that you want to add to the list.

Note 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.

4 Pass-lock



Programs ▲	Access		Server		🔒
	Trusted	Internet	Trusted	Internet	
Internet Explorer	✓	✓	?	?	🔑
LSA Executable and	✓	?	?	?	

A key in this field indicates that the program has pass-lock privilege.

To give pass lock privilege to a program, click the lock column, then choose **Pass-Lock** from the shortcut menu.

To revoke pass-lock privilege, click the lock icon, then choose **Normal** from the shortcut menu.

Tip If you grant pass-lock permission to a program, and that program uses other applications to perform its functions (for example, services.exe), be sure to give those other programs pass-lock permission as well.

5 Entry Detail

The entry detail box displays information about the program currently selected in the programs list.

Field	Information
Product name	The common name of the program, for example, Internet Explorer.

File name	The fully-qualified name of the executable file, for example, C:\\Program Files\Internet Explorer\IEXPLORE.EXE
Version	The version number of the program.
Created date	The date the program was created by its manufacturer.
File size	The size of the executable file

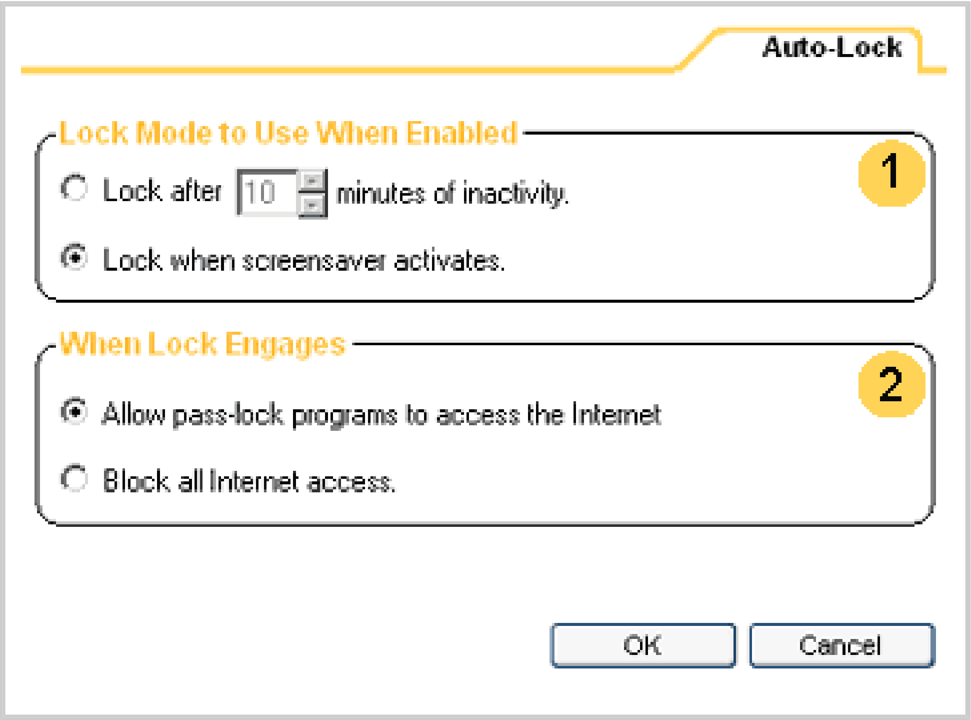
6 Add

Click **Add** to add a program to the programs list.

Related Topics

Program control

ZoneAlarm Auto-Lock tab



Auto-Lock

Lock Mode to Use When Enabled

○ Lock after 10 minutes of inactivity.

● Lock when screensaver activates.

When Lock Engages

● Allow pass-lock programs to access the Internet

○ Block all Internet access.

Click the numbers to learn about specific controls, or read an introduction.

To reach this tab:

1. To to Program Control / Main tab
2. Under Automatic Lock, click the Custom button.

Auto-Lock tab

Use these controls to determine:

- How the Automatic Internet Lock will engage
- Whether the lock will block all traffic, or allow pass-lock traffic.

Tip Settings in this tab go into effect only when the Automatic Internet Lock is turned on in the Program Control panel/Main tab.

For more information on the Internet Lock, see the related topic, *Using the Internet Lock and Stop button*.

1 Lock Mode to Use When Enabled

You can set the automatic lock to engage either:

- After a period of Internet inactivity, or
- When your computer's screen saver activates.

Use the radio buttons to select a lock mode. If you choose the inactivity option, select the number of minutes of inactivity after which the lock will activate.

2 When Lock Engages

When the Internet Lock is engaged, it can either block all traffic, or continue to allow pass-lock traffic.

Allow the pass-lock programs to access the Internet is like the Internet Lock in the control bar. When the automatic lock engages, all traffic will be blocked, except traffic authorized by programs you have specifically given permission to bypass the lock.

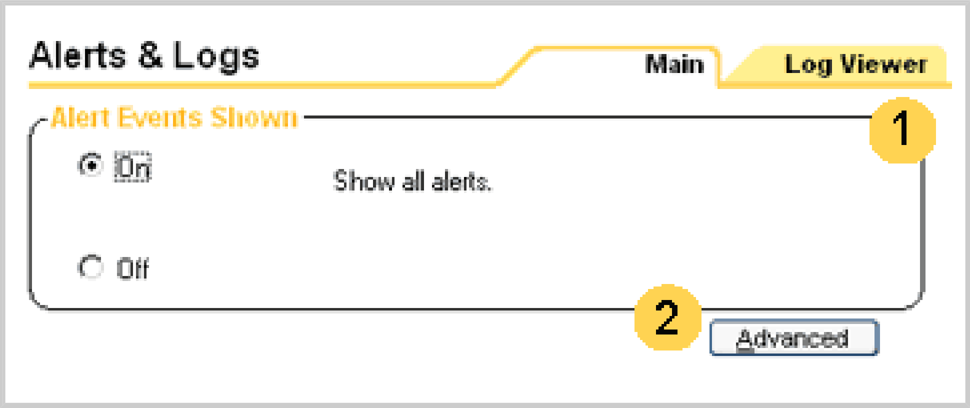
Block all Internet access is like the **STOP** button in the control bar. When the automatic lock engages, all traffic to and from your computer will be blocked.

To find out how to give pass-lock permission to a program, see the related topic *Giving pass-lock permission to a program.*

Related Topics

Using the Internet Lock and Stop button
Giving pass-lock permission to a program

ZoneAlarm® Main tab (Alerts & Logs)



Click the numbers to learn about specific controls, or read an introduction.

Main tab (Alerts & Logs)

Use this tab to turn the display of informational alerts on or off.

Note Program alerts are always displayed, because they ask you to decide whether to grant program access or not. For more information about informational alerts and program alerts, see the related topic *ZoneAlarm alerts.*

1 Alert Events Shown

This control determines what types of informational alerts ZoneAlarm will display.

Choose **On** to have ZoneAlarm display informational alerts such as Firewall alerts and Blocked Program alerts.

Choose **Off** to have ZoneAlarm display New Program, Server Program, and Changed Program alerts only.

For more information about these alert types, see the related topic *ZoneAlarm alerts*

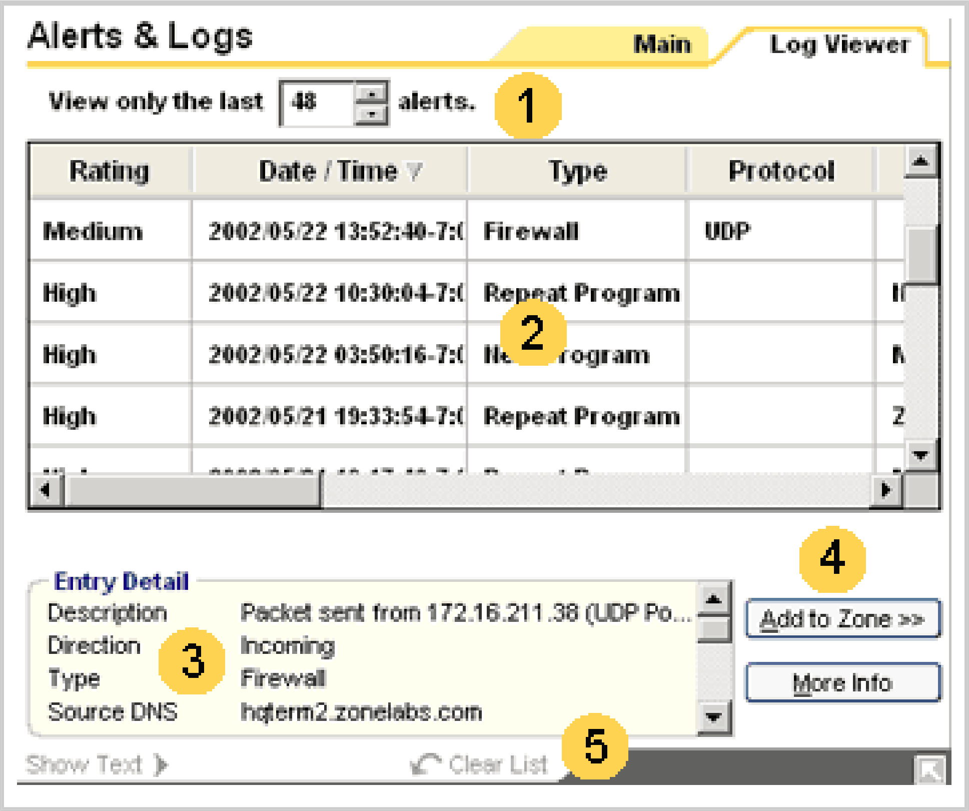
2 Advanced

Click the **Advanced** button to open the Advanced Alerts and Log Settings dialog box. There you can configure your ZoneAlarm log and set the archiving frequency (Log Control tab) .

Related Topics

Log Control tab
ZoneAlarm alerts

ZoneAlarm Log Viewer tab



View only the last 48 alerts.

Rating	Date / Time	Type	Protocol	
Medium	2002/05/22 13:52:40-7:(	Firewall	UDP	
High	2002/05/22 10:30:04-7:(	Repeat Program		I(
High	2002/05/22 03:50:16-7:(	Ne rogram		N
High	2002/05/21 19:33:54-7:(	Repeat Program		Z

Entry Detail

Description	Packet sent from 172.16.211.38 (UDP Po...
Direction	Incoming
Type	Firewall
Source DNS	hqterm2.zonelabs.com

Click the numbers to learn about specific controls, or read an introduction.

Log Viewer tab

The Log Viewer tab lists recent alerts. You can use each alert entry to:

- Submit the alert to Zone Labs AlertAdvisor for analysis. How?
- Add the source of the traffic that generated the alert to your Trusted Zone. How?

1 View only the last *n* alerts

Select the number of alerts (starting with the most recent) to display in the alerts list.

2 Alerts list

The alerts list shows Firewall alerts, Program alerts, and other alerts that have been recorded in the

ZoneAlarm log.

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.

Alert list fields

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, or Lock Enabled.
Protocol	The communications protocol used by the traffic that caused the alert.
Program	The name of the program attempting to send or receive data. (Applies only to Program alerts).
Source IP	The IP address of the computer that sent the traffic that ZoneAlarm 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 ZoneAlarm.
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 computer that sent the traffic that caused the alert.
Destination DNS	The domain name of the intended addressee of the traffic that caused the alert.

Adding the source of the alert to the Trusted Zone

If you determine that you received a firewall alert because ZoneAlarm blocked traffic from a computer that you want to share resources with, you can add that computer to the Trusted Zone directly from the alerts list. Follow these steps:

1. Right-click the source IP address you want to add.
2. Choose **Add to Zone** and Trusted from the shortcut menu.

Submitting the alert to Zone Labs AlertAdvisor

To have Zone Labs AlertAdvisor analyze an alert for you, follow these steps:

1. Right click anywhere in the alert record you want to submit.
2. Choose **More Info** from the shortcut menu.

3 Entry Detail box

The Entry Detail box displays details of the alert currently selected in the alerts list. Entry detail fields are the same as those in the alerts list, but displayed in an easily readable format.

4 Add to Zone / More Info

Click **Add to Zone** to add the Source IP of the selected alert to the Trusted Zone.

Click **More Info** to have Zone Labs' Alert Advisor analyze the selected alert, and provide advice on any action you may need to take.

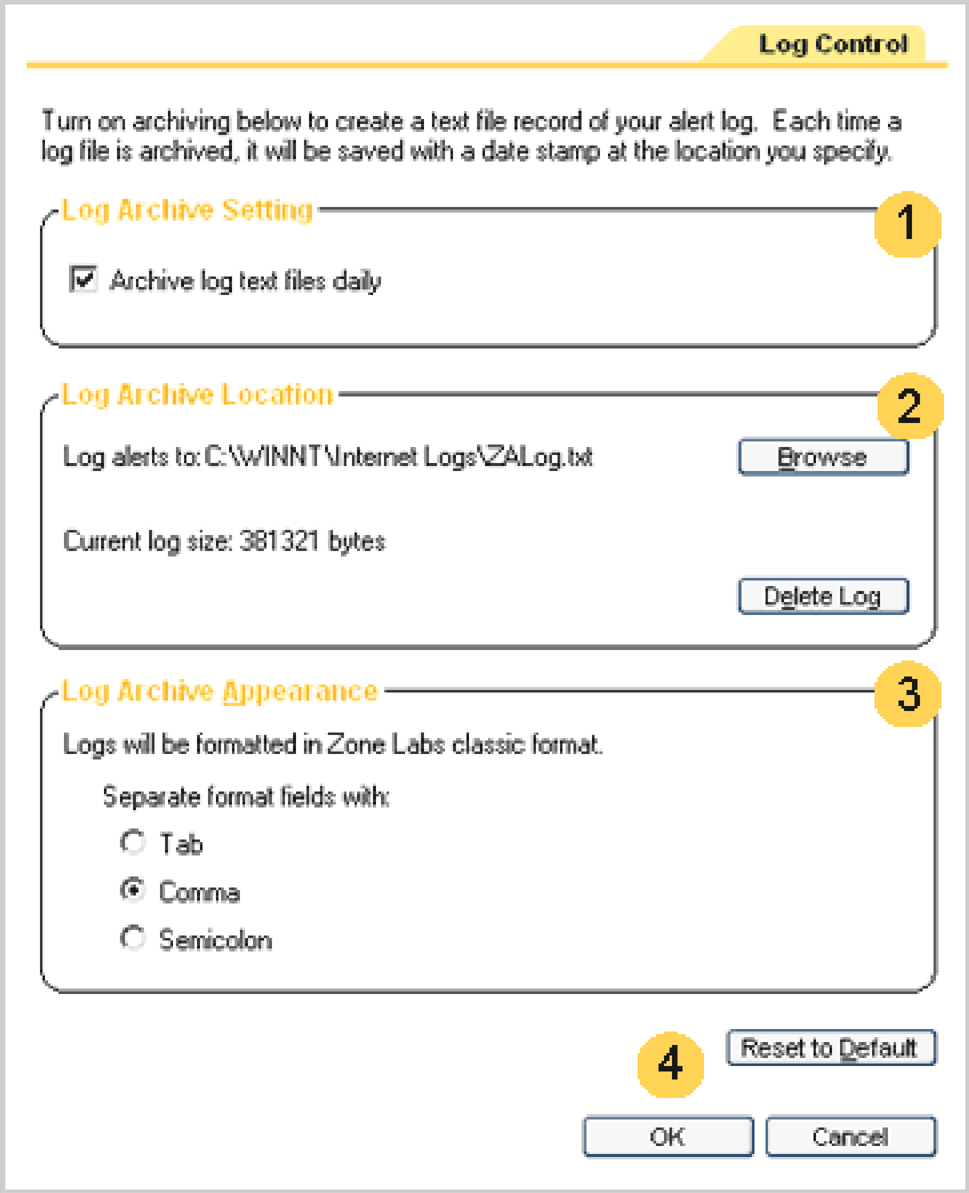
5 Clear List

Click Clear List to clear all entries from the Log Viewer. You can still view all of these entries in the ZoneAlarm log. How?

Related Topics

Viewing the ZoneAlarm log
Reading log entries

ZoneAlarm Log Control tab



Turn on archiving below to create a text file record of your alert log. Each time a log file is archived, it will be saved with a date stamp at the location you specify.

Log Archive Setting

☑ Archive log text files daily

Log Archive Location

Log alerts to: C:\WINNT\Internet Logs\ZALog.txt

Current log size: 381321 bytes

Log Archive Appearance

Logs will be formatted in Zone Labs classic format.

Separate format fields with:

○ Tab
● Comma
○ Semicolon

Click the numbers to learn about specific controls, or read an introduction.

To reach this tab:

1. Go to Alerts & Logs / Main tab
2. Click the Advanced button.
3. Click the Log Control tab.

Log Control tab (Advanced Alerts & Log Settings dialog)

Use the Log Control tab to determine when, where and how ZoneAlarm will save and archive log files. To access this tab, click the **Advanced** button in the Main tab of Alerts & Logs.

---

1 Log Archive Setting

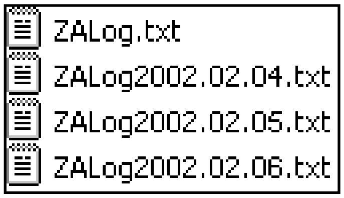
To turn daily log archiving on:

1. Select the **Archive log text files daily** check box.

Note If the check box is not selected, ZoneAlarm continues to log events for display in the Log Viewer tab, but does not archive them to the ZAlog.txt file.

2 Log Archive Location

About ZoneAlarm logs



ZALog.txt
ZALog2002.02.04.txt
ZALog2002.02.05.txt
ZALog2002.02.06.txt

ZoneAlarm logs events to a text file, named ZAlog.txt.

At regular intervals, the contents of ZAlog.txt are archived to a date-stamped file, for example, ZALog2002.02.04.txt (for February 4, 2002). This prevents ZAlog.txt from becoming unmanageably large.

For information on how to find, read, and interpret log files, see Related Topics.

The ZAlog.txt file and all archived log files are stored in the same directory. The default locations are C:\Windows\Internet Logs (for Windows 95, Windows98, Windows ME, and Windows XP); and C:\Winnt\Internet Logs (for Windows NT, Windows 2000).

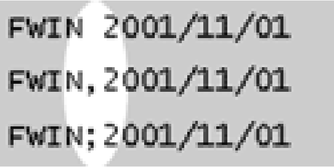
Use the **Browse** button to designate the location for the current log and archived log files. You can also change the name of the log file.

Use the **Delete Log** button to delete the current log file. This will not delete the archived log files.

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

3 Log Archive Appearance

Use these controls to determine the field separator for your log files.



```
FWIN 2001/11/01
FWIN,2001/11/01
FWIN;2001/11/01
```

Select **Tab** to separate fields with a tab character.

Select **Comma** to separate log fields with a comma.

Select **Semicolon** to separate log fields with a semicolon.

---

4 Buttons

Click **Reset to Default** to return log control settings to Zone Labs defaults.

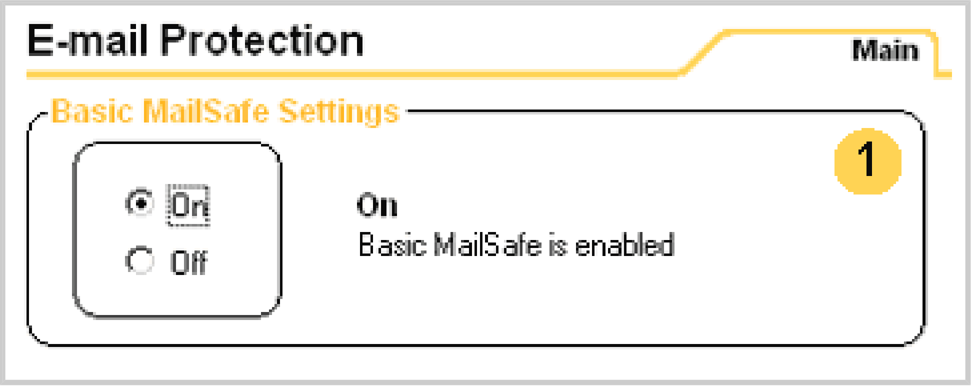
Click **Cancel** to close the dialog box without saving any changes you have made.

Click **OK** to save your changes and close the dialog box.

Related Topics

[Reading log entries](#)
[Viewing the ZoneAlarm log](#)

ZoneAlarm Main tab (E-mail Protection panel)



E-mail Protection

Basic MailSafe Settings

● On
○ Off

On
Basic MailSafe is enabled

Click the numbers to learn about specific controls, or read an introduction.

Main tab (E-mail protection panel)

Use this tab to turn basic MailSafe protection on or off.

Note Basic MailSafe quarantines .VBS attachments only. To obtain automatic protection against additonal attachment types, and to be able to edit the quarantine list, upgrade to ZoneAlarm Pro.

For more information about how MailSafe works, see the related topic *E-mail protection.*

1 MailSafe Setting

Use the radio buttons to turn MailSafe on or off.

- If **On** is selected, e-mail attachments with the filename extension .vbs will be quarantined.
- If **Off** is selected, no attachments will be quarantined.

Related Topics

E-mail protection

ZoneAlarm Viewing the ZoneAlarm log

To view the current log in the Log Viewer:

- In the Alerts & Logs panel, choose the Log Viewer tab.

To view the current log as a text file:

- Navigate to the location of the log file and open manually. By default, alerts generated by ZoneAlarm 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.

Reading log entries

By default, alerts generated by ZoneAlarm 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.

Log fields

Log entries contain the fields described in the table below.

Field	Description	Example
Type	The type of event recorded (see "Event types" below).	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.)
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 (FW events)
		Microsoft Outlook (PE events)

Destination	The IP address and port of the computer the blocked packet was addressed to.	192.168.1.101:0
Transport	The protocol (packet type) involved.	UDP

Event types

The first field in a log entry indicates the type of event recorded.

Event type code	**Meaning**
FWIN	The firewall blocked an inbound packet of data coming to your computer. Some, but not all, of these packets are connection attempts.
FWOUT	The firewall blocked an outbound packet of data from leaving your computer.
FWROUTE	The firewall blocked a packet that was not addressed to or from your computer, but was routed through it.
FWLOOP	The firewall blocked a packet addressed to the loopback adapter (127.0.0.1)
PE	An application on your computer requested access permission.

ACCESS	Program Control prevented an application on your computer from accessing remote resources.
LOCK	The firewall blocked a packet because the Internet Lock was engaged.
MS	MailSafe quarantined an e-mail attachment.

ICMP message types

When ZoneAlarm blocks an ICMP packet, the log displays a number indicating what type of ICMP message it was.

- 0 - Echo Reply
- 3 - Destination Unreachable
- 4 - Source Quench
- 5 - Redirect
- 8 - Echo Request
- 9 - Router Advertisement
- 10 - Router Solicitation
- 11 - Time Exceeded
- 12 - Parameter Problem
- 13 - Timestamp Request
- 14 - Timestamp Reply
- 15 - Information Request
- 16 - Information Reply
- 17 - Address Mask Request
- 18 - Address Mask Reply

TCP flags

The TCP Flags are:

- S (SYN)
- F (FIN) R (RESET)
- P (PUSH)
- A (ACK)
- U (URGENT)
- 4 (low-order unused bit)
- 8 (high-order unused bit)

Log samples

Sample 1: FWIN

FWIN,2000/03/07,14:44:58,-8:00 GMT, Src=192.168.168.116:0, Dest=192.168.168.113:0, Incoming, ICMP

FWIN indicates that the firewall blocked an incoming request to connect to your computer. The entry also includes the following information:

- Date and Time
- Source IP Address and port number
- Destination IP Address and port number
- Transport-Indicates that the transport was either TCP, UDP, ICMP, or IGMP

Sample 2: FWOUT

FWOUT,2000/03/07,14:47:02,-8:00 GMT,QuickTime Player Application tried to access the Internet. Remote host: 192:168:1:10

ZoneAlarm blocked an outbound request. FWOUT indicates that the firewall blocked an outbound request from your computer. The entry also includes the following information:

- Date and Time
- Source IP Address and port number
- Destination IP Address and port number
- Transport-Indicates that the transport was either TCP, UDP, ICMP, or IGMP

Sample 3: PE

PE,2000/03/22,17:17:11 -8:00 GMT,Netscape Navigator application file,192.168.1.10

The PE entry informs you that an application on your computer attempted to access the Internet. The entry also includes the following information:

- Date and Time
- The application on your computer that attempted to access the Internet
- The IP Address and Port number that the application was trying to connect to.

Sample 4: LOCK

LOCK,2000/09/07,16:43:30 -7:00 GMT,Yahoo! Messenger,207.181.192.252,N/A

The LOCK entry informs you that an application on your computer attempted to access the Internet while the Internet Lock was engaged. The entry also includes the following information:

- Date and Time
- The application on your computer that attempted to access the Internet
- The IP Address that the application was trying to connect to.

Sample 5: ACCESS

ACCESS,2000/09/07,16:45:57 -5:00 GMT,Microsoft Internet Explorer was not allowed to connect to the Internet (64.55.37.186).,N/A,N/A

The ACCESS entry informs you that Program Control prevented an application on your computer from accessing remote resources. The entry also includes the following information:

- Date and Time
- The application on your computer that attempted to access the Internet
- The IP Address that the application was trying to connect to.

Sample 6: MS

MS,2000/09/08,09:45:56 -5:00 GMT,Microsoft Windows(TM) Messaging Subsystem Spooler,Renamed e-mail attachment of type .HLP to .zla,N/A

The MS entry informs you that an e-mail containing an attachment of a file type that you have asked MailSafe to quarantine was received by your e-mail client. The entry also includes the following information:

- Date and Time
- The system that handles e-mail delivery on your system, like Microsoft Windows(TM) Messaging Subsystem Spooler
- The name of the file, including file type, that was quarantined.

ZoneAlarm Getting updates to ZoneAlarm

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

Checking for updates manually

To find out if there are any updates available:

1. Go to the Preferences tab of the Overview panel.
2. When you want to check for an update, click the **Check for Update** button.

Checking for updates automatically

To have ZoneAlarm automatically notify you when an update is available, follow these steps:

1. Go to the Preferences tab in the Overview panel.
2. Under Check for Updates, select **Automatically**.

Note After your one-year product update subscription expires, both manual and automatic update checking are disabled. Contact Zone Labs to renew your subscription.

What version of ZoneAlarm do I have?

To find out what version of ZoneAlarm you have:

1. Go to the Product info tab in the Overview panel.
2. Read the information in the box labeled Version Information.

Glossary

A

access permission

Access permission allows a program on your computer to initiate communications with another computer. This 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.

Several common applications may need access permission to operate normally. For example, your browser needs access permission in order to contact your ISP's servers. Your e-mail client (for example, MS Outlook) needs access permission in order to send or receive e-mail.

The following basic options are available for each program:

□ **Allow** the program to connect to computers in the Internet Zone / Trusted Zone

□ **Block** the program from accessing computers in the Internet Zone / Trusted Zone

□ **Ask** whether the program should have access permission (show Repeat Program alert)

Top

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.

ZoneAlarm prevents programs on your computer from acting as servers unless you grant server permission.

Top

AlertAdvisor

Zone Labs AlertAdvisor is an online utility that enables you to instantly analyze the possible causes of an alert, and helps you decide whether to respond Yes or No to a Program alert. To use AlertAdvisor, click the **More Info** button in an alert pop-up. ZoneAlarm sends information about your alert to AlertAdvisor. AlertAdvisor returns an article that explains the alert and gives you advice on what, if anything, you need to do to ensure your security.

B

Blocked Zone
The Blocked Zone contains computers you want no contact with. This Zone is available only in ZoneAlarm Pro and ZoneAlarm Plus.

Top

C

D

Top

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.

Top

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.

Top

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.

Top

DNS (Domain Name System)
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).

E

F

(no entries)

G

H

I

Internet Zone
The Internet Zone contains all the computers in the world—except those you have added to the Trusted Zone or Blocked Zone.

ZoneAlarm 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.

Top

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.

Top

ISP (Internet Service Provider)
A company that provides access to the Internet. ISP's 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.

Top

J

(no entries)

K

(no entries)

L

(no entries)

M

Top

mail server

The remote computer from which the e-mail program on your computer retreives e-mail messages sent to you.

Top

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.

Top

More Info button
A button that appears in ZoneAlarm alerts. By clicking it, you submit information about the alert to Zone Labs' Alert Advisor, which then displays a Web page with an analysis of the alert.

N

Top

NetBIOS (Network Basic Input/Output System)
A program that allows applications on different computers to communicate within a local network. By default, ZoneAlarm 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.

O

(no entries)

P

Top

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.

Top

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.

Top

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.

Top

port
A channel in or out of your computer. Some ports are associated with standard network protocols; for example, HTTP (Hypertext Transfer Protocol) is traditionally addressed to port 80. Port numbers range from 1 to 65535.

Top

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.

Top

program authentication
When a program on your computer asks for Internet access, ZoneAlarm examines its recorded MD5 checksum to verify that it has not been tampered with since its last request. You can set ZoneAlarm to authenticate only the program itself, or the program and the shared components (such as DLLs) it uses.

Top

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.

Top

protected system files
Windows system components that are guarded by Windows File Protection. Built in to Windows 2000 and later, file protection keeps other programs from replacing system files with anything but Microsoft-certified updates.

Top

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.

Q

Top

Quarantine
ZoneAlarm's MailSafe quarantines incoming e-mail attachments whose filename extensions indicate the possibility of auto-executing code. By changing the filename extension, quarantining prevents the attachment from opening without inspection. This helps protect you from worms, viruses, and other malware that hackers distribute as e-mail attachments. (ZoneAlarm quarantines only .VBS extentions. To be able to quarantine other extension types, upgrade to ZoneAlarm Pro.)

R

(no entries)

S

Top

script
A series of commands that execute automatically, without the user intervening. These usually take the form of banners, menus that change when you move your mouse over them, and popup ads.

Top

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 distinct from access permission, which allows a program to initiate a communications session with another computer.

Several common types of applications, such as chat programs, e-mail clients, and Internet Call Waiting programs, may need server permission to operate properly. Grant server permission only to programs you're sure you trust, and that require it in order to work.

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

The following basic options are available for each program

□ **Allow** the program to listen for connection requests

□ **Block** the program from listening for connection requests

□ **Ask** me whether to allow the program to listen for connection requests (show Server Program alert)

Top

stealth mode
When ZoneAlarm 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.

T

Top

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.

Top

TrueVector security engine
The primary component of ZoneAlarm security. It is the TrueVector engine that examines Internet traffic and enforces security rules.

Top

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 ZoneAlarm 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.

U

(no entries)

V

W

XYZ

(no entries)