ZoneAlarm Plus Help Contents

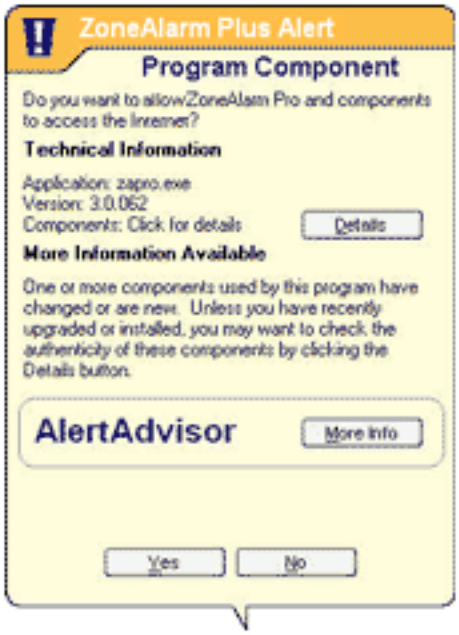
Getting started

How ZoneAlarm Plus protects you

Troubleshooting

Contact Zone Labs *

Program Component alert



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

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

Click the **Details** button to see what component(s) the program was loading.

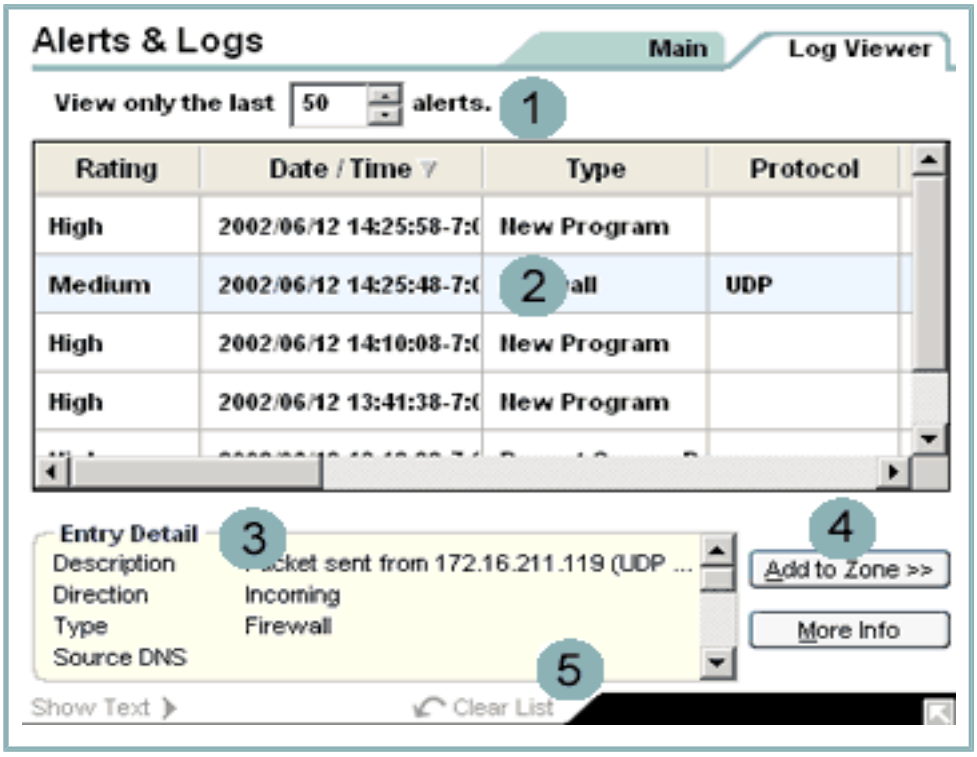
Why these alerts occur

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

Note ZoneAlarm Plus automatically secures the components that a program is using at the time you grant it access permission. This prevents you from seeing a Component alert for every component loaded by your browser. To learn how ZoneAlarm Plus secures program components see the related topic *Program authentication.*

.

Log Viewer tab



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 Plus 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 Plus 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 Plus.
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 Plus 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 either the Blocked Zone or 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.

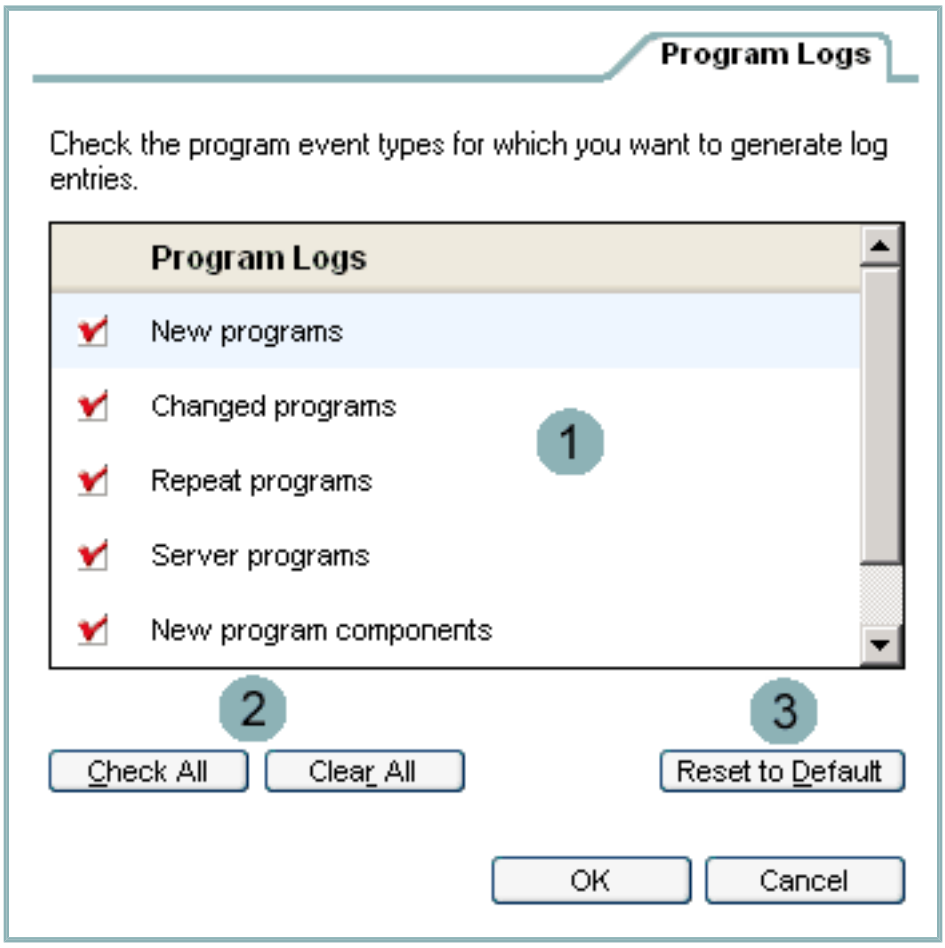
5 Clear List

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

Related Topics

Viewing the ZoneAlarm Plus log
Reading log entries

Program Logs tab



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

To reach this tab:

1. Go to Alerts & Logs/Main tab
2. Under Program Logging, click the Custom button.

Program Logs tab (Custom Alerts & Log Settings dialog)

Use the Program Logs tab to choose which types of Program alerts to record in the ZoneAlarm Plus log.

Note By default, ZoneAlarm Plus logs all program alerts. Alerts that are not recorded in the log cannot be reviewed later.

1 Program Logs list

Select the types of Program alerts you want recorded in the ZoneAlarm Plus log.

Deselect the types of Program alerts you do not want recorded in the log.

For information on the different program alert types, and on opening and reading the ZoneAlarm Plus log, see Related Topics.

---

2 Check All / Clear All

Click **Check All** to have ZoneAlarm Plus display all types of Program alerts

Click **Clear All** to to have ZoneAlarm Plus hide all types of Program alerts

---

3 Reset to Default

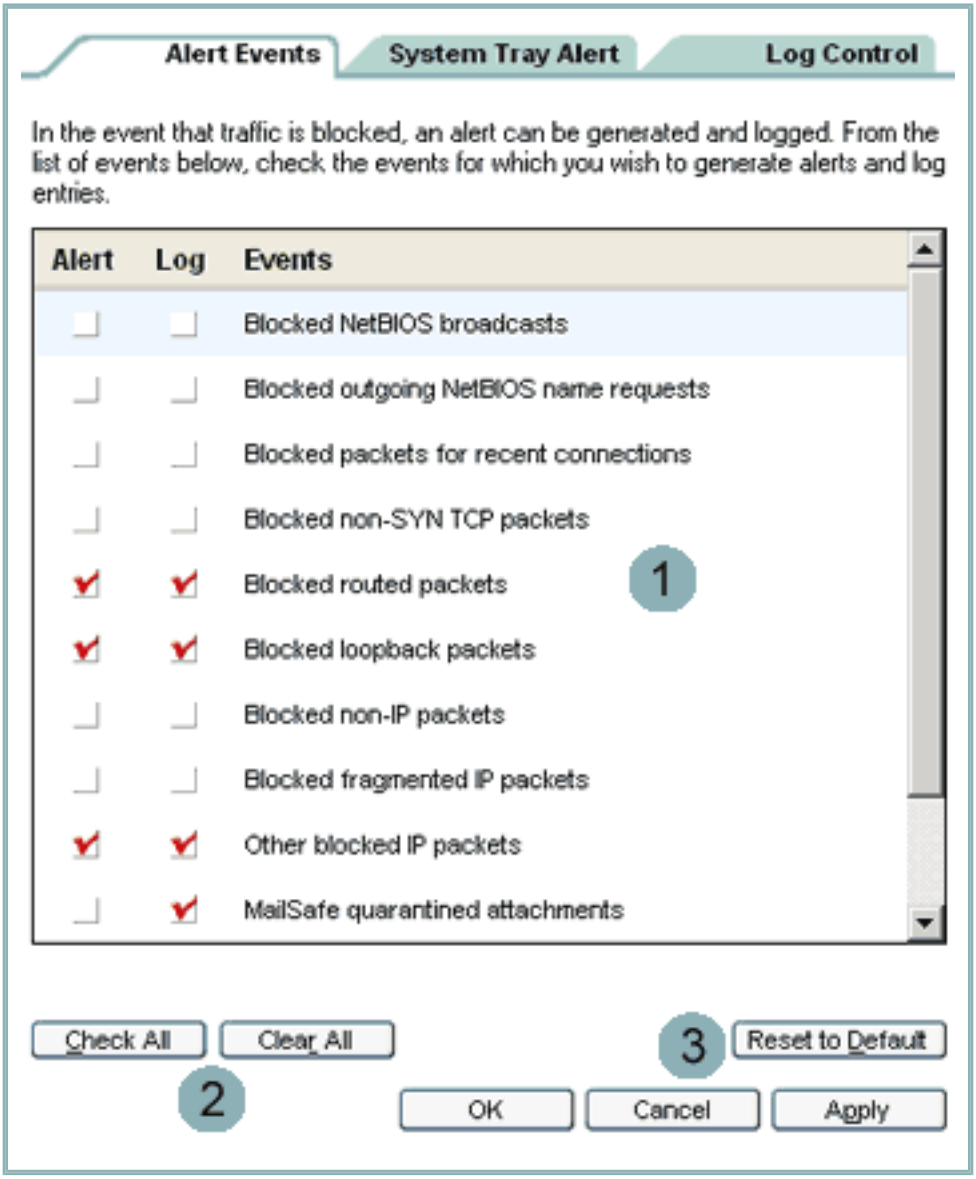
Click **Reset to Defaul**t to return Program alert settings to Zone Labs defaults.

Related Topics

ZoneAlarm Plus Alerts
Viewing the ZoneAlarm Plus log
Reading log entries

Program Logs tab

Alert Events tab



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

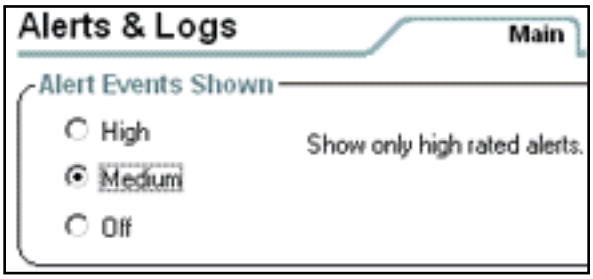
To reach this tab:

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

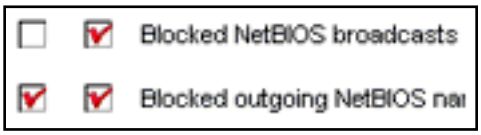
Alert Events tab (Advanced Alerts & Log Settings dialog)

Use the Alert Events tab to control in detail the display and logging of Firewall alerts, MailSafe alerts, Internet Lock alerts, and Blocked Program alerts. To open this tab, click the Advanced button in the Main tab of the Alerts & Logs panel.

The relationship between Main tab settings and Alert Events tab settings



The Alert Events Shown control, in the Main tab of Alerts & Logs, lets you control the display of Firewall Alerts and other alerts by rating. The **High** setting displays all alerts types, while the **Medium** setting displays only alerts probably caused by hacker activity. This control does not affect logging.



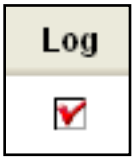
The Alert Events tab gives you more detailed control of alert display, as well as logging. You can specify which types of Firewall alerts to display and log by type of traffic blocked.

Tip New Program alerts, and the other program alerts that require a "yes" or "no " response from you, are always displayed. You can control the logging of these alerts by using the Program Logs tab.

---

1 Firewall Events list

For each type of event in the list:



Select the **Log** box to have ZoneAlarm Plus record the event in the log.

Select the **Alerts** box to have ZoneAlarm Plus display an alert box when that type of event occurs.

---

2 Check All / Clear All

Click **Check All** to log and display alerts for all of the event types listed.

Click **Clear All** to suppress logging and alert display for all of the event types listed.

---

3 Reset to Default

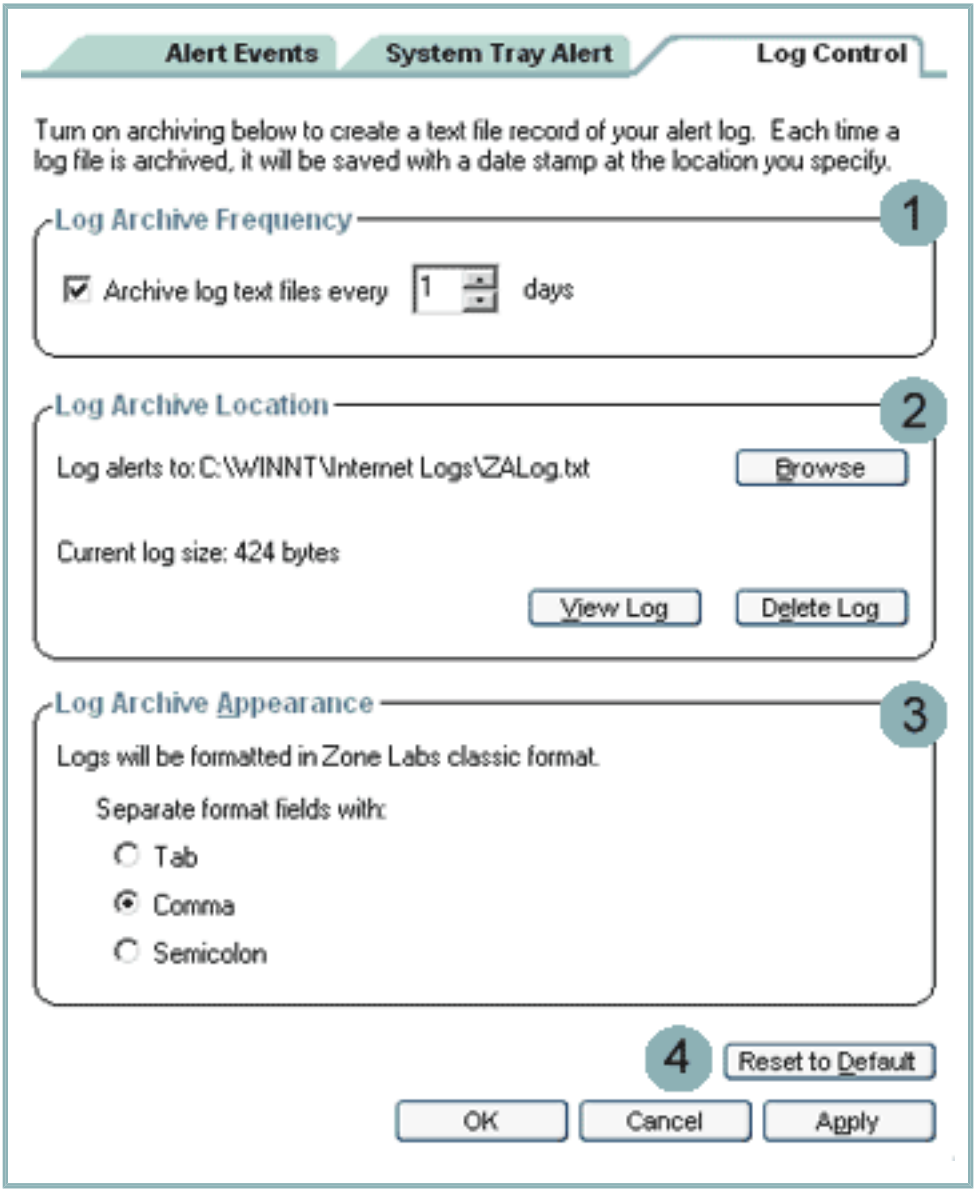
Click **Reset to Default** to restore settings in the Alert Events tab to their Zone Labs defaults.

Related Topics

Alerts & Logs
Firewall alerts
Reading log entries
Program Logs tab
Viewing the ZoneAlarm Plus log

Alert Events tab

Log Control tab



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 Plus will save and archive log files. To access this tab, click the **Advanced** button in the Main tab of Alerts & Logs.

1 Log Archive Frequency

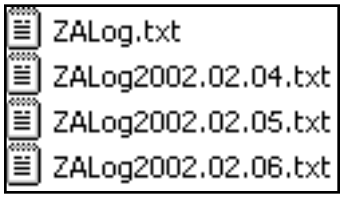
To turn log archiving on and to determine how often logs will be archived, follow these steps:

1. To turn log archiving on, select the **Archive...** check box.
2. Use the spin box to select the log archive frequency.

Note If the **Log Archive Frequency** check box is not selected, ZoneAlarm Plus 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 Plus logs



ZoneAlarm Plus 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 **View Log** button to open the current 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.

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 **Apply** to save your changes but leave the dialog box open.

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

Related Topics

Reading log entries
Viewing the ZoneAlarm Plus log

System Tray Alert tab

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 System Tray Alert tab.

System Tray Alert (Advanced Alert & Log Settings dialog)

Use the System Tray Alert tab to enable or disable the display of an alert icon in the system tray (in the lower right corner of your Windows desktop).

---

1 System Tray Alert

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

To have ZoneAlarm Plus display the system tray icon alert, select the check box labeled **Enable system tray icon alert**.

For more information about hiding alerts, see the related topic *Showing and hiding firewall alerts*.

---

2 System Tray Icons

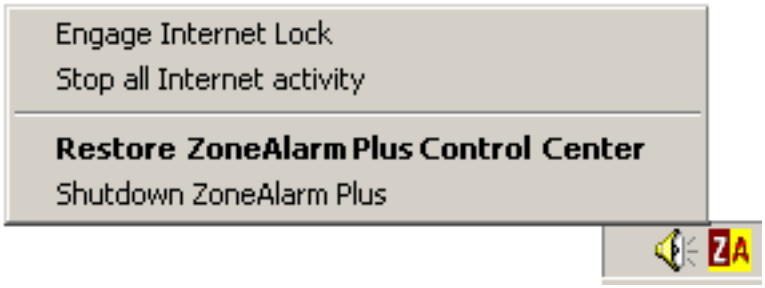
The icons displayed in the system tray let you monitor your security status and Internet activity as frequently as you wish, and access your security settings in just a few clicks.

To open the ZoneAlarm Plus control center, double-click any of the system try icons.

Icon	Meaning
	ZoneAlarm Plus is installed and running.
	Your computer is sending (red band) or receiving (green band) network traffic. This indicator does not imply that you have a security problem, or that the network traffic is dangerous.
	ZoneAlarm Plus has blocked a communication, but your settings prevent a full-sized alert from being shown.

System Tray Menu

The system tray shortcut menu, shown below, gives you quick access to the Internet Lock and other functions. To open the menu, right-click the system tray icon.

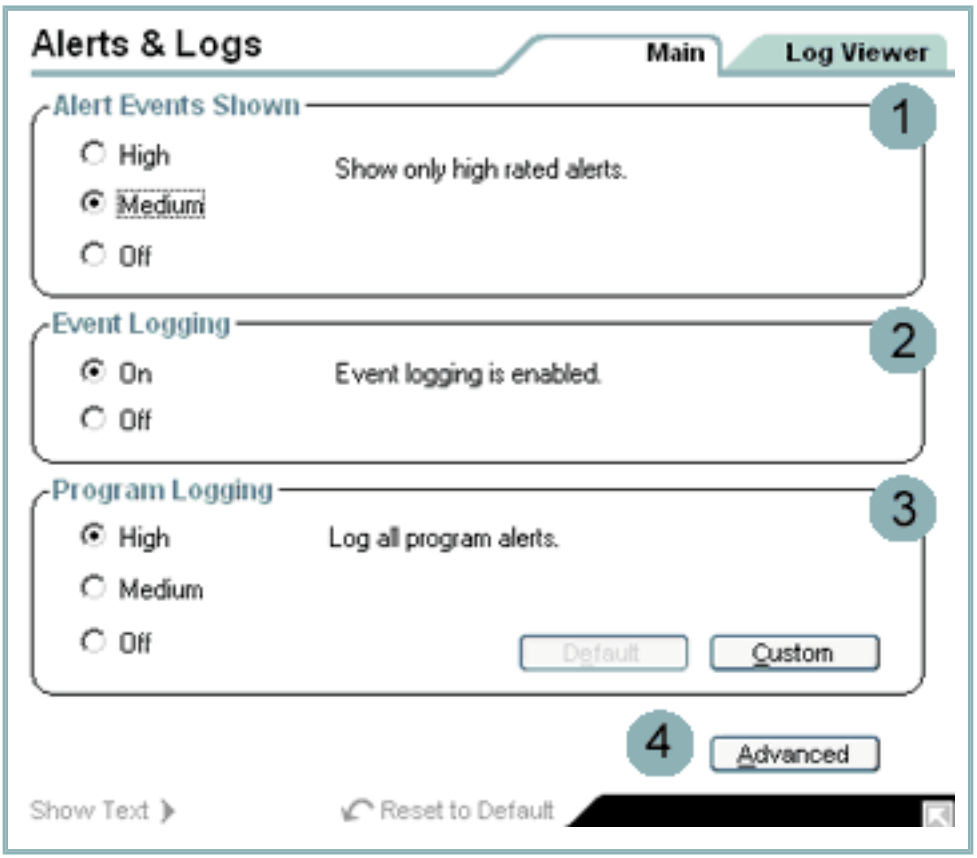


For more information about the **Engage Internet Lock** and **Stop all Internet activity functions**, see the related topic *Using the Internet Lock and Stop button*.

Related Topics

Alert Events tab
Main tab (Alerts & Logs)
Showing and hiding firewall alerts
Using the Internet Lock and Stop button

Main tab (Alerts & Logs)



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

Main tab (Alerts & Logs)

Use this tab to to choose:

- What types of informational alerts ZoneAlarm Plus will display (all, high-rated only, or none).
- What types of informational alerts ZoneAlarm Plus will log.
- What types of program alerts ZoneAlarm Plus will log.

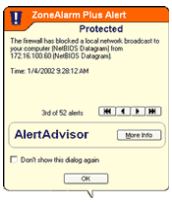
Note Program alerts are always displayed, because they ask you to decide whether to grant program access or not.

For more information about informational alerts and program alerts, see the related topic *ZoneAlarm Plus alerts.*

1 Alert Events Shown

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

The default **Medium** setting displays only high-rated alerts.



+

The **High** setting displays all firewall alerts, both medium-rated and high-rated.

For more information about informational alerts and program alerts, see the related topic *ZoneAlarm Plus alerts.*

2 Alert Events Logged

This control turns the logging of informational alerts informational alerts on and off.

3 Program Logging

This control determines what types of program alerts are to be recorded in the ZoneAlarm Plus log.

The default **Medium** setting logs only high-rated alerts.

The **high** setting logs all program alerts.

Custom Click the **Custom** button to customize program alert logging in the Program Logs tab.

If you have customized Program Logging settings, click the **Default** button to return to system defaults.

---

4 Advanced

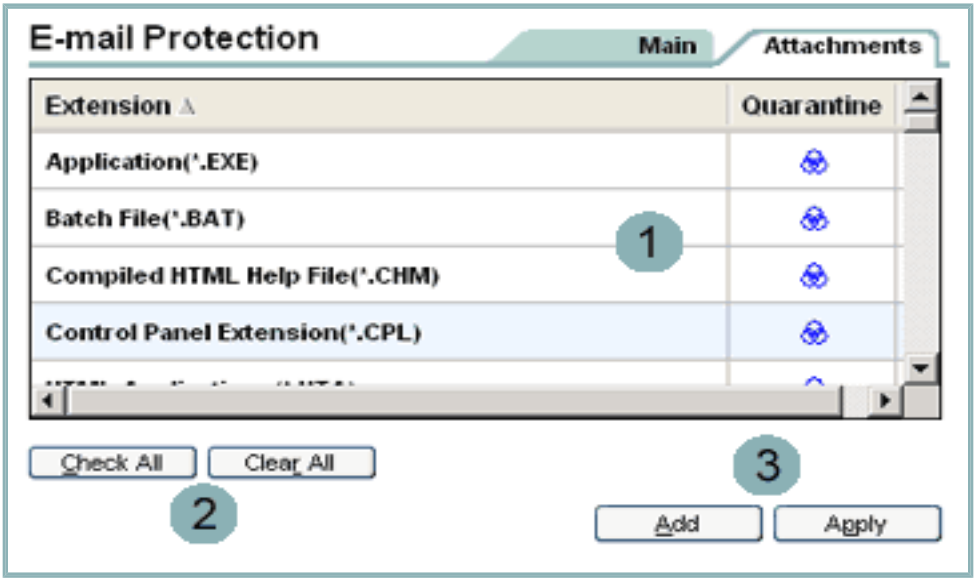
Advanced Click the **Advanced** button to open the Advanced Alerts and Log Settings dialog box. There you can:

- Specify alert display and logging by traffic type (Alert Events tab)
- Enable or disable the system tray icon alert (System Tray Alert)
- Configure your ZoneAlarm Plus log and set the archiving frequency (Log Control tab)

Related Topics

Alert Events tab
Log Control tab
System Tray Alert tab
ZoneAlarm Plus alerts

Attachments tab



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

Attachments tab

The Attachments tab lists the types of e-mail attachments that ZoneAlarm Plus's MailSafe feature will quarantine. Each attachment type is specified by its filename extension, for example, .EXE for applications.

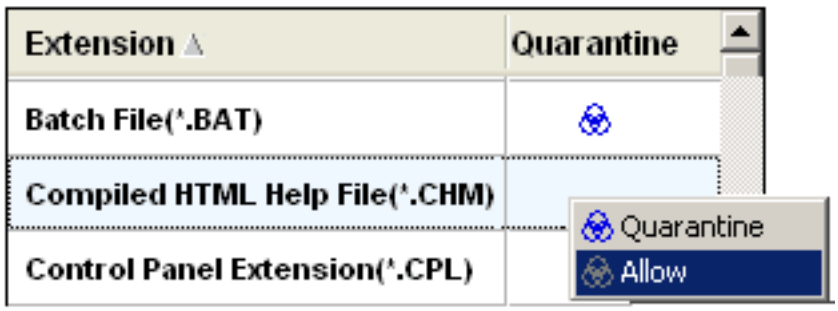
Use this tab to:

- Quarantine or allow an attachment type
- Add attachment types to the list.
- Remove attachment types from the list.

Note ZoneAlarm Plus comes preconfigured with 46 attachment types that can carry worms or other harmful code. By default, ZoneAlarm Plus quarantines all of these attachment types.

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

1 Extension / Quarantine



The Extension list displays the attachment types that can be quarantined.

You can sort the list by either 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.

To turn the quarantine function on or off for a specific attachment type, click the Quarantine column, then choose **Quarantine** or **Allow** from the shortcut menu.

---

2 Check All / Clear All

Click **Check All** to have MailSafe quarantine all attachment types in the list.

Click **Clear All** to have MailSafe allow all attachment types in the list.

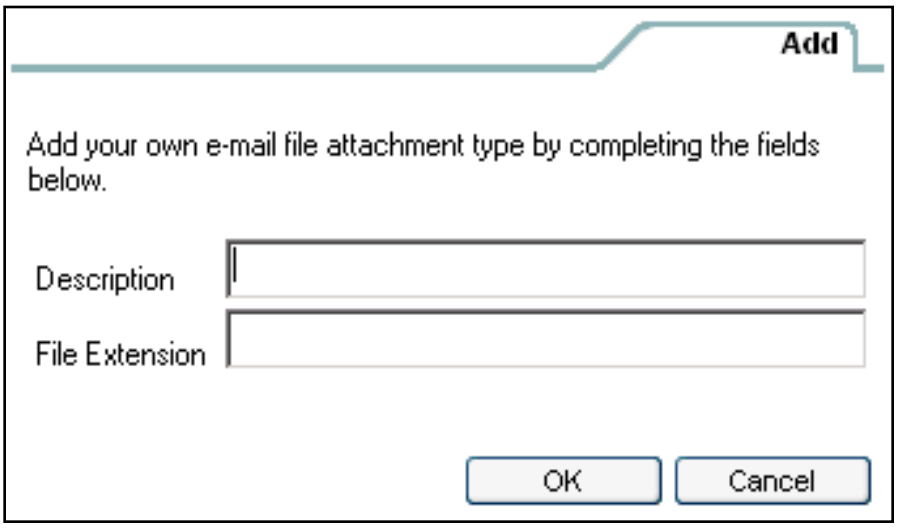
---

3 Add / Apply

Click **Add** to add an attachment type to the list using the Add dialog box.

Click **Apply** to save any changes you have made in this tab.

Add dialog box



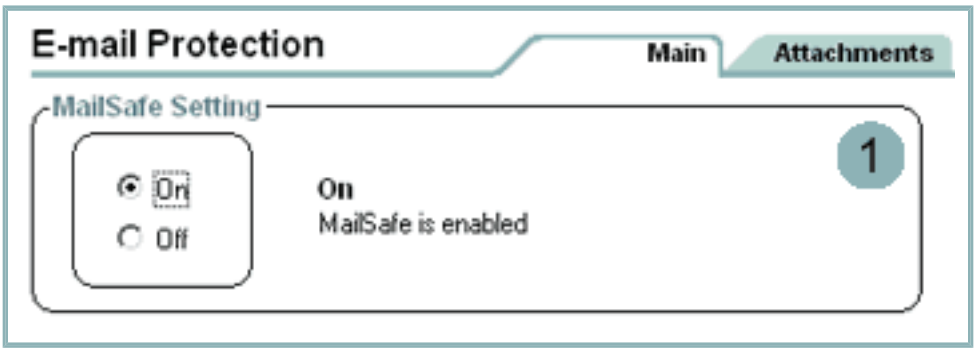
Use the Add dialog box to add an extension to the MailSafe list. To access the Add dialog, click the **Add** button in the Attachments tab.

Type a description and filename extension (with or without the "." character), then click **OK**.

Related Topics

E-mail protection

Main tab (E-mail Protection panel)



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

Main tab (E-mail protection panel)

Use this tab to turn MailSafe protection on or off.

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, the attachment types configured in the Attachments panel will be quarantined.
- If **Off** is selected, no attachments will be quarantined.

Related Topics

E-mail protection

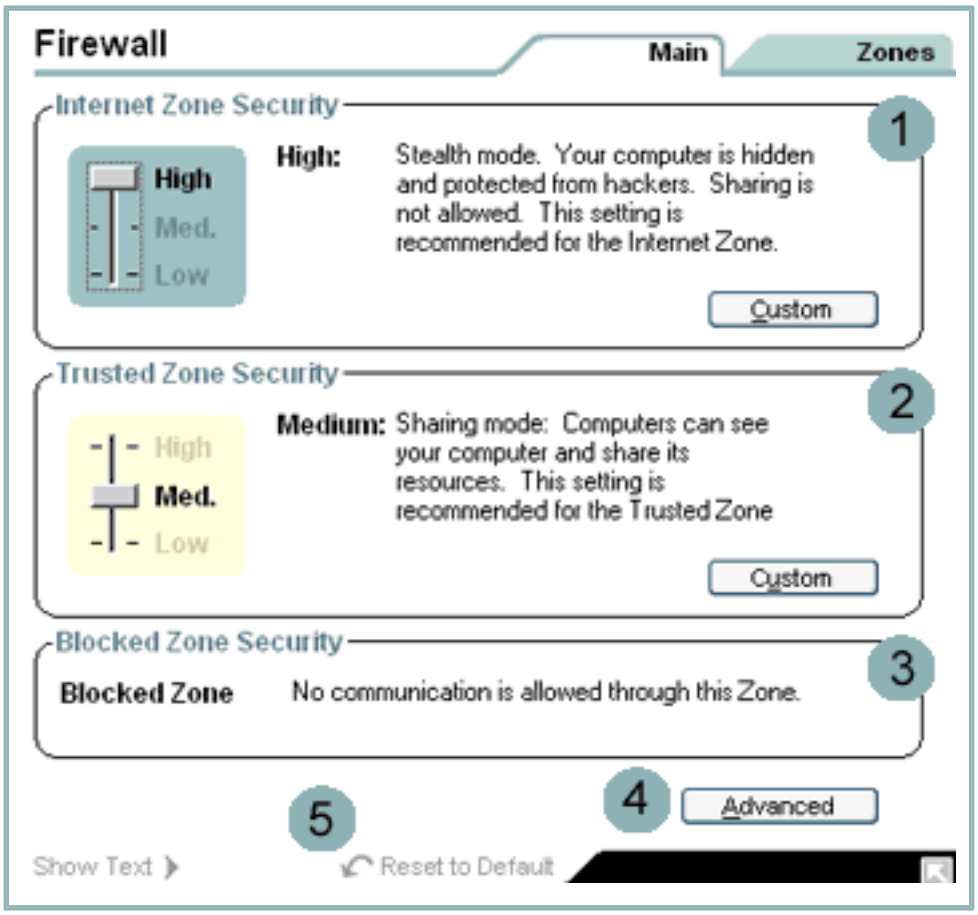
Attachments tab

Glossary

Quarantine

ZoneAlarm Plus's MailSafe quarantines incoming e-mail attachments whose filename extensions (for example, .EXE or .BAT) indicate the possibility of auto-executing code. By changing the filename extension, quarantining prevents the attachment from opening without inspection. This helps protect you from worms, viruses, and other malware that hackers distribute as e-mail attachments.

Main tab (Firewall panel)



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 Plus 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**.

Click the **Custom** button to open the Internet Zone tab, where you can block or unblock specific ports.

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**.

Click the Custom button to open the Trusted Zone tab, where you can block or unblock specific ports.

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 Restricted security

By definition, all traffic to or from the Blocked Zone is blocked by ZoneAlarm Plus.

---

4 Advanced

Click the Advanced button to access the Security tab.

---

5 Reset to Default

Click to reset the security levels for the Internet and Trusted Zones to their defaults (high and

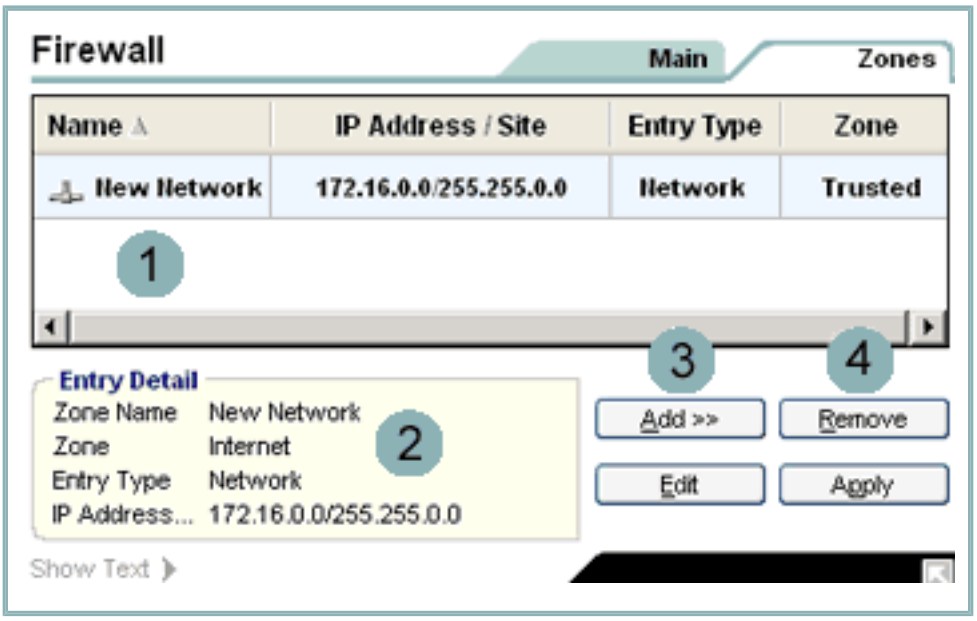
medium, respectively).

Note This does not reset the the specific port and protocol restrictions for each Zone to their defaults. To do that, click the Custom button, then use the Reset to Default button in the Custom Securities dialog box.

Related Topics

Choosing security settings
Security levels
What is a Zone?

Zones tab



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

Zones tab

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

- Move a detected network to a different Zone.
- Move a computer, host, or site to a different Zone.
- Manually add a computer, host, site, or subnet to the Trusted Zone or Blocked Zone.

Tip If you are using a single, non-networked PC, you don't need to use this tab. The traffic source list displays only your ISP's network, which should be in the Internet Zone.

1 Traffic source list

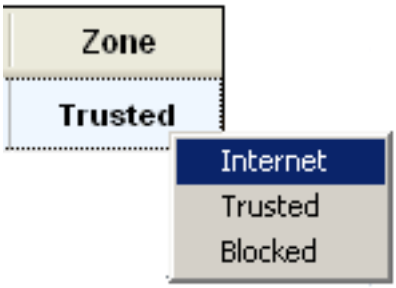
The list displays the traffic sources and the Zones they belong to. You can sort the list by any field

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

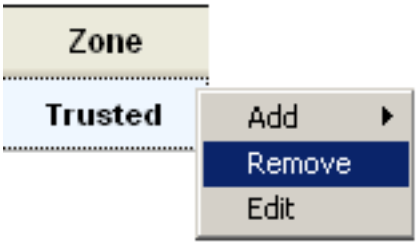
Field	Information
Name	The name you assigned to this computer, site, or network
IP Address/Site	The IP address or host name of the traffic source
Entry Type	The type of traffic source this is: Network, Host, IP, Site, or Subnet
Zone	The Zone the traffic source is assigned to: Internet, Trusted, or Blocked.

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.

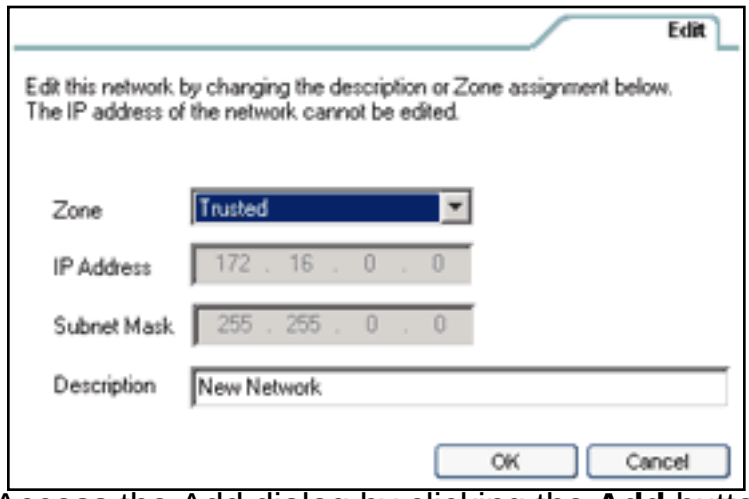
---

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



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).

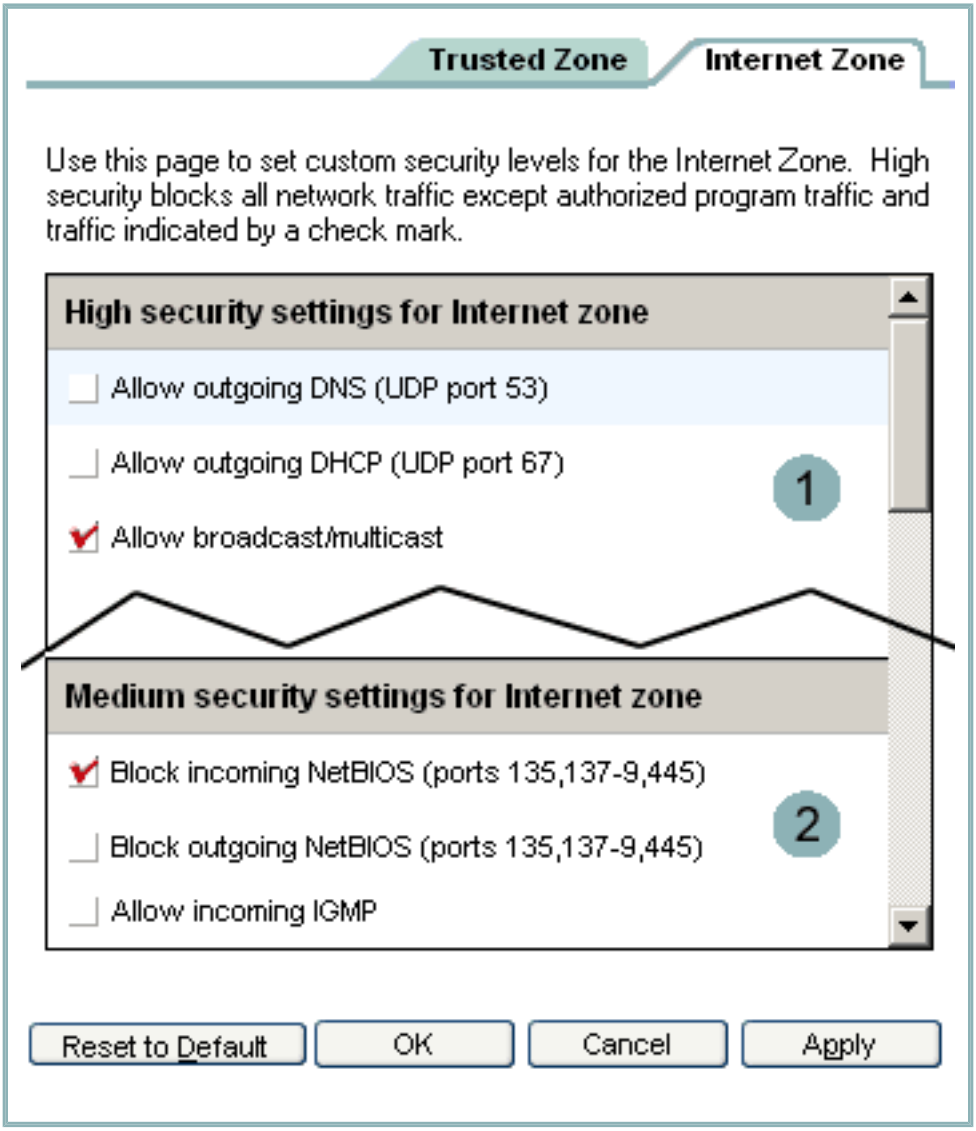
Access the Edit dialog by selecting a traffic source from the list, and clicking the **Edit** button.

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

Related Topics

What is a Zone?

Internet Zone tab



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

To reach this tab:

1. Go to Firewall / Main tab
2. Under Internet Zone Security, click the Custom button.

Internet Zone tab

Use this dialog box to customize high security and medium security settings for traffic to and from the Internet Zone.

---

1 High security settings for the Internet Zone

These are the port and protocol restrictions applied to the Internet Zone when **High** security is selected in the Main tab of the Firewall panel.

Tip To view the settings for medium security, scroll down below the high security settings.

Default configuration

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

- DHCP broadcast/multicast
- Outgoing DHCP (port 67)*
- Outgoing DNS (port 53) **

Allowing Additional Ports

You can allow communication through additional ports at high security either by selecting one of the preconfigured protocols shown (ICMP, IGMP, and so forth), or by specifying ports. To specify a ports, follow these steps:

1. Scroll to the bottom of the high security list.
2. Click the port type desired: incoming UDP, outgoing UDP, incoming TCP, or outgoing TCP. A text box labeled **Ports** appears at the bottom of the dialog box.
3. Type the ports or port ranges you want to allow in the **Ports** text box, separated by commas. **Example:** 139, 200-300
4. Click **Apply** or **OK**.

*On Windows 9x systems
**If the machine is configured as an ICS gateway in the Security tab.

---

2 Medium security settings for the Internet Zone

These are the port and protocol restrictions applied to the Internet Zone when **Medium** security is selected in the Main tab of the Firewall panel.

Default configuration

The default settings for medium security allow inbound and outbound traffic through all ports except of incoming NetBIOS raffic (ports 135, 137-139, 445). The NetBIOS protocol enables file and printer sharing on local networks. It is blocked at medium security for the Internet Zone because, if exposed to the Internet, it is vulnerable to common intrusion attempts.

Blocking Additional Ports

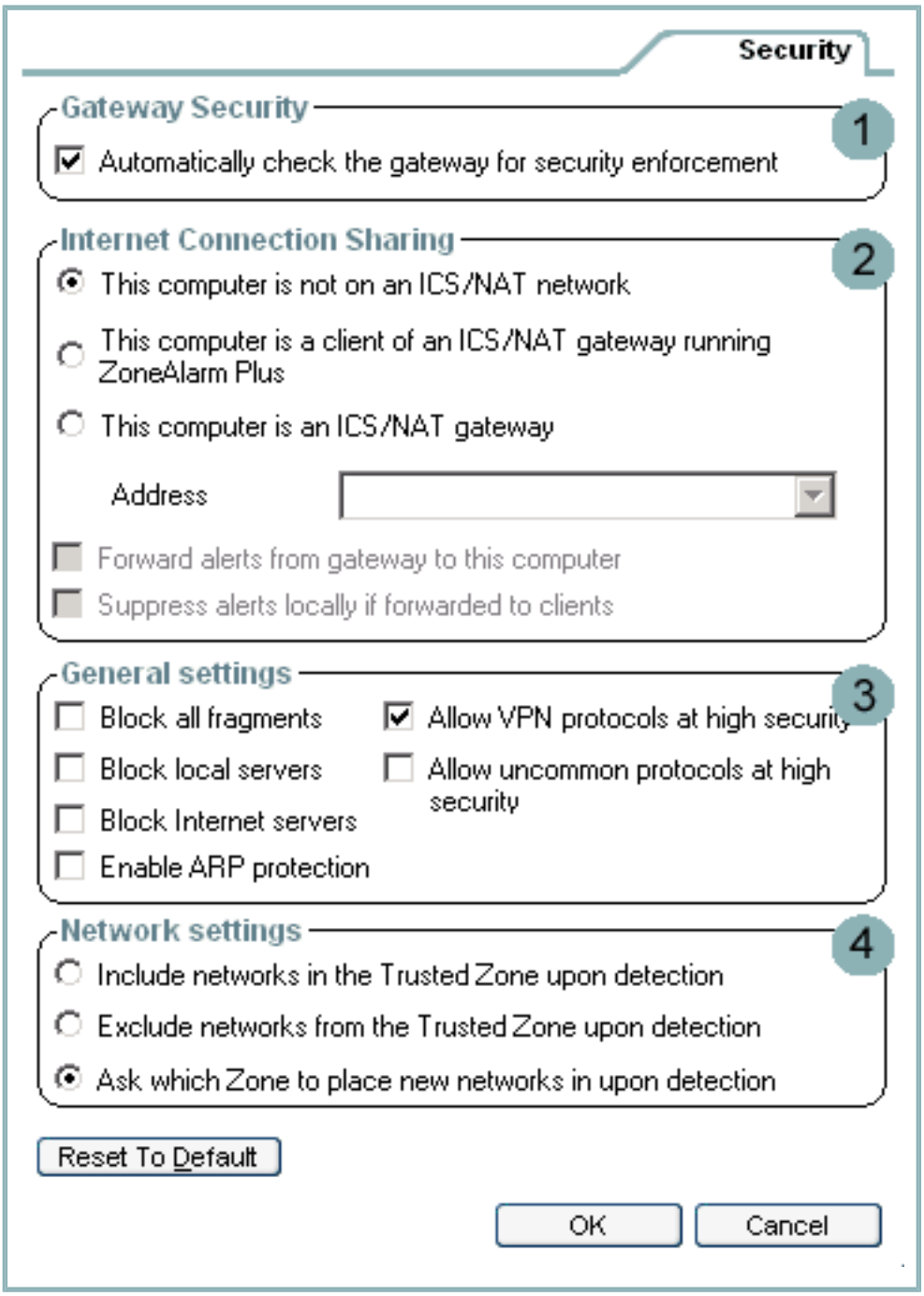
You can block additional ports at medium security either by selecting one of the preconfigured protocols shown (ICMP, IGMP, and so forth), or by specifying ports. To specify ports, follow these steps:

1. Scroll to the bottom of the medium security list.
2. Click the port type desired: incoming UDP, outgoing UDP, incoming TCP, or outgoing TCP. A text box labeled **Ports** appears at the bottom of the dialog box.
3. Type the ports or port ranges you want to block in the **Ports** text box, separated by commas.
   Example: 139, 200-300
4. Click **Apply** or **OK**.

Related Topics

Security levels

Security tab



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 Gateway Security

Some companies require their employees to use ZoneAlarm Plus when connecting to the Internet through their corporate gateway. When this control is selected, ZoneAlarm Plus checks for any compatible gateways and confirms that it is installed, so that gateways requiring ZoneAlarm Plus will grant Internet access.

You can leave this control selected even if you are not connecting through a gateway; it will not affect your Internet functions.

If you are on a network that uses gateway enforcement, and this control is not selected, you will not be able to access the network.

2 Internet Connection Sharing

If you are using Internet Connection Sharing, use these controls to configure ZoneAlarm Plus to recognize the ICS gateway and clients.

Use the radio buttons to Indicate whether your computer is an ICS client, or an ICS gateway. ZoneAlarm Plus automatically detects the IP address of the ICS gateway and displays it in the **Address** box . This box is labeled **Local Address** if you are the gateway, and **Gateway Address** if you are the client.

Note For ICS clients running ZoneAlarm Plus to work properly, the ICS gateway must run ZoneAlarm Plus as well.

Alert forwarding

You can determine whether the alerts that occur on an ICS network will be displayed and logged

on the gateway, on the client, or on both.

If you are working on a client machine, select **Forward alerts from gateway to this computer** to have alerts that occur on the gateway computer appear and be logged on the client computer.

If you are working on a gateway, select **Suppress alerts locally if forwarded to clients** if you do not want alerts forwarded from the gateway to clients to also be displayed on the gateway.

For more information, see the related topic *Internet Connection Sharing (ICS).*

---

3 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 all fragments	Blocks all incomplete (fragmented) IP data packets.
Block local servers	Prevents all programs on your computer from acting as servers to the Trusted Zone. Note that this setting overrides permissions granted in the Programs panel.
Block Internet servers	Prevents all programs on your computer from acting as servers to the Internet Zone. Note that this setting overrides permissions granted in the Programs panel.

Enable ARP protection	Blocks all incoming ARP (Address Resolution Protocol) requests except broadcast requests for the address of the target machine. Also blocks all incoming ARP replies except those in response to outgoing ARP requests.
Allow VPN Protocols at high security	Allows the use of VPN protocols (ESP, AH, GRE) even when high security is applied. When this control is not selected, these protocols are allowed only at medium security.
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.

---

4 Network Settings

Automatic network detection helps you configure your Trusted Zone easily, so that traditional local network activities such as file and printer sharing aren't interrupted.

You can have ZoneAlarm Plus silently include or exclude every detected network in the Trusted Zone; or ask you in each case whether the newly-detected network should be added.

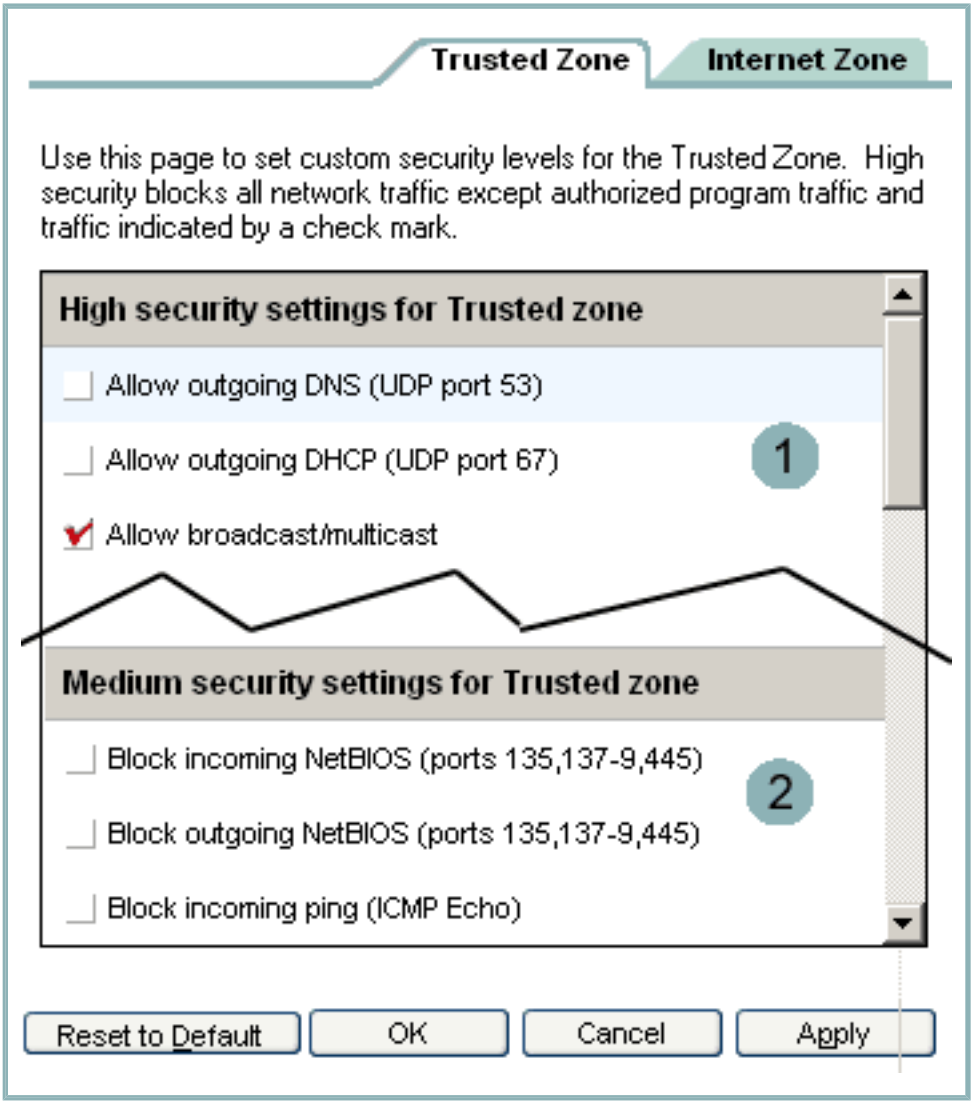
Note ZoneAlarm Plus detects only networks that you are physically connected to. Routed or virtual network connects are not detected.

Related Topics

Security tab

ICS (Internet Connection Sharing)

Trusted Zone tab



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

To reach this tab:

1. Go to Firewall / Main tab
2. Under Trusted Zone Security, click the Custom button.

Trusted Zone tab

Use this dialog box to customize high security and medium security settings for traffic to and from the Trusted Zone.

---

1 High security settings for Trusted Zone

These are the port and protocol restrictions applied to the Trusted Zone when **High** security is selected in the Main tab of the Firewall panel.

 **Tip** To view the settings for **Medium** security, scroll down below the high security settings.

Default configuration

The default settings for high security block all inbound and outbound traffic through ports not being used by programs you have given access or server permission, with the following exceptions:

- DHCP broadcast/multicast
- Outgoing DHCP (port 67)*
- Outgoing DNS (port 53) **

These protocols are permitted because they are central to basic Internet addressing functions and do not represent a serious security risk.

Allowing Additional Ports

You can allow communication through additional ports at high security either by selecting one of the preconfigured protocols shown (ICMP, IGMP, and so forth), or by specifying a port number. To specify a port number, follow these steps:

1. Scroll to the bottom of the high security list.
2. Click the port type desired: incoming UDP, outgoing UDP, incoming TCP, or outgoing TCP. A text box labeled **Ports** appears at the bottom of the dialog box.
3. Type the ports or port ranges you want to allow in the **Ports** text box, separated by commas. **Example:** 139, 200-300
4. Click **Apply** or **OK**.

*On Windows 9x systems
**If the machine is configured as an ICS gateway in the Security tab.

2 Medium security settings for Trusted Zone

These are the port and protocol restrictions applied to the Trusted Zone when Medium security is selected in the Main tab of the Firewall panel.

Default configuration

The default settings for medium security ALLOW all inbound and outbound traffic through all ports, INCLUDING incoming NetBIOS traffic (ports 135, 137-139, 445). The NetBIOS protocol enables file and printer sharing on local networks.

Blocking Additional Ports

You can block additional ports at medium security either by selecting one of the preconfigured protocols (ICMP, IGMP, and so forth), or by specifying a port number. To specify a port number, follow these steps:

1. Scroll to the bottom of the medium security list.
2. Click the port type desired: incoming UDP, outgoing UDP, incoming TCP, or outgoing TCP. A text box labeled **Ports** appears at the bottom of the dialog box.
3. Type the ports or port ranges you want to block in the **Ports** text box, separated by commas.
   Example: 139, 200-300
4. Click **Apply** or **OK**.

Related Topics

Security levels

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.

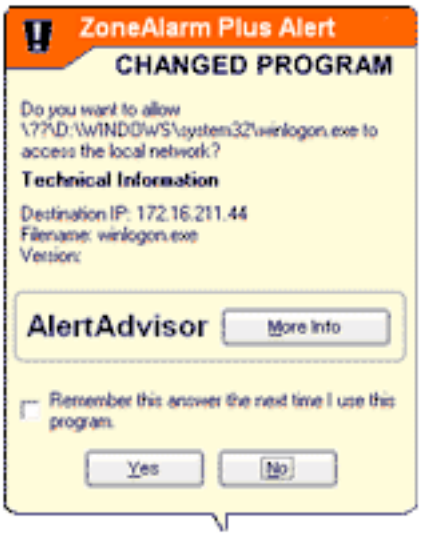
ZoneAlarm Plus protects you from malware attacks

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

- **Program authentication.** ZoneAlarm Plus makes sure your programs haven't been tampered with.
- **Program access control**. ZoneAlarm Plus 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 Plus authenticates it via its MD5 signature.



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

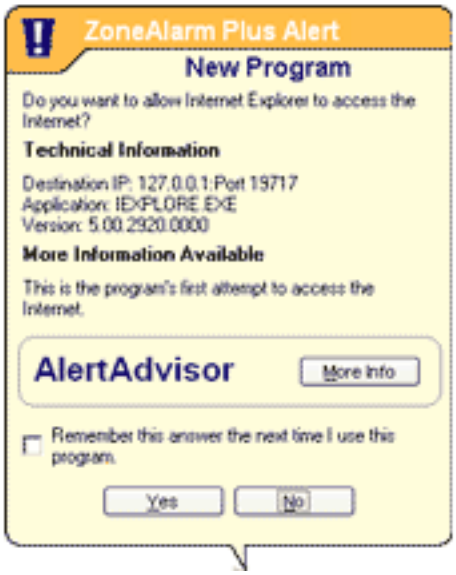
For added security, ZoneAlarm Plus also authenticates the components (for example, DLL files) associated with the program's main executable file. If a component has been altered, you'll see a Program Component alert similar in appearance to a Changed Program alert.

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

Program Access Control

When you're using ZoneAlarm Plus, 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...



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.

A Program Component alert (similar to a new program alert) lets you know if the program is using a component that is new or has changed.

If the same program requests access again...

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 Plus will silently block or allow the program.

When a program asks for server permission...

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.

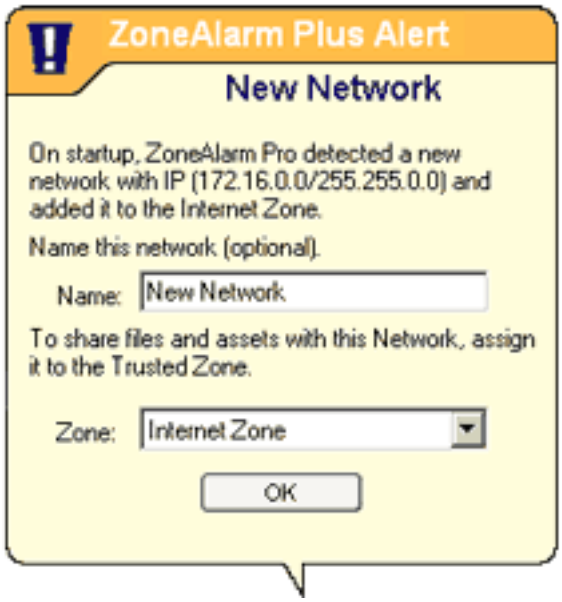
Related Topics

Program authentication
ZoneAlarm Plus alerts

Responding to alerts

When you start using ZoneAlarm Plus, you are likely to see three types of alerts: New Network 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 Plus alerts*.

New Network alert



The first time you use ZoneAlarm Plus, you will almost certainly see a New Network alert. Don't worry! This alert is a convenience tool designed to help you configure ZoneAlarm Plus.

There are two possible causes for the alert:

• ZoneAlarm Plus has detected your home or local area network.

• ZoneAlarm Plus has detected your ISP's network.

The distinction is important, because you may want to trust the computers on your home or local area network—but you probably don't want to trust all the computers connected to your ISP!

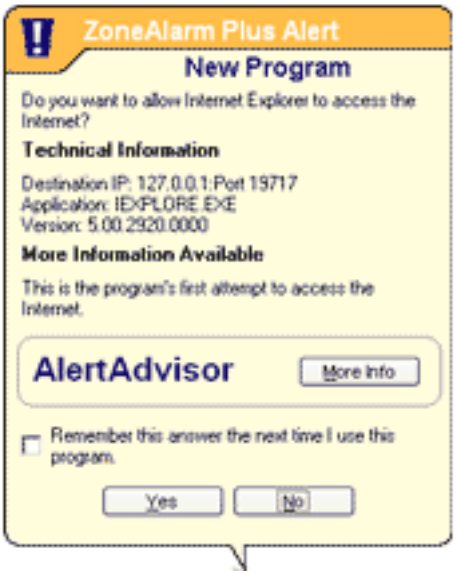
What you should do

Click the link below that best describes your situation:

- I use a home network or business LAN to connect to the Internet
- I use use a regular modem (dial-up connection), DSL, or cable modem to connect to the Internet

---

New Program alert



As you begin to work with ZoneAlarm Plus, 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")

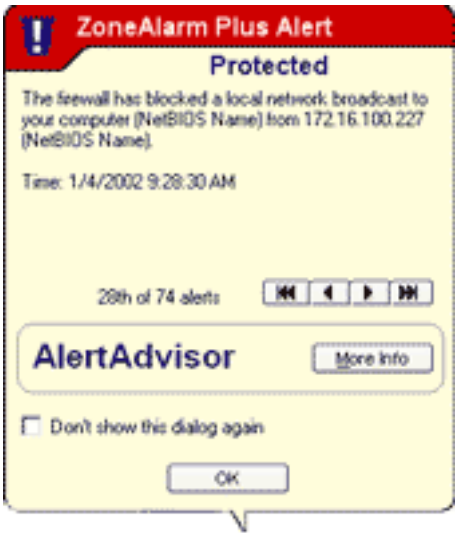
• Does it makes sense that this program would need Internet access? (For example, am I actively using this program?)

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?

Firewall alert



Firewall ("Protected") alerts occur when the ZoneAlarm Plus firewall blocks incoming or outgoing traffic based on the port and protocol restrictions set in the Firewall panel. They may have a red band at the top (for high-rated alerts), or an orange band (for medium-rated alerts).

What you should do

Click **OK** to close the alert box. You don't allow anything into your computer by doing this.

If you want to learn more about the possible causes of the alert, click **More Info.** 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 a receiving a large number of firewall alerts, and you are working on a home network or business LAN, it is possible that normal network communications are being blocked. If this is happening, you can eliminate the alerts by placing your network in the Trusted Zone. How?

Related Topics

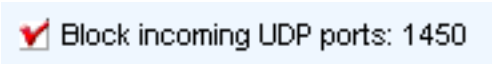
Firewall alerts
New Network alerts
New Program alerts
ZoneAlarm Plus alerts

Customizing your security

If you're not the "set it and forget it" type, ZoneAlarm Plus enables you to manage the details of your Internet security.

Firewall protection

Block or unblock ports



ZoneAlarm Plus's preconfigured security levels (Low, Medium, and High) specify the ports that are open or closed to each Zone. Customize security levels by blocking or unblocking specific ports in the Internet Zone tab and the Trusted Zone tab.

Use the Security tab to customize general firewall options.

Program control

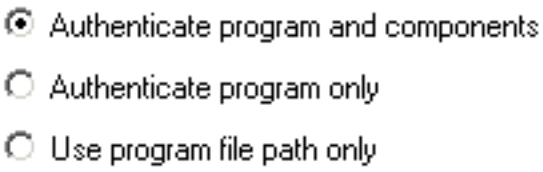
Allow or block new programs

ZoneAlarm Plus asks your permission each time a new program wants access or server rights. To avoid seeing these alerts, you can automatically allow or block new programs using the Access Permissions tab.

Specify the ports a program can use

By default, programs given access permission or server permission can use any port. Tighten program security by specifying the types of servers each program can access, and the ports it can and cannot use, in the Ports tab.

Customize authentication for a program



For each program, you can specify whether ZoneAlarm Plus will authenticate the base executable only, or the executable and the components it loads. If a program is frequently updated, you can avoid repeated alerts by using file path authentication only. Choose these options in the Security tab of the Program Options dialog box.

Alerts and logs

Show or hide informational alerts for specific firewall events

By default, ZoneAlarm Plus displays informational alerts for firewall events only if they are likely to have resulted from hacker activity. You can customize alert display by enabling or suppressing alerts for specific events in the Alert Events tab.

Enable or suppress logging for firewall events

You can also enable or suppress log entries for specific firewall events, also in the Alert Events tab.

Enable or suppress logging for program events

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

E-mail protection

Quarantine or allow specific attachment types

MailSafe quarantines 37 types of e-mail attachments. You can turn off quarantining for any type of attachment, or add more types of attachments to the quarantine list, in the Attachments tab.

Choosing security settings

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

Tip If you are an expert computer user and you want to take control of the details of your security, see the related topic *Customizing your security.*

Security and convenience

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

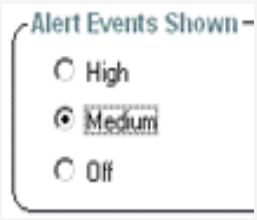
Our security professionals have chosen ZoneAlarm Plus's default security settings with this double goal in mind. They protect your computer from harm and safeguard your information, while keeping your Internet experience convenient.

---

1 ZoneAlarm Plus 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		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		Enables you to share files and printers with computers on your home or local network.
Program Control- Authentication		Programs must ask for permission and be authenticated before communicating with the Internet. **Note** Zone Labs recommends you start with this setting at **Medium**, and then raise it to **High** after a few days of normal use. This enables ZoneAlarm Plus to secure your program components without interrupting you unnecessarily. For more information, see the related topic, *Program authentication.*
Alerts & Logs		Only high rated alerts are be shown. This keeps you from being interrupted unnecessarily.
e-mail Protection		Quarantines 37 common types of e-mail attachments, like executable files (.exe) and MS-DOS applications(.com), that can contain worms or viruses.

Related Topics

Customizing your security
Program authentication

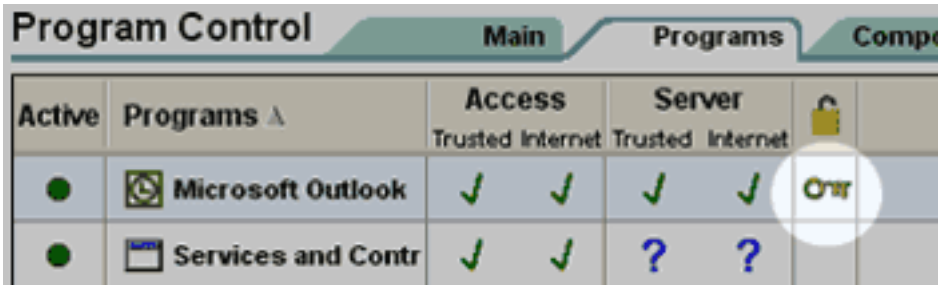
Using the Internet Lock and Stop button

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.

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

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

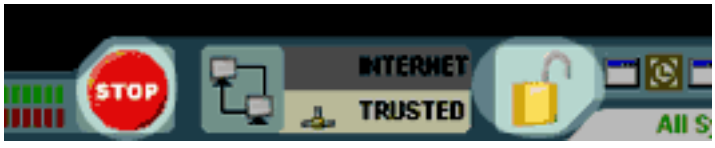
The **Internet Lock** stops all traffic to and from your computer, except traffic initiated by programs to which you have given pass-lock permission.



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 Plus 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

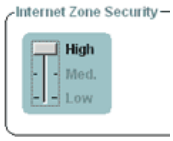
Auto-Lock tab

Setting up

Your setup is already complete!

If ZoneAlarm Plus 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 Plus'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?

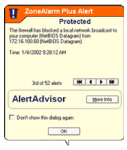
No! You don't need to close the Internet Lock except in emergency situations. For more information, see the related topic *Using the Internet Lock and Stop button.*

How do I know ZoneAlarm Plus is working?

The ZA icon in the lower right corner of your screen tells you ZoneAlarm Plus 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?



If you see alerts, don't panic! Alerts help you configure your Program Control settings, and let you know that ZoneAlarm Plus 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 Plus for your network.*

How do I customize my security?

If you are an expert computer user and you want to take control of the details of your Internet security, see the related topic *Customizing your security.*

What is a Zone?

Zones are how ZoneAlarm Plus 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.

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

ZoneAlarm Plus looks at the Zone it is in—that is, whether it is **good**, **bad**, 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 Plus 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.

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

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

Tip Advanced users can customize high and medium security for each Zone by blocking or opening specific ports. For more information, see the related topic *Blocking and unblocking ports.*

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 Plus checks in the programs list. Each program has the following permission settings:

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

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

As you use your computer, ZoneAlarm Plus 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

Adding to the Trusted Zone
Blocking and unblocking ports
Changing program permissions
Zones tab
Trusted Zone tab
Security levels

Alerts & Logging

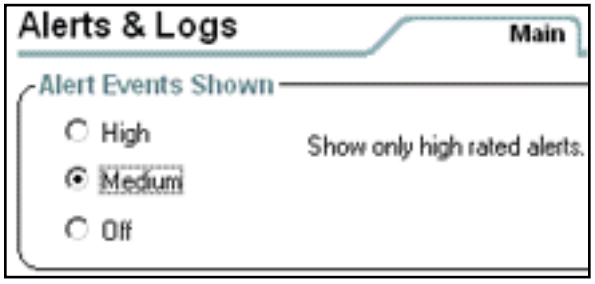
ZoneAlarm Plus's alert and logging features keep you aware of what's happening on your computer without being overly intrusive.

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.

ZoneAlarm Plus 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 Plus acts to protect you; or you can opt for quieter protection.

Alert display settings



The default **Medium** alert display setting minimizes interruptions by only showing you alerts that are high-rated--that is, that are likely to have resulted from hacker activity.

The **High** alert display setting will show you all alerts—even those probably caused by normal network traffic. If you don't want to be bothered by firewall alerts at all, just select **Off**.

Tip Use advanced alert and log settings to hide or show alerts caused by events involving specific ports, protocols, or ZoneAlarm Plus functions. How?

Logging security events

You can control logging just as completely as you control alert display. You can choose to record all alerts, only high-rated alerts, or alerts caused by specific traffic types.

ZoneAlarm Plus 3.0 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 Plus also provides easy tools for formatting and archiving text logs.

Related Topics

Showing and hiding firewall alerts
Suppressing or enabling log entries
Viewing the ZoneAlarm Plus log

E-mail protection

ZoneAlarm Plus'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 or system component can open it. Here are some examples:

.EXE (an executable file)

.JS (a javascript file)

.BAT (a batch process file)

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

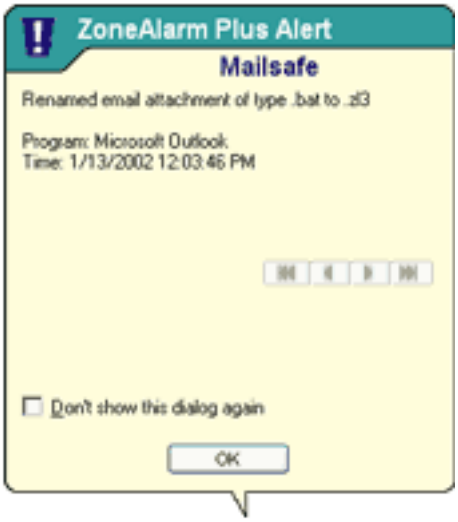
When an e-mail with an attachment arrives...

MailSafe examines the attachment's filename extension.

If that extension (in the example at right, .BAT) is in MailSafe's quarantine list, ZoneAlarm Plus changes the filename extension to ".zl*" (where * is a number or letter.)

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

When you open the e-mail containing the attachment...



ZoneAlarm Plus displays a MailSafe alert to let you know it has quarantined the attachment. Click **OK** to close the alert box.

When you try to open the attachment...

ZoneAlarm Plus 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

Attachments tab (E-mail panel)
Main tab (E-mail panel)

Firewall protection

ZoneAlarm Plus'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?

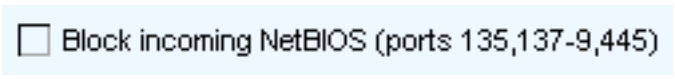
A protocol is a bit like a language—it is an agreed-on way of transmitting information. The Internet uses many protocols, and each of them is normally associated with a particular port or ports. For example, the NetBIOS protocol, which is used by Windows systems to enable resource sharing on a local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

How does it work?

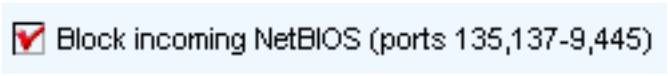
All Internet traffic—Web pages, e-mail, audio files, and so on—are transmitted in bite-sized chunks called "packets." Each packet is addressed to a particular computer, and to a particular port on that computer.

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

1. What Zone did the message come from? Trusted, Internet, or Blocked?
2. What port is it addressed to?
3. Do the rules for that Zone allow traffic through that port?
4. Are there any other rules the packet violates? (Fragmented, source-routed, etc.?)



If yes, the packet is allowed in.



If no, the packet is blocked.

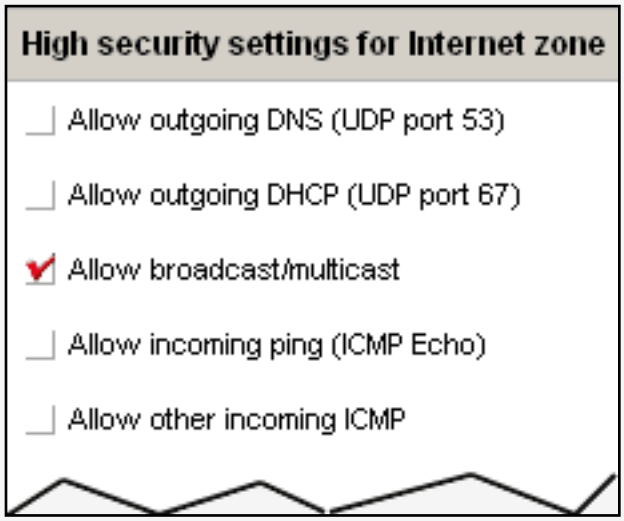
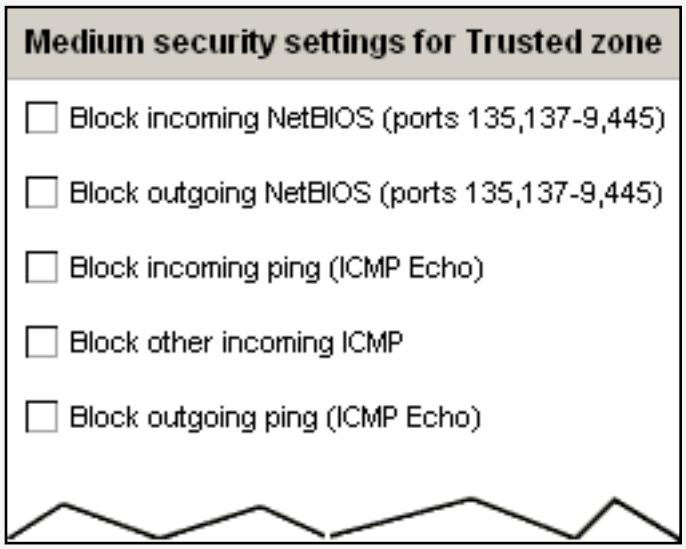
Note This describes the treatment of unsolicited traffic—that is, packets that arrive from the Internet or a local network unexpectedly. Port scans are a good example of unsolicited traffic that ZoneAlarm Plus protects you from. When a permitted program on your computer has established a communications session with another computer, Program Control rules decide what ports can be used.

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 (see the left column in the table below).

To define the meaning of each security level (that is, the ports that are blocked or allowed at that level) , use the Internet Zone tab and Trusted Zone tab in the Custom Securities dialog box (see the right column in the table below).

Zone and security level (set in the Main tab of the Firewall panel)	**What the level means** (set in Custom Securities dialog box, Internet Zone tab and Trusted Zone tab)
	
	

All ports blocked.

Related Topics

What's a Zone?
Internet Zone tab
Trusted Zone tab

Glossary

A B C D E F G H I J K L

M N O P Q R S T U V W XYZ

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 Plus 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 Plus 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. ZoneAlarm Plus prevents any communication between your computer and the machines in this Zone.

Top

C

component

A small program or set of functions that larger programs call on to perform specific tasks. Some components may be used by several different programs simultaneously. Windows operating systems provide many component DLLs (Dynamic Link Libraries) for use by a variety of Windows applications.

Top

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

DLL (Dynamic Link Library)
A library of functions that can be accessed dynamically (that is, as needed) by a Windows application.

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

Top

gateway
In networking, a combination of hardware and software that links two different types of networks. For example, if you are on a home or business Local Area Network (LAN), a gateway enables the computers on your network to communicate with the Internet.

Top

gateway enforcement
A setting in the Advanced dialog of the Firewall panel. It enables a compatible gateway device to make sure that ZoneAlarm Plus is installed on all machines accessing the Internet through it.

H

Top

high-rated alert
An alert that is likely to have been caused by hacker activity. High-rated Firewall alerts display a red band at the top of the alert pop-up. In the Log Viewer, you can see if an alert was high-rated by looking in the Rating column.

Top

HTTP referrer header field
An optional field in the message that opens a Web page, containing information about the "referring document." Properly used, this field helps webmasters administer their sites. Improperly used, it can divulge your IP address, your workstation name, login name, or even (in a poorly-implemented e-commerce site) your credit card number. By selecting Remove Private Header information in the Cookies tab, you prevent this header field from transferring any information about you.

I

ICMP (Internet Control Messaging Protocol)
An extension of the Internet Protocol that supports error control and informational messages. The "ping" message is a a common ICMP message used to test an Internet connection.

Top

ICS (Internet Connection Sharing)
ICS is a service provided by the Windows operating system that enables networked computers to share a single connection to the Internet.

Top

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 Plus 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.

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

medium-rated alert
An alert that was probably caused by harmless network activity, rather than by a hacker attack.

Top

More Info button
A button that appears in ZoneAlarm Plus 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 Plus 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

Privacy Advisor

A small display that shows you when ZoneAlarm Plus blocks cookies or mobile code, and enables you to un-block those elements for a particular page.

Top

product update service

Zone Labs subscription service that provides free updates to ZoneAlarm Plus. When you purchase ZoneAlarm Plus, you automatically receive a year's subscription to product update service.

Top

program authentication

When a program on your computer asks for Internet access, ZoneAlarm Plus examines its recorded MD5 checksum to verify that it has not been tampered with since its last request. You can set ZoneAlarm Plus 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 Plus's MailSafe quarantines incoming e-mail attachments whose filename extensions (for example, .EXE or .BAT) indicate the possibility of auto-executing code. By changing the filename extension, quarantining prevents the attachment from opening without inspection. This helps protect you from worms, viruses, and other malware that hackers distribute as e-mail attachments.

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 Plus 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 Plus 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 Plus 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

Top

Virtual Private Network (VPN)
A network that is constructed by using public wires to connect nodes. When using VPN over the Internet, encryption and other security mechanisms are used to ensure that only authorized users can access the network and the data.

W

Top

web bug

An image file, often 1x1 pixel, designed to monitor visits to the page (or HTML e-mail) containing it. Web bugs are used to find out what advertisements and Web pages you have viewed.

XYZ

(no entries)

Connecting to mail servers on a network

ZoneAlarm Plus 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 Plus 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.

Networking with ZoneAlarm Plus

File and printer sharing

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

Internet Connection Sharing

If you are using Windows Internet Connection Sharing (ICS) to share one Internet connection among several computers, set up ZoneAlarm Plus to recognize the ICS gateway and client machines. How?

Virtual Private Networking (VPN)

If you are using your computer to connect to a Virtual Private Network, configure ZoneAlarm Plus to allow VPN protocols and trust the server. How?

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?

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 Plus 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 Plus will detect your network automatically and display the New Network alert. You can use the alert itself to add your network subnet to the Trusted Zone. For more information see the related topic *New Network alert.*

Related Topics

New Network alert
Adding to the Trusted Zone

Sharing files and printers across a local network

ZoneAlarm Plus 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 Plus 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 Plus will detect your network automatically and display the New Network alert. You can use the alert itself to add your network subnet to the Trusted Zone. For more information see the related topic *New Network alert.*

Related Topics

New Network alert
Adding to the Trusted Zone

VPN (Virtual Private Network)

If you run a VPN client, ZoneAlarm Plus examines outgoing packets before encryption, and incoming packets after decryption. This prevents malicious traffic from making its way into the VPN tunnel from your computer. It also prevents any malicious traffic that might arrive on your computer via the VPN tunnel from doing any damage.

To configure ZoneAlarm Plus to protect VPN traffic:

1. Add the elements listed below to your Trusted Zone How?
    - Your VPN server or VPN concentrator
    - All of the LAN/WAN subnets that interact with the internal network that you want access to.
    - Any servers that you will need to make use of through the VPN but are not on your internal network, such as DNS, POP, or SMTP servers.
    - RADIUS or TACACS servers (if applicable).

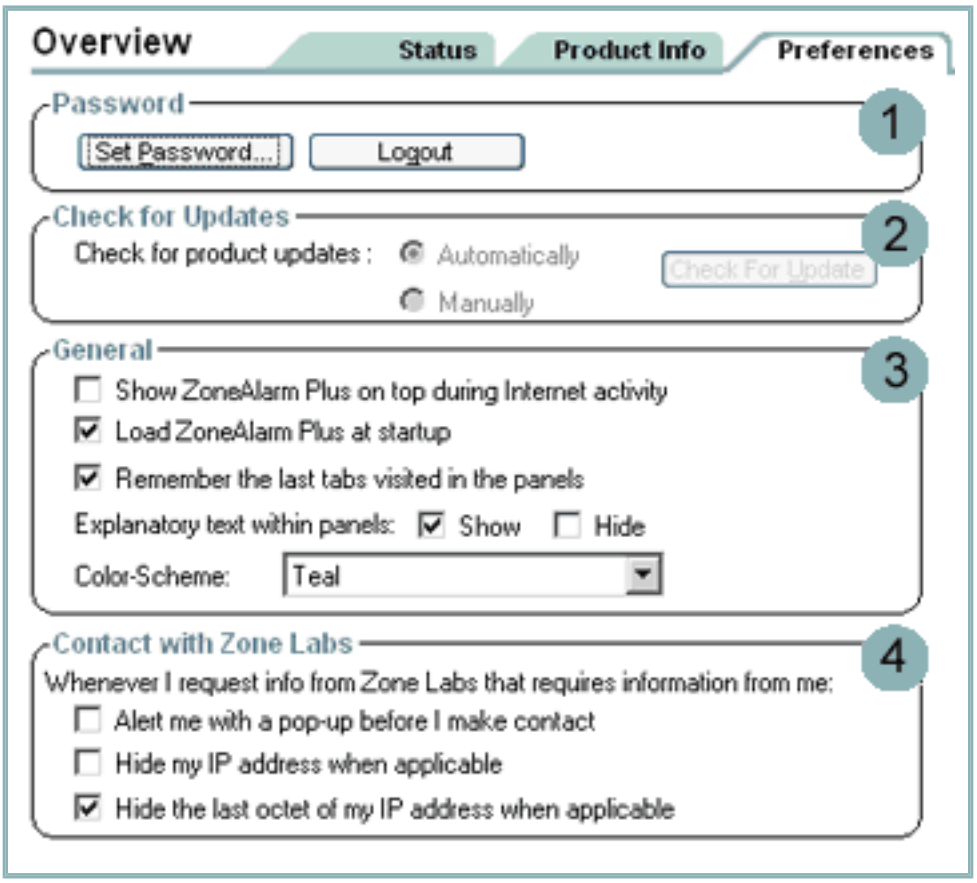
    Tip Contact your network administrator if you do not know the addresses or host names of the network elements listed.

2. If you receive a firewall alert caused by a blocked attempt to access your loopback address (127.0.0.1), add the loopback address to the Trusted Zone, and make sure there is no proxy software running on your computer.
3. In the Security tab (Advanced Settings dialog box), select **Allow VPN protocols at high security.**
4. If your VPN uses protocols other than GRE, ESP and AH, also select **Allow uncommon protocols at high security.**

Related Topics

Security tab (Advanced Settings dialog box)
Adding to the Trusted Zone

Preferences tab



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

Preferences tab

Use the Preferences tab to:

- Set or change your ZoneAlarm Plus password.
- Log in or log out.
- Configure ZoneAlarm Plus to automatically notify you of product updates.
- Set general options for the display of the ZoneAlarm Plus Control Center.
- Configure privacy settings for communications with Zone Labs.

1 Password

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

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

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

-


Note Your systems administrator may have set a password to protect security settings, or to prevent shutdown or uninstallation. If you need access to security settings or other password-protection functions but do not have the password, contact your administrator.

---

2 Check for updates

Select **Automatically** to have ZoneAlarm Plus 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**.


Tip These controls are enabled only if you have purchased ZoneAlarm Plus and if you have a current subscription to the ZoneAlarm Plus product update service.

3 General

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

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

Select **Remember the last tabs visited in the panels** to have ZoneAlarm Plus 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 Plus tab. If you select **Hide**, you can still display the text for any panel by clicking the **Show Text** link at the bottom.

4 Contact with Zone Labs

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

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

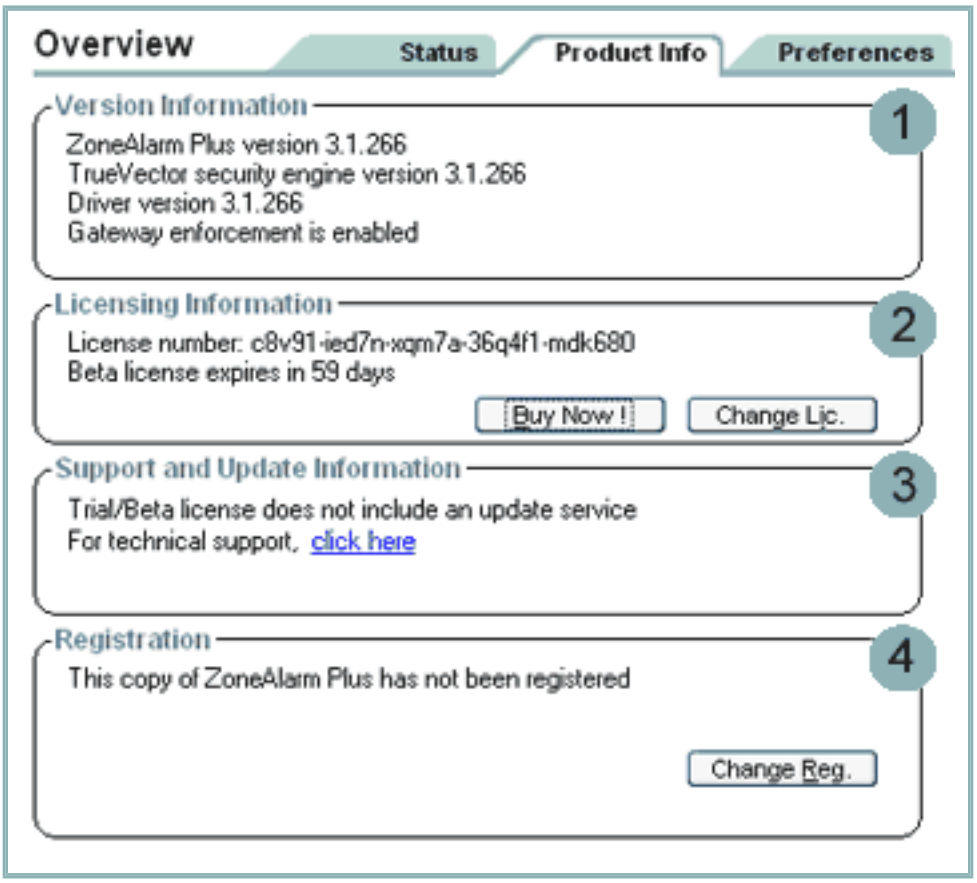
Select **Hide my IP address when applicable** to not include your IP address when you submit an alert to Zone Labs AlertAdvisor. This prevents Zone Labs, as well as anyone else who might intercept the message, from identifying your computer.

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 Plus
Setting and using a password for ZoneAlarm Plus

Product Info tab



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 Plus.

Use this tab to:

- See what version of ZoneAlarm Plus you have. How?
- Change your License key. 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 Plus, 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.

If you have a gateway license, this area also indicates whether gateway enforcement is turned on or off. "Gateway enforcement is active" indicates that ZoneAlarm Plus has established communication with the gateway.

---

2 Licensing Information

This area displays your ZoneAlarm Plus license number. If you are using a trial version of ZoneAlarm Plus, it tells you how many days are remaining in your trial period.

Click **Buy Now!** to upgrade from a trial version of ZoneAlarm Pr.

Click **Change Lic.** to change the license key under which your version of ZoneAlarm Plus is operating.

---

3 Support and Update Information

This area shows the status of your product update service. If your service has expired or is about to expire, click **Renew** to continue to get automatic updates to ZoneAlarm Plus.

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

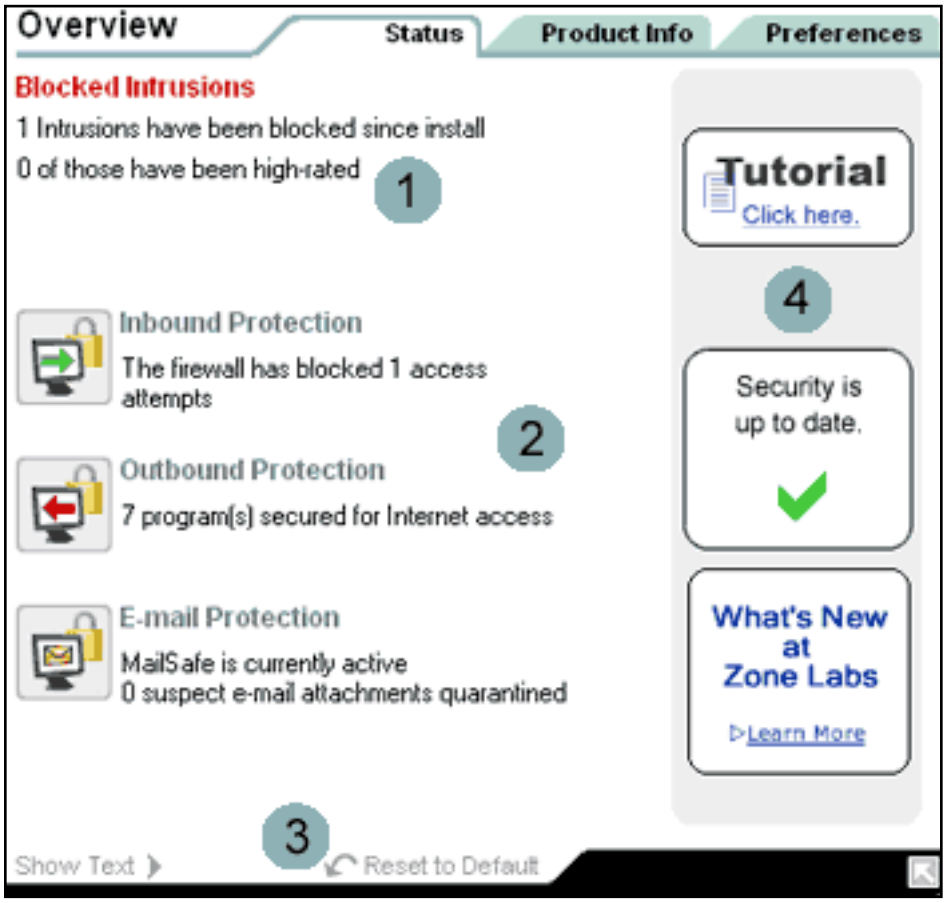
This area shows whether you have registered your copy of ZoneAlarm Plus. If your registration is "pending", you have submitted registration information, but ZoneAlarm Plus has not yet received confirmation of registration from Zone Labs.

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 PLUS Status tab



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 Plus's activity
- See if your version of ZoneAlarm Plus is up to date
- Access the ZoneAlarm Plus tutorial

1 Blocked intrusions

Blocked Intrusions shows you how many times the ZoneAlarm Plus 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 Plus will warn you if firewall security is set too low.
- How many Firewall alerts, MailSafe alerts, and Internet Lock alerts have occurred since the last reset.

Outbound Protection

Use this area to see:

- If program control is configured safely. ZoneAlarm Plus 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 Plus.

---

4 Update and tutorial information

Click **ZoneAlarm Plus Tutoria**l to learn the basics of how ZoneAlarm Plus works.

Update box

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

Message	Meaning
"Check for update"	Click the link to see if there are any important updates to ZoneAlarm Plus available for download.
"An update is available."	Your automatic update subscription indicates an update to ZoneAlarm Plus is available. Click the link to go to the Zone Labs Web site to obtain the update.

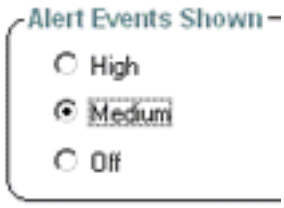
"Update subscription expired. Click to renew."	Your automatic update subscription has expired. Click the link to renew it.

Note When you purchase ZoneAlarm Plus, you receive an automatic update subscription valid for one year.

Related Topics

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

Setting the alert level



To set the global alert level for ZoneAlarm Plus:

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

Suppressing or enabling log entries

Log entries for firewall alerts

Turning firewall alert logging on or off

To turn on or off logging for firewall events and other non-program events.

1. Go to the Main tab in the Alerts & Logs panel.
2. Under Event Logging, choose **Off** or **On**.

Suppressing or enabling log entries by event type

1. Go to the Main tab in the Alerts & Logs panel.
2. Click the **Advanced** button. The Advanced Alerts and Logs dialog box opens.
3. Choose the Alert Events tab.
4. In the Log column, select the boxes for the events you want to log. Clear the boxes to suppress log entries.

Log entries for program alerts

Setting the program logging level

To set the program logging level for program events:

1. Go to the Main tab in the Alerts & Logs panel.
2. Under Program Logging, choose **High, Medium** or **Off**.

Suppressing or enabling log entries by event type

1. Go to the Main tab in the Alerts & Logs panel.

2. Under Program Logging, click the **Custom** button. The Custom Program Log Settings dialog box opens.
3. Select the boxes for the program events you want to log. Clear the boxes to suppress log entries.

Viewing the ZoneAlarm Plus 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:

1. In the Main tab of the Alerts & Logs panel, click the **Advanced** button. The Advanced Alerts & Log Settings dialog box opens.
2. Choose the Log Control tab.
3. Under Log Archive Location, click the **View Log** button.

Note By default, alerts generated by ZoneAlarm Plus 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.

Submitting alerts to AlertAdvisor

Submitting new alerts

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.

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.

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**.

Showing or hiding alerts by rating

To have ZoneAlarm Plus display alerts for medium-rated as well as high-rated firewall events:

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

Showing or hiding alerts by event type

To show or hide informational alerts for specific event types:

1. Go to the Main tab in the Alerts & Logs panel
2. Click the Advanced button. The Advanced Alerts and Logs dialog box opens.
3. Choose the Alert Events tab.
4. In the alert column, select the boxes for the events for which you want to show alerts. Clear the boxes to hide alerts.

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**.

Blocking and unblocking ports

Use controls in the Firewall panel to customize your security settings by blocking or unblocking specific ports.

Blocking or unblocking ports in the firewall

To block or unblock ports in your ZoneAlarm Plus firewall:

1. Go to the Main tab in the Firewall panel.
2. Click the **Custom** button for the Zone in which you want to adjust port settings.
3. Allow or block ports by selecting or clearing the check boxes.

Note In the Internet Zone tab and the Trusted Zone tab, scroll to the bottom of the list to access high security settings. For detailed information, see the related topics Internet Zones tab and Trusted Zones tab.

Limiting the ports a program can use

By default, programs to which you give access permission or server permission can use all ports. To restrict the ports a particular program can use:

1. Go to the Programs tab in the Program Control panel.
2. Click the program name or icon to select it.
3. Click the **Options** button. The Ports tab opens.
4. In the Ports tab, select one of the following options:
    - **Allow access for ONLY the ports and protocols checked below.**
    - **Allow access for any port EXCEPT for those checked below.**
5. Use the **Add** and **Remove** buttons to specify the ports to block or allow.

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

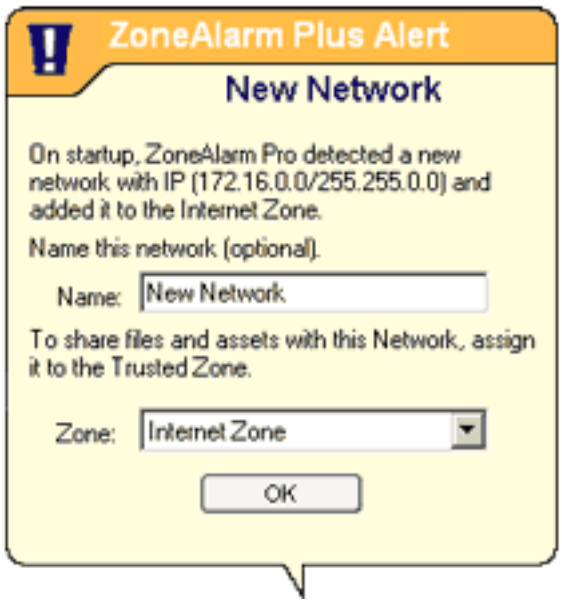
To add a host or site:

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**.

Note ZoneAlarm Plus 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 networks

Adding a new network to the Trusted Zone



If you are on a home or business Local Area Network, ZoneAlarm Plus will detect your network connection and display a New Network alert.

To add the detected network to your Trusted Zone, select Trusted Zone in the lower list box in the pop-up alert, then click **OK**.

Moving an existing network to the Trusted Zone

If you have left a detected network in the Internet Zone, follow these steps to move it to the Trusted Zone:

1. Go to the Zones tab in the Firewall panel.

2. Click the Zone field in the row containing the network, then select **Trusted** from the shortcut menu.

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**.

Getting updates to ZoneAlarm Plus

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

Hiding the ZoneAlarm Plus Control Center

To keep the ZoneAlarm Plus Control Center from opening automatically:

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

Setting and using a password for ZoneAlarm Plus

After you set a password, no one but you can change your ZoneAlarm Plus settings, shut down ZoneAlarm Plus, or uninstall ZoneAlarm Plus.

Setting or changing a password

To set a ZoneAlarm Plus password:

1. Go to the Preferences tab in the Overview panel.
2. Click the **Set Password** button.
3. Type your password and password verification in the boxes provided.
4. Click **OK.**

To change your ZoneAlarm Plus password:

1. Go to the Preferences tab in the Overview panel.
2. Click the Set Password button.
3. Type your old password in the box provided.
4. Type your new password and password verification in the boxes provided.
5. Click **OK**.

Logging in and logging out

To log in to ZoneAlarm Plus:

1. Go to the Preferences tab in the Overview panel.
2. Click the **Login** button.
3. Type your password in the box provided, then click **OK**.

While you are logged in, the **Login** button changes to **Logout**. Click it to log out.

Note You do not have to log in to be protected by ZoneAlarm Plus. If you try to change a setting without logging in, ZoneAlarm Plus prompts you for your password.

* If your version of ZoneAlarm Plus was installed by an administrator with an installation password, he can access all functions.

Adding programs to the program list

Adding programs automatically

ZoneAlarm Plus 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 Plus 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.

Allowing or blocking new programs

Access permission

To allow or block access permission for any program requesting access for the first time:

1. Go to the Main tab in the Program Control panel.
2. Click the **Advanced** button. The Advanced Program Settings dialog box opens with the Access Permissions tab on top.
3. Under Connection Attempts, choose **Always allow access** or **Always deny access** for the Zone you want to allow or block program access to.
4. Click **OK**.

Server permission

To allow or block server permission for any program requesting server rights for the first time:

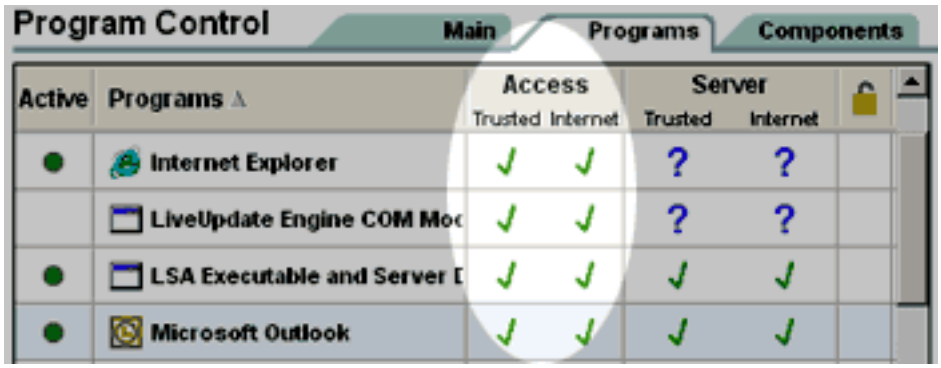
1. Follow steps 1 and 2 above.
2. User Server Attempts, choose **Always accept the connection** or **Always deny the connection.**
3. Click **OK**.

ZoneAlarm PLUS 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.

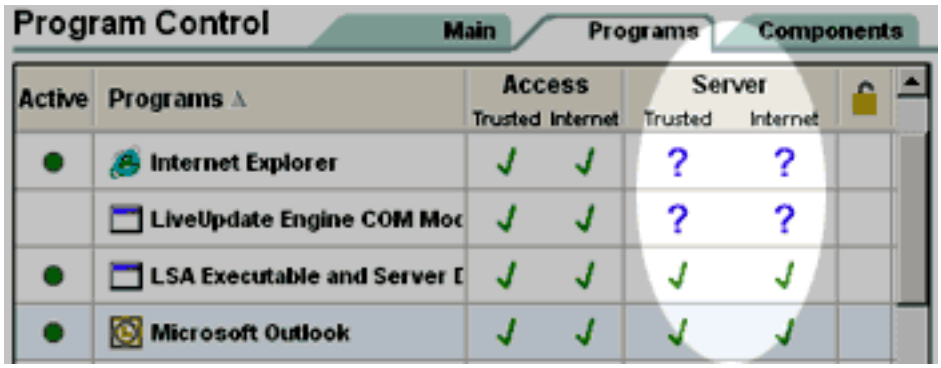


If the program is not displayed in the Programs list, click the **Add** button to locate it and add it to the list.

Blocking server permission for a program

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

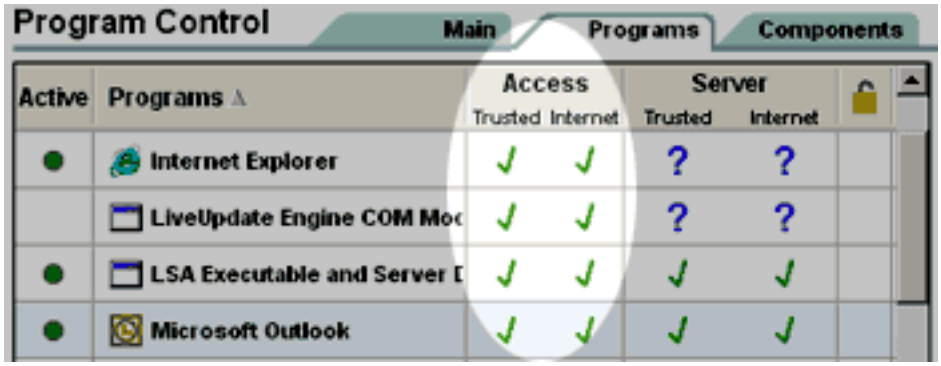
1. Go to the Programs tab of the Program Control panel.
2. Locate the program to which you want to deny server rights.
3. Click the Allow ✓ or Ask ? permission symbol in the Server column for the Zone you want to deny server rights to.
4. Choose Block ✗ from the shortcut menu.



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

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.

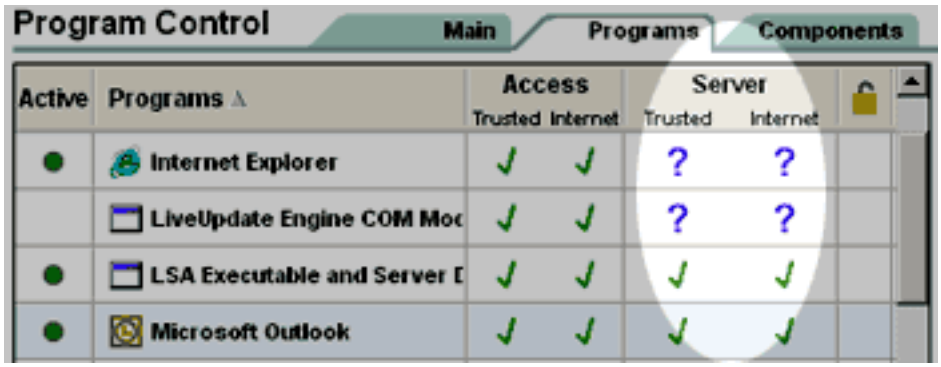
Access permission symbols

✓ = **Allow** access.

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

X = **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

Server permission symbols

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

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

 = **Block** server permission.

Investigating changed programs and components

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

Investigating changed components

When you receive a Program Component alert or Component Loading alert, It can be difficult to determine if the component is dangerous or not.

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

Follow these steps to investigate the component:

1. Go to the Microsoft support site (http://support.microsoft.com), and search the knowledgebase using the file name and description of the component as search terms.
2. Contact the technical support staff of the manufacturer of the program that loaded the changed component. They may be able to tell you why the component changed.
3. Perform an Internet search, using the file name of the component as a search term. We suggest using the Google search engine.

Turning component control on and off

To turn component control off:

1. Go to the Main tab of the Program Control panel.
2. Clear the check box labeled **Enable Component Control.**

To turn component control on:

1. Go to the Main tab of the Program Control panel.
2. Select the check box labeled **Enable Component Control.**

Deleting programs from the program list

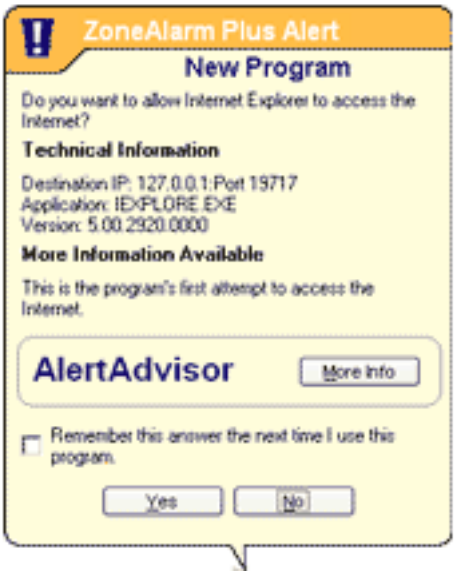
To prevent a program on your computer from accessing resources in the Internet Zone or Trusted Zone:

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 Plus 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.

Giving access permission to a program

Using alerts to give access permission



By default, ZoneAlarm Plus 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

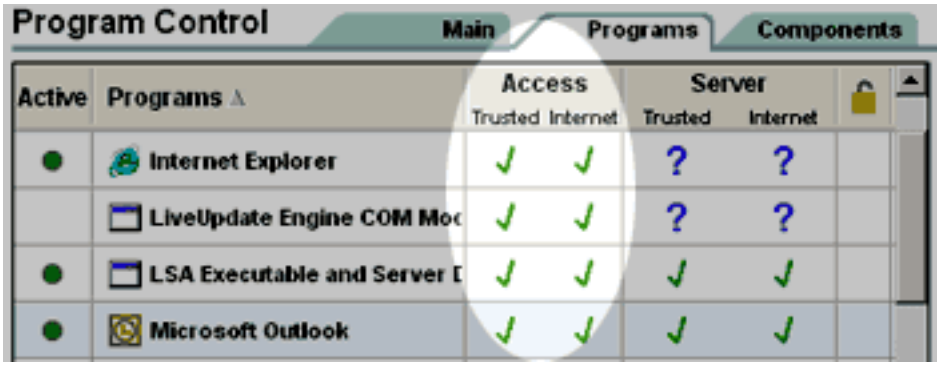
Select the **"Remember this answer..."** check box at the bottom of the alert, then click **Yes**.
The next time the program wants access, it will be allowed.

Using the Programs tab to give access permission

ZoneAlarm Plus 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.

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.

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

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.

Giving server permission to a program

Using alerts to give server permission

By default, ZoneAlarm Plus 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

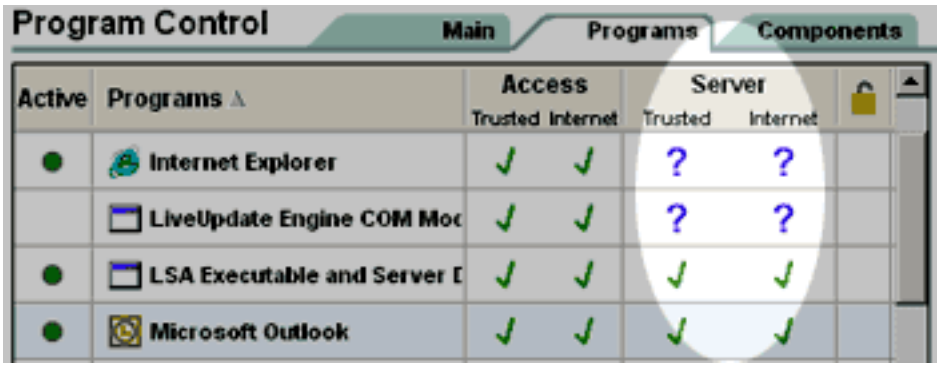
To give permanent server permission, select the the **Remember this answer...** check box at the bottom of the alert, then click **Yes**. The next time the program wants to act as a server, it will be allowed.

Tip Use the Programs tab to revoke server permission.

Using the Programs tab to give server permission

ZoneAlarm Plus 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.

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.

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.

Blocking servers

Blocking local servers

To block all programs on your computer from acting as servers to the Trusted Zone:

1. Go to the Main tab in the Firewall panel.
2. Click the **Advanced** button. The Settings tab in the Advanced Settings dialog box opens.
3. Under General, select the check box labeled **Block local servers.**

Note Choosing this setting revokes any Trusted Zone server permissions you have granted in the Programs tab.

Blocking Internet servers

To block all programs on your computer from acting as servers to the Internet Zone:

1. Go to the Main tab in the Firewall panel.
2. Click the **Advanced** button. The Settings tab in the Advanced Settings dialog box opens.
3. Under General, select the check box labeled **Block Internet servers.**

Note Choosing this setting revokes any Internet Zone server permissions you have granted in the Programs tab.

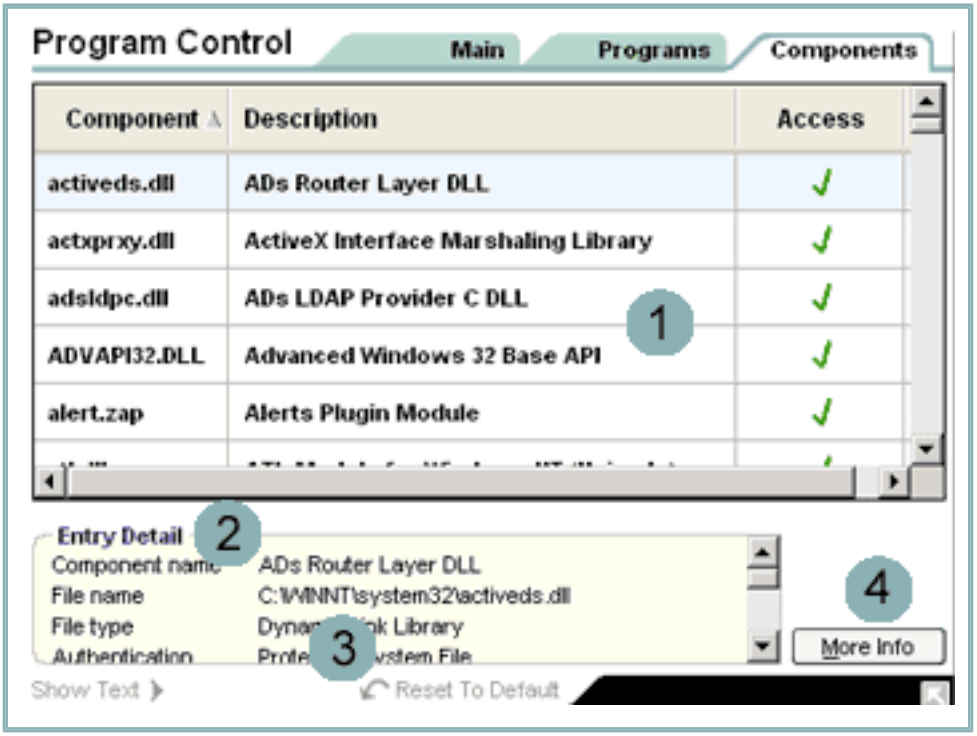
Shutting down ZoneAlarm Plus

To shut down ZoneAlarm Plus:

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

Note If you have set a password and try to shut down ZoneAlarm Plus without logging in, ZoneAlarm Plus will warn you that you do not have rights to shut down the TrueVector service. For best results, log in before shutting down ZoneAlarm Plus.

Components tab



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

Components tab

About component security

ZoneAlarm Plus's component security feature prevents hackers from employing altered or falsified DLLs and other modules used by trusted programs in order to attack your computer. Without component security, malicious programmers could modify DLLs for your trusted programs, taking advantage of the Internet access permission given to the program's main executable in order to take control of your computer.

Using the components tab

Most users never need to use the components tab, because ZoneAlarm Plus automatically secures program components.

For advanced users, the Components tab enables detailed control of specific component files. Use this tab to determine whether:

Programs that are accessing network resources can load the listed component at will.

Programs that are accessing network resources must ask permission to load the listed component (ZoneAlarm Plus displays a Program Component alert)

Note No Program Component alerts are shown if Program Control is set to **Medium** or **Low** in the Main tab.

Component learning mode

Component "learning mode" (the **Medium** Program Control setting) enables ZoneAlarm Plus to quickly learn the MD5 signatures of many frequently-used components without interrupting your work with multiple alerts. We recommend that you use this setting until you have used your Internet-accessing programs (for example, your browser, e-mail, and chat programs) at least once with ZoneAlarm Plus running.

After you have used each of your programs that need Internet access, change your Program Control setting **High.**

---

1 Component access

The Component list automatically displays all components loaded by programs that have requested access permission or server permission.

Permission for a newly listed component is automatically set to **Allow** (✓) if:

- You answered **Yes** to a Program Component alert or Component Loading alert
- Program Control is set to Medium or lower (Component learning mode)

Permission for a new component is set to **Ask** (?) if:

- You answered **No** to the Program Component alert.

Note: There is no **Block** (X) option for components.

Changing component permissions

To change access permission for a component, click in the Access column, then select **Allow** or **Ask** from the shortcut menu.

Selecting multiple components

To select a range of components from the list:

1. Select a component by clicking it.
2. Hold down the SHIFT key while dragging the mouse upward or downward.

---

2 Entry Detail

The entry detail window displays information about the component currently selected in the list.

Field	Information
Component name	The common name of the component , for example, DHCP Client API DLL
File name	The fully-qualified name of the component, for example, C:\\WINNT\system32\dnsapi.dll

File type	The type of component, for example, Dynamic Link Library
Authentication	The method used to authenticate the component. Windows Protected System Files are automatically authenticated by ZoneAlarm Plus.
Version	The version number of the component.
Created date	The date the component was created.
File size	The size of the component file.
Last written	The last time this file was modified on your machine.
Last accessed	The last time this file was accessed by a program on your machine.

3 Reset to default

Click this button to set the access permission for all components to Ask (?).

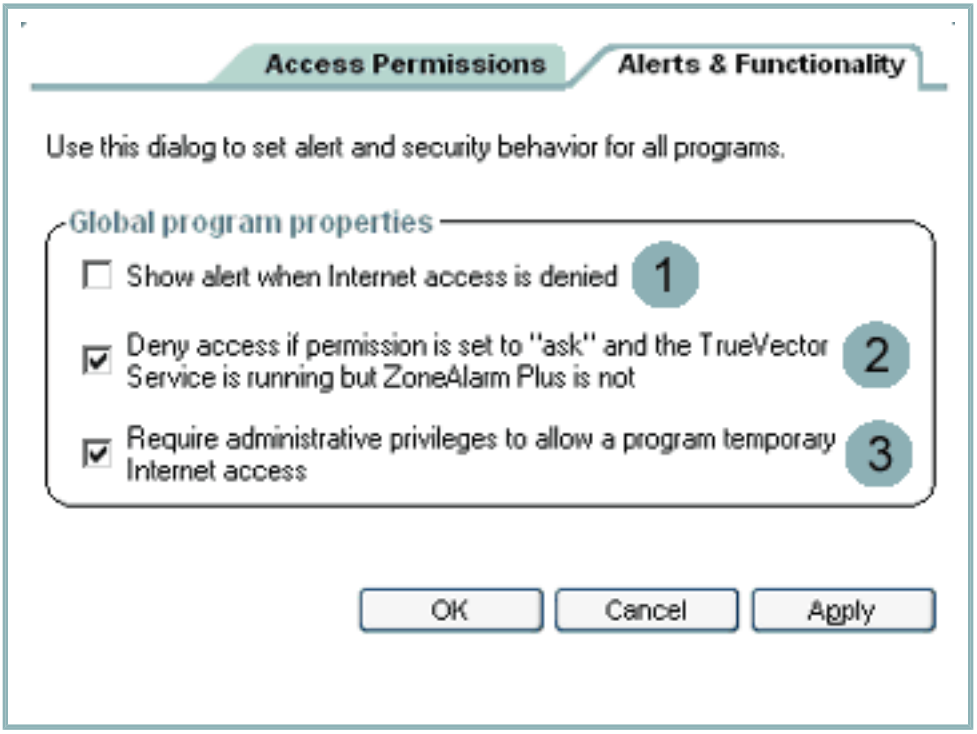
4 More Info

Click this button to set the access permission for all components to Ask (?).

Related Topics

Main tab (Program Control panel)
Program authentication

Alerts & Functionality tab



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

To reach this tab:

1. Go to Program Control / Main tab
2. Click the Advanced button.
3. Choose Alerts & Functionality

Alerts & Functionality tab (Advanced Program Options dialog)

The Alerts & Functionality tab provides access to advanced options for program control. These settings apply to all programs.

---

1 Show alert when Internet access is denied

Programs	Access		Server	
	Trusted	Internet	Trusted	Internet
XProgram.exe	X	X	X	X

If ZoneAlarm Plus is set to deny Internet access to a particular program (for example, XProgram.exe in the example at left), but you want to be notified with an alert when it attempts to gain access anyway, select this option.

If you prefer to have ZoneAlarm Plus deny access silently, deselect this option.

2 Deny access if permission is set to "ask"...

n rare cases, an independent process such as a Trojan horse could shut down the ZoneAlarm Plus user interface, but leave the TrueVector service running.

Without the interface, you would not see a Program alert when new program or a program set to "Ask" requests Internet access. This could cause the program to freeze.

Select this option to have the TrueVector engine automatically deny access to any program set to "Ask", if the ZoneAlarm Plus user interface isn't running. While the program won't be able to access network resources in this scenario, the automatic denial of access will leave it operational for other tasks (unless its tasks require network access).

3 Require administrative privileges...

If you protect your ZoneAlarm Plus settings with a password, you can't answer Yes to a program alert (thereby giving the program Internet access) unless you are logged in.

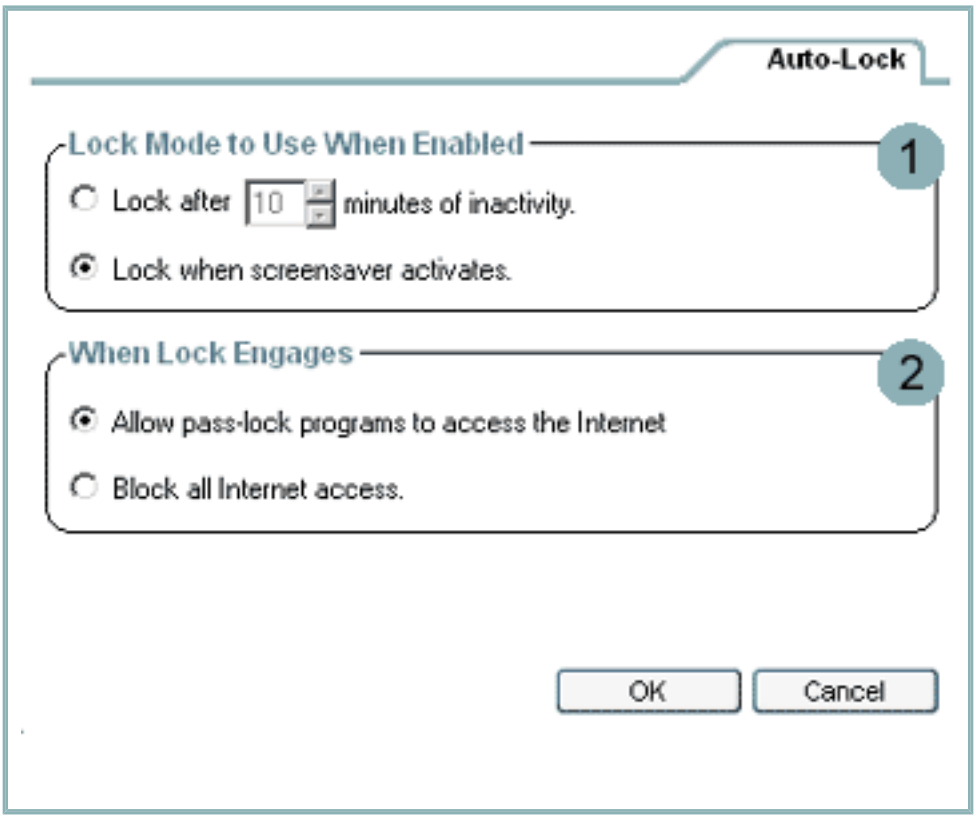
Deselect this option to allow someone who has not logged in with your ZoneAlarm Plus password to temporarily grant a program Internet access.

For information about setting a ZoneAlarm Plus password, see the related topic S*etting and using a password for ZoneAlarm Plus.*

Related Topics

Setting and using a password for ZoneAlarm Plus

Auto-Lock tab



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:

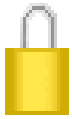
- After a period of Internet inactivity, or
- When your computer's screen saver activates.

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.

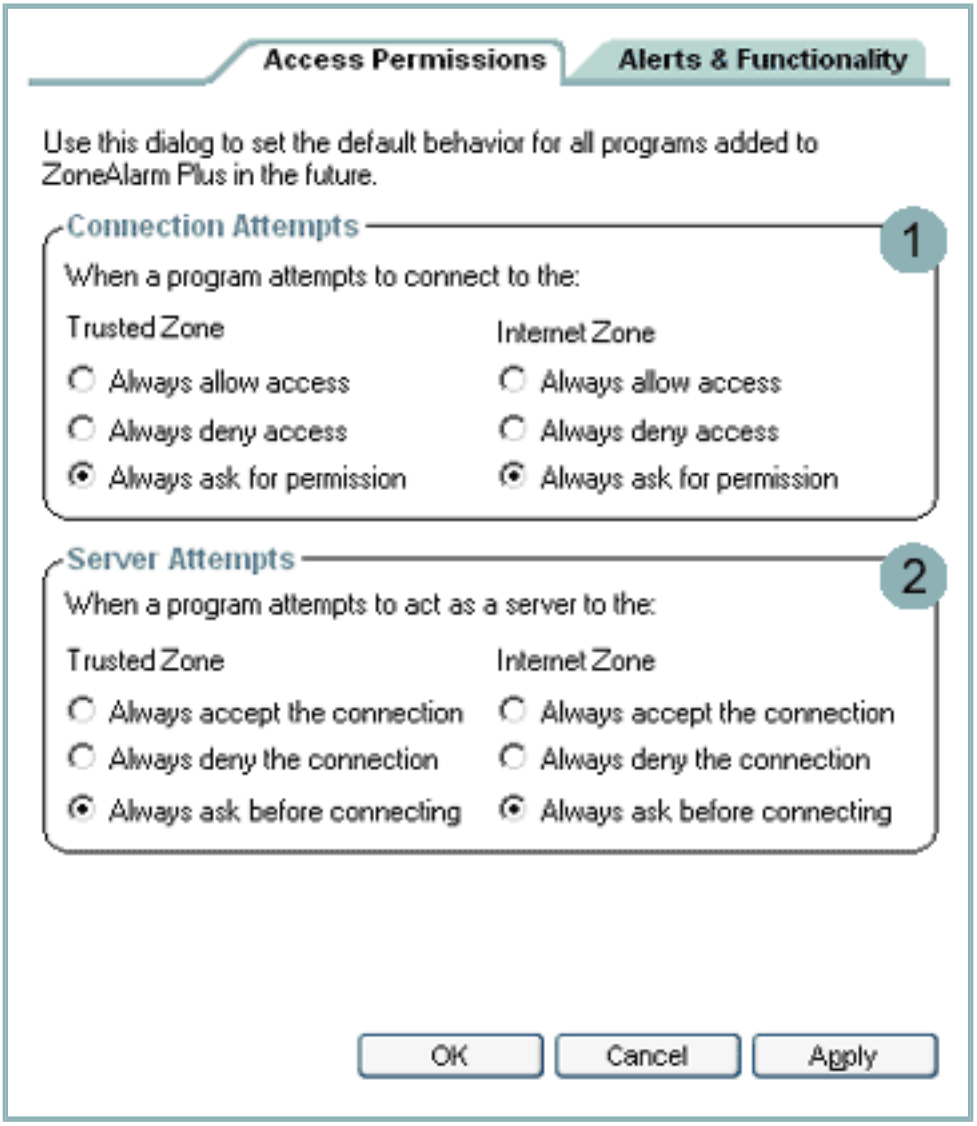
Block all Internet access is like the **STOP** button in the control bar. When the automatic lock engages, all traffic to and from your computer will be blocked.

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

Access Permissions tab



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

To reach this tab:

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

Access Permissions tab (Advanced Program Options dialog)

By default, ZoneAlarm Plus displays a New Program alert when a program on your computer tries to access the Internet or local network resources for the first time. It displays a Server Program alert when a program tries to act as a server for the first time.

Use this tab to:

- Allow or deny access permission to all new programs
- Allow or deny server permission to all new programs.

You can apply different settings to each Zone.

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

---

1 Connection Attempts

These settings determine what happens when a new program requests access permission for the Trusted Zone or Internet Zone.

Choose **Always deny...** to have ZoneAlarm Plus deny access silently

Choose **Always allow...** to have ZoneAlarm Plus allow access silently.

Choose **Always ask...** to have ZoneAlarm Plus show a New Program alert when a new program asks for access.

---

2 Server Attempts

These settings determine what happens when a new program wants server permission for the Trusted Zone or Internet Zone.

Choose **Always deny...** to have ZoneAlarm Plus deny server rights silently

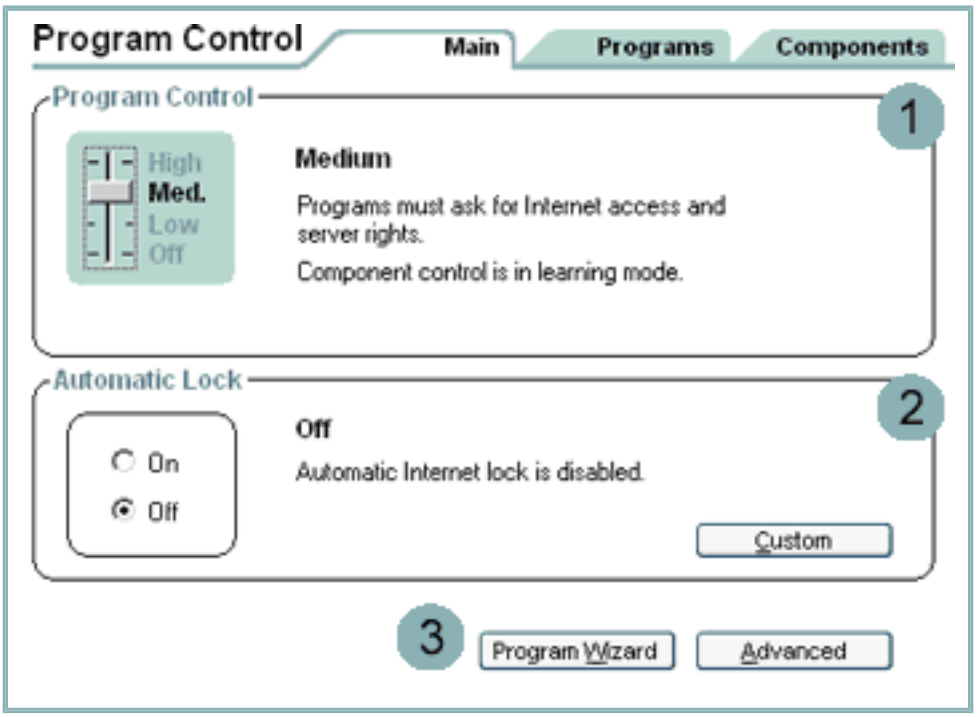
Choose **Always allow...** to have ZoneAlarm Plus allow server rights silently.

Choose **Always ask...** to have ZoneAlarm Plus show a Server Program alert when a new program asks for server rights.

Related Topics

Program control

Main tab (Program Control panel)



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.

Note Component control is currently not supported for Windows NT. If you are running NT and raise Program Control to High, you will see the message 'Program Control could not be enabled.' If you receive this message and are not running NT, try restarting your computer.

---

1 Program Control

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

Tip Zone Labs recommends the default **Medium** setting for the first few days of normal use. This enables ZoneAlarm Plus to learn and secure your program components.

High

- Programs and components are authenticated. More Info.
- Program permissions are enforced.
- Possible alerts:
  - New/Repeat/Changed Program
  - Server Program
  - Program Component / Component Loading

Medium (Component learning mode)

- Programs are authenticated; components are learned. More Info
- Program permissions are enforced.
- Possible alerts:
  - New/Repeat/Changed Program
  - Server Program

About component learning mode

Component "learning mode" (the **Medium** Program Control setting) enables ZoneAlarm Plus to quickly learn the MD5 signatures of many frequently-used components without interrupting your work with multiple alerts. We recommend that you use this setting until you have used your Internet-accessing programs (for example, your browser, e-mail, and chat programs) at least once with ZoneAlarm Plus running.

After you have used each of your programs that need Internet access, change your Program Control setting **High.**

Low (Program and Component learning mode)

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

Off

- No programs or components 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 / Advanced

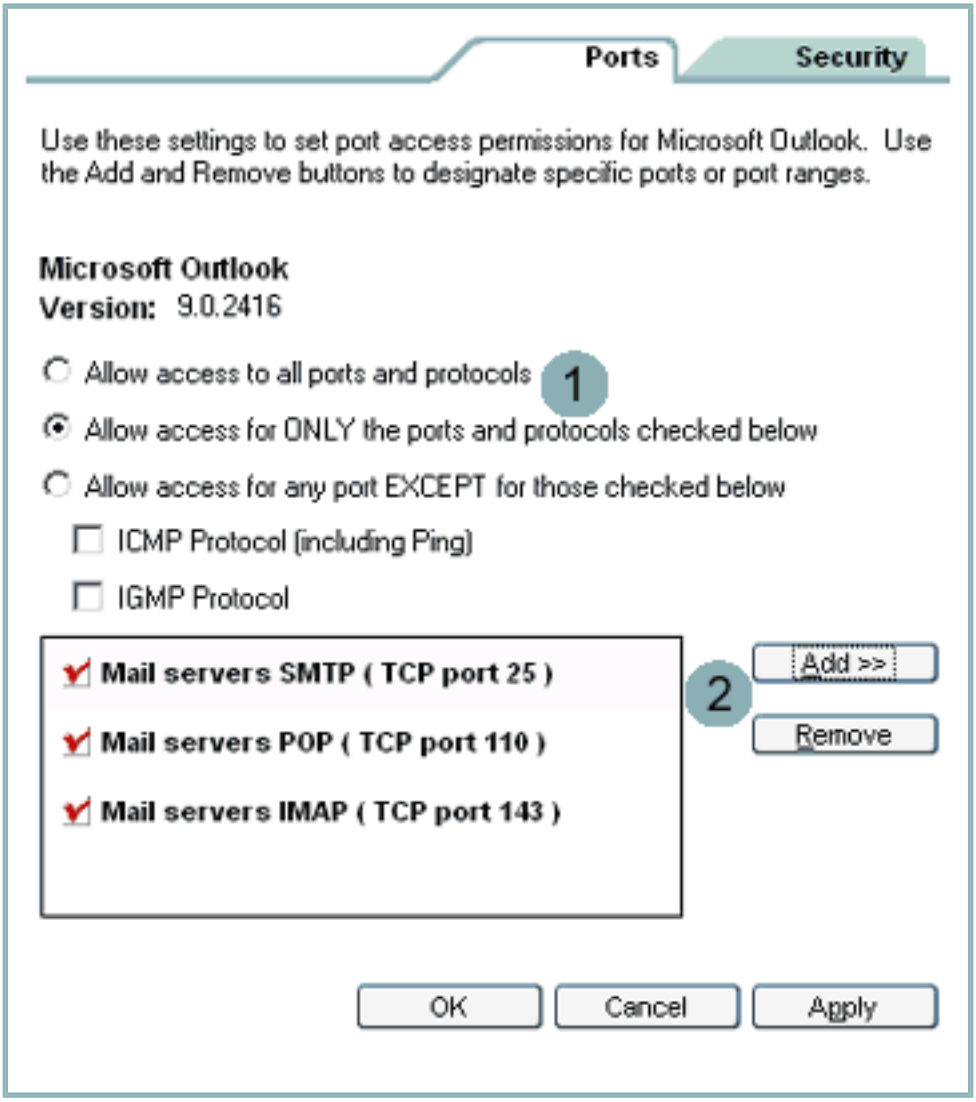
Click the **Program Wizard** button to have the ZoneAlarm Plus program wizard help you set up your programs for Internet access.

Click **Advanced** to open the Advanced Program Settings dialog box, where you can use the Access Permissions tab and the Alerts & Functionality tab to customize program control options.

Related Topics

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

Ports tab



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

To reach this tab:

1. Go to Program Control / Programs tab.
2. Select the program you want to customize.
3. Click the Options button.

Ports tab (Program Options dialog box)

Use the Ports tab to limit the ports on your computer that the selected program can use. For example, you can limit an e-mail client to SMTP, POP, and/or IMAP protocols. This provides an extra layer of security against program tampering.

Caution Use this tab to restrict a program's port access only you are very familiar with the needs of the program. Misconfiguring port permissions could cause your program to stop working properly.

1 Port and protocol options

Choose from the following options:

- **Allow access to all ports and protocols**
  The program is able to access the Internet through all ports and use any necessary protocols. (When not in use by a permitted program the ports are protected by ZoneAlarm Plus's firewall).
- **Allow access for ONLY the ports checked below**
  Select this option to limit the program's access to a few ports and protocols.
- **Allow access for any port EXCEPT for those checked below**
  Select this option to exclude only a few ports from program access.


Tip If you choose either of the last two options, use the Add button to add ports to the list.

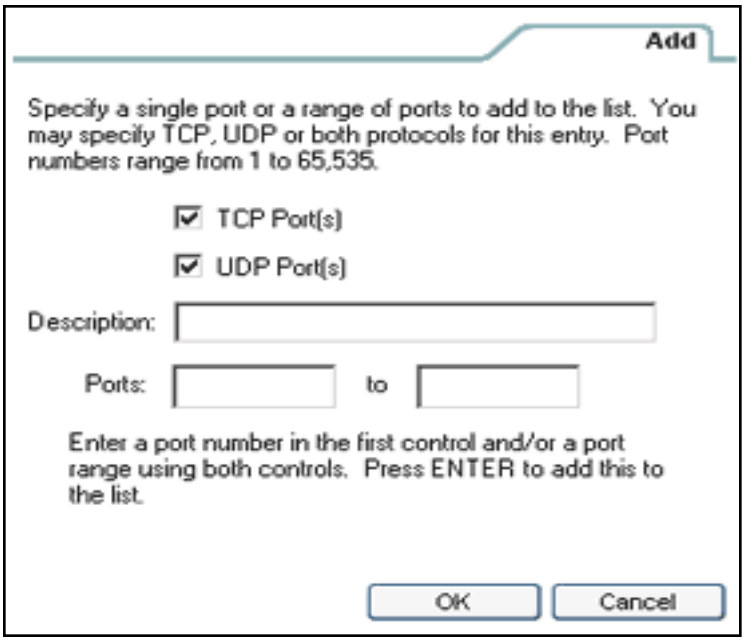
2 Adding/Removing custom ports

These controls are enabled only when **Allow access to all ports and protocols** is not selected. Use the **Add** and **Remove** buttons to modify the contents of the list.


Important! By adding to the list, you may be limiting the ports the program CAN access or CANNOT access. Be sure you have selected the option you intended at the top of the dialog box.

To add ports to the list, click the **Add** button and select the server type from the shortcut menu. To add ports other than those associated with the server types listed, choose **Custom.** The Add tab opens.

Add tab (Range of Ports dialog box)



Access this dialog box by choosing **Custom** from the Add shortcut menu.

To add a specific port or range of ports to the list:

1. Select the port type (TCP or UDP)

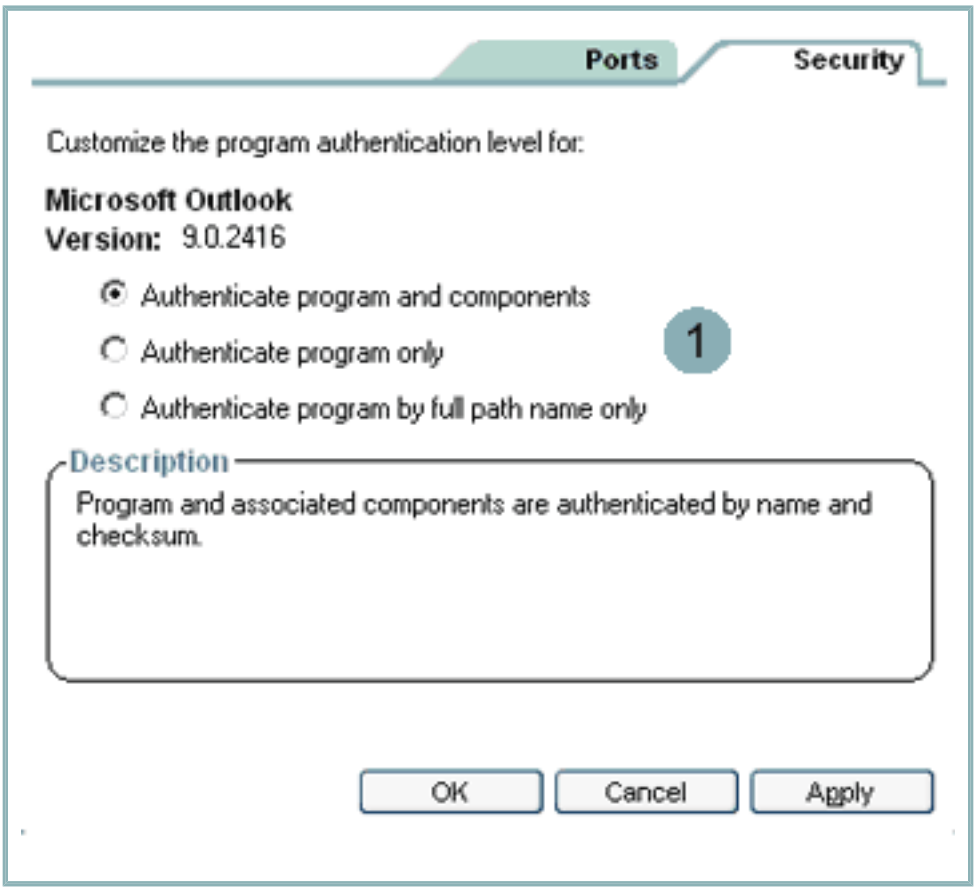
2. Type a description of the port (for display only)

3.Type the port number (if you're adding a single port) or the port range in the boxes provided, then click **OK**.

Related Topics

Program control

Security tab



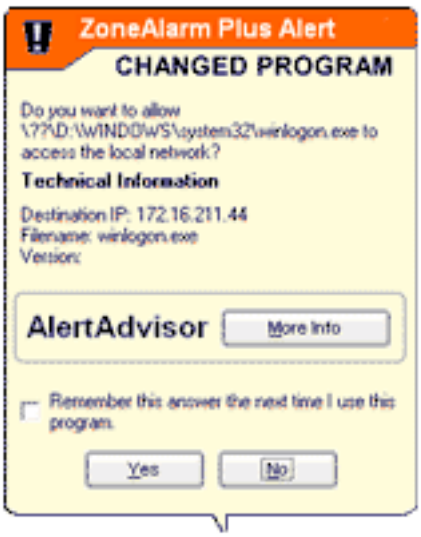
Click the numbers to learn about specific controls, or read an introduction.

To reach this tab:

1. Go to Program Control /Programs tab
2. Select the program you want to customize
3. Click the Options button.

Security tab

Use this tab to choose the type of authentication to be used for this program.



When a program accesses network resources, ZoneAlarm Plus uses the selected authentication method to ensure the that the program hasn't been tampered with. If the program has changed, ZoneAlarm Plus displays a Changed Program alert like the one at left.

1 Authentication options

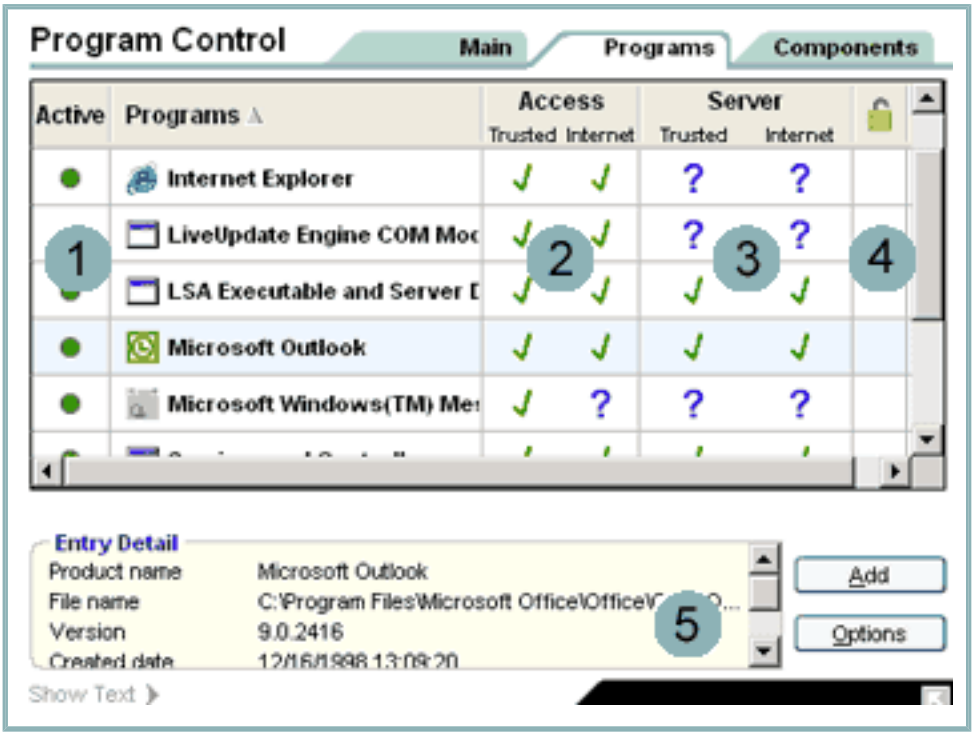
Option	If selected
Authenticate programs and components	Whenever the program accesses the Internet or your local network, ZoneAlarm Plus uses the MD5 signature to verify that it is authentic and untampered with. If the program has loaded any components, ZoneAlarm Plus authenticates them as well.
Authenticate program only	ZoneAlarm Plus authenticates the program, but allows the program to load components without authenticating them.
Use program file path only	Instead of checking the MD5 signature, ZoneAlarm Plus will only check to see that the location of the program on your computer hasn't changed. This is a low-security option, but may be useful for programs that are frequently updated.

Tip Zone Labs suggests using the **Authenticate program only** option the first two times you use an application with ZoneAlarm Plus. This enables ZoneAlarm Plus to "fingerprint" the programs components silently. After using the application twice, select **Authenticate programs and components**, so that ZoneAlarm Plus will check all components against their fingerprints when a program accesses the Internet.

Related Topics

Program authentication

Programs tab



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 Plus 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 Plus 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.

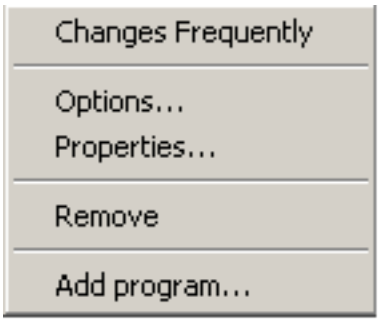
2–3 Access permission / Server permission

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 select from a variety of other options. See the table below for a description of each option.

Menu item	Description
Changes Frequently	If this option is selected, ZoneAlarm Plus will use only file path information only to authenticate the program. The MD5 signature will not be checked. **Caution** This is a low-security setting.
Options	Opens the Program Options dialog box, in which you can customize port permissions and security options for the program.
Properties	Opens your operating system's properties dialog box for the program.
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

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/Options buttons

Use these buttons to add a program to the programs list, or to access program options for the currently selected program.

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

Click **Options** to access the Ports tab and Security tab in the Program Options dialog box.

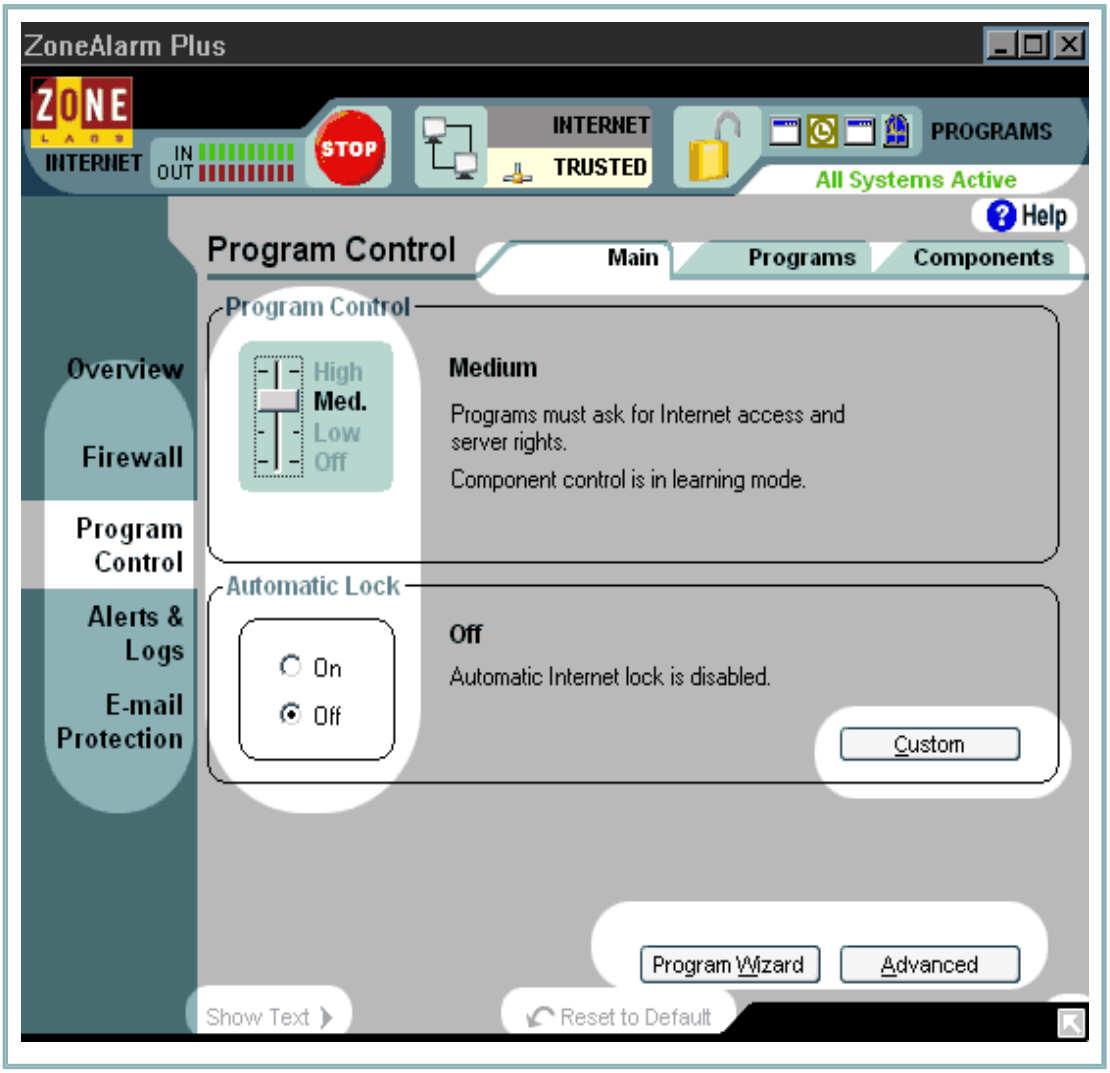
For more information about the Program Options dialog, see the related topics, *Ports tab* and *Security tab.*

Related Topics

Program control
Ports tab
Security tab

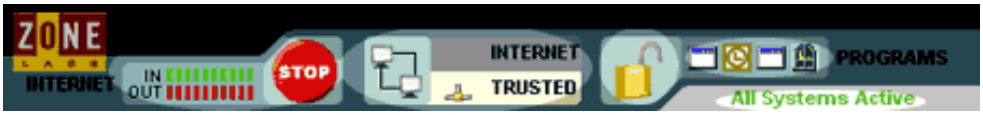
ZoneAlarm Plus Control Center

The ZoneAlarm Plus 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.



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 Plus'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.

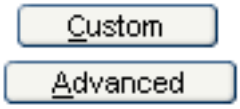
With the exception of the Overview panel, each panel in the Control Center has a Main tab and one or two other tabs. The Main tab contains the global controls for that panel.

Global Controls

The Main tabs of most panels contain global controls for each of ZoneAlarm Plus'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

The ZoneAlarm Plus dashboard

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

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*

Networks

The networks indicator shows you when you have wired or wireless networks in either the Trusted Zone or Internet Zone. In the example at left, there is one wired network in the Trusted Zone.

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

Internet Lock

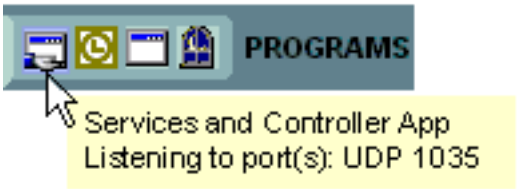
Click the lock icon to close the Internet lock. Click again to disengage.

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



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.

All systems active

This area can display two messages.

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

Related Topics

Logging in and logging out
Setting and using a password for ZoneAlarm Plus
Using the Internet Lock and Stop button

Keyboard access

All ZoneAlarm Plus functions are available through the keystrokes described below.

Navigation

Use these keystrokes to navigate through ZoneAlarm Plus'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 Plus.

Shortcut menu items

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

Programs Tab/Components 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

Attachments Tab

Keystroke	Chooses in left-click shortcut menu
Q	Quarantine
A	Allow

Zones Tab

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

Site List Tab

Keystroke	Chooses in right-click shortcut menu
A	Allow

B	Block

Keystroke	Chooses in left-click shortcut menu
R	Remove
O	Options

Button shortcuts

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

Product Info Tab

Keystroke	Equivalent to clicking this button
ALT+I	Change License
ALT+B	Buy Now
ALT+N	Renew
ALT+R	Change Reg

Preferences Tab

Keystroke	Equivalent to clicking this button
ALT+P	Set Password
ALT+O	Log in

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

Attachments Tab

Keystroke	Equivalent to clicking this button
ALT+A	Add

Dialog box commands

Use the keystrokes below when a dialog box is open.

Product Info Tab

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.

Reading log entries

By default, alerts generated by ZoneAlarm Plus 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	192.168.1.1:7138 (FW events)

	program on your computer that requested access permission	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 Plus 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 Plus 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.

Program Authentication

ZoneAlarm Plus's program authentication feature makes sure that only legitimate programs on your computer can access the Internet. Component authentication offers extra protection by verifying the shared components the program uses.

How ZoneAlarm Plus authenticates programs and components

ZoneAlarm Plus authenticates your programs and their shared components 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...

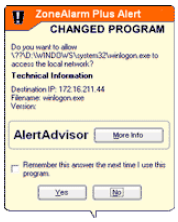
ZoneAlarm Plus adds the program to the Programs tab and records the MD5 signature of the program.

The components the program is using are added to the Components tab, and their signatures are recorded.

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

```
4839845957849O...
        ||
4839845957849O...
```

ZoneAlarm Plus compares the recorded MD5 signatures of the program and any components it is using with their current signatures.



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.

If any component signature doesn't match, or if the program is using any component that has not yet had a signature recorded, a Program Component alert is displayed. By clicking **No**, you can deny access to the program while it is using the unauthenticated component.

Note Program Component alerts occur only if the Program Control setting in the Main tab of the Program Control panel is set to **High**. At lower settings, ZoneAlarm Plus records component signatures and ads them to the component list, but does not authenticate them.

Component learning mode

Windows programs frequently load ten, twenty, or more components at a time in the course of normal operations. Component "learning mode" enables ZoneAlarm Plus to quickly learn the MD5 signatures of many frequently-used components without interrupting your work with multiple alerts. The default Medium Program Control setting establishes component learning mode. We recommend that you use this setting for the first few days of normal Internet use after installing ZoneAlarm Plus. After a few days of normal use, ZoneAlarm Plus will have learned the signatures of the majority of the components needed by your Internet-accessing programs, and will remind you to raise the Program Authentication level to High.

Related Topics

Main tab (Program Control panel)
Security tab
Changed Program alert
Program Component alert

Glossary

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.

component
A small program or set of functions that larger programs call on to perform specific tasks. Some components may be used by several different programs simultaneously. Windows operating systems provide many component DLLs (Dynamic Link Libraries) for use by a variety of Windows applications.

Security levels

ZoneAlarm Plus security levels make it easy to configure your firewall settings. You can apply a default security level (High, Medium or Low) to each Zone, or you can customize the port and protocol restrictions for each level.

High security default configuration

High security default configuration 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.

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 default configuration

Medium security default configuration 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.

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

Low security defaults allow all types of traffic.

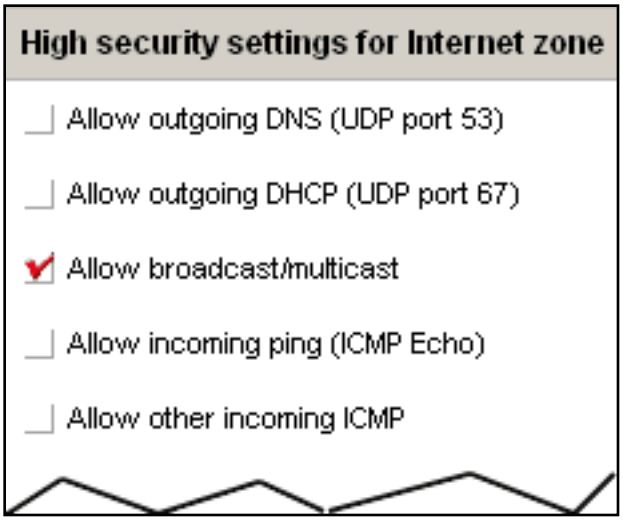
Traffic Type	High Security	Medium Security	Low Security
DNS outgoing	allow	allow	allow
DHCP outgoing	allow	allow	allow

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)	allow
		block (Internet Zone)	

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

Customizing port and protocol restrictions

You can customize the firewall configuration for each security level in each Zone by blocking or opening additional ports. Do this in the Internet Zone tab and the Trusted Zone tab.


High security settings for Internet zone
Allow outgoing DNS (UDP port 53)
Allow outgoing DHCP (UDP port 67)
Allow broadcast/multicast
Allow incoming ping (ICMP Echo)
Allow other incoming ICMP

What version of ZoneAlarm Plus do I have?

To find out what version of ZoneAlarm Plus you have:

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

Internet Connection Sharing (ICS)

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

Tip Before you configure ZoneAlarm Plus, use your ICS software to set up the gateway and client relationships. If you use hardware such as a server or router, rather than a host PC, to perform Internet connection sharing, do not follow the steps below.

On the ICS gateway machine:

1. Go to Main tab of the Firewall panel.
2. Click **Advanced**.
3. Under Internet Connection Sharing, select **This computer is an ICS gateway.**
4. In the combination box, select or type the IP address of the gateway machine.
5. Select **Suppress alerts locally if forwarded to clients** if you do not want to see alerts that are forwarded to a client. .Note that if you do not install ZoneAlarm Plus on the client machines, all alerts will be displayed on the gateway.
6. For best security, make sure the security level for the Internet Zone is set to **High**. Make sure outgoing DNS and DHCP are allowed for the Internet Zone at High security.

On the ICS client machines:

1. Go to Main tab of the Firewall panel.
2. Click **Advanced**.
3. Under Internet Connection Sharing, select **This computer is a client of an ICS gateway running ZA Pro.**
4. In the combination box, select or type the IP address of the gateway machine.
5. Select **Forward alerts from gateway to this computer** if you want alerts occurring on the gateway machine to be displayed on this client.

Using Web meeting software with ZoneAlarm Plus

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.

Making sure your browser has access permission

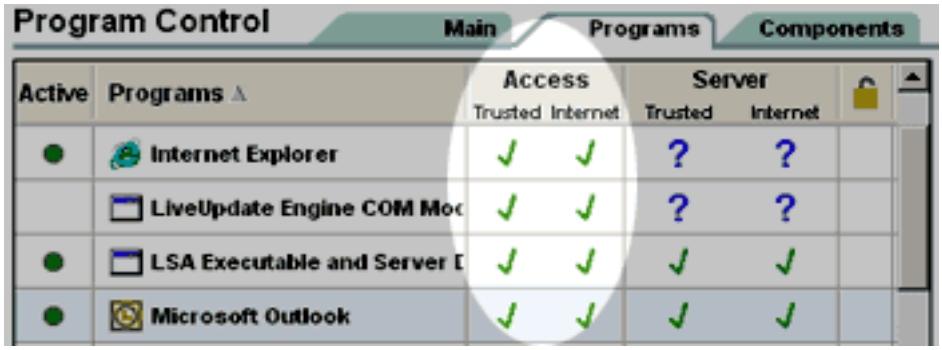
In order for your browser to retrieve Web pages, it must have access permission for both Zones.

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.



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

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

You may need to configure ZoneAlarm Plus 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 all alerts.

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

1. Click the **Advanced** button on the Main tab of the Alerts & Logs panel.
2. Click the Check All button in the **Alert Events** tab, then click **OK**.

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

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

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.

Glossary

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).

Back

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.

Back

Determining if your connection problem involves ZoneAlarm Plus

---

If you are having Internet connection trouble after installing ZoneAlarm Plus, the first troubleshooting step is to determine whether ZoneAlarm Plus 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 Plus 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 Plus 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 Plus 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 Plus at startup box), contact Zone Labs technical support.

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 Plus 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. Allow DHCP and DHCP broadcast/multicast in the Trusted Zone.
3. Make sure the security level for the Trusted Zone is medium, and that DHCP and broadcast/multicast are allowed in the Trusted Zone at medium security.

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
Blocking and unblocking ports
Adding to the Trusted Zone

Glossary

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.

Back

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.

Back

Troubleshooting Internet connection

What sort of trouble are you having?

- I can't connect to the Internet.
- I can connect, but am disconnected after a short time

Troubleshooting your Internet connection

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

1. Determine whether the problem involves ZoneAlarm Plus. How?
2. Make sure your browser has access permission and server permission. How?
3. Make sure ZoneAlarm Plus isn't blocking all servers. How?
4. Make sure ZoneAlarm Plus 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?

If you still cannot connect after doing all of the above, please contact Zone Labs technical support.

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 Plus 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 any of the three 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?

Allow ping messages through the Internet Zone.

If your ISP uses ICMP echo (or ping) messages for connectivity checks, use the Internet Zone tab (Custom Securities dialog box) to configure ZoneAlarm Plus to allow ping messages from the Internet Zone. To do this:

1. Go to the Main tab in the Firewall Panel.
2. In the Internet Zone section, click Custom
3. Select check box labeled **Allow incoming ping (ICMP echo).**

4. Click OK.

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

Internet Zone tab (Custom Securities dialog box)
Security levels
Setting Internet Zone security to medium

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.
- I can't connect to my Virtual Private Network (VPN)
- 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.

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

Using anti-virus software with ZoneAlarm Plus

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 Plus's MailSafe feature may conflict with the e-mail protection features of anti-virus software. If this occurs, you can adjust ZoneAlarm Plus and anti-virus settings so that you benefit from both anti-virus and ZoneAlarm Plus 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 Plus, enable MailSafe. How?
3. In the Alert Events tab (accessed by clicking the **Advanced** button in the Alerts & Logs Main tab), turn off alert display for quarantined MailSafe attachments.

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](#)

Using browsers with ZoneAlarm Plus

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 Plus 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 Plus . If you are using Navigator version 4.73 or higher are still experiencing difficulty accessing the web with ZoneAlarm Plus 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

Using chat programs with ZoneAlarm Plus

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

Using e-mail programs with ZoneAlarm Plus

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

Using file sharing with ZoneAlarm Plus

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 Plus.

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

Related Topics

Giving server permission to a program

Using FTP programs with ZoneAlarm Plus

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

- 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 Plus 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

Using games with ZoneAlarm Plus

In order to play games over the Internet while using ZoneAlarm Plus, 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 Plus 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 Plus 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

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

---

To use Internet answering machine programs (such as CallWave) with ZoneAlarm Plus, 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

Main tab (E-mail Protection panel)

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 Plus 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

Using streaming media applications with ZoneAlarm Plus

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 Plus.

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

Related Topics

Giving server permission to a program

Using Voice over IP (VoIP) programs with ZoneAlarm Plus

To use Voice over IP (VoIP) programs with ZoneAlarm Plus, 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

Making sure ZoneAlarm Plus isn't blocking all servers

ZoneAlarm Plus 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 local servers** and **Block Internet 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 Plus isn't blocking your ISP's servers. How?

ZoneAlarm Plus alerts

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

Informational alerts

Informational alerts tell you that ZoneAlarm Plus 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

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 Plus 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 Plus to block it. More info
- **Program Component** alerts occur when a program requests access permission, and it is using a component that has not yet secured by ZoneAlarm Plus, or a component that has changed since it was secured. More info
- **Component Loading** alerts occur when a program that has already launched, and already has access permission, loads a new, unsecured.

New Network Alert

New Network alerts occur when ZoneAlarm Plus detects that you're connected to a network you haven't seen before. You can use the alert pop-up to enable file and printer sharing with that network. More info

MailSafe Alerts

MailSafe alerts occur when you open an e-mail with an attachment that has been quarantined by ZoneAlarm Plus. More info

Internet Lock alerts

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

Remote Alerts

Remote alerts are displayed on an ICS client machine when ZoneAlrm Pro blockes traffic at the ICS gateway. More info

---

Related Topics

Responding to alerts

Blocked Program alert

Blocked Program alerts tell you that ZoneAlarm Plus 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 Plus 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:

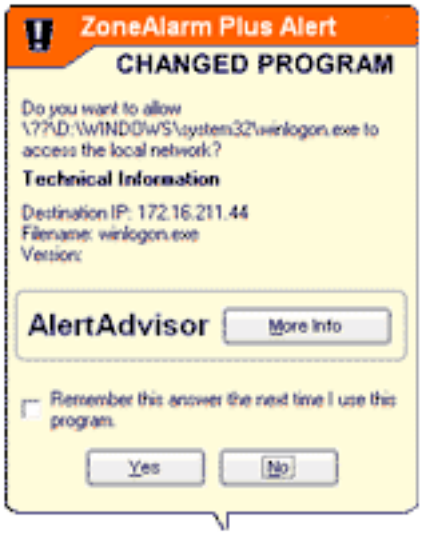
- When you see a Blocked Program alert, select **Do not show this dialog again** before clicking **OK**. From then on, all Blocked Program alerts will be hidden. Note that this will not affect New Program, Repeat Program, or Server Program alerts.
- In the Program Control panel, click Advanced to access 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 PLUS Changed Program alert



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

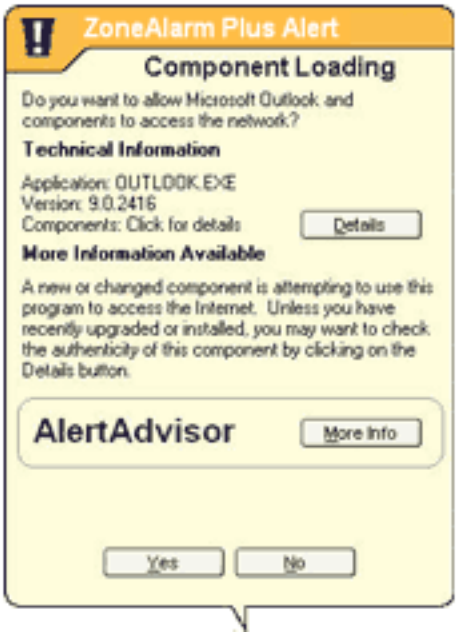
How you can see fewer of these alerts

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

Component Loading alert



Use the Component Loading alert to allow or deny Internet access to program that is loading a new or changed component some time after the program was launched. This helps protect you from hackers who try to use altered or faked components to get around your program control restrictions.

By clicking **Yes**, you allow the program to continue to access the Internet or local network resources while using the new or changed component. By clicking **No**, you prevent the program from accessing the Internet while using that component.

Tip Click the **Details** button to see what component(s) the program was loading.

Why these alerts occur

A Component Loading alert can occur in several normal situations. For example, if you click a link to a .pdf document, and your browser has not yet loaded the components necessary to read .pdf files, you will see a Component Loading alert as the browser loads that component.

However, a Component Loading alert can also occur if someone has tampered with a component, or created a malicious component designed to use a known program as a resource.

Component Loading alerts occur when all of the following are true:

- The Program Control level is set to **High**.
- A repeat program (one that has requested Internet access before, and whose MD5 signature has been recorded by ZoneAlarm Plus) loads a new component some time after the program itself has loaded.
- That component is new or has changed, or has **Ask** permission set in the Components tab.

What you should do

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

1. Are you actively using the application that loaded the component?
2. If the program that loaded the component was your browser, did you just try to access functionality that might require the browser to load a new component? Some examples of such functionality are flash videos and .pdf files.

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

If you cannot answer yes both questions, or if you feel unsure about the component for any reason, it is safest to answer **No**.

Investigating the alert

If you're not sure what to do, or if you decide to answer **No**, or if investigate the component to determine if it is safe. How?

How you can see fewer of these alerts

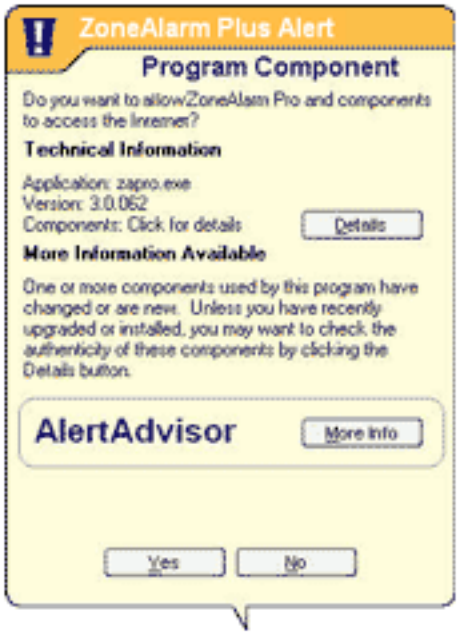
It is unusual to see a large number of Component Loading alerts. However, you may receive a large number of alerts if you raised the Program Authentication level to high soon after installing ZoneAlarm Plus. With authentication set to High, ZoneAlarm Plus cannot automatically secure the large number of DLLs and other components commonly used by browsers and other programs.

To greatly reduce the number of alerts, lower the authentication level to medium for the first few days after installing ZoneAlarm Plus How?

Related Topics

Program authentication
Program control

Program Component alert



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

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

Click the **Details** button to see what component(s) the program was loading.

Why these alerts occur

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

Note ZoneAlarm Plus automatically secures the components that a program is using at the time you grant it access permission. This prevents you from seeing a Component alert for every component loaded by your browser. To learn how ZoneAlarm Plus secures program components see the related topic *Program authentication.*

What you should do

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

1. Are any of the following true?
    - You just installed or reinstalled ZoneAlarm Plus.
    - You recently updated the application that is loading the component (For the application name, look under Technical Information in the alert pop-up.)
    - The application that is loading the component ha an automatic update function.
    - Someone else (for example, a systems administrator at your workplace) may have updated a program on your computer without your knowledge.
2. Are you actively using the application that loaded the component?

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

If you cannot answer yes both questions, or if you feel unsure about the component for any reason, it is safest to answer **No**.

Investigating the alert

If you're not sure what to do, or if you decide to answer **No**, investigate the component to determine if it is safe. How?

How you can see fewer of these alerts

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

To greatly reduce the number of alerts, lower the authentication level to medium for the first few days after installing ZoneAlarm Plus How?

If you have been using ZoneAlarm Plus for more than a few days, it is very rare to see large numbers of program alerts.

Related Topics

Program authentication
Program control

Firewall alert

When you see a Firewall alert, it means that ZoneAlarm Plus 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 Plus 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 Plus 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 Plus 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

Internet Lock alert

Internet Lock alerts let you know that ZoneAlarm Plus 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:

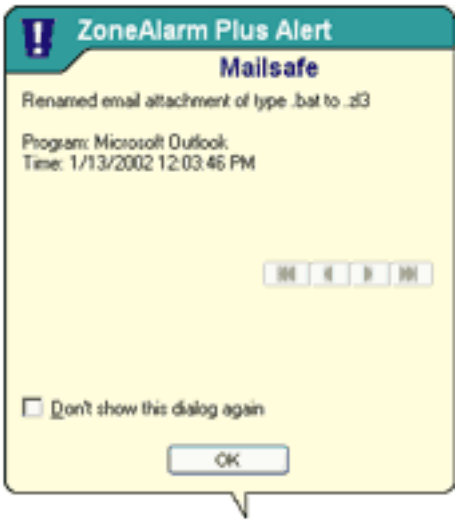
- In the Programs tab, turn the Automatic Internet Lock off.
- In the Auto-Lock tab, Increase the number of minutes of inactivity required for the Automatic Lock to engage.

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

MailSafe alert



MailSafe alerts let you know that ZoneAlarm Plus has quarantined a potentially dangerous attachment to an incoming e-mail message. By clicking **OK**, you're not letting anything into your computer.

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

Why these alerts occur

MailSafe alerts occur when you open an e-mail that has an attachment whose filename extension is on the list of extensions to be quarantined in the MailSafe panel. The alert informs you that ZoneAlarm Plus has changed the extension to prevent the attachment being opened without warning.

About e-mail borne viruses and worms

E-mail messages are the most common way Internet viruses and worms are spread. Some worms can raid your e-mail address book and forward themselves to everyone in it. When your friends see the message, they'll think it came from you, and open it--thus repeating the cycle.

For best security, you should never open an e-mail attachment that ZoneAlarm Plus has quarantined without first confirming the following three things:

- That it actually came from someone you know and trust
- That that person sent it intentionally
- That that person is sure that the attachment is harmles

What you should do

Click OK to close the alert box, then follow the steps below to ensure your security.

1. Examine the e-mail message carefully. Are you sure it's from someone you know and trust? Remember, hackers can fake e-mail messages so that they look like they are from a friend. Also, if a friend has accidentally opened a file containing an e-mail worm, that worm may have sent itself to you, using your friend's e-mail program.
2. If you're not completely sure the message is genuine, contact the sender by telephone or e-mail before trying to open the attachment.
3. If you're certain the attachment is harmless, you can open it by clicking the quarantine icon (which replaces the normal file icon).

Tip When you try to open a quarantined attachment, ZoneAlarm Plus will display a warning dialog box to remind you that the attachment is potentially dangerous.

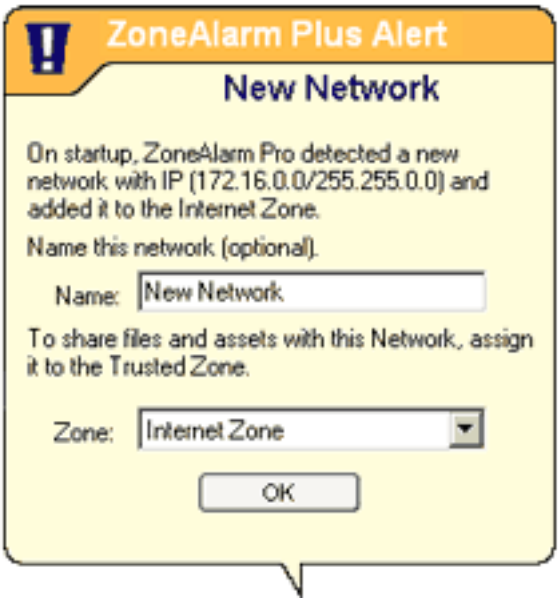
How you can see fewer of these alerts

It is extremely unusual to receive a large number of MailSafe alerts, unless you regularly receive e-mail with executable files attached. If you frequently receive executable attachments from trusted sources, have them compress the attachments into .zip files before sending.

Related Topics

E-mail protection

New Network alert



If you're on a home or local network, New Network alerts let you instantly configure ZoneAlarm Plus to allow you to share resources with the network.

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

Why these alerts occur

New Network alerts occur when you connect to any network--be it a wireless home network, a business LAN, or your ISP's network.

What you should do

Click the link that best describes your situation:

- I use home network or business LAN to connect to the Internet
- I use use a regular modem (dial-up connection), DSL, or cable modem to connect to the Internet.

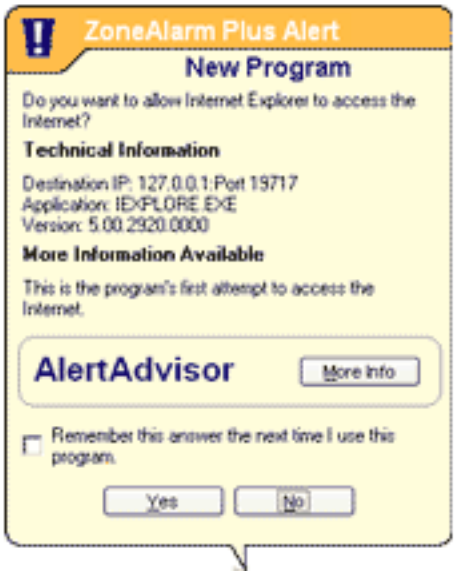
How you can see fewer of these alerts

It is unusual to receive a lot of NewNetwork alerts.

Related Topics

Alert details
What's a Zone?

New Program alert



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 Plus, 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 Plus. 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

Dial-up, DSL, or cable modem connection

If you are connected to the Internet through a standard modem and dial-up connection, a Digital Subscriber Line (DSL), or a cable modem, it is likely that ZoneAlarm Plus has detected your ISP 's network.

To secure your Internet connection, click **OK** in the New Network alert pop-up.

Caution If you click **Cancel**, you will ZoneAlarm Plus will block your Internet connection. Do not add your ISP network to your Trusted Zone.

New Network alert - Home or business network

If you receive a New Network alert when you start ZoneAlarm Plus, and you are connected to a home or business local network, it is likely that ZoneAlarm Plus has detected that network.

If you want to share resources with the other computers on the network, put the network in the Trusted Zone by following the steps below:

1. In the New Network alert pop-up, type a name for the network (for example "Home NW") in the Name box.
2. Select **Trusted Zone** from the Zone drop-down list.
3. Click **OK**.

Caution If you are not certain what network ZoneAlarm Plus has detected, write down the IP address displayed in the alert box. Then consult your home network documentation, systems administrator, or ISP to determine what network it is.

About wireless networks

Use caution if ZoneAlarm Plus detects a wireless network. It is possible for your wireless network adapter to is pick up a network other than your own. Be sure that the IP address displayed in the New Network alert is your network's IP address before you add it to the Trusted Zone.

Remote alerts

Remote alerts inform the user of an ICS client machine about ZoneAlarm Plus activity on the gateway machine. If you are not on a machine that is a client in an ICS network, you will never see this alert.

By clicking OK, you are not allowing anything into your computer.

Why these alerts occur

Remote alerts occur when:

- ZoneAlarm Plus starts up on the the ICS gateway. The alert displays the message **The remote firewall has started.**
- ZoneAlarm Plus shuts down on the ICS gateway. The alert displays the message **The remoted firewall has stopped.**
- The Internet Lock has engaged on the ICS gateway. This may prevent the client machine from performing some tasks. The alert displays the message **The remote firewall has engaged the Internet Lock.**
- The Internet Lock is opened on the ICS gateway. The alert displays the message **The remote firewall has disengaged the Internet Lock.**

What you should do

Click **OK** to close the alert box. You do not have to do anything else to ensure your security.

How you can see fewer of these alerts

If you do not want to see Remote alerts on the ICS client machine:

1. Go to the Main tab in the Firewall panel.
2. Click the **Advanced** button.
3. Under Internet Connection Sharing, clear the check box labeled **Forward alerts from gateway to this computer.**

Related Topics

Using the Internet Lock and Stop button
ICS (Internet Connection Sharing)

Repeat Program alert

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 Plus, 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?

Server Program alert

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 Plus to grant permission before you start using the program. How?

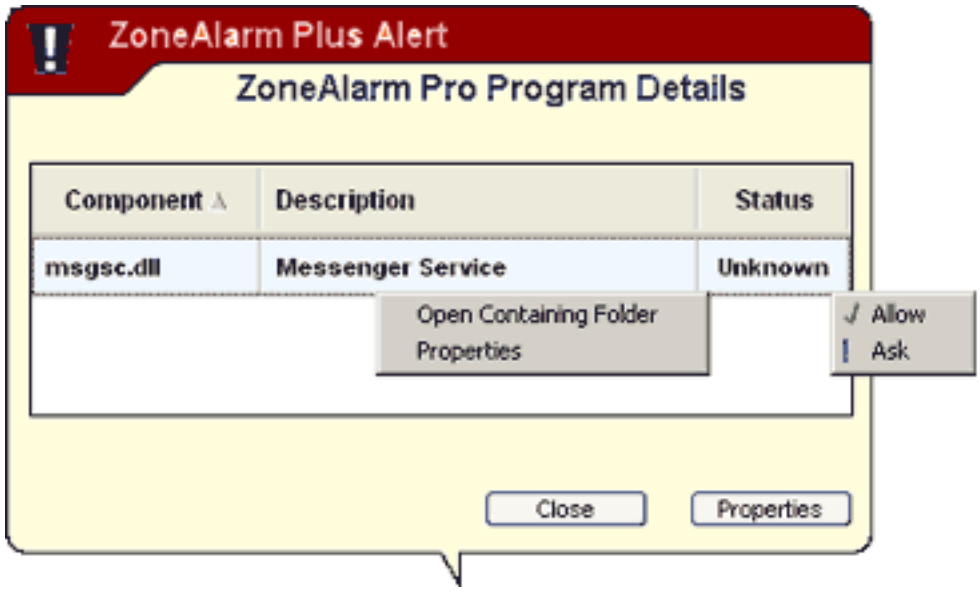
Related Topics

Alert details

[What's a Zone?](#)

Program details box

The Program Details box provides information about changed or new program components.



Use the Program Details box to find out the name, location, and properties of the component(s) that caused a Program Component alert or Component Loading alert, as well as the program that loaded it.

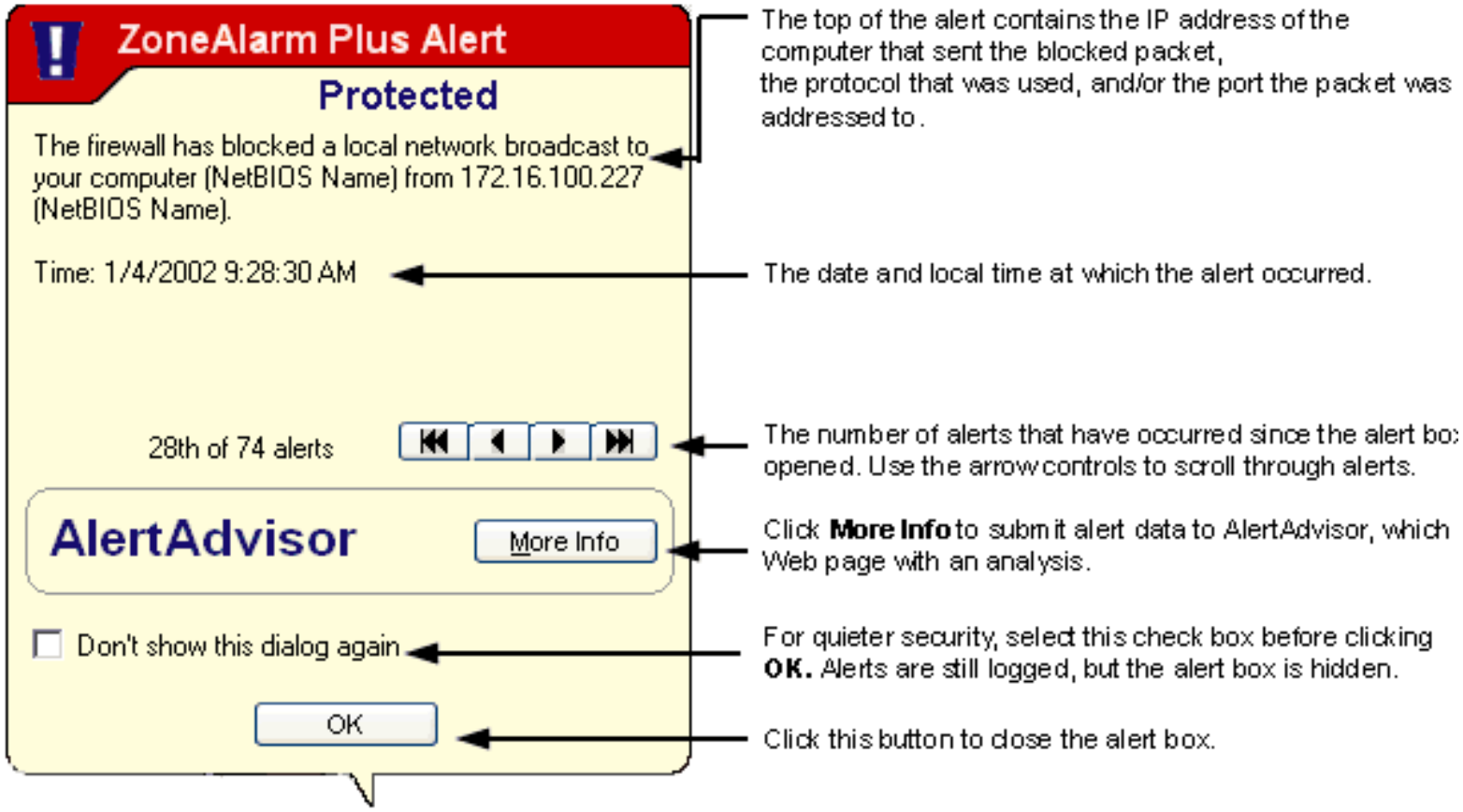
• To view the properties of the component, click the description, then choose **Properties** from the shortcut menu.

• To view the Windows directory that the component is located in, click the description, then choose **Open containing folder** from the shortcut menu.

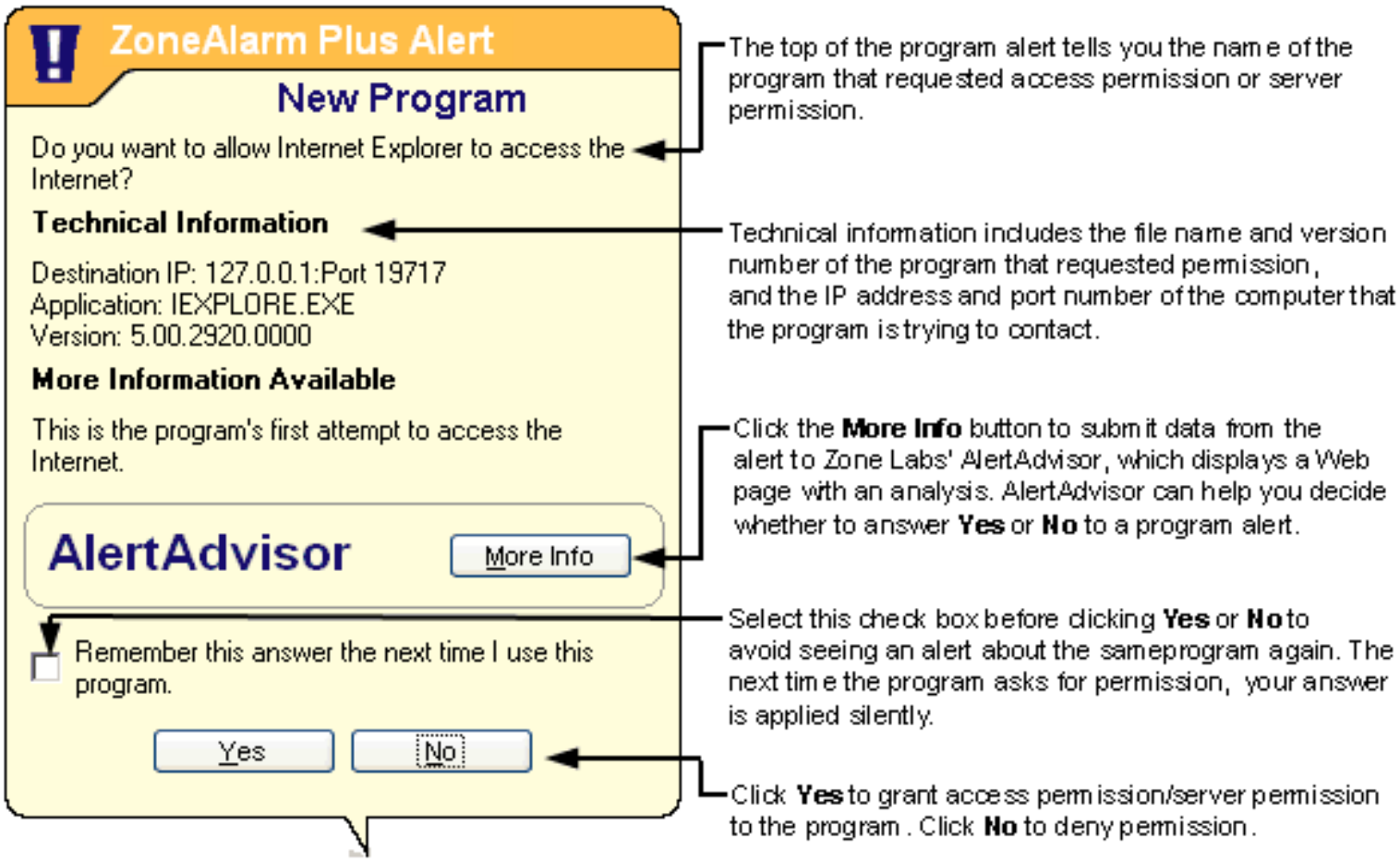
Tip Access the Program Details box by clicking the **Details** button in a Program Component alert or Component Loading alert.

Alert details

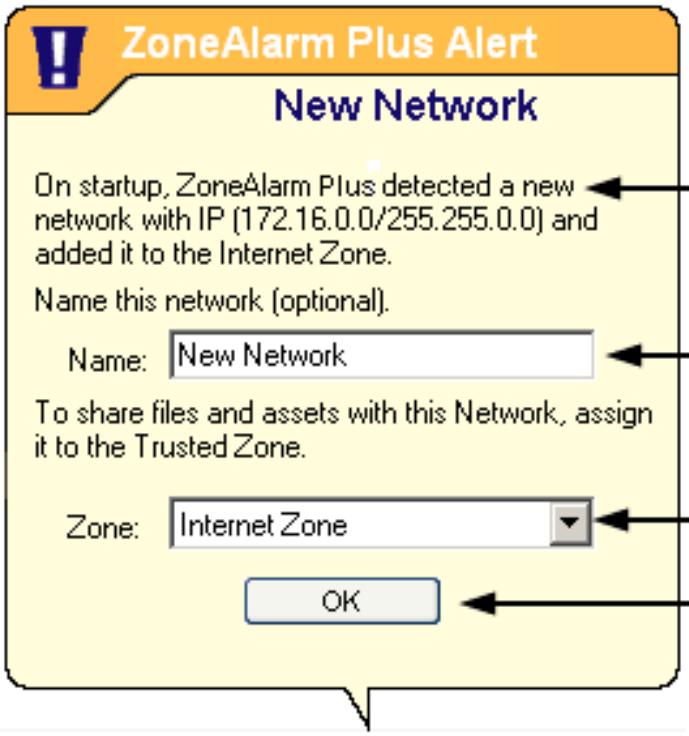
Firewall alerts



Program alerts



New Network alerts



The top of the alert tells you the type (wireless or other), IP address, and subnet mask of the detected network.

Type a name for the network here. This name will be displayed in the Zones tab, so that you can recognize the network later.

Use this list box to select a Zone in which to put the new network. Put the network in your Trusted Zone only if you it's your home or business LAN, not your ISP.

Click **OK** to add the network to the selected Zone and close the alert box.