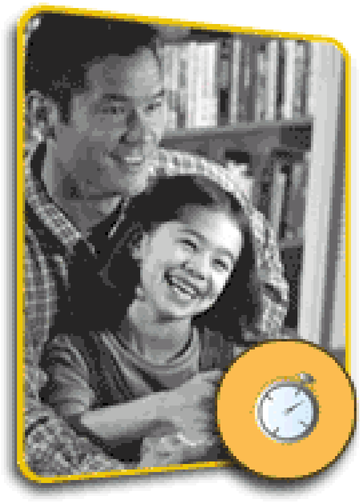
ZONE LABS ZoneAlarm

Step 1 of 7

What to expect from ZoneAlarm

"Talkative at first, then quiets down."



Welcome to ZoneAlarm. This product introduction and installation wizard takes you from download to complete protection in about three minutes.

Please click the Next button to start.

Back Next

Internet Components

This page provides an introduction to the basics of the Internet and how ZoneAlarm and ZoneAlarm Pro serve as protectors of individual machines.

The Internet

The Internet is a worldwide infrastructure that allows millions of computers, each of which is part of a smaller network, to communicate with each other. Participants on the Internet include individual users, corporations, government agencies, universities, ISPs and various online services.

Data traffic between networks is managed by routers. The primary function of a router is to make sure that data traffic, in the form of packets, arrives at its destination.

The concept of a firewall is to be a sentry, allowing authorized network traffic while blocking unauthorized network traffic through the network. However, many threats and vulnerabilities exist on the Internet which makes protection only on the network impractical. Since time and experience have proven that unseen threats can penetrate a network, additional protection has become a necessity at the desktop, especially for users with "always on" connections to the Internet.

ZoneAlarm and ZoneAlarm Pro are desktop firewalls, ensuring a secure environment while connected to the Internet by allowing the user to dynamically control traffic in and out of the PC. Unseen threats to the desktop include viruses, worms, Trojan horses, denial of service attacks, various direct intrusion methods and many other forms of privacy invasion. ZoneAlarm and ZoneAlarm Pro are equipped with sophisticated means of reporting suspicious activity to log files as well as alert notifications. Since Internet activity is unpredictable, ZoneAlarm and ZoneAlarm Pro arm users with the ability to protect their PCs from unwanted and potentially damaging occurrences.

Connections

Networks can be connected by a variety of transports. The most common examples of Internet access include ordinary telephone lines (dial-up), broadband services such as DSL and cable, ISDN, T1 and T3 lines. Modems and leased lines are the most common methods of transport.

- Traditional dial-up modems provide Internet access via the public telephone network at up to 56 Kbps.
- ISDN modems are capable of speeds up to 10 Mbps.
- DSL modems transmit and receive data digitally with a capacity of 1.544 Mbps.
- Cable modems provide high-speed Internet access through a cable

television network at more than 1 Mbps. This is approximately 20 times faster than dial-up modems.

- T1 lines don't require a modem and can transmit and receive data with a capacity of 1.544 Mbps.
- T3 lines don't require a modem and can transmit and receive data with a capacity of 45 Mbps.

TCP/IP

TCP/IP is the standard protocol for data traffic on the Internet. All data moving through the Internet constitute segmented packets. Routers read the IP packet headers to determine their appropriate destination for the traffic. Once the packets reach their destination, they are reassembled and read by the receiving computer.

An IP address is a unique identifier for each computer or device on the Internet and any TCP/IP network. An example of an IP address would be *127.0.0.1*.

The known and verifiable IP addresses of computers that you trust can be input into the Local Zone so that ZoneAlarm and ZoneAlarm Pro recognize them.

If you are on a network, please click here for instructions on adding your subnet adapter to the Local Zone.

Firewall Protection

Many firewalls use a packet filtering method for distinguishing permissible traffic. This type of protection only examines the IP packet headers. A packet filtering firewall does not protect against attacks directed at the application layer. For instance, if a packet filtering firewall was set to allow incoming e-mail from the Internet, then an attack on the SMTP service would pass through the firewall without a problem. In other words, as long as the rule set is passed, a connection is made directly from outside the firewall to inside the firewall.

One step up from packet filtering is the Stateful Inspection model of firewall. This type of firewall will analyze incoming packets until it has enough information (using information such as TCP sequence numbers) to determine the state of the connection. Then, if the packets pass the rules set, they're forwarded to the correct interface. Using this information, the firewall builds dynamic state tables. It uses these tables to keep track of the connections that go through the firewall. Rather than allowing all packets that meet the rule set's requirements to pass, it allows only those packets which are part of a valid, established connection.

Like packet filtering, a Stateful Inspection does not guard the application layer where many types of attacks are focused.

A core feature of ZoneAlarm is providing protection at the application layer, ensuring nefarious applications such as Trojan horses and spyware are unable to achieve their purpose of reaching the Internet from your computer.

BACK HOME NEXT

Copyright © 1999-2001 Zone Labs, Inc.

All rights reserved. ZoneAlarm and ZoneAlarm Pro include TrueVector Technology, covered by U.S. Patent

No. 5,987,611. Zone Labs, ZoneAlarm, ZoneAlarm Pro, and TrueVector are registered trademarks of Zone Labs, Inc.

For our partners Select One...

Site Search go

Products & Solutions | Download & Buy | Service & Support | About Zone Labs, Inc.

Our strong commitment to privacy

About Zone Labs

Quotes & Reviews | Management Team | Awards | Legal | Privacy

Privacy Policy

This privacy statement discloses the privacy practices for www.zonelabs.com.

Zone Labs, Inc. ("Zone Labs") has created this privacy policy to demonstrate our strong commitment to privacy. The following statement explains our information-gathering and dissemination practices for our site (the "Site") on the World Wide Web. This policy may change from time to time so please check back periodically. Zone Labs uses "Digital River, Inc.," a third party provider of e-commerce solutions, and back-end facilitator to process your credit card information. Click here to read the Digital River Privacy Statement.

For more information about the Zone Labs privacy statement, please see the following Frequently Asked Questions (FAQs).

We have established the following guiding principles for our privacy policy and practices:

Principle 1. Zone Labs lets you visit the Site without revealing any information about yourself. We do, however, keep track of the domains from which people visit us on the World Wide Web, and log IP addresses for statistical purposes to identify trends and the results of our marketing efforts in aggregate. IP addresses are not linked to "Personally Identifiable Information" (see below). We also use this information to help diagnose problems with our server and to administer the Site.

Principle 2. Some Zone Labs products ask you for "Personally Identifiable Information" as part of the registration process, including your connection type and number of computers. You choose whether or not to provide this information without affecting the product's performance. If you choose to provide us with Personally Identifiable Information, we use this information to notify you about product upgrades, updates, and new products. Zone Labs keeps your Personally Identifiable Information confidential and does not sell, trade or exchange mailing lists with any organization. Zone Labs maintains this information for not less than two but not more than four years, and will only disclose your Personally Identifiable Information to third parties if acting under good faith belief that such action is necessary to (1) conform to legal requirements; (2) protect and defend the rights or property of Zone Labs; or (3) enforce the Zone Labs Terms of Service.

Principle 3. Zone Labs will not send you any unsolicited information, including email, except where you authorize us to do so.

Principle 4. At your request, Zone Labs will change or delete your information and not use it for further contact with you. To request that your information be changed or deleted and not used for further contact with you, please e-mail us at privacy@zonelabs.com or write to us at Attn: Privacy Contact, Zone Labs, Inc., 1060 Howard Street, San Francisco, CA 94103.

Principle 5. Zone Labs collects and uses information that can be divided into the following categories:
Registration Information: This is information that you provide during the ZoneAlarm or

ZoneAlarm Pro product registration download process. You provide your first and last name, email address, and information about your use of ZoneAlarm or ZoneAlarm Pro.

Personally Identifiable Information: This is optional information that you may choose to provide to us. If you choose to provide Personally Identifiable Information, we will only use this information to notify you about product upgrades, product updates and new products. In addition, internal security provides that this information is coded with restricted access, and our servers are kept in a secure, locked environment.

Credit Card Information: Zone Labs uses "Digital River, Inc.," a third party provider of e-commerce solutions, and back-end facilitator to process your credit card information. Click here to read the Digital River Privacy Statement. Your credit card information does not pass through the Zone Labs Site under the terms of Zone Labs' agreement with Digital River. Digital River keeps your credit card information confidential and protects your credit card information through the use of industry-standard Secure Sockets (SSL) encryption technology.

Use of Information for Analyzing Security Breaches: If the Zone Labs product detects a security threat to your computer, you can click on the "More Information" button from the product dialogue box. At that point, the product sends the information about the threat and your IP address to the Zone Labs Site to be analyzed. Zone Labs will send you more specific guidance about the security information. Zone Labs will not release your IP address or any Personally Identifiable Information that could be extracted from your IP address to any third party.

No-Cookie Policy: "Cookies" are small pieces of information that your browser stores on your computer on behalf of a Web site that you have visited. The Zone Labs Site does not use cookies. Digital River's cookies are used only to identify the customer, not to identify any specific customer traits. This allows Digital River to maintain consistency in the shopping basket and enable a more pleasant shopping experience. Click here to read the Digital River Privacy Statement.

Principle 6. Zone Labs' Site contains links to other web sites. Please note that when you click on one of these links, you are moving to another web site. We encourage you to read the privacy statements of these linked sites - as well as any site on the World Wide Web - as their privacy policy may differ from ours.

Principle 7. Zone Labs will post on its home page (www.zonelabs.com) notification of any changes to this Privacy Policy, with a direct link to the new policy statement(s).

What Constitutes My Acceptance of this Privacy Policy?

By using the Site or any services provided through the Site, you expressly consent to the use and disclosure of information as described in this Privacy Policy. Zone Labs reserves the right to change this Privacy Policy at any time by electronic notice posted on our Site. Your continued use of our Site after the date that such notices are posted will be deemed to be your agreement to the changed terms.

Contacting the Site

If you have any questions about this privacy statement, the practices of this Site, or your dealings with this Site, you can contact us:

By Email
privacy@zonelabs.com

By Mail

Attn: Privacy Contact
Zone Labs, Inc.
1060 Howard Street
San Francisco, CA 94103

If at any time, you believe that Zone Labs has not adhered to these principles, please notify us by email at privacy@zonelabs.com or by writing to Attn: Privacy Contact, Zone Labs, Inc., 1060 Howard Street, San Francisco, CA 94103, and we will make all commercially reasonable efforts to promptly determine and correct the problem.

Frequently Asked Questions

What information does Zone Labs collect about me, and how will this information be used?
Zone Labs collects and uses information that can be divided into the following categories:

Registration Information: This is information that you provide and input during the ZoneAlarm or ZoneAlarm Pro product registration download process. You provide your first and last name, email address, and information about your use of ZoneAlarm or ZoneAlarm Pro.

Personally Identifiable Information: This is opt-in information that you may choose to provide to us. If you choose to provide Personally Identifiable Information, we will only use this information to notify you about product upgrades, product updates and new products.

Credit Card Information: Zone Labs uses "Digital River, Inc.," a third party provider of e-commerce solutions, and back-end facilitator to process your credit card information. Click here to read the Digital River Privacy Statement. Your credit card information does not pass through the Zone Labs Site under the terms of Zone Labs agreement with Digital River. Digital River keeps your credit card information confidential and protects your credit card information through the use of industry-standard Secure Sockets (SSL) encryption technology.

Use of Information for Analyzing Security Breaches: If the ZoneAlarm product detects a security threat to your computer, you can click on the "More Information" button from the ZoneAlarm dialogue box. At that point, the ZoneAlarm product sends the information about the threat and your IP address to the Zone Labs Site to be analyzed. ZoneAlarm will send you more specific guidance about the security information. Zone Labs will not release your IP address and any Personally Identifiable Information that could be extracted from your IP address to any third party.

What about cookies?
"Cookies" are small pieces of information that your browser stores on your computer on behalf of a website that you have visited. The Zone Labs website does not use cookies. DigitalRiver's cookies are used only to identify the customer, not to identify any specific customer traits. This allows DigitalRiver to maintain consistency in the shopping basket and enable a more pleasant shopping experience. Click here to read the Digital River Privacy Statement.

Privacy Policies of Other Sites on the World Wide Web
Zone Labs' site contains links to other sites. Zone Labs is not responsible for the privacy practices or the content of such other websites and recommends that you review the privacy policies of other sites on the World Wide Web that you visit.

What constitutes my acceptance of this privacy policy?

By using the Site or any services provided through the Site, you expressly consent to the use and disclosure of information as described in this Privacy Policy. Zone Labs reserves the right to change this Privacy Policy at any time by electronic notice posted on our Site. Your continued use of our Site after the date that such notices are posted will be deemed to be your agreement to the changed terms.

Contacting the Site
If you have any questions about this privacy statement, the practices of this Site, or your dealings with this Site, you can contact us in the following ways:

By email:
privacy@zonelabs.com

By Mail:
Attn: Privacy Contact
Zone Labs, Inc.
1060 Howard Street
San Francisco, CA 94103

● Press Room ● Careers ● Volume Sales ● Contact Us ● Site Map ● News & Articles
● Affiliates

Copyright ©1999-2001 Zone Labs, Inc., 1060 Howard Street, San Francisco, CA 94103, USA.
All rights reserved. All other trademarks are the property of their respective owners.

ZONE LABS

For our partners Select One...

Site Search go

Products & Solutions | Download & Buy | Service & Support | About Zone Labs, Inc.

The best security just got better

Download & Buy

ZoneAlarm PRO
Easy and Powerful Network Security

ZoneAlarm™ Pro for the Home and Home Office
The best security just got better.
All the features that made ZoneAlarm a winner, but with new layers of security that will keep you up-to-date with the latest threats. ZoneAlarm Pro is compatible with Windows 95/98/Me/NT/2000.

List Price:
$39.95 US

Available as download only (2 MB)

Download Now! | More Info

To order by phone, call toll-free (877) 546-3823

ZoneAlarm
Easy, Always-On Internet Security

ZoneAlarm™ 2.1
Always there. Always on. Always secure.
Only ZoneAlarm can offer that kind of peace of mind. Protect your home office, cable and DSL connections from unwanted intruders and unwelcome viruses. ZoneAlarm is compatible with Windows 95/98/Me/NT/2000

List Price:
$19.95

Available as download only (1.6 MB)

Free Download | Buy Now! | More Info

To order by phone, call toll-free (877) 546-3823

ZoneAlarm Free Download!
ZoneAlarm is still free* for personal and non-profit use.

* ZoneAlarm is free for personal and non-profit use (excluding governmental entities and educational institutions); business users must purchase a valid end-user license after 60 days in order to continue using the software.

Click here to read the ZoneAlarm Pro End-User License Agreement
Click here to read the ZoneAlarm End-User License Agreement

● Press Room ● Careers ● Volume Sales ● Contact Us ● Site Map ● News & Articles
● Affiliates

Copyright ©1999-2001 Zone Labs, Inc., 1060 Howard Street, San Francisco, CA 94103, USA.
All rights reserved. All other trademarks are the property of their respective owners.

ZONE LABS

Site Search [ ] go

- Products & Solutions
- Download & Buy
- Service & Support
- About Zone Labs, Inc.

Smart Security

Customer Solutions

- Personal/SOHO
- Small Business
- Enterprise
- Partners

ZoneAlarm Pro

Easy and Powerful Internet Security

Download Now!

ZoneAlarm Pro delivers powerful new features and comprehensive Internet security for **all** users of always-on Internet-connected PCs. Click here for more info.

ZoneAlarm FREE Download

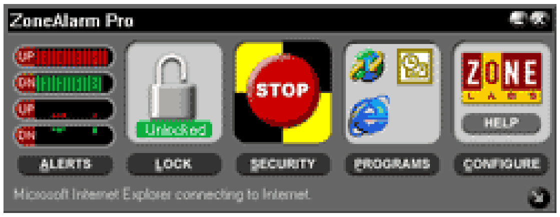
ZoneAlarm is still free for personal and non-profit use.

Download ZoneAlarm Now!

Protect your PC with this award-winning utility.

ZoneAlarm Pro

ZoneAlarm Pro is compatible with Windows 95/98/Me/NT/2000.



Microsoft Internet Explorer connecting to Internet.

Download Now!

More Info

INTERNETWEEK ONLINE

"[**ZoneAlarm Pro** is] Excellent! Buy it, even if you have a hardware firewall..." Full article

ZoneAlarm FREE Download

Free Download

ZoneAlarm™ is essential for DSL and Cable modem users, providing rock-solid protection against Internet thieves, vandals and hackers - stopping them dead in their tracks. If you can't be seen, you can't be attacked! More than **9 million** PC users have downloaded ZoneAlarm. Shouldn't you?

ZoneAlarm is compatible with Windows 95/98/Me/NT/2000.

Zone Labs Enterprise Sales

Hundreds of thousands of enterprise desktops are secured by Zone Labs

New ZoneAlarm Pro Affiliate Program

Become a ZoneAlarm Pro Affiliate

News

Important update release for ZoneAlarm Pro

Zone Labs Launches Security Resource Center

Announcing Zone Labs

Integrity

Zone Labs Teams Up with VPN Vendors

Zone Labs Forms Strategic Technology Partnership with SafeNet

Zone Labs Teams Up with NEC

Home Office Computing declares ZoneAlarm a winner

MSNBC, CNET, PC World, and ZDNET are some of our fans

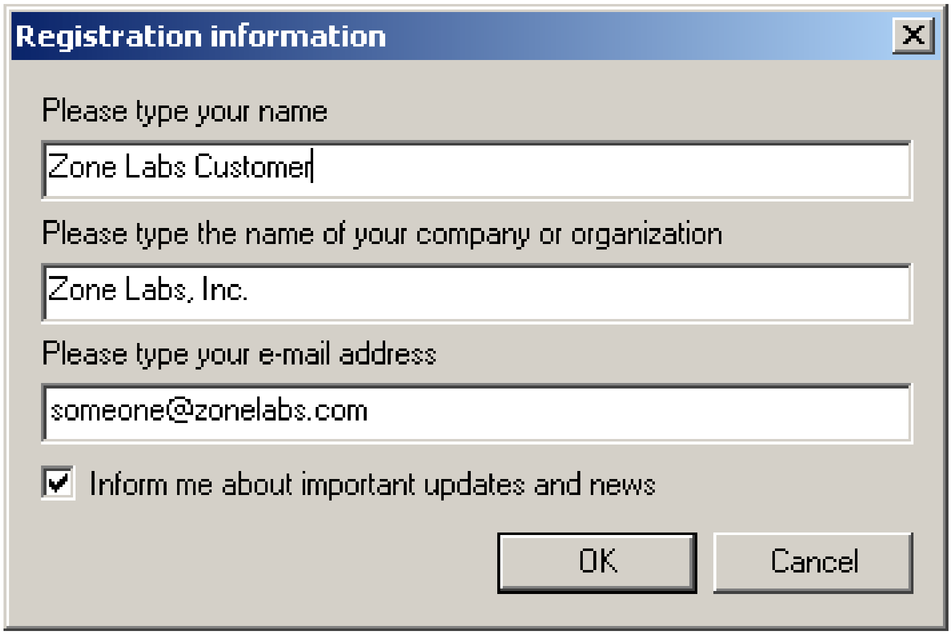
● Press Room ● Careers ● Volume Sales ● Contact Us ● Site Map ● News & Articles
● Affiliates

Copyright ©1999-2001 Zone Labs, Inc., 1060 Howard Street, San Francisco, CA 94103, USA.
All rights reserved. All other trademarks are the property of their respective owners.

Privacy Policy

The Change Registration Button

Click the Change Registration button to review or modify your ZoneAlarm registration information. Provide any new information, such as a new name, address, telephone number or e-mail address, in the Registration Information dialog, shown below:



Registration information

Please type your name

Zone Labs Customer

Please type the name of your company or organization

Zone Labs, Inc.

Please type your e-mail address

someone@zonelabs.com

☑ Inform me about important updates and news

When changing the registration information, ZoneAlarm automatically records the update. ZoneAlarm displays the date and time of your last registration.

BACK HOME

Copyright © 1999-2001 Zone Labs, Inc.

All rights reserved. ZoneAlarm and ZoneAlarm Pro include TrueVector Technology, covered by U.S. Patent No. 5,987,611. Zone Labs, ZoneAlarm, ZoneAlarm Pro, and TrueVector are registered trademarks of Zone Labs, Inc.

Keyboard Shortcuts

You can use a combination of keystrokes on your keyboard to access many features of ZoneAlarm. This provides an alternative to using your mouse.

A list of features you can activate with keystrokes is provided below. To perform most shortcuts, press either the Ctrl or the Alt key in conjunction with one of the letter keys on your keyboard:

Ctrl+L	Lock/Unlock
Ctrl+S	Emergency Stop
Ctrl+H	Zone Labs Information Overview
Alt+A	Expand/Close the Alerts Panel
Alt+L	Expand/Close the Lock Panel
Alt+S	Expand/Close the Security Panel
Alt+P	Expand/Close the Programs Panel
Alt+C	Expand/Close the Configure Panel
Alt+Z	Zoom/Unzoom - Expand/Close the current panel
ESC	Unzoom - Close the open panel
F1	Access the help file

In the alert popup dialog, these keys let you navigate multiple alerts:

PgUp	Previous Alert
PgDn	Next Alert
Home	First Alert
End	Last Alert

BACK HOME NEXT

Copyright © 1999-2001 Zone Labs, Inc.

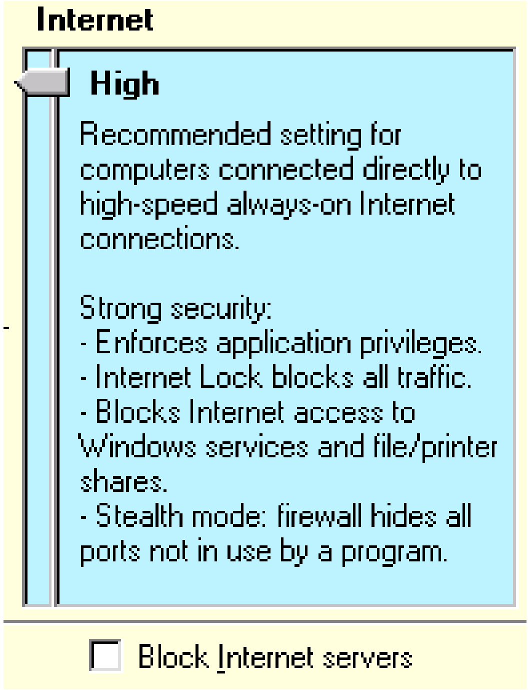
All rights reserved. ZoneAlarm and ZoneAlarm Pro include TrueVector Technology, covered by U.S. Patent No. 5,987,611. Zone Labs, ZoneAlarm, ZoneAlarm Pro, and TrueVector are registered trademarks of Zone Labs, Inc.

Change Default Settings

Go through the ZoneAlarm panels to change default security settings if they don't suit your needs.

An example: change Internet Zone security

You can change the Internet Zone security setting by simply dragging the slider up or down:



Internet

High

Recommended setting for computers connected directly to high-speed always-on Internet connections.

Strong security:
- Enforces application privileges.
- Internet Lock blocks all traffic.
- Blocks Internet access to Windows services and file/printer shares.
- Stealth mode: firewall hides all ports not in use by a program.

□ Block Internet servers

This is a change of the default setting. The default MailSafe setting is that all file types in the dialog are preselected as quarantined. This gives your machine maximum protection.

What are default values?

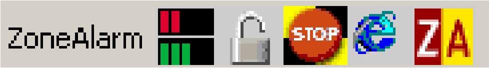
Default values are security options that are set as turned on when ZoneAlarm is installed.

If you downloaded the product as a single user, the default options that are set at installation time represent ZoneLabs judgment of optimal security settings on your machine. If your system administrator was the person who configured and installed your copy of ZoneAlarm, those values represent your company's security strategy.

You can change these options by going into each panel and changing the selections. Most options are changed by selecting or deselecting the checkboxes and radio buttons in each panel.

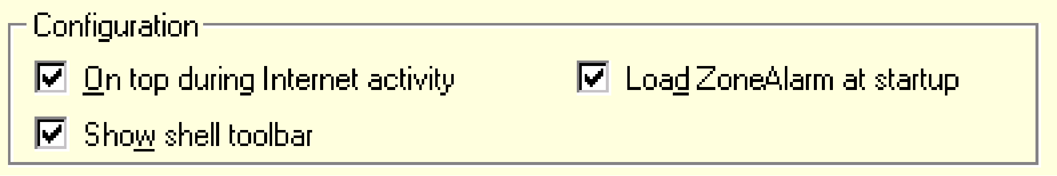
Remove the DeskBand Toolbar from your desktop

Another default setting you can change is the display of the DeskBand Toolbar. You'll see the DeskBand Toolbar in the lower right corner of your desktop if you set it up to be shown.



It shows Internet traffic, allows you to easily turn on the Internet Lock, and other things.

If you would prefer to have the DeskBand Toolbar displayed, go to the the Configuration panel and deselect the Show shell toolbar checkbox that was selected by default when ZoneAlarm was installed:



Configuration

☑ On top during Internet activity ☑ Load ZoneAlarm at startup

☑ Show shell toolbar

The DeskBand toolbar will be added. Go back and select the checkbox if you want to remove the DeskBand Toolbar.

BACK HOME NEXT

Copyright © 1999-2001 Zone Labs, Inc.

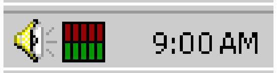
All rights reserved. ZoneAlarm and ZoneAlarm Pro include TrueVector Technology, covered by U.S. Patent No. 5,987,611. Zone Labs, ZoneAlarm, ZoneAlarm Pro, and TrueVector are registered trademarks of Zone Labs, Inc.

QuickTour of ZoneAlarm

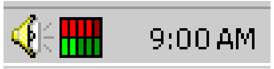
This QuickTour won't take long. But it will save you the trouble of figuring things out for yourself.

OPEN the main panel

To open the main panel whenever it is not open, double-click on the ZA icon in your system tray, directly below the Desk Band Toolbar:



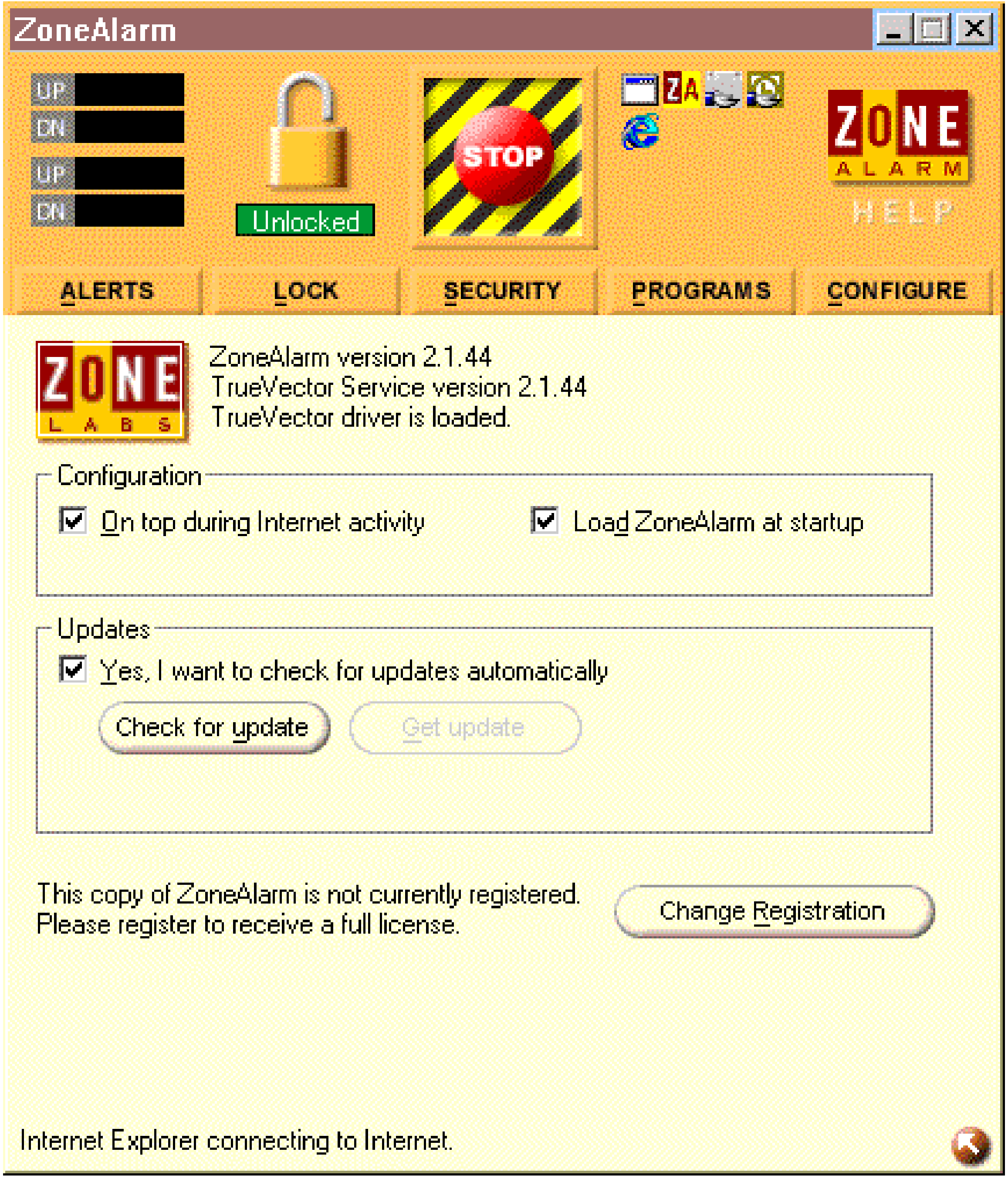
The ZA icon also lights up with red and green bars whenever Internet traffic is happening. Double-clicking on this icon will still open the main ZoneAlarm panel even though Internet traffic is showing:



* As long as ZoneAlarm is installed on your machine and has not been shut down, the ZA icon will remain in the System Tray. You cannot remove it.

Main ZoneAlarm panel

ZoneAlarm has five different panels. Each one has a different function. The panel shown here is the Configuration panel where you set some general behavior options in the Configuration field at the top of this panel.



ZoneAlarm version 2.1.44
TrueVector Service version 2.1.44
TrueVector driver is loaded.

Configuration

☑ On top during Internet activity ☑ Load ZoneAlarm at startup

Updates

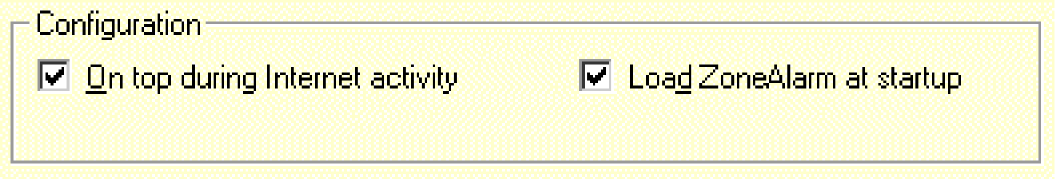
☑ Yes, I want to check for updates automatically

This copy of ZoneAlarm is not currently registered.
Please register to receive a full license.

Internet Explorer connecting to Internet.

The checkboxes at the top of the Configuration panel also allow you to determine overall behavior:

- should this panel be on top all apps during Internet traffic?
- should the Desk Band toolbar be visible
- should you load ZoneAlarm at startup time?



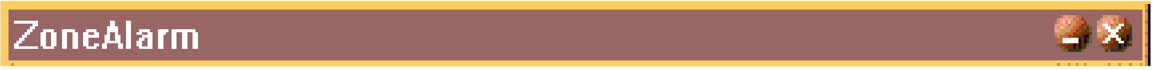
Configuration

☑ On top during Internet activity

☑ Load ZoneAlarm at startup

Brown bar along the top of the panel

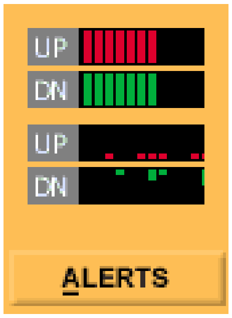
A brown title bar with the name ZoneAlarm spans the very top of the main panel.



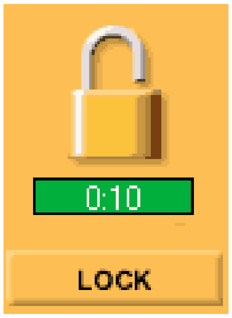
At the extreme right of the title bar, you can use the ⊖ tool to minimize ZoneAlarm.

Five main icons

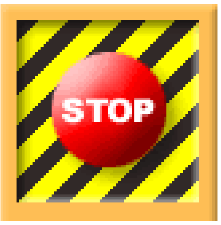
Directly below the title bar you have a row with five icons. Each icon has a specific function. The first one lights up when Internet traffic is occurring on your PC.



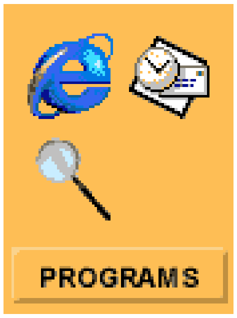
Watch this icon! It contains four small bars: two UP rows and two DOWN rows. These bars show a graphic display of uploading & downloading. The top two bars show real time Internet traffic on your PC; the lower two bars show Internet traffic over a period of time.



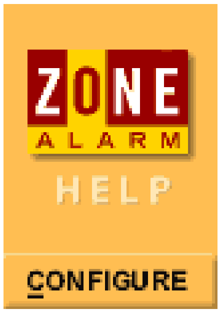
Click on this icon to block Internet traffic! When you do, the padlock will close and the green text will change to this:



This is the Stop button! Click on it when you think trouble has arrived. It will immediately stop all Internet Traffic and, unlike the Lock button described directly above, it will allow no exceptions, thereby not respecting the passlock.



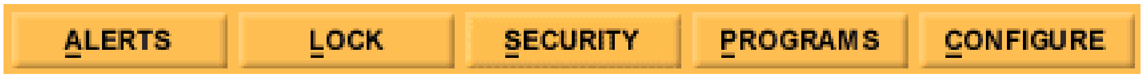
Watch this icon to get a quick graphical look at which applications are currently connected to the Internet. Inside this icon, ZoneAlarm displays the icon for each program on your PC that has a current Internet connection.



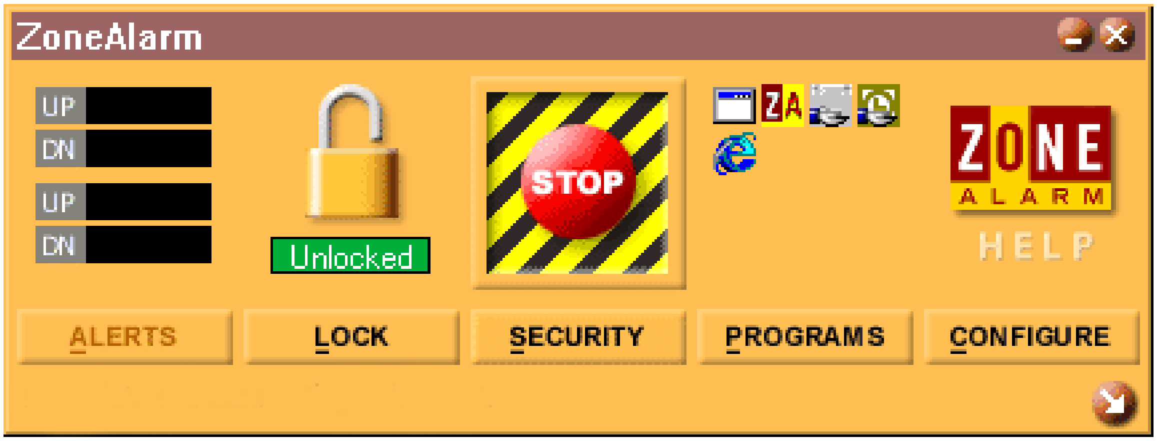
Click on this icon to open the Help file. The Help file not only provides reference material, but also Internet basics, information on how other software programs interact with ZoneAlarm, and much more.

Buttons below the Icons

Use these buttons to navigate between ZoneAlarm panels. This means that the entire display in lower portion of the panel changes. Click on the buttons below to see how it works.

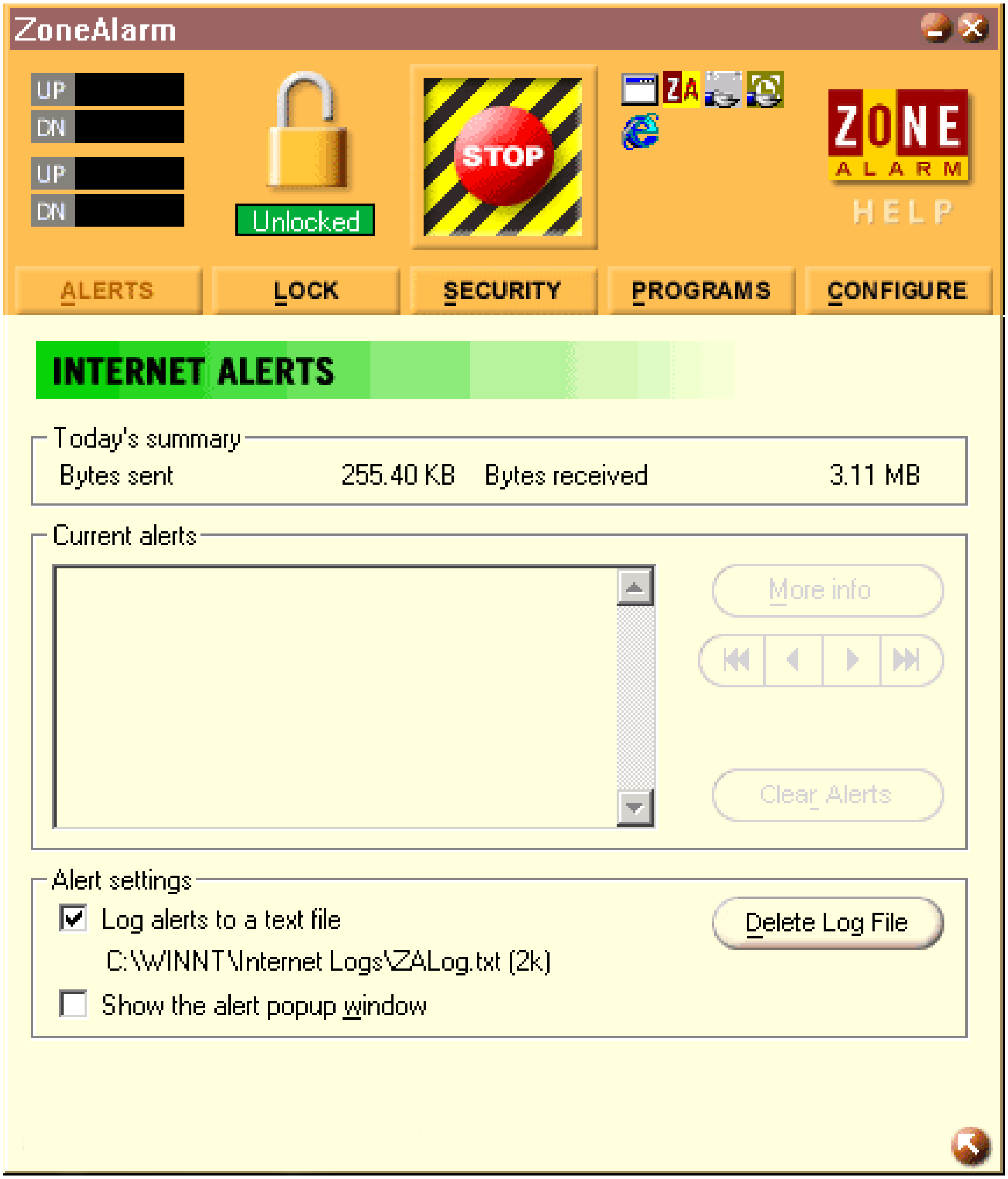


If you are already using the panel represented by a button, like the Configuration panel we looked at briefly above, and you click on the Configuration button, notice that the lower part of the main panel is removed, leaving only the icons and buttons:



The Alerts Panel

Use this panel to see statistics about Internet traffic alerts on your PC and to minimize the display of alerts if you find there are so many that the displays become distracting.



Today's summary

Bytes sent 255.40 KB Bytes received 3.11 MB

Current alerts

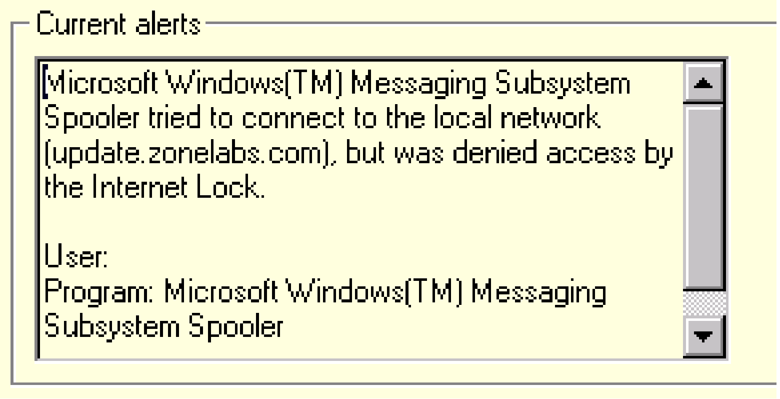
Alert settings

☑ Log alerts to a text file

C:\WINNT\Internet Logs\ZALog.txt (2k)

□ Show the alert popup window

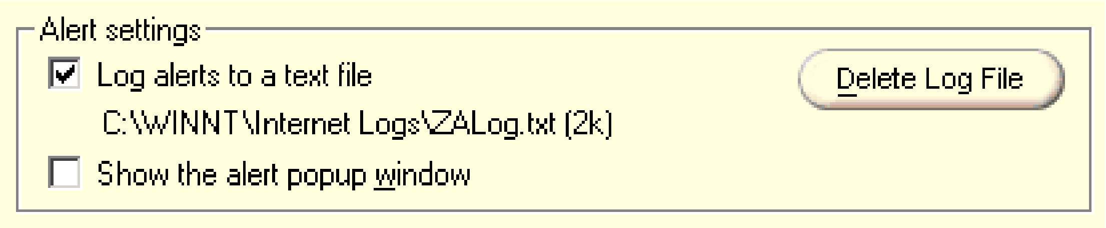
To find out the IP address, the time and, when appropriate, the application involved in an Internet traffic alert, look in the Current alerts box in the middle of the panel:



Microsoft Windows(TM) Messaging Subsystem Spooler tried to connect to the local network (update.zonelabs.com), but was denied access by the Internet Lock.

User:
Program: Microsoft Windows(TM) Messaging Subsystem Spooler

Go to the checkboxes at the bottom of the panel to instruct ZoneAlarm to save alerts to a text file that you can comfortably read at any time. You can also initiate the alert popup alert from here, so that each time an alert occurs, a balloon alert is displayed with pertinent information.

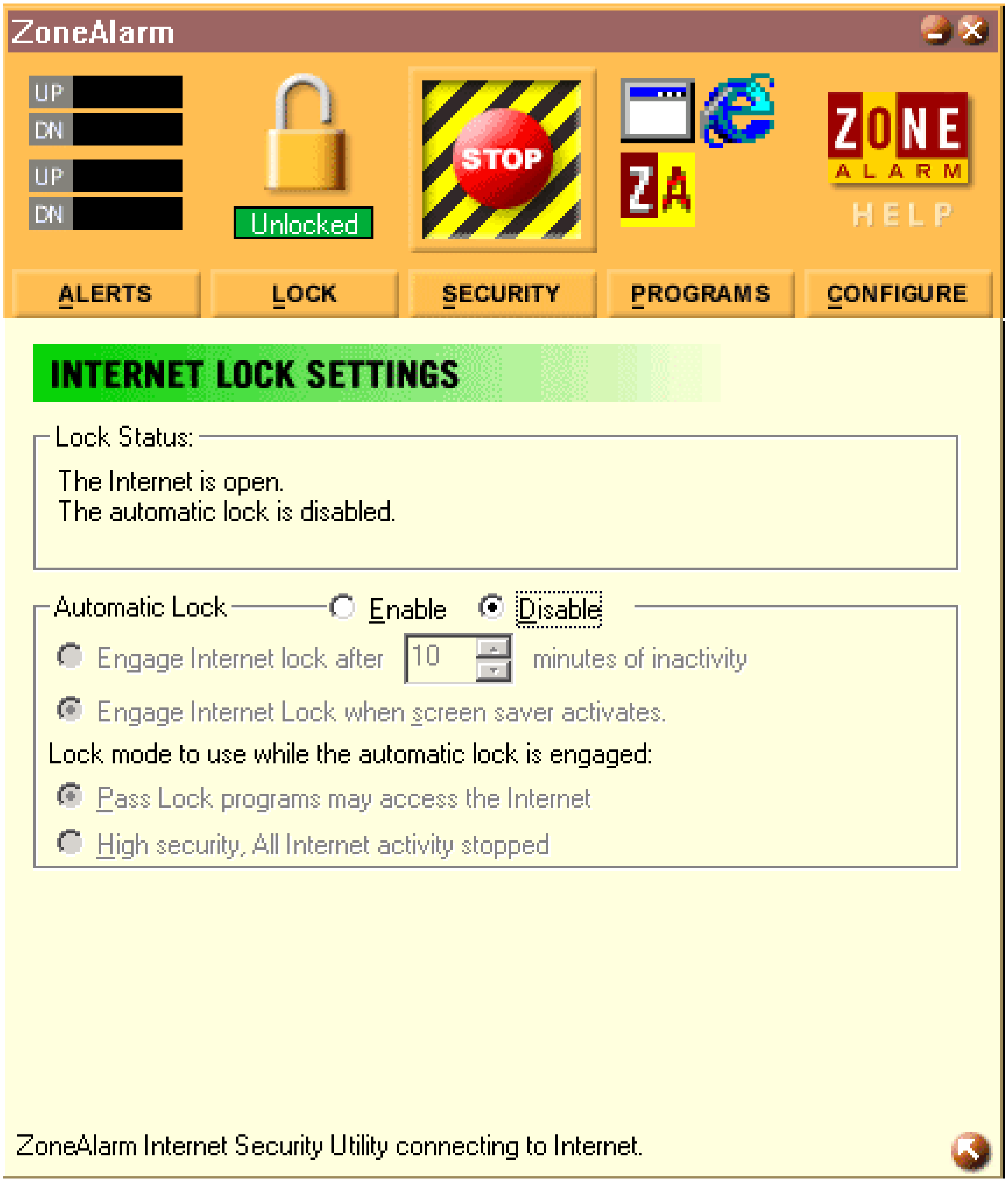


☑ Log alerts to a text file
C:\WINNT\Internet Logs\ZALog.txt (2k)
□ Show the alert popup window

The Advanced button lets you set log file options to prevent your alert log file from getting too large.

Lock Panel

ZoneAlarm has a programmable lock to stop Internet traffic. Use the Lock panel to determine whether the lock should be turned on after a time of inactivity on your PC or whether your screen saver should turn it on.



INTERNET LOCK SETTINGS

Lock Status:

The Internet is open.
The automatic lock is disabled.

Automatic Lock ○ Enable ● Disable

○ Engage Internet lock after 10 minutes of inactivity

● Engage Internet Lock when screen saver activates.

Lock mode to use while the automatic lock is engaged:

● Pass Lock programs may access the Internet

○ High security, All Internet activity stopped

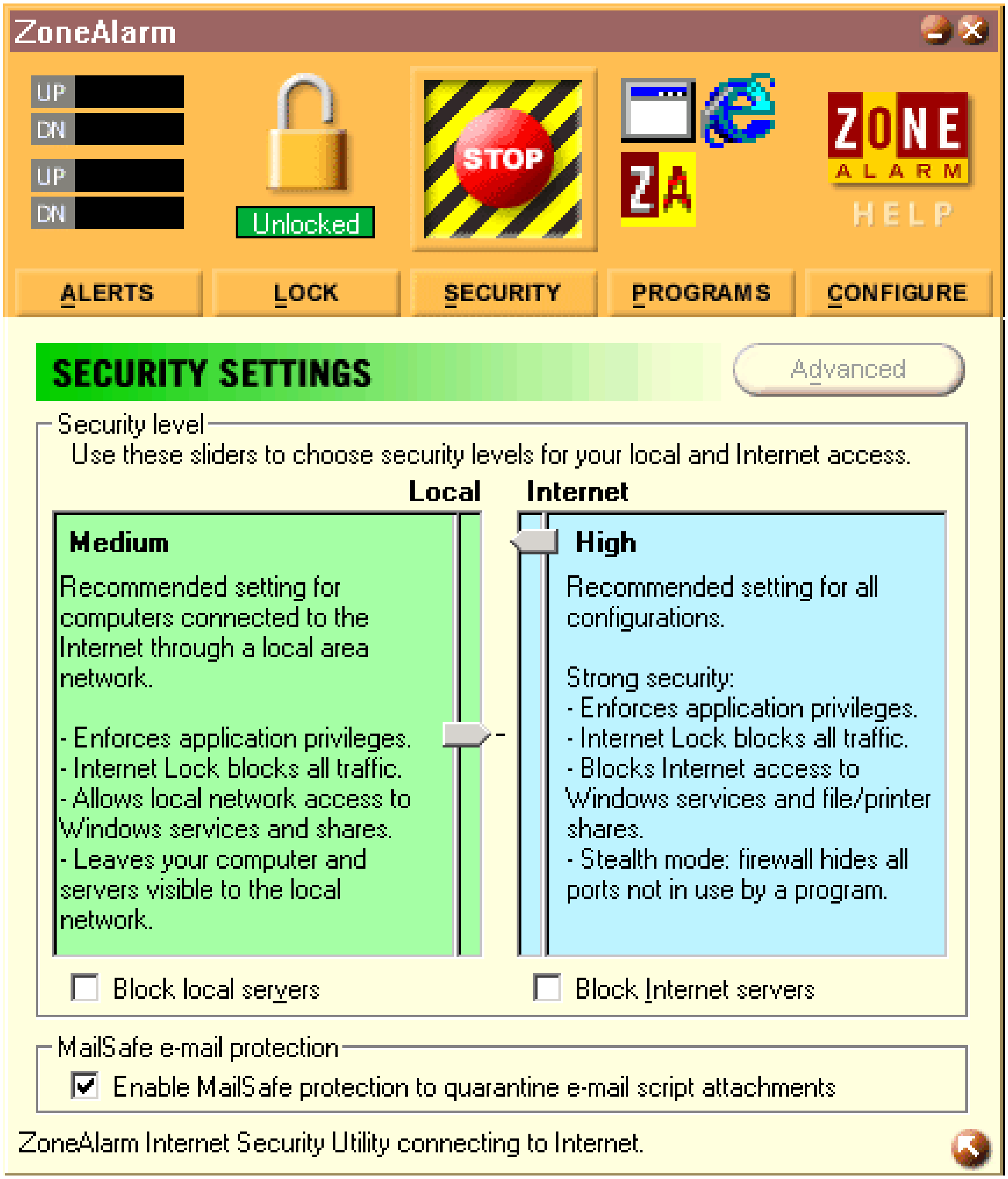
ZoneAlarm Internet Security Utility connecting to Internet.

Passlock, the ability for a program to disregard the lock and access the Internet, is enabled or disabled in this panel. If pass lock is enabled, individual applications that you select in the Programs panel will be able to break through the lock. This is useful for programs like e-mail.

Security Panel

This panel is where you set up your zones. Use the yellow and blue boxes in the middle of the panel to set overall security for your Local Zone and your Internet Zone.

For maximum security, it is a good idea to keep security in the Internet Zone set to High. This panel also controls MailSafe.



SECURITY SETTINGS

Security level

Use these sliders to choose security levels for your local and Internet access.

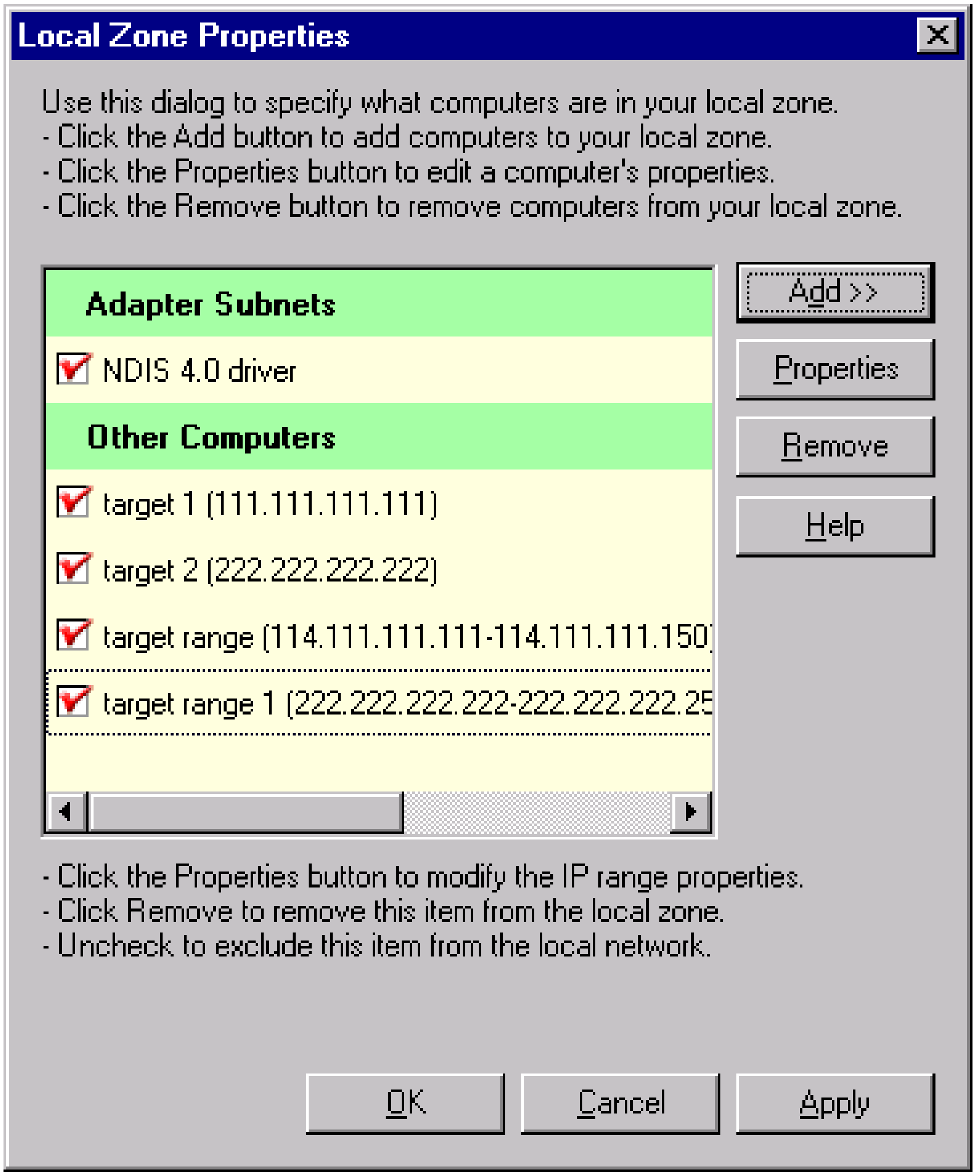
Local	Internet
Medium Recommended setting for computers connected to the Internet through a local area network. - Enforces application privileges. - Internet Lock blocks all traffic. - Allows local network access to Windows services and shares. - Leaves your computer and servers visible to the local network.	**High** Recommended setting for all configurations. Strong security: - Enforces application privileges. - Internet Lock blocks all traffic. - Blocks Internet access to Windows services and file/printer shares. - Stealth mode: firewall hides all ports not in use by a program.
□ Block local servers	□ Block Internet servers

MailSafe e-mail protection

☑ Enable MailSafe protection to quarantine e-mail script attachments

ZoneAlarm Internet Security Utility connecting to Internet.

The Advanced button puts you more in the driver's seat. This button takes you to a dialog where you populate your Local Zone with trusted computers and addresses.



Local Zone Properties

Use this dialog to specify what computers are in your local zone.
- Click the Add button to add computers to your local zone.
- Click the Properties button to edit a computer's properties.
- Click the Remove button to remove computers from your local zone.

Adapter Subnets

☑ NDIS 4.0 driver

Other Computers

☑ target 1 (111.111.111.111)

☑ target 2 (222.222.222.222)

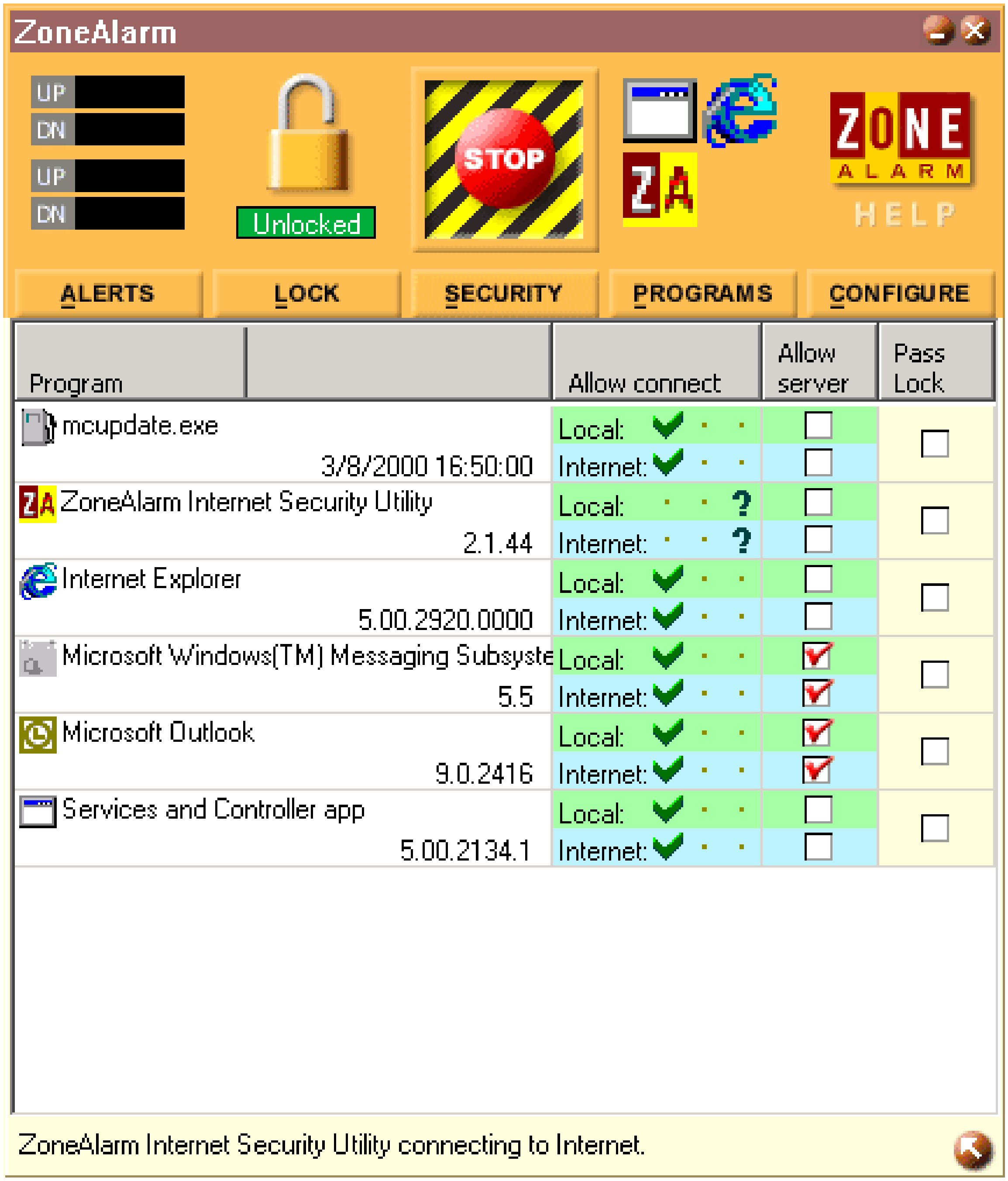
☑ target range (114.111.111.111-114.111.111.150)

☑ target range 1 (222.222.222.222-222.222.222.25

- Click the Properties button to modify the IP range properties.
- Click Remove to remove this item from the local zone.
- Uncheck to exclude this item from the local network.

Programs Panel

Use the Programs Panel to see which programs have been connecting to the Internet and also to restrict or broaden a program's ability to access the Internet. Every line in the panel is dedicated to one of your programs that has been accessing the Internet.



Program	Allow connect	Allow server	Pass Lock
mcupdate.exe 3/8/2000 16:50:00	Local: ✓ · · Internet: ✓ · ·	□ □	□
ZoneAlarm Internet Security Utility 2.1.44	Local: · · ? Internet: · · ?	□ □	□
Internet Explorer 5.00.2920.0000	Local: ✓ · · Internet: ✓ · ·	□ □	□
Microsoft Windows(TM) Messaging Subsyste 5.5	Local: ✓ · · Internet: ✓ · ·	☑ ☑	□
Microsoft Outlook 9.0.2416	Local: ✓ · · Internet: ✓ · ·	☑ ☑	□
Services and Controller app 5.00.2134.1	Local: ✓ · · Internet: ✓ · ·	□ □	□

ZoneAlarm Internet Security Utility connecting to Internet.

BACK HOME NEXT

Copyright © 1999-2001 Zone Labs, Inc.

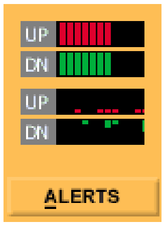
All rights reserved. ZoneAlarm and ZoneAlarm Pro include TrueVector Technology, covered by U.S. Patent No. 5,987,611. Zone Labs, ZoneAlarm, ZoneAlarm Pro, and TrueVector are registered trademarks of Zone Labs, Inc.

The Alerts Panel

Up/Down Graphs

Click on the ALERTS button to display the entire Alerts panel.

Notice the two sets of UP/DN (Up/Down) graphs inside the Alerts icon. On your machine, whenever data is being uploaded to the Internet, red bars are displayed inside the two UP graphs. Whenever data is being received (downloaded), green bars are displayed inside the DN graphs. If there is no activity to/from the Internet, ZoneAlarm will display "ZA" on a red and yellow background.



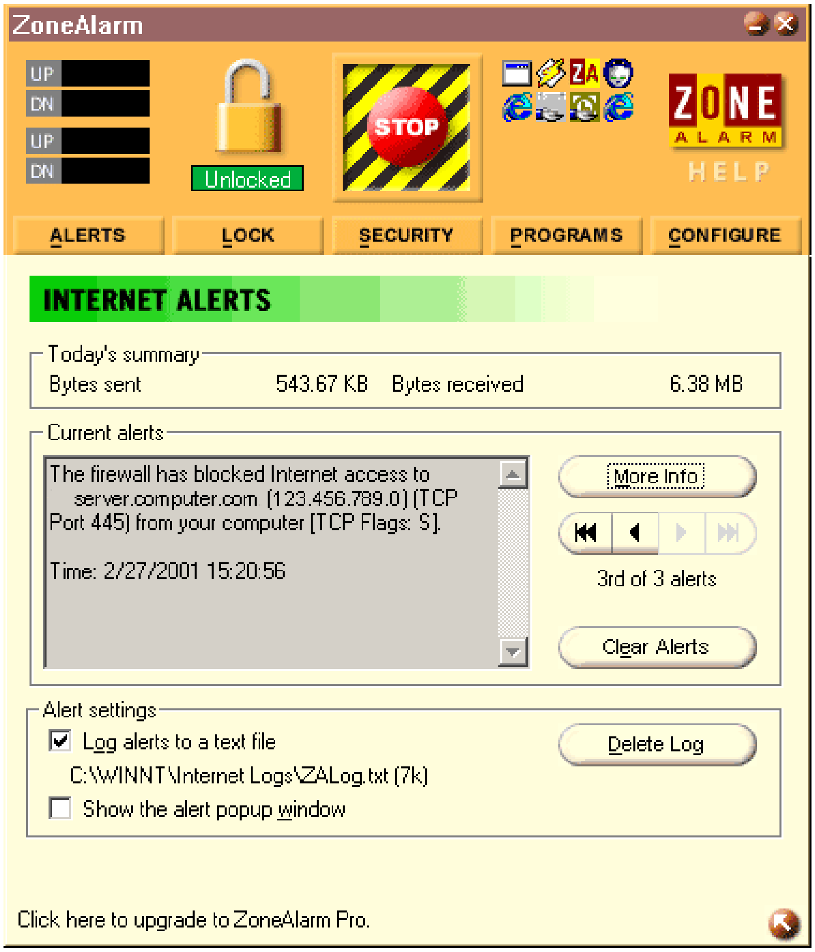
- The two graphs in the top portion of the icon display Internet traffic as it occurs.
- The two graphs in the lower portion of the icon display a chronological history of Internet traffic as it is generated on your machine.
- Whenever red or green flashing bars appear in the Alerts icon, the application receiving or sending traffic is shown as a blinking icon inside the Programs icon.

You might also notice traffic being displayed when you are not on the Internet. This is local broadcast traffic from your NIC. Broadcast messages are sent to all computers that are part of a specific network. A computer's network adapter filters traffic on the hardware level. Any traffic that does not have the hardware address of your network interface card is automatically discarded so therefore, it is not being transmitted to the Internet.

Similarly, there may be times when you are not logged into the Internet yet you see activity lights on your DSL/Cable Modem. Depending on the equipment used by your DSL/Cable provider, your computer may be receiving broadcast messages that are transmitted throughout the Internet or a Local Area Network. The Ethernet card on your computer automatically discards these broadcast messages if the data is not intended for your computer.

Expanded Alert Panel

At the top of the panel, *Today's Summary* shows the total amount of data sent and received by all applications. The middle portion of the panel details Current Alerts. In the Alert Settings area, at the bottom of the panel, there are options to display and save alerts.



Today's summary

Bytes sent 543.67 KB Bytes received 6.38 MB

Current alerts

The firewall has blocked Internet access to server.computer.com (123.456.789.0) (TCP Port 445) from your computer [TCP Flags: S].

Time: 2/27/2001 15:20:56

Alert settings

☑ Log alerts to a text file

C:\WINNT\Internet Logs\ZALog.txt (7k)

□ Show the alert popup window

More Info button: The Alert messages generated by ZoneAlarm contain information on what ZoneAlarm is blocking. Internet traffic is identified by unique IP addresses. Pressing the More Info button calls the Zone Labs Alert Analyzer which provides additional information on traffic blocked by ZoneAlarm.

Sample Log Entries — See samples of the three types of alerts in the log file.

BACK HOME NEXT

Copyright © 1999-2001 Zone Labs, Inc.

All rights reserved. ZoneAlarm and ZoneAlarm Pro include TrueVector Technology, covered by U.S. Patent No. 5,987,611. Zone Labs, ZoneAlarm, ZoneAlarm Pro, and TrueVector are registered trademarks of Zone Labs, Inc.

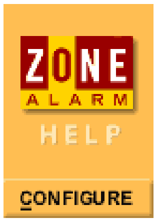
The Configuration Panel

Use the configuration panel to set the basic operational characteristics for ZoneAlarm.

Configuration Panel
Older Windows Versions

Configuration Panel

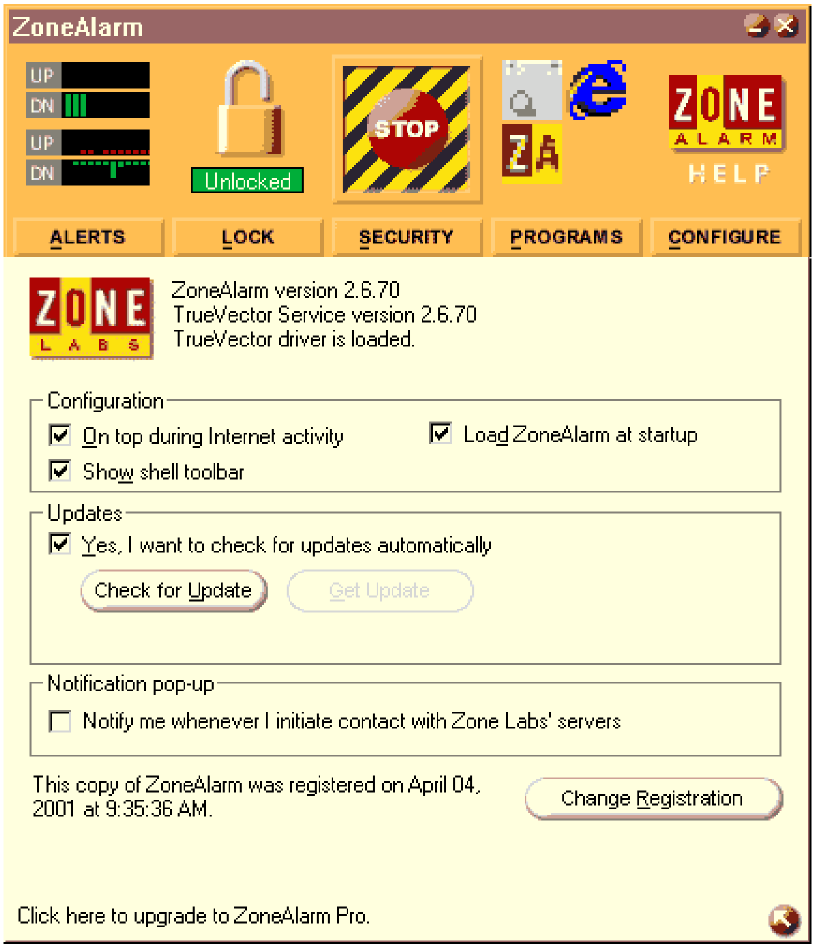
Click the CONFIGURE button to display the Configuration panel. This button is located directly below the Help button in the top right corner of ZoneAlarm. Use the checkboxes and pushbuttons in the Configuration Panel to determine whether:



- ZoneAlarm should be displayed on top of other applications on your computer screen when Internet activity is selected
- The Desk Band Tool bar should be displayed (applies to Win95 and NT4 only)
- ZoneAlarm should load when you start your computer
- To check for product updates
- To change the registration information you've submitted to Zone Labs

The first checkbox on the Configuration Panel is *On top during Internet activity*. This checkbox controls whether or not ZoneAlarm will be displayed ON TOP of other applications whenever Internet activity is detected.

The *Load ZoneAlarm at Startup* checkbox is selected by default. This causes ZoneAlarm to be loaded when you start your computer. If you uncheck this checkbox, Internet traffic monitoring will not begin until you start ZoneAlarm on your machine.



ZoneAlarm version 2.6.70
TrueVector Service version 2.6.70
TrueVector driver is loaded.

Configuration
☑ On top during Internet activity ☑ Load ZoneAlarm at startup
☑ Show shell toolbar

Updates
☑ Yes, I want to check for updates automatically
Check for Update Get Update

Notification pop-up
☐ Notify me whenever I initiate contact with Zone Labs' servers

This copy of ZoneAlarm was registered on April 04, 2001 at 9:35:36 AM.
Change Registration

Click here to upgrade to ZoneAlarm Pro.

Older Windows Versions

Older versions of Windows 95 or Windows NT (those without the Windows Shell

Update) let you choose a "Show shell toolbar" checkbox.

Under newer versions and Windows 98 or Windows 2000, this option is part of the Windows Shell. See the Desk Band toolbar for more information.

- The Check for update button: Click to check the web for ZoneAlarm product updates
- The Change Registration button: Click to review and change your ZoneAlarm registration information

BACK HOME NEXT

Copyright © 1999-2001 Zone Labs, Inc.

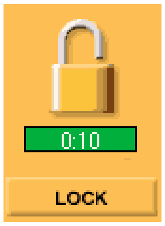
All rights reserved. ZoneAlarm and ZoneAlarm Pro include TrueVector Technology, covered by U.S. Patent No. 5,987,611. Zone Labs, ZoneAlarm, ZoneAlarm Pro, and TrueVector are registered trademarks of Zone Labs, Inc.

The Lock Panel

The purpose of the lock is block all network activity inbound and outbound from your computer. Therefore, only use the lock during extended inactivity of your PC.

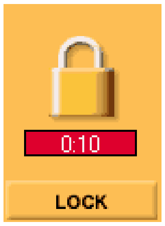
Locking

Click on the LOCK button to display the entire Lock panel, where you can set options for the Internet Lock. The Lock button is located at the bottom of the Lock Icon, shown below. A locked or unlocked padlock is displayed in the middle of the icon. To immediately turn Internet access on or off for all the applications installed on your machine that are not set to bypass the lock, click directly on the padlock.



When the Timer Bar below the Lock button is green, the Internet Lock is not on. This means that ZoneAlarm is allowing Internet traffic in and out of your computer.

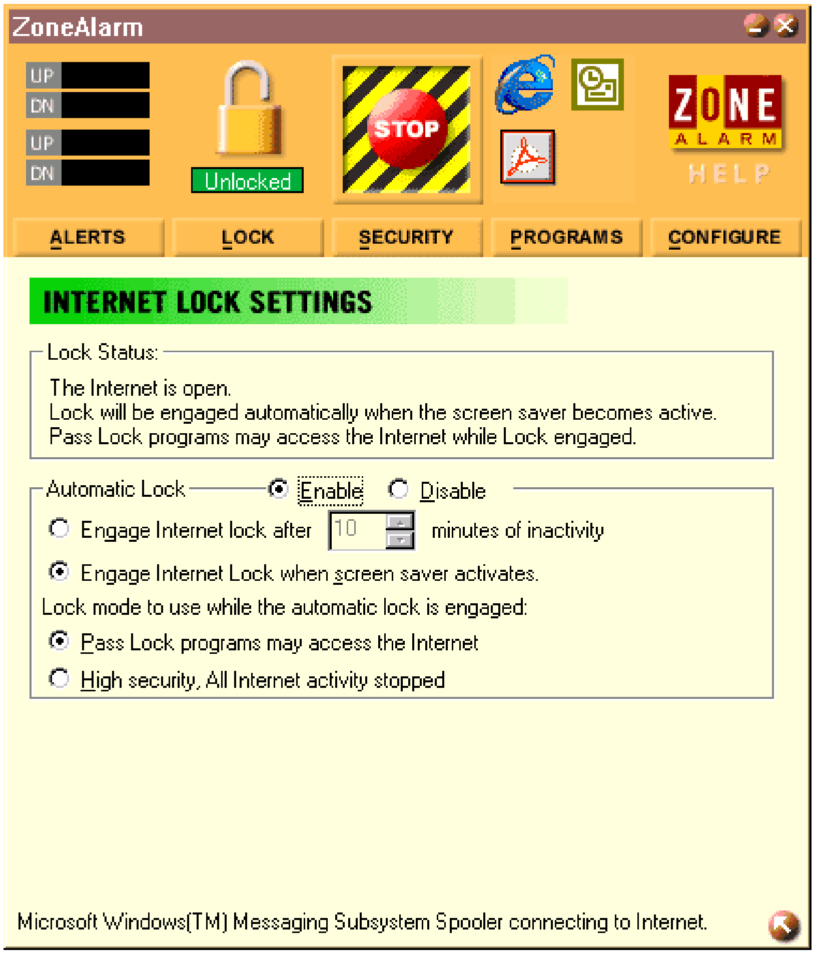
If the timer bar displays a countdown timer, this is the time remaining before the Automatic Lock will engage.



When the timer bar is red, the lock is closed and no in-and-out Internet traffic is allowed. When the lock is closed, the countdown timer counts upwards, showing the amount of time the lock has been active.

Expanded Lock Panel

When expanded, the Internet lock settings panel allows you to configure the Automatic Lock. You can choose to lock Internet access automatically when your screen saver activates or after a *period of Internet inactivity* on your computer.



INTERNET LOCK SETTINGS

Lock Status:

The Internet is open.
Lock will be engaged automatically when the screen saver becomes active.
Pass Lock programs may access the Internet while Lock engaged.

Automatic Lock ● Enable ○ Disable

○ Engage Internet lock after 10 minutes of inactivity

● Engage Internet Lock when screen saver activates.

Lock mode to use while the automatic lock is engaged:

● Pass Lock programs may access the Internet

○ High security, All Internet activity stopped

Microsoft Windows(TM) Messaging Subsystem Spooler connecting to Internet.

If Internet access is locked when the screen saver activates, it will be unlocked when the screen saver is deactivated.

Note, however, that if the Automatic Lock is engaged by the period of inactivity option, you will need to click on the Lock button to unlock Internet Access.

The Lock Mode for the Automatic Lock can be set so that "Pass Lock programs may access the Internet." This allows Internet activity for applications that have been given rights to bypass the lock. Typically programs like e-mail clients will be set to check for e-mail while other applications are denied Internet Access.

High Security mode will STOP all applications' Internet activity regardless of the program's access settings. See Programs for more information.

BACK HOME NEXT

Copyright © 1999-2001 Zone Labs, Inc.

All rights reserved. ZoneAlarm and ZoneAlarm Pro include TrueVector Technology, covered by U.S. Patent No. 5,987,611. Zone Labs, ZoneAlarm, ZoneAlarm Pro, and TrueVector are registered trademarks of Zone Labs, Inc.

The Programs Panel

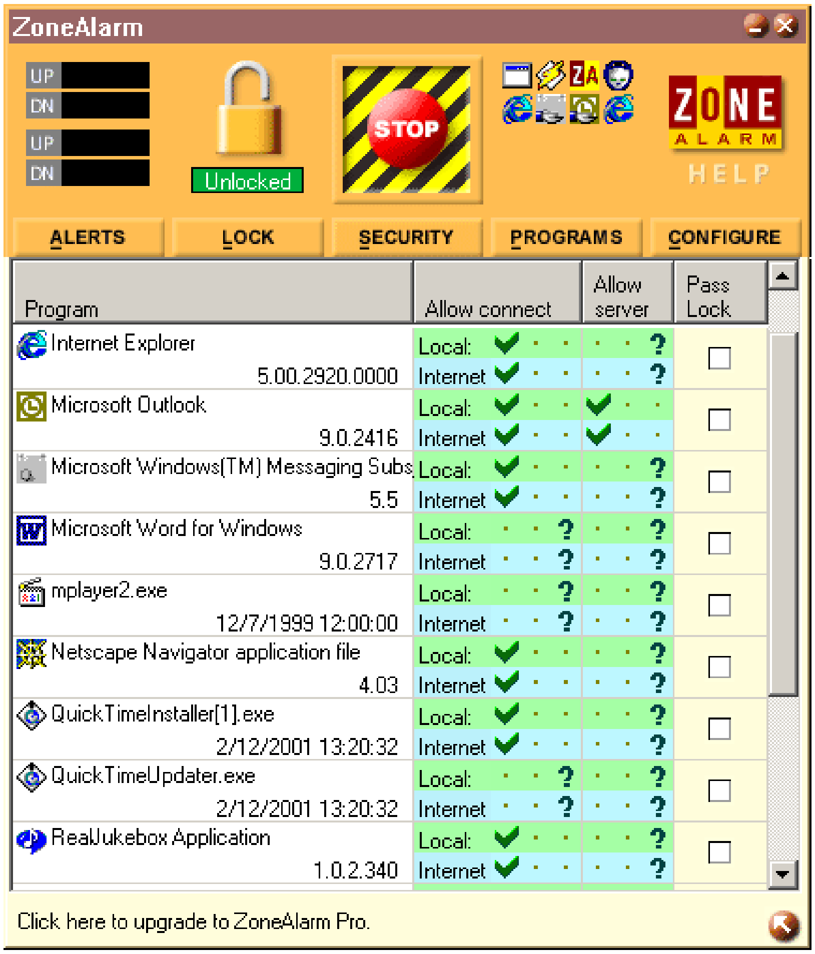
The programs panel shows programs that have attempted to access the Internet.

Programs Panel

The main portion of the Programs panel is the Program List. This is the list of programs installed on your machine that have attempted to connect to the Internet. Use the checkboxes in this panel to control the connection behavior of any program on the list or to specify each program's access rights for the Local Zone or the Internet Zone.

The same functions are available in the popup menu which you call by right-clicking on a program name in the Program list.

In the Program List, the Allow server column lets you control which applications can perform server functions. Run your cursor over the Programs List or right-click an entry in the list to see more statistics.



Program		Allow connect	Allow server	Pass Lock
Internet Explorer 5.00.2920.0000	Local:	✓ · ·	· · ?	☐
	Internet	✓ · ·	· · ?	
Microsoft Outlook 9.0.2416	Local:	✓ · ·	✓ · ·	☐
	Internet	✓ · ·	✓ · ·	
Microsoft Windows(TM) Messaging Subs 5.5	Local:	✓ · ·	· · ?	☐
	Internet	✓ · ·	· · ?	
Microsoft Word for Windows 9.0.2717	Local:	· · ?	· · ?	☐
	Internet	· · ?	· · ?	
mplayer2.exe 12/7/1999 12:00:00	Local:	· · ?	· · ?	☐
	Internet	· · ?	· · ?	
Netscape Navigator application file 4.03	Local:	✓ · ·	· · ?	☐
	Internet	✓ · ·	· · ?	
QuickTimeInstaller[1].exe 2/12/2001 13:20:32	Local:	✓ · ·	· · ?	☐
	Internet	✓ · ·	· · ?	
QuickTimeUpdater.exe 2/12/2001 13:20:32	Local:	· · ?	· · ?	☐
	Internet	· · ?	· · ?	
RealJukebox Application 1.0.2.340	Local:	✓ · ·	· · ?	☐
	Internet	✓ · ·	· · ?	

Click here to upgrade to ZoneAlarm Pro.

Using the Panel

Go to the Allow connect column in the main body of the panel to change a program's permissions. Click directly on the . . . to change the access level from ? to check mark to X. Click on the . . . in the same way in the Allow server column.

In the Program column, the program's name and version number are displayed. Run your mouse over the program name to see more statistics:

- Product name
- The name of the file used to access the Internet
- The location of the file

- Product version
- Creation date and file size

BACK HOME NEXT

Copyright © 1999-2001 Zone Labs, Inc.

All rights reserved. ZoneAlarm and ZoneAlarm Pro include TrueVector Technology, covered by U.S. Patent No. 5,987,611. Zone Labs, ZoneAlarm, ZoneAlarm Pro, and TrueVector are registered trademarks of Zone Labs, Inc.

The Security Panel

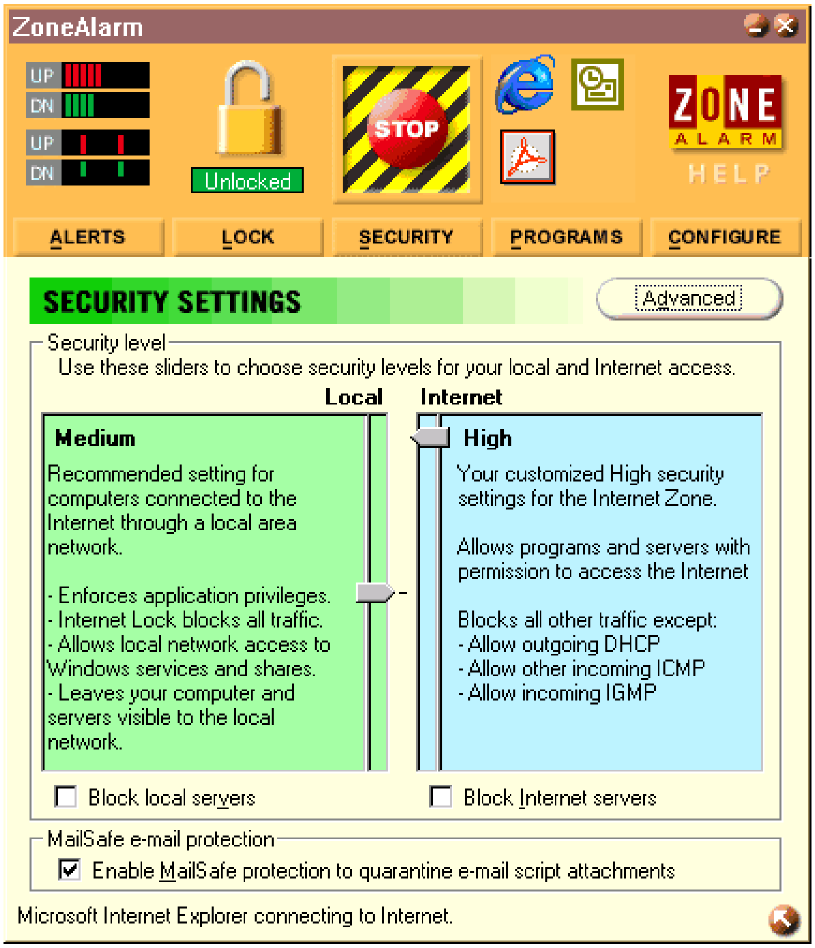
The Security panel is used to regulate ZoneAlarm's protection levels.

Security Panel
Related Links

Security Panel

The Local and Internet Zone each have a security level selector, that you drag up and down to change the security level. Local Zone security is displayed in green, and Internet Zone security in blue. The default settings are:

- medium for the Local Zone
- high for the Internet Zone



Security level
Use these sliders to choose security levels for your local and Internet access.

Local	Internet
Medium Recommended setting for computers connected to the Internet through a local area network. - Enforces application privileges. - Internet Lock blocks all traffic. - Allows local network access to Windows services and shares. - Leaves your computer and servers visible to the local network.	**High** Your customized High security settings for the Internet Zone. Allows programs and servers with permission to access the Internet Blocks all other traffic except: - Allow outgoing DHCP - Allow other incoming ICMP - Allow incoming IGMP
□ Block local servers	□ Block Internet servers

MailSafe e-mail protection
☑ Enable MailSafe protection to quarantine e-mail script attachments

Microsoft Internet Explorer connecting to Internet.

Use the block servers checkbox for each zone to prevent all programs from acting as servers for that zone. By checking this option, no application will be allowed to listen for incoming connections in that zone, even if you've checked the Allow Server option in the Programs panel.

Related Links

- For a definition of the Local and Internet Zones, click here.
- For instructions how to use the Advanced button, to add computers to your Local Zone, click here.
- For a description of MailSafe features, click here.

BACK HOME NEXT

Copyright © 1999-2001 Zone Labs, Inc.

All rights reserved. ZoneAlarm and ZoneAlarm Pro include TrueVector Technology, covered by U.S. Patent No. 5,987,611. Zone Labs, ZoneAlarm, ZoneAlarm Pro, and TrueVector are registered trademarks of Zone Labs, Inc.

The Programs List

This page describes the Program List, where you manage applications on your computer that access the Internet.

About the Program List

Software applications are automatically added to the Programs list the first time they attempt to access the Internet.

You can find detailed information about an application by hovering the mouse pointer over the entry. A tool tip will display the location and other information about the application. If there is a problem with the colors of a tool tip, the problem could be related to your video driver and/or display settings. If this occurs, try using 256 colors. You can set display options in the Windows Control Panel/Display.

There are a few ways to learn more about file names. You can contact the software vendor for any questions you may have regarding the location of the executable or the name of the file in your programs list. You can also run an Internet search.

Viewing the Programs List

Empty Programs List? Unless a system administrator configured the installation on your network, the Programs panel will probably display an empty white area when you first open it.

The white area of the Programs panel starts filling up as your applications start accessing the Internet. A separate line in the white area is reserved for each program that connects.

Adding a Program to the List

Programs are automatically added to the Programs List when they have attempted accessing the Internet. After the program has been added to the Program List, you have the ability to:

- Prevent the program from connecting to the Internet or from listening as a server.
- Remove the program from the Programs List.

BACK HOME NEXT

Copyright © 1999-2001 Zone Labs, Inc.

All rights reserved. ZoneAlarm and ZoneAlarm Pro include TrueVector Technology, covered by U.S. Patent

No. 5,987,611. Zone Labs, ZoneAlarm, ZoneAlarm Pro, and TrueVector are registered trademarks of Zone Labs, Inc.

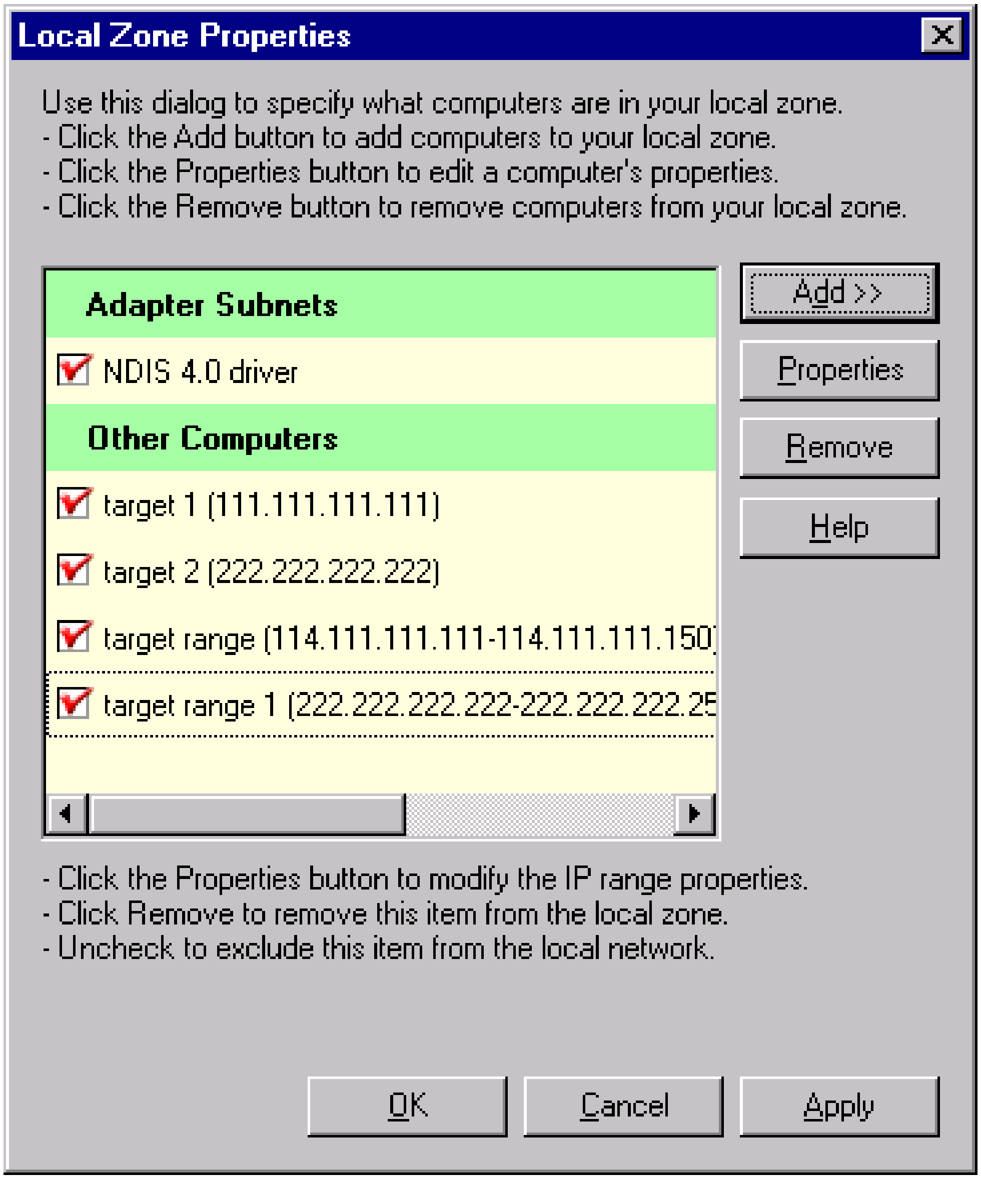
Adding Sites to the Local Zone

This page explains how to add the subnets and computers you trust to your Local Zone.

Managing the Local Zone

For LAN users, check the box next to a subnet that ZoneAlarm placed in the dialog at installation. To add other computers and web sites, first add the computer then check the box next to it.

To open the dialog, click the Advanced button.



Use this dialog to specify what computers are in your local zone.
- Click the Add button to add computers to your local zone.
- Click the Properties button to edit a computer's properties.
- Click the Remove button to remove computers from your local zone.

Adapter Subnets

☑ NDIS 4.0 driver

Other Computers

☑ target 1 (111.111.111.111)

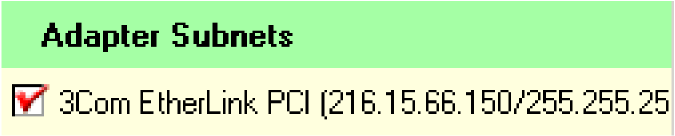
☑ target 2 (222.222.222.222)

☑ target range (114.111.111.111-114.111.111.150

☑ target range 1 (222.222.222.222-222.222.222.25

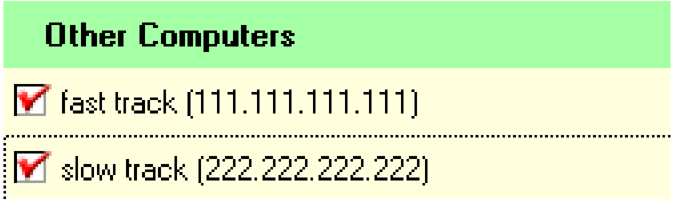
- Click the Properties button to modify the IP range properties.
- Click Remove to remove this item from the local zone.
- Uncheck to exclude this item from the local network.

The dialog has two sections. Click on either of the graphics below for a quick explanation:



Adapter Subnets

☑ 3Com EtherLink PCI (216.15.66.150/255.255.25



Other Computers

☑ fast track (111.111.111.111)

☑ slow track (222.222.222.222)

After checking the box for any network or computer in this dialog, it becomes a member of your Local Zone. A security setting of Medium or High will allow secure communications and file and printer sharing between all components you've added here.

For Single PC Home Users

If you are a single PC user at home, you are not required to use this dialog because your PC is probably the only machine you are trying to protect. As a single user, you don't really need to add any more computers in order to work safely.

The Network section of the dialog will always have an entry in it displaying the subnet your modem or DSL connection installed on your machine. You don't need to check the box if you are working by yourself.

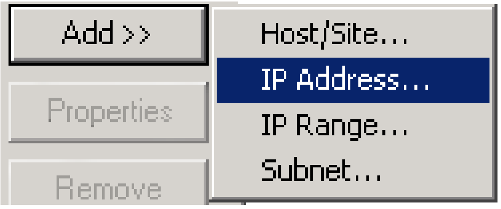
The Other Computers section is where you add any trusted web site or the IP address of a computer that you trust and want to do file sharing with.

If You Are Connected to A LAN

If you are user working as part of a Local Area Network (LAN), make sure the entry in the Network section is checked if it represents the subnet of your LAN adapter. The red checkmark tells ZoneAlarm that you trust your LAN connection and that you really want to share connectivity with the users on that LAN.

If your company or work group has more than one subnet, you need to go to the Other Computers section to add the subnets that are not identified by the LAN adapter on your machine. ZoneAlarm picked up the adapter subnet from your LAN adapter at installation time and placed it in the Network section.

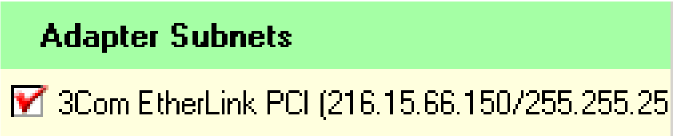
You have to manually add additional subnets you have in your organization by clicking on the Add button then entering the IP address and subnet mask in the Other Computers Section of this dialog:



With ZoneAlarm installed and running, all the IP addresses of subnets that are not identified in your LAN adapter have to be included here so that applications residing on those subnets can be accessed from your PC whenever Local Zone security is set to Medium or High.

Add a Network Subnet

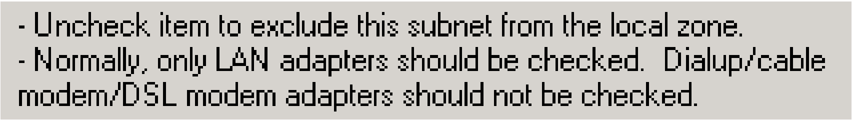
The green Adapter Subnets section lists subnets identified by your LAN adapter or by your DSL or dial-up modem connection to the Internet:



Adapter Subnets

☑ 3Com EtherLink PCI (216.15.66.150/255.255.25

When you click directly on the yellow area, the message at the bottom of the panel changes to tell you that you can't manually add Network Subnets yourself:



- Uncheck item to exclude this subnet from the local zone.
- Normally, only LAN adapters should be checked. Dialup/cable modem/DSL modem adapters should not be checked.

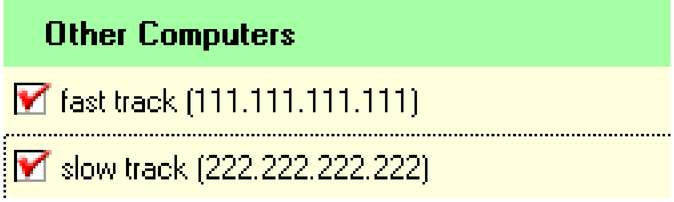
When you check the box, the message changes to tell you what your checkmark will do, and not to check the box if the entry corresponds to a dialup or cable modem adapter or a DSL connection.

The red checkmark identifies the adapter as something you want ZoneAlarm to allow your PC to communicate with. Once the network is checked, you can access programs and sites located on the subnet.

Remember that if you are a single user, you don't need to worry about checking anything in this dialog until you become part of a LAN or for certain VPN installations.

Add Computers

The green Other Computers section is where you add IP addresses representing computers and web sites located on other LANs or somewhere on the Internet. You add them because you know enough about them to allow connections with them over the Internet.

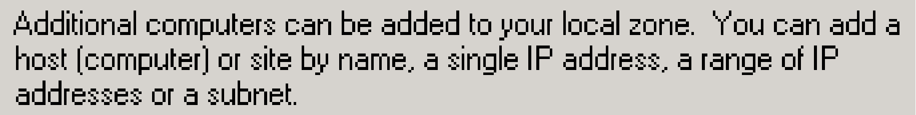


Other Computers

☑ fast track (111.111.111.111)

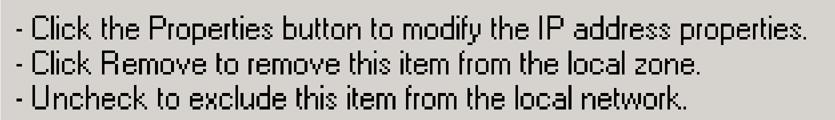
☑ slow track (222.222.222.222)

When you click on the yellow area directly, the message at the bottom of the panel changes to tell you about adding a computer here:



Additional computers can be added to your local zone. You can add a host (computer) or site by name, a single IP address, a range of IP addresses or a subnet.

When you click on the checkbox, the message changes to tell you what your check mark will do. It also tells you that clicking on Properties lets you see the definition that was entered for the computer or address represented by the entry.



- Click the Properties button to modify the IP address properties.
- Click Remove to remove this item from the local zone.
- Uncheck to exclude this item from the local network.

Any web sites and computers you add here will be those that are not specifically part of the LAN identified by your LAN adapter.

If you are a home user, this is where you add web sites and addresses that you know well enough to place inside your Local Zone. An individual user would use this dialog to add any computer other than his or her own PC that is familiar enough to be trusted.

For LAN users, if your company or work group has more than one subnet, here is where you add IP addresses of the subnets not identified by your LAN adapter.

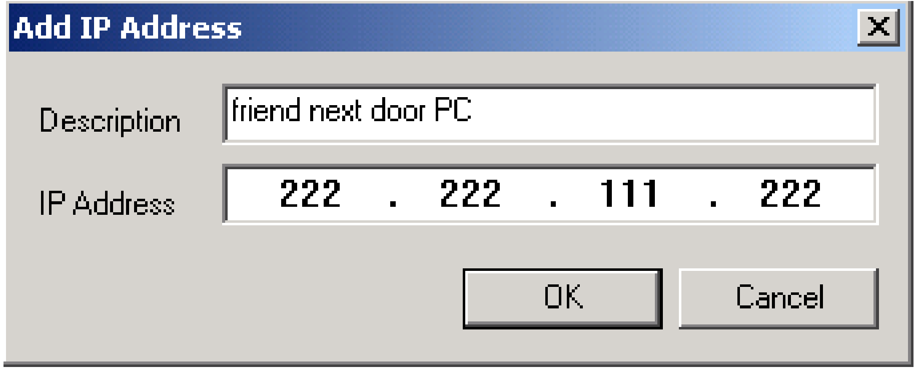
Steps to Add Computers

This section provides an example of how to add a computer to your Local Zone. (The message at the top of the dialog never changes. It displays the basic steps you need to follow to use the Add, Properties or Remove button.) Here is an example of the basic steps:

1. Click the Add button. The popup menu provides these choices:
   Host/Site...
   IP Address...
   IP Range...
   Subnet...

2. For this example, we click IP Address... to add your next-door neighbor's computer identified by its IP address.

3. Enter a short Description for display purposes only, and then your neighbor's IP address.



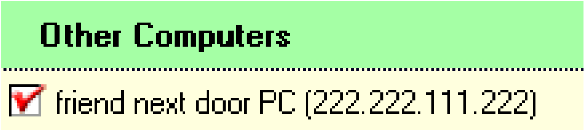
Add IP Address

Description: friend next door PC

IP Address: 222 . 222 . 111 . 222

4. Click the OK button.

You'll see your friend's computer, including the description you entered, displayed under Other Computers.



Other Computers

☑ friend next door PC (222.222.111.222)

This means that that computer is now in the Local Zone. Therefore, ZoneAlarm will allow you to communicate with your neighbor over the Internet. Other computers won't have that privilege because you have not told ZoneAlarm you trust them.

BACK HOME

Copyright © 1999-2001 Zone Labs, Inc.

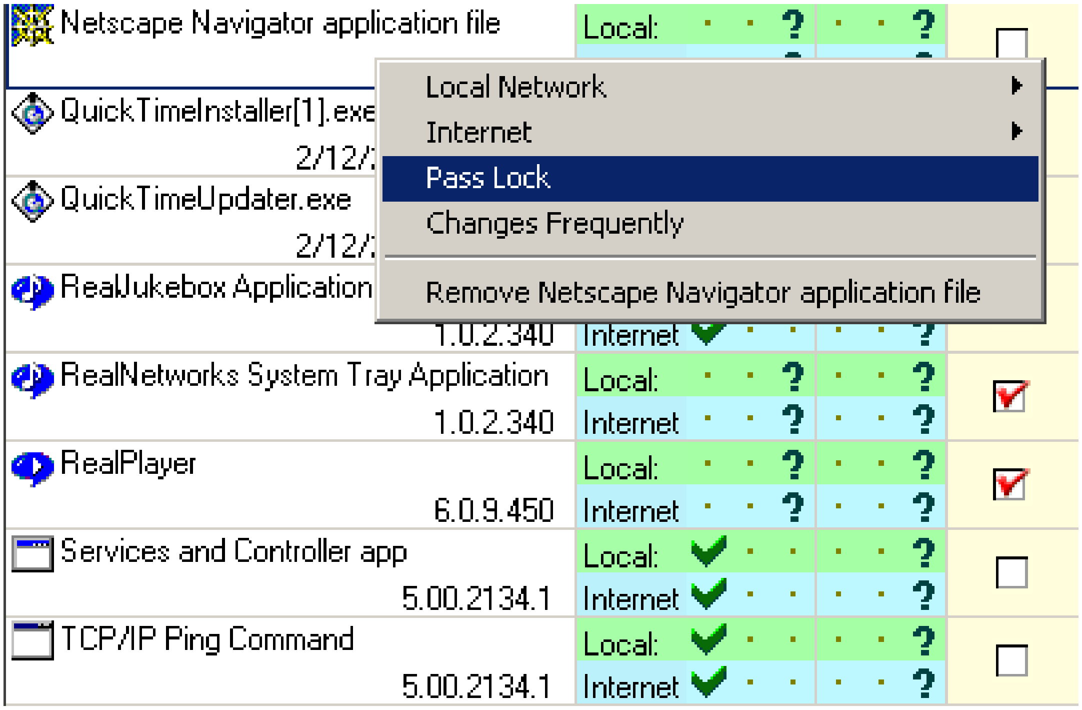
All rights reserved. ZoneAlarm and ZoneAlarm Pro include TrueVector Technology, covered by U.S. Patent No. 5,987,611. Zone Labs, ZoneAlarm, ZoneAlarm Pro, and TrueVector are registered trademarks of Zone Labs, Inc.

Passing a Program Through the Lock

How to set the Pass Lock

There are two different Locks that you can click on whenever you feel that your system shows an Internet security threat: the Lock icon and the Stop button. The Pass Lock function only works with the Lock icon because the Stop button stops ALL Internet traffic.

Right-click on a program, then select Pass Lock from the popup menu to allow a specific program to be able to bypass the lock whenever you stop other Internet traffic using the Lock icon.

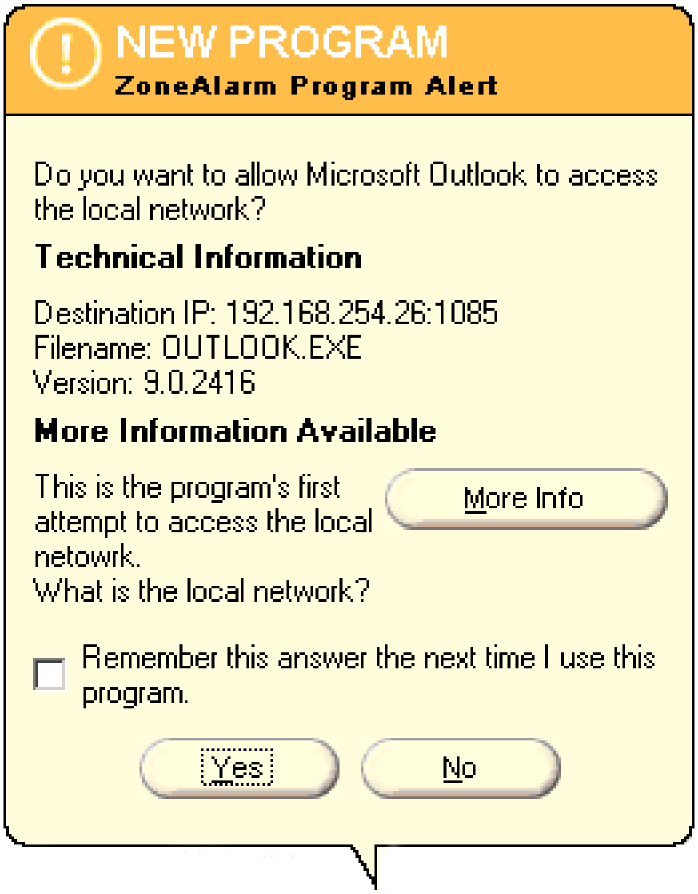


After making your selection, a check mark will be displayed to the left of the Pass Lock selection. You can view this check mark to verify that the Program has pass lock turned on by looking for the checkmark either on the popup menu that comes up when you right-click on the program; or, under the "Pass Lock" column to the right of the program name in the list.

This means that the program will be allowed to get around the Internet Lock and therefore access the Internet while the Lock remains in effect for all of your programs that are not specifically earmarked to bypass the lock.

Adding a program to the List

Adding a program to the list occurs only when the program issues an alert asking for permission to connect to the Internet. Until this time, a program will not be listed under "programs" in ZoneAlarm.



Do you want to allow Microsoft Outlook to access the local network?

Technical Information

Destination IP: 192.168.254.26:1085
Filename: OUTLOOK.EXE
Version: 9.0.2416

More Information Available

This is the program's first attempt to access the local netowrk.
What is the local network?

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

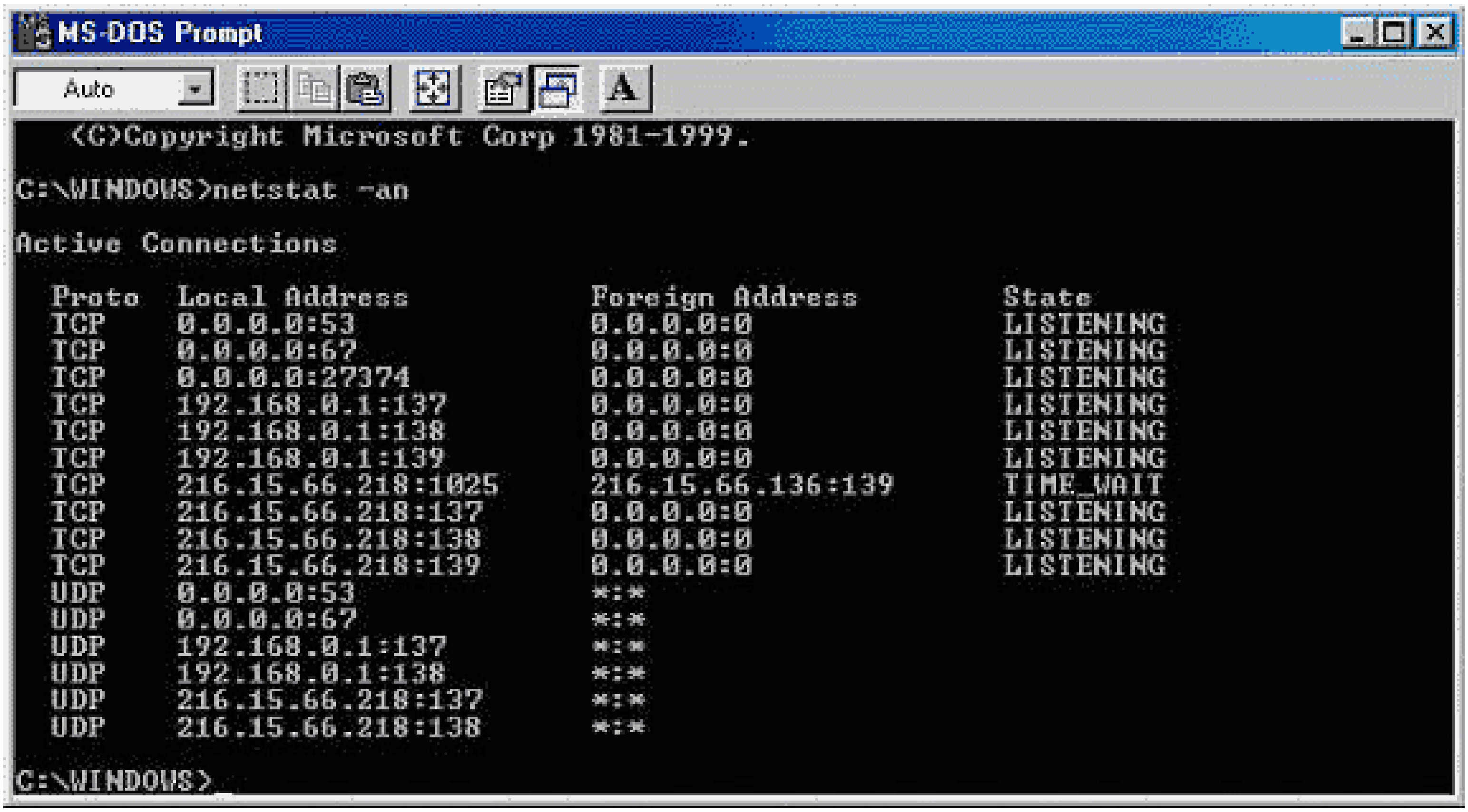
BACK HOME

Copyright © 1999-2001 Zone Labs, Inc.

All rights reserved. ZoneAlarm and ZoneAlarm Pro include TrueVector Technology, covered by U.S. Patent No. 5,987,611. Zone Labs, ZoneAlarm, ZoneAlarm Pro, and TrueVector are registered trademarks of Zone Labs, Inc.

MD5 Checksum

If you run Netstat or another port monitoring utility, you might notice an unidentified application listening on a given port. You might even notice an application listening on a port when ZoneAlarm did not request permission for it to access the Internet. Applications in the Programs List not allowed to connect are the usual culprits to this phenomena. On the surface, it is easy to misconstrue listening on a port as a breach of security, but, in fact, ZoneAlarm is performing exactly as designed.



```
   (C)Copyright Microsoft Corp 1981-1999.

C:\WINDOWS>netstat -an

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:53             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:67             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:27374          0.0.0.0:0              LISTENING
  TCP    192.168.0.1:137        0.0.0.0:0              LISTENING
  TCP    192.168.0.1:138        0.0.0.0:0              LISTENING
  TCP    192.168.0.1:139        0.0.0.0:0              LISTENING
  TCP    216.15.66.218:1025     216.15.66.136:139      TIME_WAIT
  TCP    216.15.66.218:137      0.0.0.0:0              LISTENING
  TCP    216.15.66.218:138      0.0.0.0:0              LISTENING
  TCP    216.15.66.218:139      0.0.0.0:0              LISTENING
  UDP    0.0.0.0:53             *:*
  UDP    0.0.0.0:67             *:*
  UDP    192.168.0.1:137        *:*
  UDP    192.168.0.1:138        *:*
  UDP    216.15.66.218:137      *:*
  UDP    216.15.66.218:138      *:*

C:\WINDOWS>_
```

ZoneAlarm's dual-layer security architecture actually permits traffic attempting to bypass a normal socket layer to pass through to the point where it reaches the firewall. At that point, having the impression that it successfully bypassed the port, the application may attempt to communicate to the Internet. ZoneAlarm intercepts that communication. ZoneAlarm authenticates applications through an MD5 checksum, a process that detects and prevents Trojans renamed as legitimate applications from getting through. The full stateful inspection firewall is enhanced with True Vector to have one main rule: "Don't let anything in or out." After that rule, it goes on to check whether applications are allowed or disallowed, verifies ports and protocols, and specifies configurations and so forth.

Many of the other firewalls today, do their application verification process through name recognition. Hackers can easily exploit this weakness. In a matter of minutes, a hacker can create his or her own malicious application that has the same name or properties as a legitimate application and it will glide through the firewall. With ZoneAlarm, even if a hacker changes the name of an application to make it look legitimate, it will still be stopped because of the MD5 Checksum verification process.

BACK HOME NEXT

Copyright © 1999-2001 Zone Labs, Inc.

All rights reserved. ZoneAlarm and ZoneAlarm Pro include TrueVector Technology, covered by U.S. Patent No. 5,987,611. Zone Labs, ZoneAlarm, ZoneAlarm Pro, and TrueVector are registered trademarks of Zone Labs, Inc.

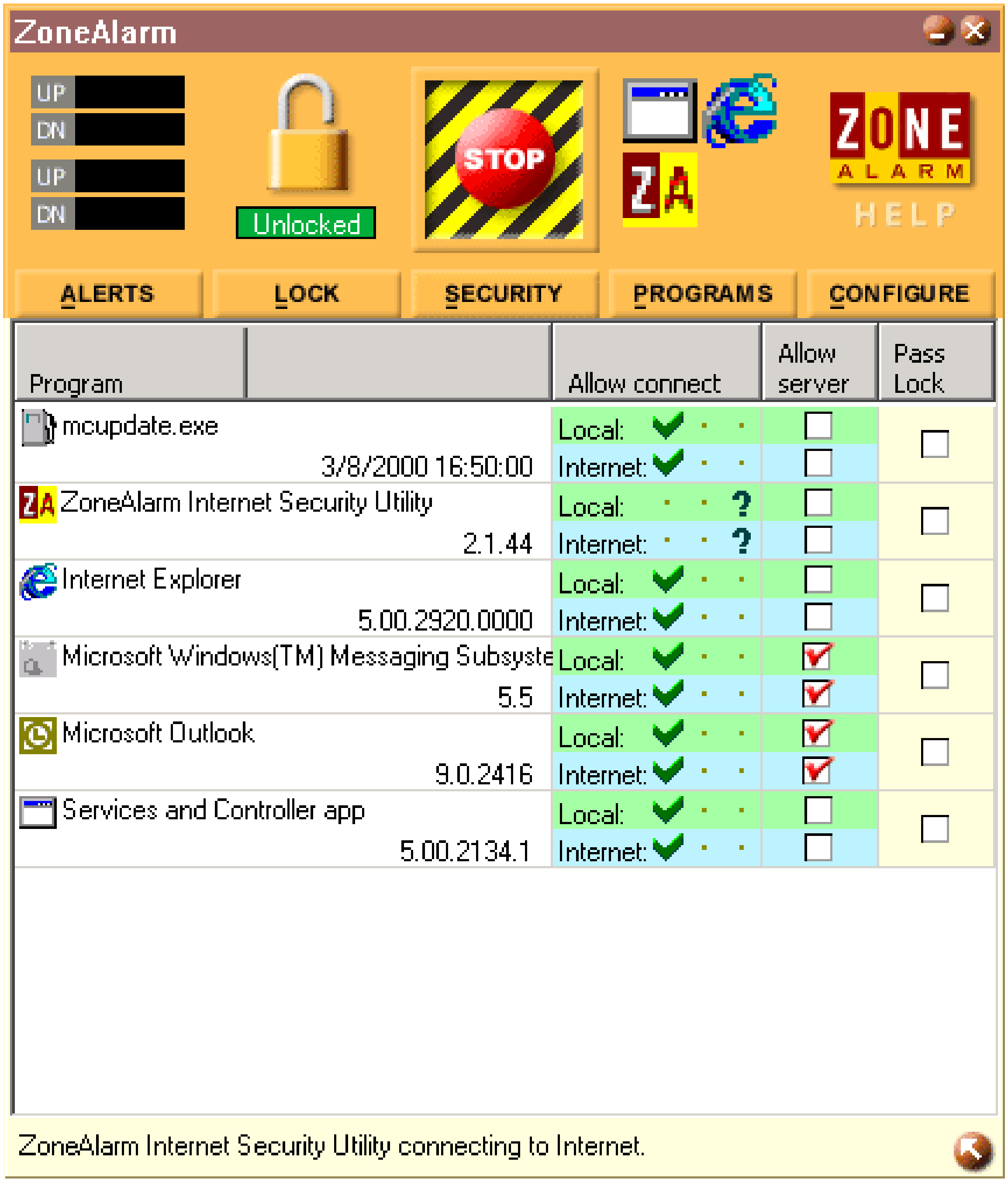
Using the Programs List

The Programs List is your tool for controlling the Internet connection behavior of your applications — what they are and are not allowed to do on the Internet.

Viewing Programs in the List

If you have just installed ZoneAlarm for the first time, your Programs List will be empty. To display the Program List, click Programs on the ZoneAlarm Main panel:

The list panel is displayed, showing all programs which have accessed the Internet since the installation of ZoneAlarm.

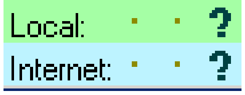


Program		Allow connect	Allow server	Pass Lock
mcupdate.exe	3/8/2000 16:50:00	Local: ✓ · · Internet: ✓ · ·	□ □	□
ZoneAlarm Internet Security Utility	2.1.44	Local: · · ? Internet: · · ?	□ □	□
Internet Explorer	5.00.2920.0000	Local: ✓ · · Internet: ✓ · ·	□ □	□
Microsoft Windows(TM) Messaging Subsyste	5.5	Local: ✓ · · Internet: ✓ · ·	☑ ☑	□
Microsoft Outlook	9.0.2416	Local: ✓ · · Internet: ✓ · ·	☑ ☑	□
Services and Controller app	5.00.2134.1	Local: ✓ · · Internet: ✓ · ·	□ □	□

ZoneAlarm Internet Security Utility connecting to Internet.

Allowing a Program to Connect

On each program line, the second column is the Allow connect column. Use this column to allow or deny the program access to the Internet.



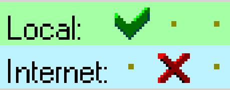
Local: · · ?
Internet: · · ?

If you have not changed anything, two question marks appear in the column, meaning you will always receive a ZoneAlarm message asking your permission when this program attempts access to the Internet.

Controlling Access to a Program

Remember, question marks mean your permission will be asked each time a program attempts to access the Internet.

Click on the ". . ." dots to change settings.



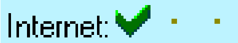
- The left one sets a checkmark (allow)
- The middle one sets an X (deny)
- The right one sets a question mark (ask)

Permissions and Zones

In the Programs List,

The TOP section governs the Local Zone:

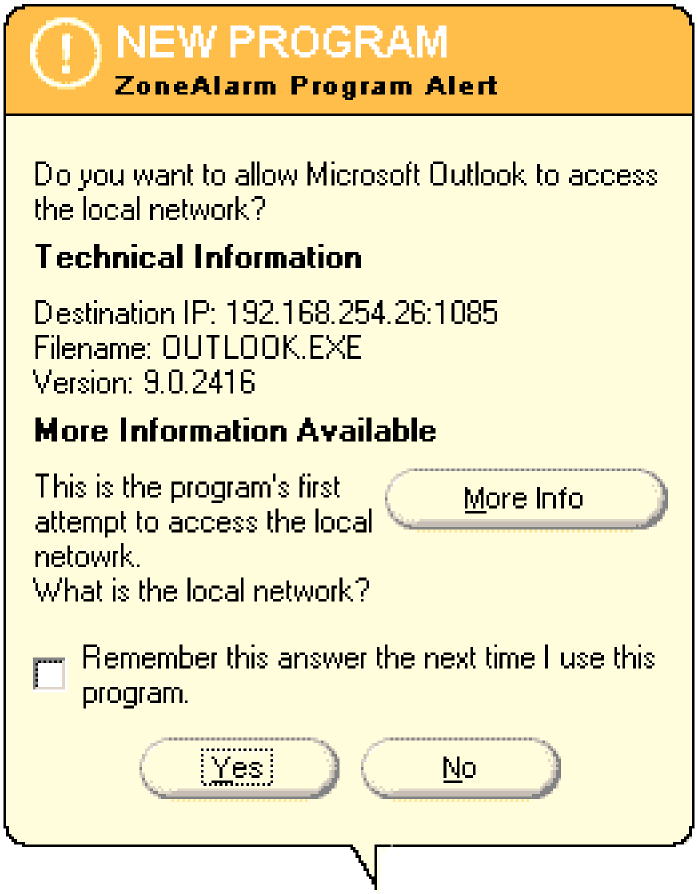
The BOTTOM section governs the Internet Zone:



Keep those zone-specific distinctions in mind and it will be clear that when you click on the top section, you are managing the program's access to locations you have defined in your Local Zone. When you click on the bottom section, you are managing the program's access to the entire Internet.

About Permission Messages

When ZoneAlarm asks your permission for a program to connect, a message like this one is displayed, containing the name of the program and your IP address:



NEW PROGRAM
ZoneAlarm Program Alert

Do you want to allow Microsoft Outlook to access the local network?

Technical Information

Destination IP: 192.168.254.26:1085
Filename: OUTLOOK.EXE
Version: 9.0.2416

More Information Available

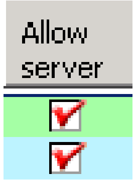
This is the program's first attempt to access the local netowrk.
What is the local network?

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

If you click the Remember this answer... checkbox, ZoneAlarm will not ask you about this permission again.

Allowing a Program to be a Server

Programs can play the role of a server, waiting or listening for incoming connections from the Internet. This column gives you the choice to stop or allow *server behavior* for each program.

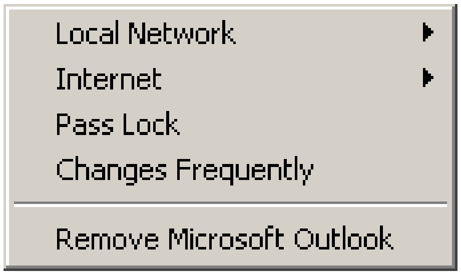


The Allow server column gives you the same choices as the Allow Connect column. ZoneAlarm can request your permission each time, or you can allow or deny server behavior to each program. These permissions also function by zone.

(See the Controlling Access and Permissions and Zones sections, above for a full explanation of settings.)

Right-clicking To Set Options

When you right-click a program in the Program List, the following choices are available to you. Click here for details about the menu choices.



Right-clicking a program in the list lets you define access rights for that program, or to remove it from the list. The rights you define are specific to either the *Local Zone* or the *Internet Zone*.

BACK HOME

Copyright © 1999-2001 Zone Labs, Inc.

All rights reserved. ZoneAlarm and ZoneAlarm Pro include TrueVector Technology, covered by U.S. Patent No. 5,987,611. Zone Labs, ZoneAlarm, ZoneAlarm Pro, and TrueVector are registered trademarks of Zone Labs, Inc.

Changed program

Do you want to allow a specific program to access the Internet?

What is a changed program?

CAUTION! A changed program is a program that has asked you for Internet or local network access rights in the past but has now CHANGED in some way. When a program changes, ZoneAlarm requires the program to ask for permission again so you're best protected.

How should I answer?

A changed program can be safe

If you've updated or reinstalled this program since the last time it accessed the Internet or local network or if this program automatically updates itself, it could show up as a changed program. If this is the case, it is probably safe to grant access rights to this program.

A changed program can be dangerous!

If you did not update this program since the last time it accessed the Internet or local network, it could be a malicious program planted on your computer that imitates a legitimate program. If this is the case, do not give this program access rights.

After you deny access rights, investigate the program as follows:

- Make a note of the program name, file name, and path of this program. Scan the file with your current virus scanner.
- If you have a dedicated Trojan scanner, scan with that as well. Make sure your virus or Trojan definitions are up to date.
- Check with the company Web site or Help support for the changed program,

to see if there are any legitimate reasons why the program might change.

Consider all of the above before deciding if your decision was right. You may change your decision at any time in the Programs panel.

How do I find out what the program is that that's asking for access?

Sometimes you can tell what a program is by its name; other times you may not. An unfamiliar program may be an important component of a known program, and may be needed by the known program in order to function:

- "Services and controller app" is a Windows component used by Microsoft Internet Explorer(TM) to access the Internet.
- "Microsoft Windows(TM) Messaging Subsystem Spooler" is a component of Microsoft Outlook(TM), used to get e-mail.

Therefore, some unfamiliar programs do need Internet access. Other unfamiliar programs, however, may be potentially harmful. If you don't recognize a program, start by reading our FAQ for a list of commonly unrecognized programs. If you can't find your answer there, try entering the program name into a search engine.

What else should I know?

There are a few ways you may answer a pop-up:

- Answer, "Yes," to give a program access rights just this one time. The next time the program needs to access the Internet , it will ask again.
- Answer, "No," to deny access rights just this one time. The next time the program needs to access the Internet, it will ask again.
- If you check, "Remember this answer the next time I use this program," before you click "Yes," or "No," the program will NOT ask you again. Your answer will be saved and applied each time the program tries to access the local network or the Internet.

You may change your answer any time in the Programs panel for any program by clicking on the interface.

A red X = deny access, a green checkmark = allow access, a black ? means ask me every time.

For further information

Knowledgebase Main Page
Zone Labs Home Page
Zone Labs Support Page

BACK HOME NEXT

Copyright © 1999-2001 Zone Labs, Inc.

All rights reserved. ZoneAlarm and ZoneAlarm Pro include TrueVector Technology, covered by U.S. Patent No. 5,987,611. Zone Labs, ZoneAlarm, ZoneAlarm Pro, and TrueVector are registered trademarks of Zone Labs, Inc.

Server program

ZoneAlarm has detected a program attempting to connect to, or to accept a connection from, the network.

More Information

The AlertAnalyzer is not able to determine whether this is a new, changed, repeat, or server program. The following general information is offered to help you understand the alert you received from ZoneAlarm or ZoneAlarm Pro.

Detailed Information

Rest assured, that ZoneAlarm or ZoneAlarm Pro will not permit this application to communicate with the local network or the Internet, until you give permission.

Some alerts result from not configuring ZoneAlarm or ZoneAlarm Pro optimally for your applications, your network or your ISP. To assist you in configuring and using ZoneAlarm, check out our Frequently Asked Questions pages, which are accessible from http://www.zonelabs.com/support.htm. Technical support is available via e-mail at support@zonelabs.com for questions not answered on the web site.

A wealth of information about firewalls and the interpretation of alerts can be found on the Internet. The Usenet newsgroup comp.security.firewalls, and the security-oriented discussion groups in the ShieldsUp section of grc.com, are particularly good sources of information.

For further information

Knowledgebase Main Page
Zone Labs Home Page
Zone Labs Support Page

BACK HOME NEXT

Copyright © 1999-2001 Zone Labs, Inc.

All rights reserved. ZoneAlarm and ZoneAlarm Pro include TrueVector Technology, covered by U.S. Patent No. 5,987,611. Zone Labs, ZoneAlarm, ZoneAlarm Pro, and TrueVector are registered trademarks of Zone Labs, Inc.

ZoneAlarm Overview

ZoneAlarm provides Internet security for any individual computer. It is an ideal tool for blocking unwanted Internet connections for machines using always-on DSL or cable modem connections. ZoneAlarm protects you from malicious programs, like Spyware and Trojan horses, by allowing you to control your computer's Internet traffic and the way applications access the Internet.

When an application on your computer tries to access the Internet, ZoneAlarm makes sure it has your permission first.

ZoneAlarm provides a dynamic firewall which allows you to independently establish protection levels for several zones. Set up the appropriate security level, such as Medium or High, for the computers in your Local Zone to allow secure file-sharing and print-sharing operations within your LAN.

The Internet Zone is usually set to High Security, making your computer invisible to computers throughout the Internet. By using High Security in the Internet Zone, you won't be a target for hackers or other types of intruders. It's very easy to set up security levels. Simply go to the Security Panel and drag the sliders up or down. This is all you need to do to configure the firewall. You don't need to be an expert in program protocols and ports.

You can then go further and customize security settings by clicking on the Advanced button on Security Panel, or apply application-specific security by right-clicking on a program name in the Programs Panel.

ZoneAlarm appears as a panel on your Windows desktop, shown below. You can also interact with ZoneAlarm using the Desk Band Toolbar.

BACK HOME NEXT

Copyright © 1999-2001 Zone Labs, Inc. All rights reserved. ZoneAlarm includes TrueVector Technology, covered by U.S. Patent No. 5,987,611. Zone Labs, ZoneAlarm, and TrueVector are registered trademarks of Zone Labs, Inc.

Troubleshooting and Technical Support

Deciphering a technical problem on your computer can be a complex task but there are a few methods of making the process easier. The first one is to carefully note specifics to what is occurring as the problem occurs. The sequence of events, the type of software and operating system in use as well as the limitations of hardware all play a factor. Then of course there are anomalies on the Internet which make additional deciphering necessary. For suspected problems with your Internet service, bookmark the web page for system status on your ISP.

Q: I can't access the Internet.
A: In ZoneAlarm and ZoneAlarm Pro, check your Security Panel and see what your Internet security settings are. If at high, lower to medium.

Can you ping your gateway? To determine what your gateway is, go to a DOS (or command) prompt and type `ipconfig/all`.

Your default gateway address should be displayed (along with other information, but for the moment, all you need is the gateway). From the command prompt, type `ping` *`[gateway address]`*. If you get a reply, it means you can communicate to and from the Internet.

If you run into a technical problem using ZoneAlarm, please visit the ZoneAlarm Support Site.

To provide you the answers you need as quickly as possible, our technical support site provides links to:

- Quick Support: This page provides quick answers to questions about using ZoneAlarm.
- FAQ Page: Get up-to-date answers by visiting the Frequently Asked Questions page.
- Release History: Use this page to check the release history for ZoneAlarm or use the automatic check for update feature.

BACK HOME NEXT

Copyright © 1999-2001 Zone Labs, Inc.

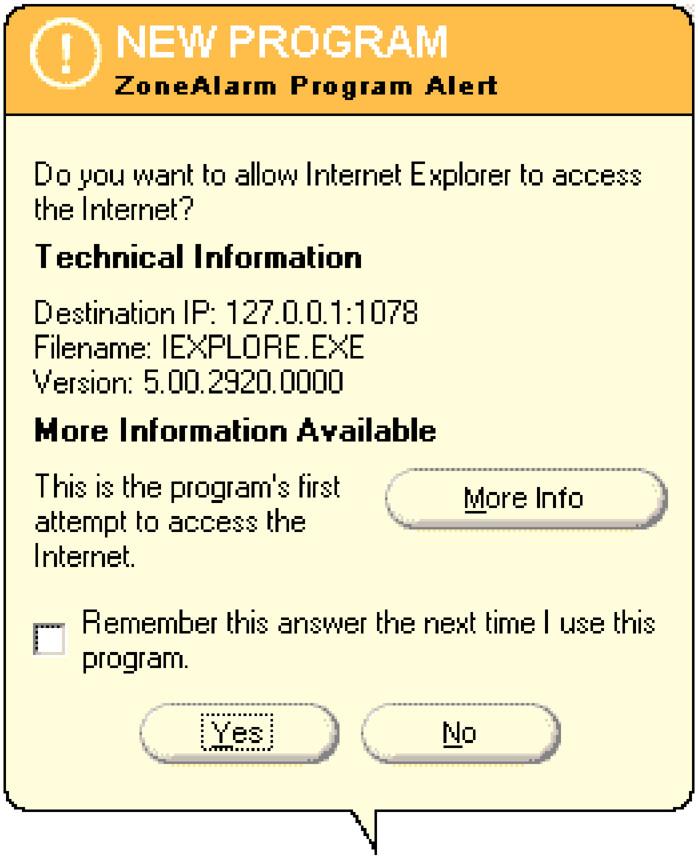
All rights reserved. ZoneAlarm and ZoneAlarm Pro include TrueVector Technology, covered by U.S. Patent No. 5,987,611. Zone Labs, ZoneAlarm, ZoneAlarm Pro, and TrueVector are registered trademarks of Zone Labs, Inc.

Program Permissions

Program permissions allow you to control program access by zone.

Permissions

When a program attempts to access the Internet for the first time, ZoneAlarm displays an alert, like the one shown below, and asks if you want to give that program permission to access the Internet.



NEW PROGRAM
ZoneAlarm Program Alert

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

Technical Information

Destination IP: 127.0.0.1:1078
Filename: IEXPLORE.EXE
Version: 5.00.2920.0000

More Information Available

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

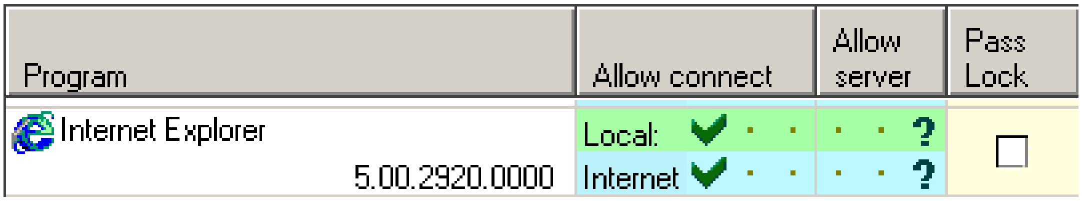
□ Remember this answer the next time I use this program.

- Selecting Yes allows the program to access the Internet until you quit the program.
- Selecting No denies the program Internet access until you close the program and open it again.

The default Internet access mode for all applications is to ask for permission each time you run the program. Check the Remember this answer checkbox to enforce your Yes or No decision without ZoneAlarm displaying the alert again. This is useful for programs that you always grant Internet access to, like your web browser.

Programs Panel

The Programs panel allows you to specify different access permissions for a program to each Zone. For example, you can allow an FTP Client access to the full Internet, but restrict your e-mail program to the Local zone.



Program	Allow connect	Allow server	Pass Lock
Internet Explorer 5.00.2920.0000	Local: ✓ · · Internet ✓ · ·	· · ? · · ?	□

BACK HOME

Copyright © 1999-2001 Zone Labs, Inc.

All rights reserved. ZoneAlarm and ZoneAlarm Pro include TrueVector Technology, covered by U.S. Patent No. 5,987,611. Zone Labs, ZoneAlarm, ZoneAlarm Pro, and TrueVector are registered trademarks of Zone Labs, Inc.

Server Activity

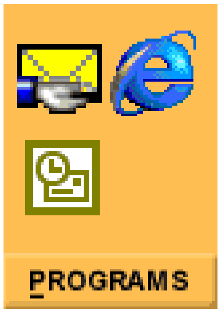
This page explains how to stop applications from accepting connections from outside your computer.

Detecting Possible Intrusion Requests

Many Trojan Horse programs are designed to be servers, waiting for connections and instructions from remote clients. You can use ZoneAlarm to detect server programs that are listening for such requests.

When ZoneAlarm detects server activity, the firewall will block the incoming connection for any program that is already on your Programs List where a red X appears in the Allow Server column.

Examples of server programs include Web, FTP, and e-mail servers.



The Programs icon indicates Internet servers and applications listening for connections by a hand holding the program icon.

To grant a specific program the right to act as a server, go to the Programs panel and check the Allow Server checkbox for that program. ZoneAlarm will deny connection, and display a popup warning when a program you have not given server permission to tries to connect.

Communication applications like ICQ or NetMeeting, usually require server rights in order to function properly with ZoneAlarm.

BACK HOME

Copyright © 1999-2001 Zone Labs, Inc.

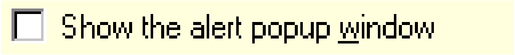
All rights reserved. ZoneAlarm and ZoneAlarm Pro include TrueVector Technology, covered by U.S. Patent No. 5,987,611. Zone Labs, ZoneAlarm, ZoneAlarm Pro, and TrueVector are registered trademarks of Zone Labs, Inc.

Popup Alerts

This page explains how to manage ZoneAlarm popup alerts boxes.

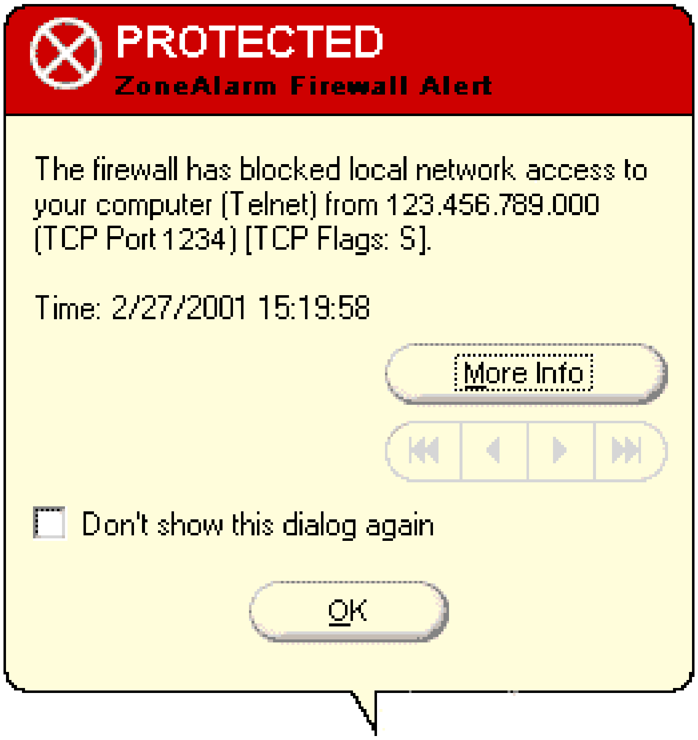
About Popup Alerts

The checkbox shown here controls whether Internet alerts are displayed on your computer screen. You can find this checkbox at the bottom of the Alerts panel. Unless you select this checkbox, you will not receive a popup display for Internet alerts.



□ Show the alert popup window

When the checkbox is checked, ZoneAlarm displays an alert popup whenever it blocks an Internet communication. A sample alert popup is shown here.



PROTECTED

ZoneAlarm Firewall Alert

The firewall has blocked local network access to your computer (Telnet) from 123.456.789.000 (TCP Port 1234) [TCP Flags: S].

Time: 2/27/2001 15:19:58

□ Don't show this dialog again

For more information on understanding alerts, check the section on Current Alerts. In the Alert Settings area, at the bottom of the panel, there are options to display and save alerts.

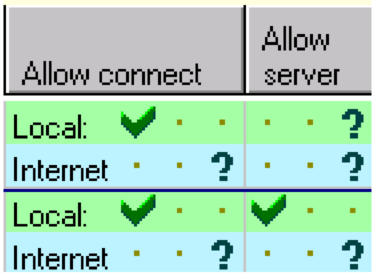
BACK HOME

Copyright © 1999-2001 Zone Labs, Inc.

All rights reserved. ZoneAlarm and ZoneAlarm Pro include TrueVector Technology, covered by U.S. Patent No. 5,987,611. Zone Labs, ZoneAlarm, ZoneAlarm Pro, and TrueVector are registered trademarks of Zone Labs, Inc.

Application Permissions

Programs installed on your computer have access rights to computers in two different zones: the Local Zone and the Internet Zone. ZoneAlarm security rules do not allow a program to have greater access to the Internet Zone than it has to the Local Zone.



	Allow connect	Allow server
Local:	✓ · ·	· · ?
Internet	· · ?	· · ?
Local:	✓ · ·	✓ · ·
Internet	· · ?	· · ?

A program's access rights are identified by a check mark, X or ?. To change a program's access rights, go to the Program List and make a selection in the Allow connect column, or right-click the program name. If you right-click, select Local Network to define Local Zone settings. Select Internet to define Internet Zone settings.

A check mark means that the program always has permission to connect without asking for your explicit permission.
SECURITY RULE: When you grant a program permission to access the Internet Zone at this level, ZoneAlarm automatically allows the program to have the same access to the Local Zone. You will see this when a check mark is automatically added to the Local Zone area.

An X means that the selected program is denied Internet access until you reset the permission.
SECURITY RULE: When Local Zone access permission is denied using the X, the selected program will automatically inherit the same access restrictions to the Internet Zone. You will see this when an X is automatically placed in the Internet Zone area of the Program List. This is the result of the following security rule: the Internet Zone cannot have greater access rights than the Local Zone.

A ? means that the program will ask permission each time it tries to connect. The permission request will be displayed on your computer screen in a popup window. In response, you decide whether or not to grant the requested permission by clicking on Yes or No. This is the default permission level assigned to all programs when they are added to the Program List.
SECURITY RULE: For any given program, you cannot enter a check mark for Internet Zone access if that program's Local Zone access is only established as a ?.

BACK HOME

Copyright © 1999-2001 Zone Labs, Inc.

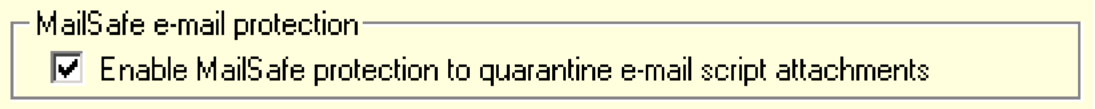
All rights reserved. ZoneAlarm and ZoneAlarm Pro include TrueVector Technology, covered by U.S. Patent No. 5,987,611. Zone Labs, ZoneAlarm, ZoneAlarm Pro, and TrueVector are registered trademarks of Zone Labs, Inc.

How to Manage MailSafe

MailSafe stops specific types of e-mail attachments from launching on your machine by quarantining them.

How to Turn on MailSafe

Go to the bottom of the Security panel to set up MailSafe. MailSafe is active by default, as shown by the selected checkbox below:



MailSafe e-mail protection

☑ Enable MailSafe protection to quarantine e-mail script attachments

The checkbox must be selected for MailSafe to work.

File Types that will be Quarantined

MailSafe protects your machine against viruses that come in the form of attachments, such as .vbs and .exe.

When an attachment is detected, ZoneAlarm quarantines it by changing the extension to .ZL#, where the # is a number or letter. For example, a file called SERVER.VBS will be renamed SERVER.ZL1.

BACK HOME NEXT

Copyright © 1999-2001 Zone Labs, Inc.

All rights reserved. ZoneAlarm and ZoneAlarm Pro include TrueVector Technology, covered by U.S. Patent No. 5,987,611. Zone Labs, ZoneAlarm, ZoneAlarm Pro, and TrueVector are registered trademarks of Zone Labs, Inc.

ZoneAlarm Help

GET STARTED

ADVANCED FEATURES

TROUBLESHOOT

USING THE INTERNET

GET SPECIAL INFO

* Articles with an asterisk require
you be connected to the Internet.

ZoneAlarm Overview

ZoneAlarm provides Internet security for any individual computer running a Windows platform using TCP/IP, which is the the standard protocol used for Internet traffic. In addition, ZoneAlarm works with any network transport (such as DSL, cable, T1/T3) as well as with dial-up connections.

ZoneAlarm protects you from malicious programs such as sniffers and Trojan horses by allowing you to control applications seeking access to the Internet. When an application on your computer tries to access the Internet, ZoneAlarm makes sure it has your permission first. In addition, ZoneAlarm is equipped with MailSafe, which guards your PC against potentially harmful .vbs attachments that are so rife on the Internet.

Upon installation, the default security setting for ZoneAlarm is set to High Security. This is a feature known as "stealth mode." By using High Security in the Internet Zone, you won't be a target for hackers.

Stealth mode does not mean that your IP address is invisible. What stealth mode does is make your computer's most vulnerable entry points invisible to tools that hackers use in order to seek out online targets. Using ZoneAlarm is a big advantage in protecting your privacy and protecting your PC from unwanted intrusions. It is important however, to not lose sight of the inherent risks associated with using the Internet and software designed for interaction such as chat and games as well as browsing. Everything we do online leaves a footprint that can potentially be used in an adverse fashion so while we all want to maximize our computing experience, a healthy dose of common sense in combination with savvy use of the ZoneAlarm firewall will go a long way in keeping your systems secure.

Depending on what applications you use, you will likely want to explore Security settings. You don't need to be an expert in program protocols and ports to use ZoneAlarm. A few easy configurations enable users of all levels of knowledge to establish a secure computing environment for Internet and local networking usage.

Establishing trusted traffic through ZoneAlarm can be customized via the Advanced button in the Security Panel, or by right-clicking on a program name in the Programs Panel.

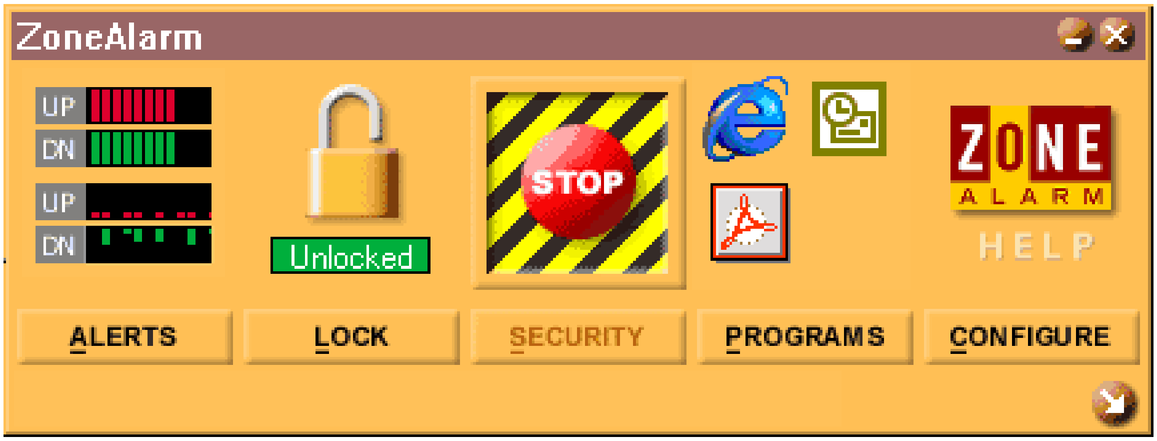
As your primary desktop security interface, ZoneAlarm can be configured to operate "on top" of Windows. Another option is use the Desk Band Toolbar.

BACK HOME NEXT

Copyright © 1999-2001 Zone Labs, Inc. All rights reserved. ZoneAlarm includes TrueVector Technology, covered by U.S. Patent No. 5,987,611. Zone Labs, ZoneAlarm, and TrueVector are registered trademarks of Zone Labs, Inc.

QuickClick Help

The graphic below is an image map. Hover your mouse over and then click on a ZoneAlarm feature for online help.



What platforms can I use with ZoneAlarm?

ZoneAlarm is compatible with:

- Microsoft Windows 95 (original with WinSock 2 or OSR2)
- Windows 98 (original, SP1 and SE)
- Windows ME
- Windows NT 4.0 Workstation (SP3, SP4, SP5 or SP6)
- Windows 2000 Professional (Final Release or SP1, SP2)

an 80386 or faster processor (486 recommended) 8 Mb of system memory.

A full installation requires approximately 3 Mb of hard disk space.

ZoneAlarm works with most types of TCP/IP connections, including Ethernet LAN, DSL, cable modem and dial-up connections.

Windows beta releases are unsupported. Additionally, if you use Windows platforms other than what is listed above, please read the section on running ZoneAlarm on a server.

Why does ZoneAlarm ask me if I want to grant access to services and controller app on installation?

Granting access to a default web browser

How do I make a backup copy of ZoneAlarm in case of hard drive crash?

Copy the original installation file to a safe place, such as a network drive, online storage, tape backup or any other way that you manage backups (ZoneAlarm is over 2Mb and will not fit onto a standard floppy diskette).

The ZoneAlarm executable is named zonealarm.exe and should be located in the default directory established upon installation: Program Files\Zone Labs\ZoneAlarm

Can I get ZoneAlarm on CD?

ZoneAlarm is currently available only as a download.

Check our web site for additional FAQs

BACK HOME NEXT

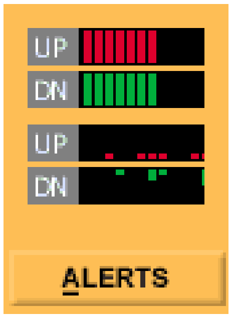
Copyright © 1999 - 2001 Zone Labs, Inc. All rights reserved. ZoneAlarm includes TrueVector Technology, covered by U.S. Patent No. 5,987,611. Zone Labs, ZoneAlarm, and TrueVector are registered trademarks of Zone Labs, Inc.

The Alerts Panel

Up/Down Graphs

Click on the ALERTS button to display the entire Alerts Panel.

Notice the two sets of UP/DN (Up/Down) graphs on top of the Alerts button. On your machine, whenever data is being uploaded to the Internet, red bars are displayed inside the two UP graphs. Whenever data is being received (downloaded), green bars are displayed inside the DN graphs. If there is no activity to/from the Internet, ZoneAlarm will display "ZA" on a red and yellow background.

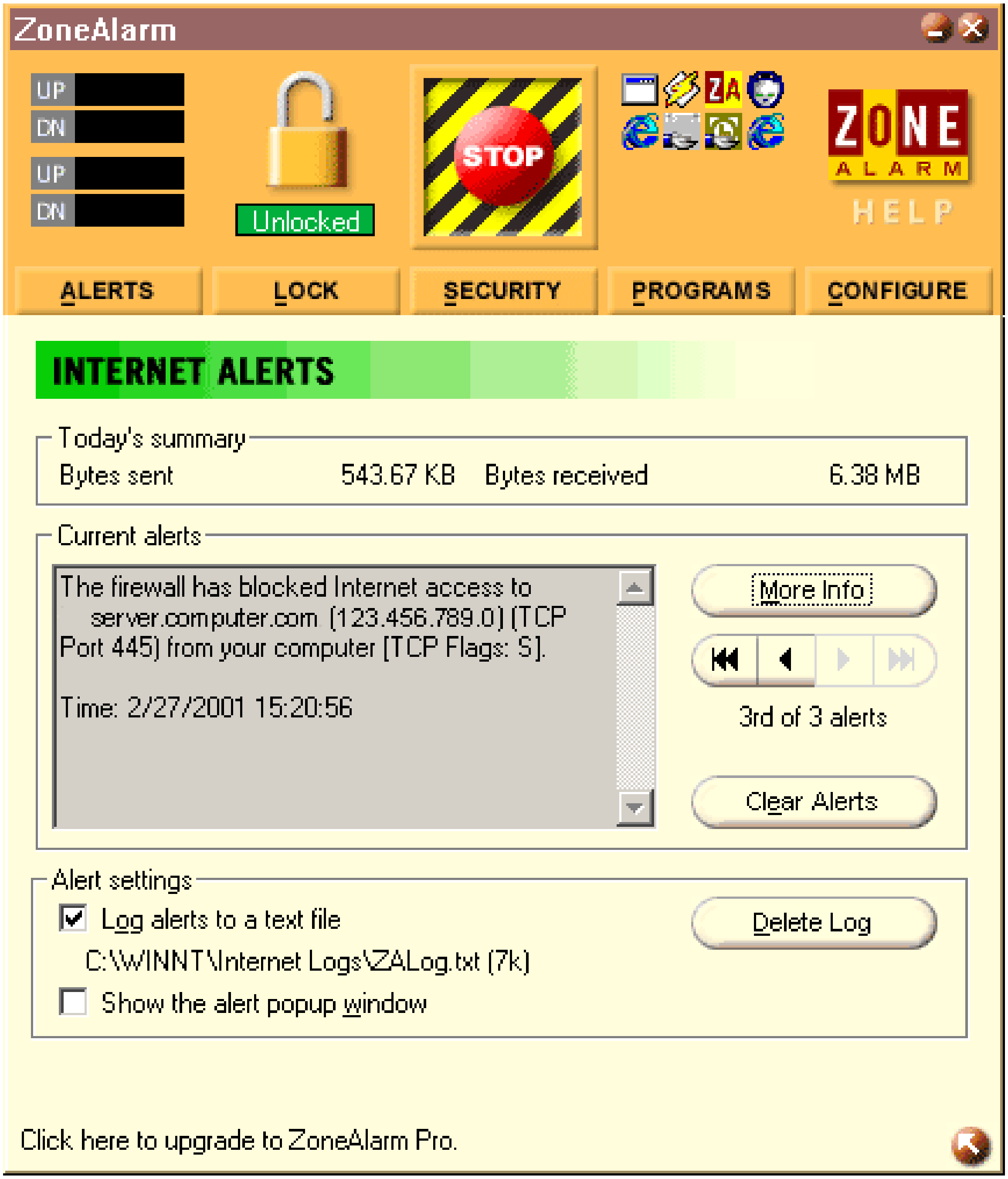


- The two graphs in the top portion of the icon display Internet traffic as it occurs.
- The two graphs in the lower portion of the icon display a chronological history of Internet traffic as it is generated on your machine.
- Whenever red or green flashing bars appear in the Alerts icon, the application receiving or sending traffic is shown as a blinking icon inside the Programs icon.

You might also notice traffic being displayed when you are not on the Internet. This is local broadcast traffic from your Network Interface Card (NIC). This traffic is sent to the Internet.

Expanded Alert Panel

At the top of the panel, *Today's Summary* shows the total amount of data sent and received by all applications. The middle portion of the panel details Current Alerts. In the Alert Settings area, at the bottom of the panel, there are options to display and save alerts.



Today's summary

Bytes sent 543.67 KB Bytes received 6.38 MB

Current alerts

The firewall has blocked Internet access to server.computer.com (123.456.789.0) (TCP Port 445) from your computer [TCP Flags: S].

Time: 2/27/2001 15:20:56

3rd of 3 alerts

Alert settings

☑ Log alerts to a text file

C:\WINNT\Internet Logs\ZALog.txt (7k)

☐ Show the alert popup window

Click here to upgrade to ZoneAlarm Pro.

More Info button: The Alert messages generated by ZoneAlarm contain information on what ZoneAlarm is blocking. Pressing the More Info button invokes the Zone Labs Alert Analyzer which provides additional information on traffic blocked by ZoneAlarm.

Check here for additional information on More Info functionality.

Learn More About:
Alert Settings
Current Alerts
Understanding Alerts
Alert Logs — See samples of the three types of alerts in the log file.

BACK HOME NEXT

Copyright © 1999-2001 Zone Labs, Inc.

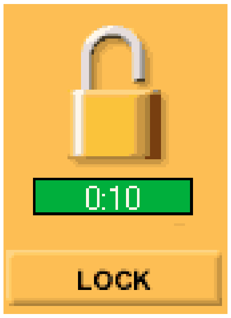
All rights reserved. ZoneAlarm and ZoneAlarm Pro include TrueVector Technology, covered by U.S. Patent No. 5,987,611. Zone Labs, ZoneAlarm, ZoneAlarm Pro, and TrueVector are registered trademarks of Zone Labs, Inc.

The Lock Panel

The purpose of the lock is to block all network activity inbound and outbound from your computer. Therefore, only use the lock during extended inactivity of your PC.

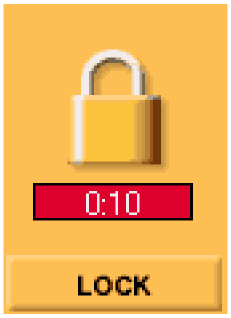
Locking

Click on the LOCK button to display the entire Lock panel. A locked or unlocked padlock is displayed in the middle of the icon. To allow certain applications access to the Internet while in locked mode, configure those programs to bypass the lock.



When the Timer Bar below the Lock button is green, the Internet Lock is not active. This means that ZoneAlarm is allowing inbound and outbound Internet traffic.

If the timer bar displays a countdown timer, this is the time remaining before the Automatic Lock will engage.

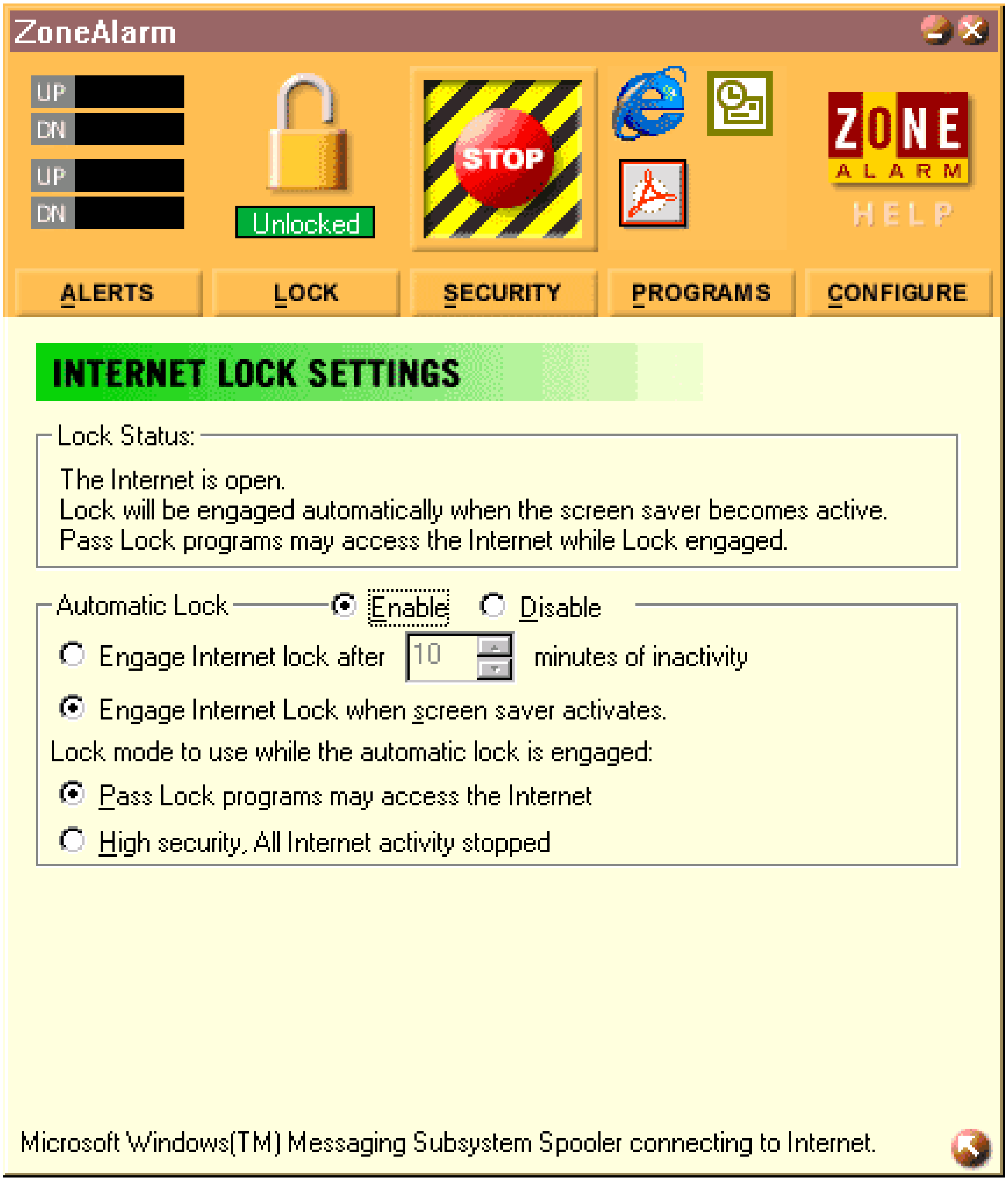


When the timer bar is red, the lock is closed and no inbound and outbound Internet traffic is allowed. When the lock is closed, the countdown timer counts upwards, showing the amount of time the lock has been active.

Expanded Lock Panel

When expanded, you can configure the Automatic Lock and determine lock status.

An example of when you might choose to lock Internet access automatically is when your screen saver activates or after a period of Internet inactivity on your computer.



INTERNET LOCK SETTINGS

Lock Status:

The Internet is open.
Lock will be engaged automatically when the screen saver becomes active.
Pass Lock programs may access the Internet while Lock engaged.

Automatic Lock ● Enable ○ Disable

○ Engage Internet lock after 10 minutes of inactivity

● Engage Internet Lock when screen saver activates.

Lock mode to use while the automatic lock is engaged:

● Pass Lock programs may access the Internet

○ High security, All Internet activity stopped

Microsoft Windows(TM) Messaging Subsystem Spooler connecting to Internet.

If Internet access is locked when the screen saver activates, it will be unlocked when the screen saver is deactivated.

Note, however, that if the Automatic Lock is engaged by the period of inactivity option, you will need to click on the Lock button to unlock Internet Access.

The Lock Mode for the Automatic Lock can be set so that "Pass Lock programs may access the Internet." This allows Internet activity for applications that have been given rights to bypass the lock. Typically programs such as e-mail clients will be set to check for e-mail while other applications are denied Internet Access.

BACK HOME NEXT

Copyright © 1999-2001 Zone Labs, Inc.

All rights reserved. ZoneAlarm and ZoneAlarm Pro include TrueVector Technology, covered by U.S. Patent

No. 5,987,611. Zone Labs, ZoneAlarm, ZoneAlarm Pro, and TrueVector are registered trademarks of Zone Labs, Inc.

The Security Panel

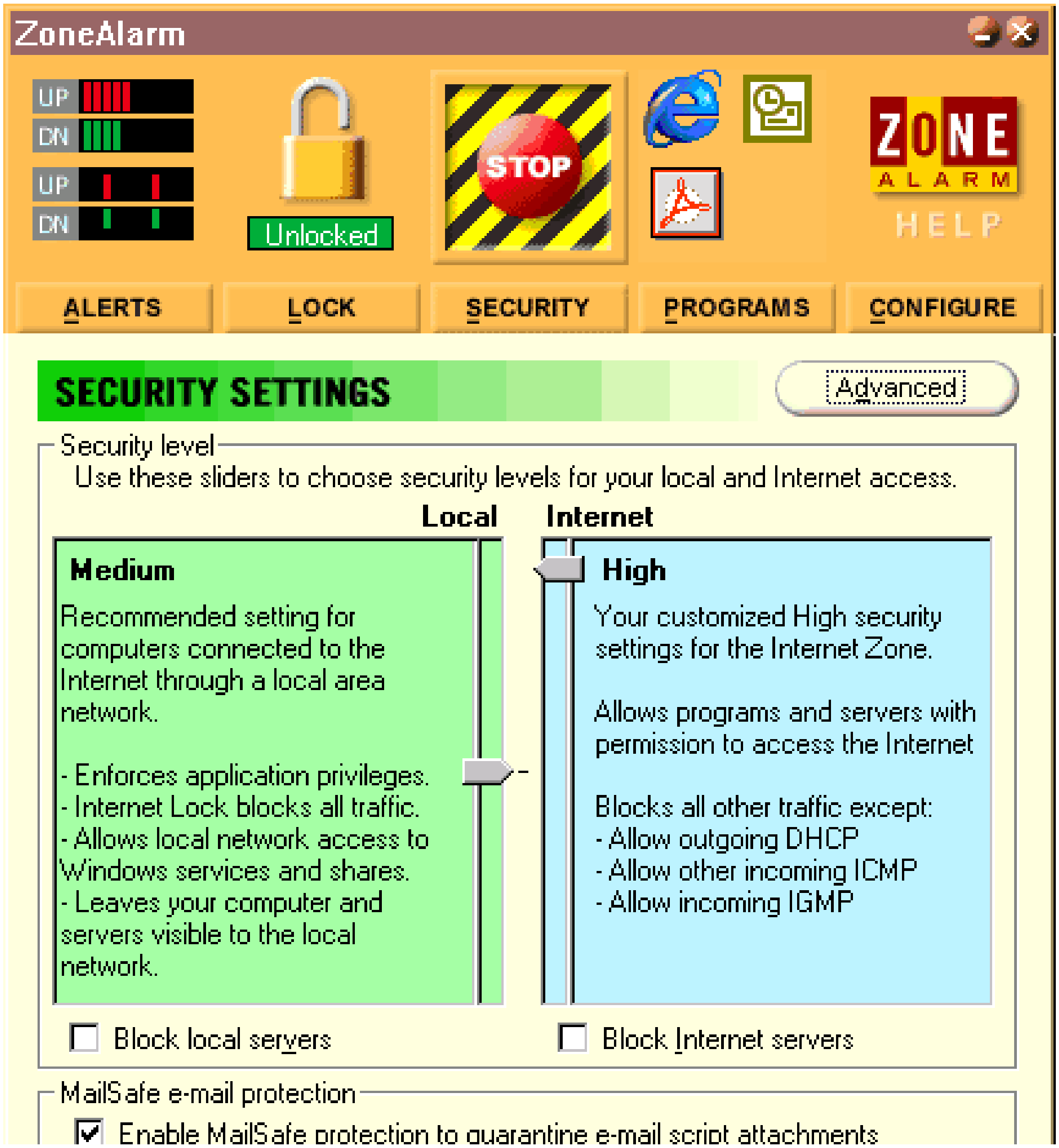
The Security panel is used to regulate ZoneAlarm's protection levels.

Security Panel
Related Links
Stop button

Security Panel

The Local and Internet Zone each have a security level selector, that slide up and down and accordingly change the security level. Local Zone security is displayed in green, and Internet Zone security in blue. The default settings are:

- medium for the Local Zone
- high for the Internet Zone



SECURITY SETTINGS

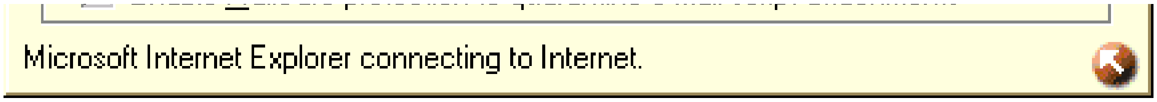
Security level

Use these sliders to choose security levels for your local and Internet access.

Local	Internet
Medium Recommended setting for computers connected to the Internet through a local area network. - Enforces application privileges. - Internet Lock blocks all traffic. - Allows local network access to Windows services and shares. - Leaves your computer and servers visible to the local network.	**High** Your customized High security settings for the Internet Zone. Allows programs and servers with permission to access the Internet Blocks all other traffic except: - Allow outgoing DHCP - Allow other incoming ICMP - Allow incoming IGMP
□ Block local servers	□ Block Internet servers

MailSafe e-mail protection

☑ Enable MailSafe protection to quarantine e-mail script attachments



Microsoft Internet Explorer connecting to Internet.

Use the block servers checkbox for each zone to prevent all programs from acting as servers for that zone. By checking this option, no application will be allowed to listen for incoming connections in that zone, even if you've checked the Allow Server option in the Programs panel.

Related Links

- For a definition of the Local and Internet Zones, click here.
- For instructions how to use the Advanced button, to add computers to your Local Zone, click here.
- For a description of MailSafe features, click here.

BACK HOME NEXT

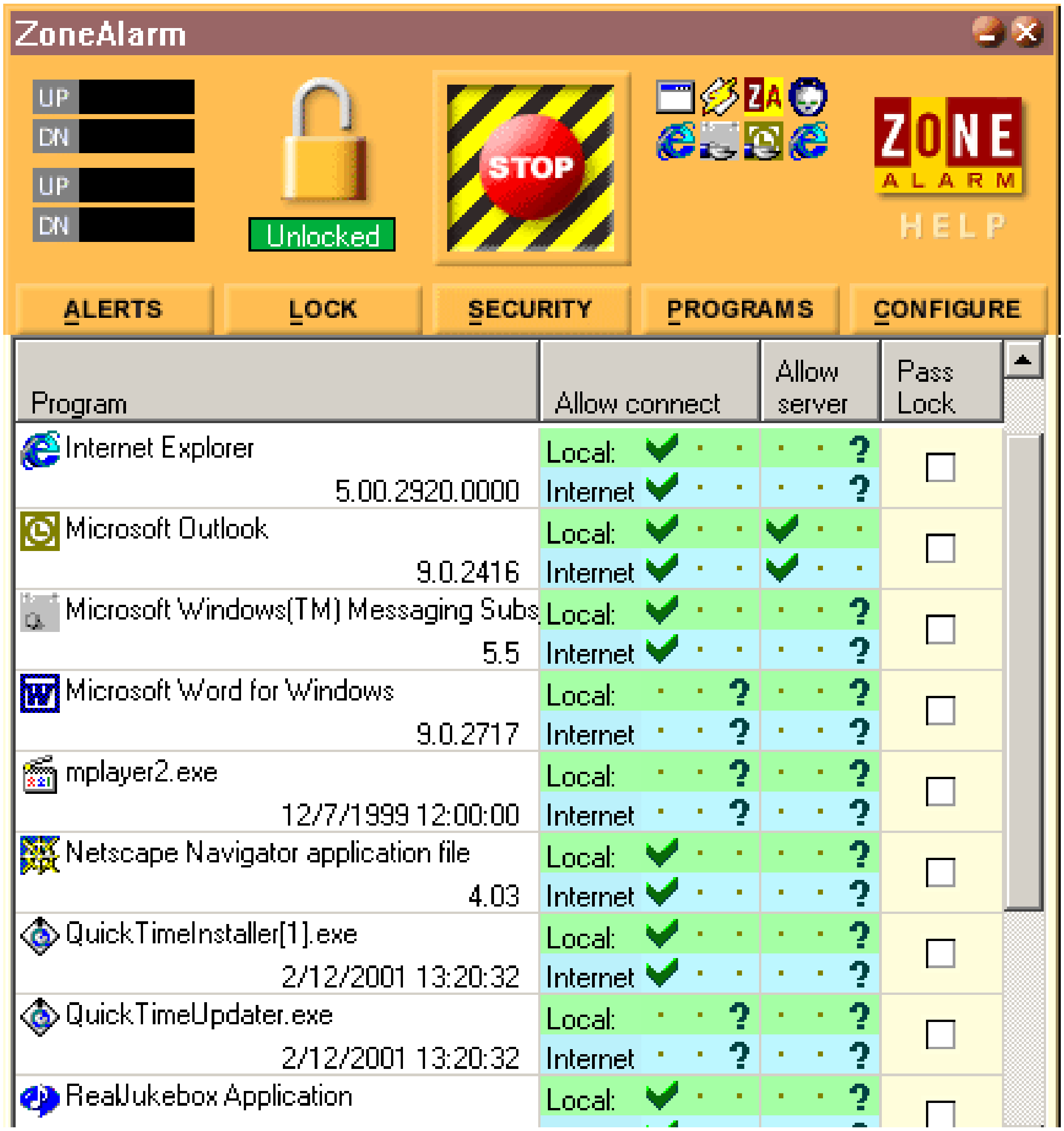
Copyright © 1999-2001 Zone Labs, Inc.

All rights reserved. ZoneAlarm and ZoneAlarm Pro include TrueVector Technology, covered by U.S. Patent No. 5,987,611. Zone Labs, ZoneAlarm, ZoneAlarm Pro, and TrueVector are registered trademarks of Zone Labs, Inc.

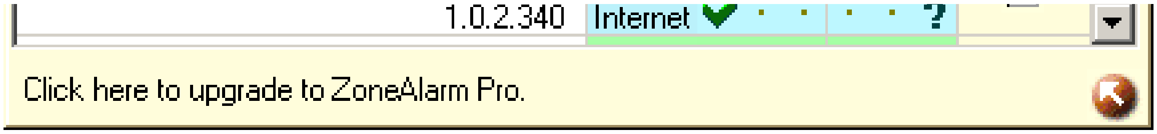
The Programs Panel

The Programs Panel is your central console for application control. You can see what applications are currently in use by checking the Programs Icon. The concept of application control involves establishing permissions and security options for programs accessing the Internet.

The main portion of the Programs Panel is the Program List. This list displays programs that have requested access the Internet.



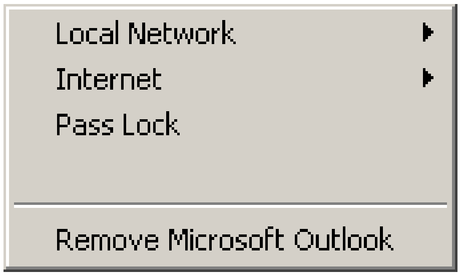
Program		Allow connect	Allow server	Pass Lock
Internet Explorer 5.00.2920.0000	Local:	✓	?	□
	Internet	✓	?	
Microsoft Outlook 9.0.2416	Local:	✓	✓	□
	Internet	✓	✓	
Microsoft Windows(TM) Messaging Subs 5.5	Local:	✓	?	□
	Internet	✓	?	
Microsoft Word for Windows 9.0.2717	Local:	?	?	□
	Internet	?	?	
mplayer2.exe 12/7/1999 12:00:00	Local:	?	?	□
	Internet	?	?	
Netscape Navigator application file 4.03	Local:	✓	?	□
	Internet	✓	?	
QuickTimeInstaller[1].exe 2/12/2001 13:20:32	Local:	✓	?	□
	Internet	✓	?	
QuickTimeUpdater.exe 2/12/2001 13:20:32	Local:	?	?	□
	Internet	?	?	
RealJukebox Application	Local:	✓	?	□



The Program Column contains program names and the version number of the application. Hover your mouse cursor over the program name to see more statistics such as:

- Product name
- The name of the file used to access the Internet
- The location of the file
- Product version
- Creation date and file size

Right-clicking on entries corresponds to the Program Panel's configuration options.



By right-clicking and selecting the "Local Network" menu, options correspond to the Allow Connect function and Allow Server functions for the Local Zone, while the "Internet" menu access configuration options for the Internet Zone.

Right-clicking on a program entry also accesses the Pass Lock permissions, and Remove Programs feature.

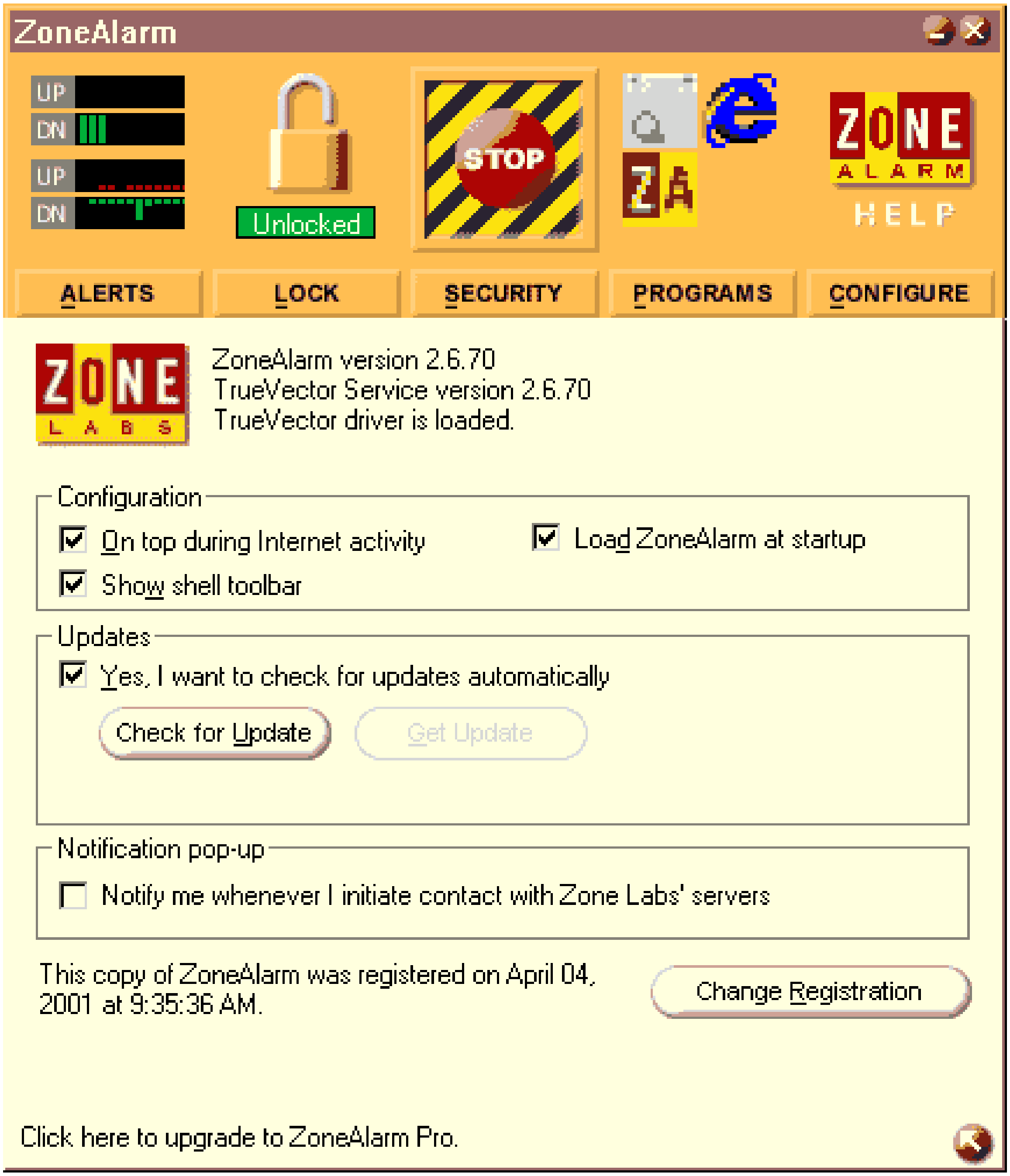
BACK HOME NEXT

Copyright © 1999-2001 Zone Labs, Inc.

All rights reserved. ZoneAlarm and ZoneAlarm Pro include TrueVector Technology, covered by U.S. Patent No. 5,987,611. Zone Labs, ZoneAlarm, ZoneAlarm Pro, and TrueVector are registered trademarks of Zone Labs, Inc.

The Configuration Panel

The Configure button displays the Configuration Panel. Use the Configuration Panel to set the basic operational characteristics for ZoneAlarm.



ZoneAlarm version 2.6.70
TrueVector Service version 2.6.70
TrueVector driver is loaded.

Configuration
☑ On top during Internet activity
☑ Load ZoneAlarm at startup
☑ Show shell toolbar

Updates
☑ Yes, I want to check for updates automatically

Notification pop-up
□ Notify me whenever I initiate contact with Zone Labs' servers

This copy of ZoneAlarm was registered on April 04, 2001 at 9:35:36 AM.

Click here to upgrade to ZoneAlarm Pro.

On Top during Internet activity

This checkbox controls whether or not ZoneAlarm will be displayed on top of Windows when other applications are open

Load ZoneAlarm at Startup

The Load ZoneAlarm at startup checkbox is selected by default. This enables ZoneAlarm to be loaded as a service at bootup. If you uncheck this checkbox, Internet traffic monitoring will not begin until you manually start ZoneAlarm on your machine.

Show Shell Toolbar

You will only see this option in particular versions of Windows 95 and Windows NT (those without the Windows Shell Update). Otherwise, you will not see the Show Shell Toolbar option in the Configure Panel. If this box is checked, the Desk Band activates. The toolbar will not dock to the Windows taskbar and will only float on top of all other windows - including icons in the system tray.

To show the toolbar on Windows 98, Windows ME, or Windows 2000, right-click on the Windows Taskbar and select "Toolbars" and then "ZoneAlarm Desk Band". On these systems, the toolbar will dock to the Taskbar. You can drag the toolbar by clicking on the far left side. Refer to the page on the Desk Band for more information.

Updates

The Check for update button contacts a Zone Labs server for product updates.

Notification pop-up

ZoneAlarm will only contact a Zone Labs server when the check for update feature is marked or during the registration process. Otherwise, Zone Labs does not collect, monitor or cull any information from a ZoneAlarm or ZoneAlarm Pro client and is not designed in any way to retreive any other information from your computer. If you prefer to receive a pop-up notification whenever ZoneAlarm checks for an update or acknowledges a registration submittal, mark this checkbox.

For more on the Zone Labs privacy policy, visit our web site.

Registration

The Change Registration button enables you to review and change your ZoneAlarm registration information

---

BACK HOME NEXT

Copyright © 1999-2001 Zone Labs, Inc.

All rights reserved. ZoneAlarm and ZoneAlarm Pro include TrueVector Technology, covered by U.S. Patent No. 5,987,611. Zone Labs, ZoneAlarm, ZoneAlarm Pro, and TrueVector are registered trademarks of Zone Labs, Inc.

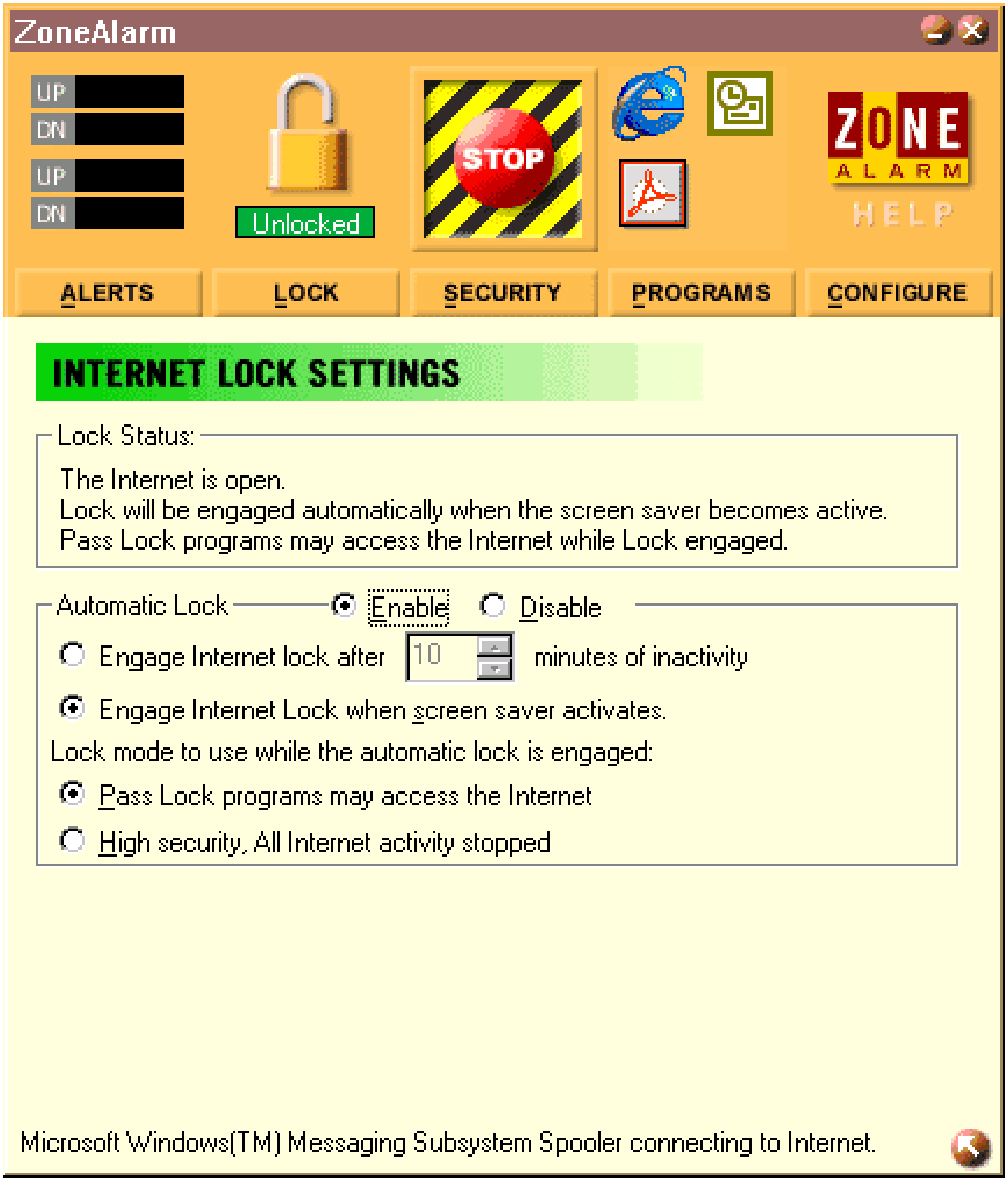
The Automatic Lock

Automatic Lock

The Automatic Lock will activate at whatever set intervals you select in the Automatic Lock section of the Lock panel. It is a very useful tool for stopping Internet traffic at times when you are not using your computer. By simply selecting a few radio buttons on the Lock panel, you can program the Automatic Lock to activate in the following situations:

- Whenever you are not using the Internet
- Whenever your computer has not been used for a preset number of minutes
- Whenever the screen saver takes control of your desktop

It is easy to grant one or more applications the permission to bypass the Lock. Using this bypass feature, you can allow programs like your e-mail client to bypass the lock in order to check for mail during intervals when the Automatic Lock is in effect for all your other applications.



INTERNET LOCK SETTINGS

Lock Status:

The Internet is open.
Lock will be engaged automatically when the screen saver becomes active.
Pass Lock programs may access the Internet while Lock engaged.

Automatic Lock ● Enable ○ Disable

○ Engage Internet lock after 10 minutes of inactivity

● Engage Internet Lock when screen saver activates.

Lock mode to use while the automatic lock is engaged:

● Pass Lock programs may access the Internet

○ High security, All Internet activity stopped

Microsoft Windows(TM) Messaging Subsystem Spooler connecting to Internet.

To turn on the Automatic Lock, select the Enable radio button.

Engage Internet Lock buttons:

- Select the first button to set a time of inactivity at the end of which the lock is to be activated.
- Select the second button to have screen saver activation turn on the lock rather than a number of minutes.

Lock Mode buttons:

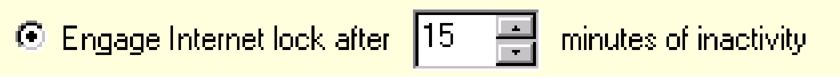
Make a choice with these radio buttons by either allowing certain programs to break through the Automatic Lock, or allowing no exceptions at all.

- The Pass Lock radio button stops all traffic except programs that bypass the Lock.
- The High Security radio button stops ALL TRAFFIC.

To turn off the Automatic Lock, select the Disable radio button at the top of the panel . Whenever this radio button is selected, any options you've selected, such as the minutes-of-inactivity or the screen saver option, will not apply during machine inactivity.

Undoing an Inactivity Lock

If you have activated the Automatic Lock using the minutes-of-inactivity option, unlock the lock by clicking on the padlock inside the Lock icon. After clicking on the padlock to deactivate the lock, the Timer Bar under the padlock will be set to green. This means that the lock is no longer stopping Internet traffic.



● Engage Internet lock after 15 minutes of inactivity

BACK HOME

Copyright © 1999-2001 Zone Labs, Inc.

All rights reserved. ZoneAlarm and ZoneAlarm Pro include TrueVector Technology, covered by U.S. Patent No. 5,987,611. Zone Labs, ZoneAlarm, ZoneAlarm Pro, and TrueVector are registered trademarks of Zone Labs, Inc.

The Stop Button

Pressing the STOP button immediately stops ALL network traffic. This includes Internet as well as local throughput, regardless if you are on a LAN or stand-alone workstation. The only reason to use this button is if you are monitoring activity and encounter a compromise in progress.

The STOP button overrides the Pass Lock settings in the Programs panel. This is useful for stopping Trojan horses and other programs that want to gain access to the Internet from your PC. To re-activate Internet access, press the stop button again.

Note that using the emergency stop button completely cuts off connections to the Internet. Connections and data transfer by all programs on your computer must be restarted.

BACK HOME NEXT

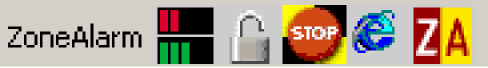
Copyright © 1999-2001 Zone Labs, Inc.

All rights reserved. ZoneAlarm and ZoneAlarm Pro include TrueVector Technology, covered by U.S. Patent No. 5,987,611. Zone Labs, ZoneAlarm, ZoneAlarm Pro, and TrueVector are registered trademarks of Zone Labs, Inc.

The Desk Band Toolbar

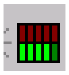
The ZoneAlarm Desk Band Toolbar is the minimized format of ZoneAlarm. It shows the status of the running ZoneAlarm application.

The Toolbar



This is the ZoneAlarm Desk Band Toolbar. It is the *minimized format* of ZoneAlarm. It shows a capsule status of the running ZoneAlarm application.

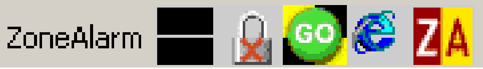
The red and green bars on the leftmost icon indicate whether or not Internet activity is taking place — you don't have to display the entire ZoneAlarm panel. You can remove the Desk Band Toolbar by using a checkbox in the Configuration panel. To display the main ZoneAlarm panel, click on the ZoneAlarm *System Tray* icon on your toolbar, usually in the lower right corner of your computer screen:



The System Tray Icon displays Internet activity as it happens.

You never have to display the main ZoneAlarm panel to know whether or not Internet traffic is happening on your machine. You cannot remove this icon from the Toolbar.

When Internet access has been locked with High Security, the center STOP button on the Desk Band Toolbar will change to a green GO button, as shown below. When this happens, click the GO button to restore Internet access.

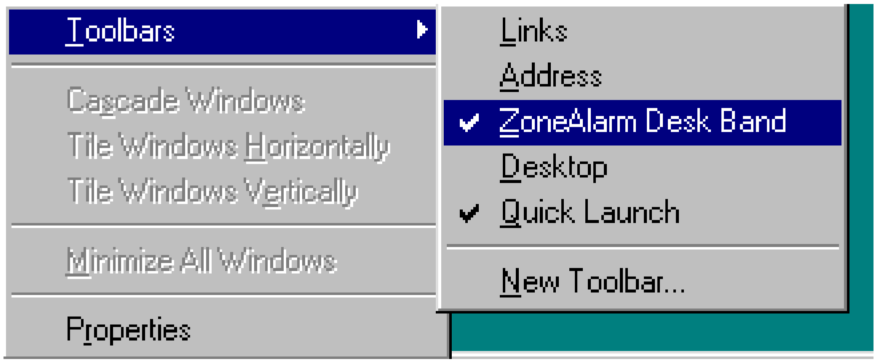


If the Automatic Lock has been turned on, the Lock icon will show a red X inside the padlock. Click on the Lock icon to lock/unlock Internet access.

If a program is currently accessing the Internet, its icon will show up to the right of the "GO" or "STOP" button. In this case, the "E" for Internet Explorer is currently running.

Activating the Desk Band

To activate the toolbar on Windows 98, Windows 2000 or other Windows versions that have the Internet Explorer 4 Shell Update, right-click on the Windows Taskbar and select Toolbars, then ZoneAlarm Desk Band.



When running on Windows 95 or Windows NT 4.0 without the Internet Explorer 4 Shell Update, go to the Configuration panel and click the Show shell toolbar checkbox to activate the Desk Band toolbar. Note that in this configuration, the toolbar can only float above the desktop and in some instances can cover icons in the system tray.

The name of the Desk Band can be removed by right-clicking on the name and deselecting the Show Title option. Then you can resize the Desk Band by moving the left side to the right.

BACK HOME NEXT

Copyright © 1999-2001 Zone Labs, Inc.

All rights reserved. ZoneAlarm and ZoneAlarm Pro include TrueVector Technology, covered by U.S. Patent No. 5,987,611. Zone Labs, ZoneAlarm, ZoneAlarm Pro, and TrueVector are registered trademarks of Zone Labs, Inc.

The Check for Update Button

Click the Check for Update button to see if a newer ZoneAlarm version is available for download from the Zone Labs web site. To have ZoneAlarm perform this check automatically, check the Check for Update checkbox in the Configure Panel.

If an update is available, you will be directed to the Zone Labs web site. Please make sure to save the download rather than running it from our web server. After downloading the update, it is advised to follow the proper installation sequence.

BACK HOME

Copyright © 1999-2001 Zone Labs, Inc.

All rights reserved. ZoneAlarm and ZoneAlarm Pro include TrueVector Technology, covered by U.S. Patent No. 5,987,611. Zone Labs, ZoneAlarm, ZoneAlarm Pro, and TrueVector are registered trademarks of Zone Labs, Inc.

Press F1 Key for specific help

All ZoneAlarm panels and dialogs are linked to a specific topic in the help system.

To display help information about a panel or dialog in the product where you are currently working, press the F1 key. In response, help information will be displayed in your browser.

BACK HOME NEXT

Copyright © 1999-2001 Zone Labs, Inc.

All rights reserved. ZoneAlarm and ZoneAlarm Pro include TrueVector Technology, covered by U.S. Patent No. 5,987,611. Zone Labs, ZoneAlarm, ZoneAlarm Pro, and TrueVector are registered trademarks of Zone Labs, Inc.

ZONE LABS

Understanding Alerts

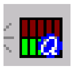
What is a ZoneAlarm Alert?

There are two basic concepts behind ZoneAlarm alerts: a) ZoneAlarm is notifying you of something that has occurred or b) ZoneAlarm has notified you that something attempted to occur.

There are several types of alerts: Program Alerts, Firewall Alerts, Lock Alerts and MailSafe Alerts.

Additonally, there are two methods of receiving alerts: pop-up and silent.

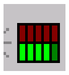
A silent alert will appear as a blue letter "a" in the system tray icon. The flashing blue "a" feature cannot be supressed except if you are using ZoneAlarm Pro.



System Tray Icon

ZoneAlarm monitors all Internet traffic on the machine it is installed on. This includes all connection attempts from your machine to the Internet and vice versa.

You will know ZoneAlarm is active if you see red and green traffic bars in the system tray icon.



The system tray icon is not removable.

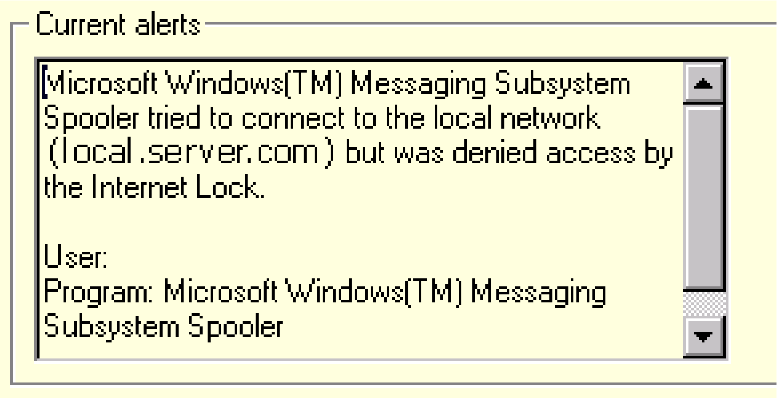
You might see red and green lights in the system tray icon when you are not connected to the Internet. This is due to broadcast messages being sent to all computers that are part of a specific network. This can include something as basic as a home network configuration, an office network or even a standalone computer using cable or DSL.

A computer's network adapter filters traffic on the hardware level. Any traffic that does not have the hardware address of your Network Interface Card (NIC) is automatically discarded so therefore, it is not being transmitted to the Internet.

Similarly, there may be times when you are not logged into the Internet yet you see activity lights on your DSL/Cable Modem. Depending on the equipment used by your DSL/Cable provider, your computer may be receiving broadcast messages that are transmitted throughout the Internet or a Local Area Network. The Ethernet card on your computer automatically discards these broadcast messages if the data is not intended for your computer.

Lock Alerts

In the Current Alerts area of the Alerts Panel, information is available after an alert is detected. If you have configured the lock and an application attempts to access the Internet, data such as the example provided below will show up in the Current Alerts area.



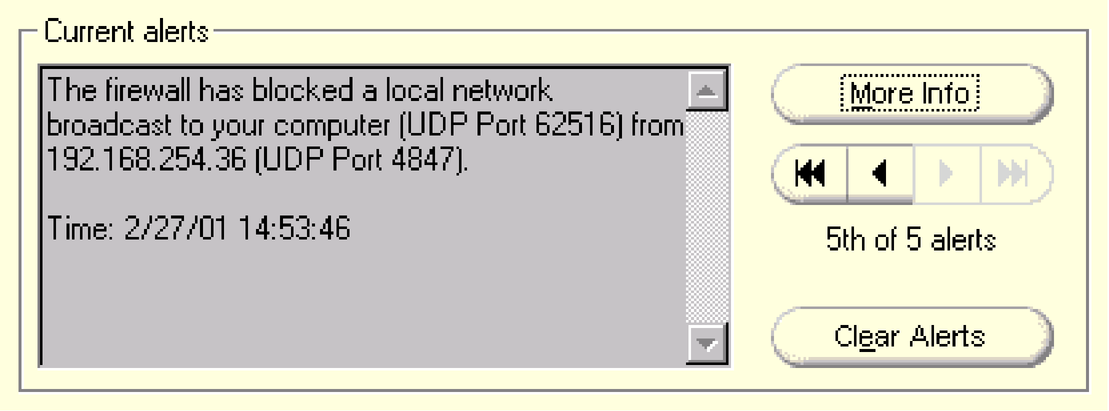
Microsoft Windows(TM) Messaging Subsystem Spooler tried to connect to the local network (local.server.com) but was denied access by the Internet Lock.

User:
Program: Microsoft Windows(TM) Messaging Subsystem Spooler

More Info Button

Clicking on the More Info button, located to the right of the alert description, gives you access to the Alert Analyzer, located on the Zone Labs web site.

There are two distinct and very different instances where you would make use of the More Info button. The first one is when you recieve a firewall alert, either as a popup or in the Current Alerts area as depicted below. The second is when you receive a program alert popup.



The firewall has blocked a local network broadcast to your computer (UDP Port 62516) from 192.168.254.36 (UDP Port 4847).

Time: 2/27/01 14:53:46

BACK HOME NEXT

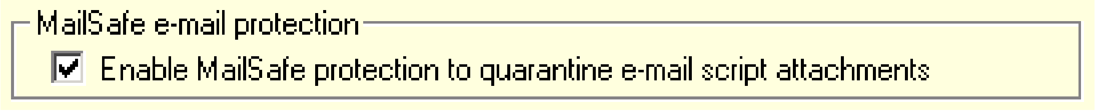
Copyright © 1999-2001 Zone Labs, Inc.

All rights reserved. ZoneAlarm and ZoneAlarm Pro include TrueVector Technology, covered by U.S. Patent No. 5,987,611. Zone Labs, ZoneAlarm, ZoneAlarm Pro, and TrueVector are registered trademarks of Zone Labs, Inc.

MailSafe

MailSafe protects your machine against viruses that can potentially arrive as e-mail attachments in the form of .VBS (Visual Basic script) files.

MailSafe is active by default; the option to enable or disable it can be found in the Security Panel.



MailSafe e-mail protection

☑ Enable MailSafe protection to quarantine e-mail script attachments

MailSafe works with mail clients that use POP3 and IMAP, the most common Internet e-mail protocols.

When an attachment is detected, ZoneAlarm quarantines it by changing the extension to .ZL and ends with either a letter or number. For example, a file called SERVER.VBS will be renamed SERVER.ZL1.

MailSafe does not automatically delete files attached to your e-mails and it is not a virus scanner. Rather than scanning and deleting viruses, it quarantines the attachment file and gives you the opportunity to keep the identified .VBS program from running. Visual Basic Script files can only cause damage when they are allowed to run on your machine.

To re-name a quarantined file, save the attachment with the proper file extension (you would have to know the file type in order to accomplish this) though it is strongly advised to be absolutely sure the file is legitimate before launching.

MailSafe can cause a conflict with other mail-checking software. Either disable MailSafe or disable the mail-checking feature of your anti-virus software.

BACK HOME NEXT

Copyright © 1999-2001 Zone Labs, Inc.

All rights reserved. ZoneAlarm and ZoneAlarm Pro include TrueVector Technology, covered by U.S. Patent No. 5,987,611. Zone Labs, ZoneAlarm, ZoneAlarm Pro, and TrueVector are registered trademarks of Zone Labs, Inc.

Definition of Zones

ZoneAlarm divides traffic into two separate zones: the Local Zone and the Internet Zone.

The purpose of the Local Zone is to enable ZoneAlarm to recognize what you as the user, deem as permissible traffic. The Local Zone can be customized according to need and you can also manage security levels within the Local Zone as well.

In a networked environment, including all domains, subnets and IP addresses within your Local Zone enables connectivity to the Internet and to other computers on a local network.

The Internet Zone is defined as all computers and addresses not included in your trusted Local Zone.

BACK HOME NEXT

Copyright © 1999-2001 Zone Labs, Inc.

All rights reserved. ZoneAlarm and ZoneAlarm Pro include TrueVector Technology, covered by U.S. Patent No. 5,987,611. Zone Labs, ZoneAlarm, ZoneAlarm Pro, and TrueVector are registered trademarks of Zone Labs, Inc.

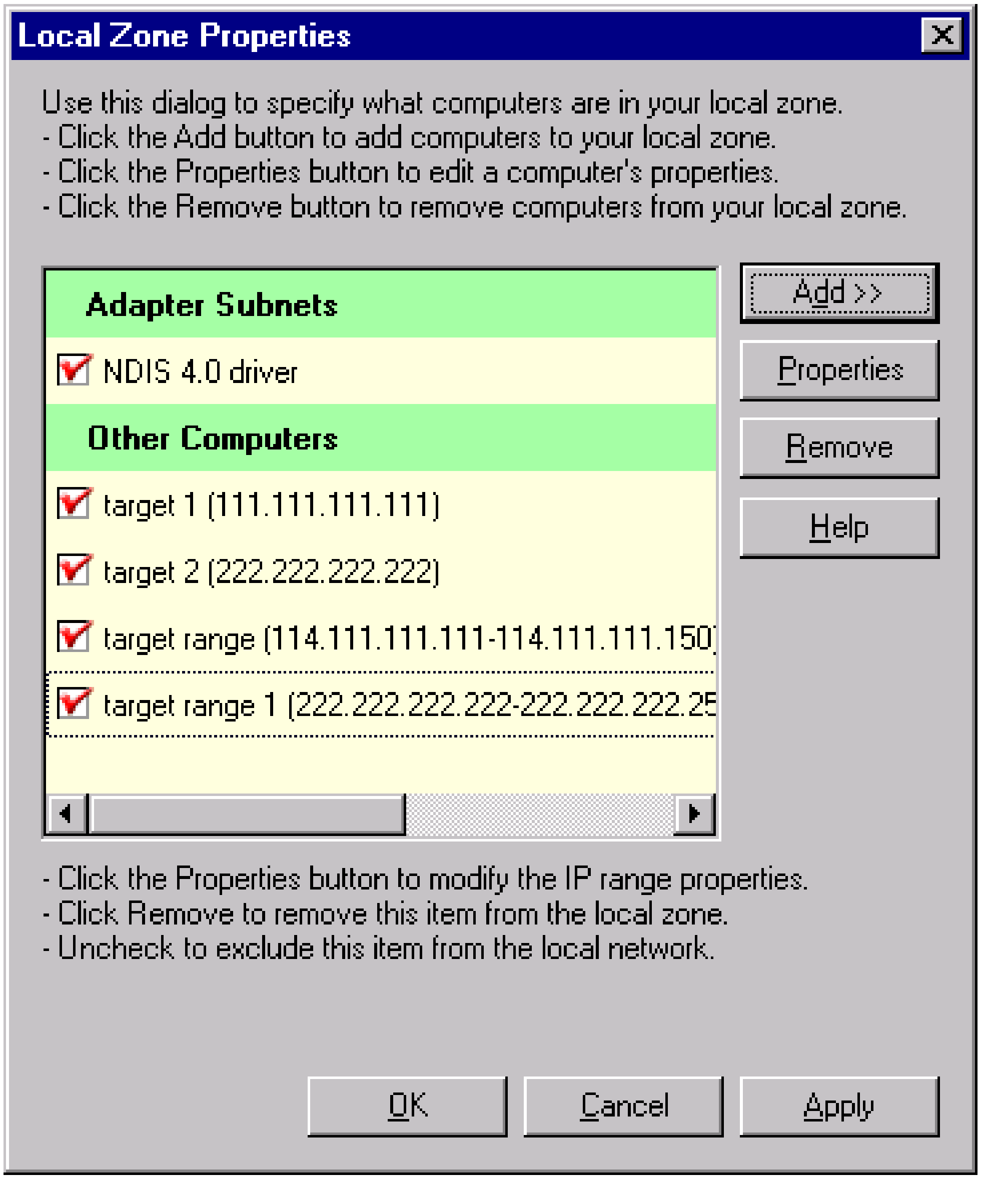
Networking Issues

Recognizing the Local Network

If you are a business user on a LAN or a home user connected to the Internet via DSL or dial-up, you will need to enable ZoneAlarm to recognize local traffic. Check to make sure that your Network Interface Card (NIC) is included in your Local Zone:

Click the Advanced button in the Security panel.

Under "Adapter Subnets", verify the network adapter that corresponds to your network is checked



Local Zone Properties

Use this dialog to specify what computers are in your local zone.
- Click the Add button to add computers to your local zone.
- Click the Properties button to edit a computer's properties.
- Click the Remove button to remove computers from your local zone.

Adapter Subnets

☑ NDIS 4.0 driver

Other Computers

☑ target 1 (111.111.111.111)

☑ target 2 (222.222.222.222)

☑ target range (114.111.111.111-114.111.111.150)

☑ target range 1 (222.222.222.222-222.222.222.25

- Click the Properties button to modify the IP range properties.
- Click Remove to remove this item from the local zone.
- Uncheck to exclude this item from the local network.

If you are having difficulty accessing areas of your network, you might need to add a domain, IP address or subnet to your Local Zone. This is a simple process and ZoneAlarm will resolve host names to IP addresses so you don't need to be a network administrator to figure out how to make ZoneAlarm work correctly on your LAN. Check here for easy instructions on populating your Local Zone.

Cable modem users, check here for important information regarding these instructions.

Proxy Setups

To enable proxy access, you'll need to add the proxy server addresses to the local zone.

ICS & NAT

NAT and ICS are both compatible with ZoneAlarm. However, flexibility of the firewall on the gateway PC will be minimal. If you are looking for a flexible desktop firewall for your gateway PC, it is highly recommended that you upgrade to ZoneAlarm Pro. You can use ZoneAlarm on the client machines in such a setup.

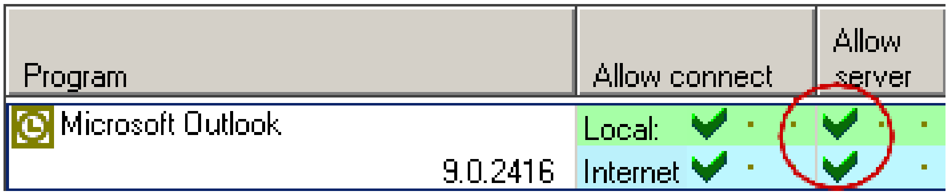
Applications Not Working

The first concept to bear in mind is that the firewall will only block applications launched after ZoneAlarm. Second, ZoneAlarm will recognize all applications that seek connectivity on a network and prompt you for permission to access. Via the Programs panel, you can control the behavior of all applications on your machine. A quick way to troubleshoot "non-functioning" application problems is to remove the entry from the Programs Panel, re-launch the application and apply permissions again.

There are a lot of different kinds of Windows operating systems and even more variations in ISP software as well as unique characteristics to each machine using ZoneAlarm. Therefore, there is the possibility that unknown applications will request access to the network. A first step is checking the More Info button within the program alert. Another is to run an Internet search on the application in question or you can conduct searches on Microsoft's KnowledgeBase as well as your own ISP's technical support web pages. Some software has multiple components which are needed in order to function properly. Check out in-depth details of the application as well. For information on how ZoneAlarm protects, go here.

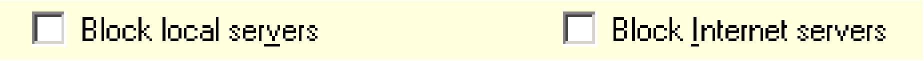
Still can't get your application to work?

Make sure you apply server rights to applications requiring incoming connections to function properly.



Program	Allow connect	Allow server
Microsoft Outlook 9.0.2416	Local: ✓ ·	✓ ·
	Internet ✓ ·	✓ ·

Make sure the "Block Local Servers" and "Block Internet Servers" option is not checked. To do this, go to the Security panel, at the bottom of the panel.



□ Block local servers   □ Block Internet servers

Make sure that the Automatic Lock is not enabled, or that your application has permission to bypass the lock. Go to the Programs panel to find this option.

Need more tips?

Check out some specifics to making applications function properly with ZoneAlarm

BACK HOME NEXT

Copyright © 1999-2001 Zone Labs, Inc.

All rights reserved. ZoneAlarm and ZoneAlarm Pro include TrueVector Technology, covered by U.S. Patent No. 5,987,611. Zone Labs, ZoneAlarm, ZoneAlarm Pro, and TrueVector are registered trademarks of Zone Labs, Inc.

Using Applications with ZoneAlarm

The key with software interoperability and a firewall is ensuring traffic you want to see is trusted. Most of the time, all you need to do is make sure known IP addresses and domains are input within the Local Zone and apply server rights to the application.

PCAnywhere & other remote administration tools

For PCAnywhere and ZoneAlarm to work together, be sure to add the IP address of the PCAnywhere client or host to your Local Zone. If a dynamic IP address is assigned to the remote machine then the DHCP server address or range of addresses need to added.

Netmeeting

Be sure to input the remote server into the Local Zone. If you experience problems with Netmeeting when ZoneAlarm is running, you can temporarily turn off Remote Desktop Sharing via the Netmeeting system tray icon.

E-mail

If your e-mail client cannot make the proper connections for sending and receiving your e-mail, make sure that the mail server has been added to your Local Zone. This would include your POP and SMTP server. If you are unsure of your POP and SMTP server addresses, try checking the properties of your mail software account or checking your ISP's web site for the specific mail server name(s). Most ISPs have online tutorials on setting up mail accounts and would have this information readily available.

Also, make sure the e-mail software has server rights. Some e-mail software might have more than one component requiring server rights. For example, MS Outlook requires the Messaging Subsystem to have server rights as well.

News Reader

If your News Reader client cannot make the proper connections for sending and receiving your news postings, make sure that the news server has been added to your Local Zone. If you are unsure of your news server addresses, try checking the properties of your news reader software the newsgroup web site for the specific news server name(s).

Also, make sure the News Reader software has server rights.

Stock Ticker

When streaming or push technology is running with ZoneAlarm, the application must be assigned server rights.

The Datek streaming stock ticker conflicts with ZoneAlarm. The reason for this is when a program writes data to memory, it writes that data in chunks called pages. When a program is accessing data from memory it pulls data from one page at a time. If the program gets to the end of a page and still needs more data, a page fault is created and the program will move on to the next page to get the rest of the data. A page fault by itself is not an error, it is perfectly normal. However, when a program produces a page fault and switches to a different page only to find that the page is not there, an invalid page fault is produced and the program crashes.

ZoneAlarm writes data into memory address that are also being used by Datek Streamer. So when Streamer tries to access a page in memory that page is no longer there, it has been either overwritten by ZoneAlarm or modified by ZoneAlarm when it scans the incoming data stream. The result is an invalid page fault.

If you are using BackWeb, check your Communication method. BackWeb software options are: *Polite Agent* or *HTTP*. The correct BackWeb settings for compatibility with ZoneAlarm are *HTTP* and *Detect Internet connection*.

If you are using Polite Agent, there are two issues:

- What do you have as your Network priority? The available options are:
  Give higher priority to other networking programs or
  Use the network normally.

- What do you have as Client port? Options are:
  Let BackWeb select port automatically or
  A client port number that can be modified by the user.
  You can try changing the Internet zone Security level to medium, but only during the time when you are using Polite Agent.

BackWeb and BackWeb Infocenter should be configured with server privileges. In BackWeb, options should be set to *Detect connection* to the Internet.

Voice Over IP & CallWave

Make sure you assign server privileges to CallWave and any Voice Over IP application you use. If they are availabel on the vendor's web site, you might try adding the IP Addresses of the VoIP provider's servers into the Local Zone.Though, most VoIP providers use a wide range of servers and therefore, are less likely to divulge this information on their web pages. A better solution for CallWave and VoIP applications is to apply security settings at medium.

Windows Critical Update Notification

Microsoft's Windows Critical Update Notification program is an example of an application that can make a web request rather often. If you install Windows Critical Update Notification, we suggest that you change the schedule that this program uses via the Task Scheduler in the System Tray (at the bottom right of your screen).

The current workaround is to either delete WCUN from your machine or you can allow it server rights. It will have two executables so it will ask you twice.

If you choose to delete WCUN, Microsoft advises an uninstall from Start-->Settings-->Control Panel-->Add/Remove Programs.

If you choose to keep WCUN, there are two executables to be aware of:
1. "wucrtupd.exe"
2. "wuloader.exe"

These two executables have the same Product Name, "Windows Critical Update Notification". This can be confusing because each executable makes separate attempts to access the Internet. ZoneAlarm correctly prompts users for permission at the time the appropriate executable attempts access. However, ZoneAlarm displays the product name, which is the same for both. The end user only sees "Do you want to allow Windows Critical Update Notification to access the Internet?". Here is a very short summary of the "Windows Critical Update Notification" sequence:

1. "wucrtupd.exe" attempts to access the Internet. ZoneAlarm displays the following message:

"Do you want to allow Windows Critical Update Notification to access the Internet? Destination IP: 127.0.0.1:1032"

2. "wuloader.exe" attempts to access the Internet. ZoneAlarm displays the following message:

"Do you want to allow Windows Critical Update Notification to access the Internet? Destination IP: 127.0.0.1:1039"

3. "wucrtupd.exe" attempts to access http://windowsupdate.microsoft.com on port 80. ZoneAlarm displays the following message:

"Do you want to allow Windows Critical Update Notification to access the Internet? Destination IP: 207.46.177.16:80".

This occurs under Windows 98 and Windows 2000 (nonSP1) when using ZoneAlarm or ZoneAlarm Pro.

Netscape or Internet Explorer

Always bear in mind that applications that are launched before ZoneAlarm will not be able to gain access to the Internet or network. Therefore, if you start ZoneAlarm manually *after* your browser is launched, you may have problems accessing the Internet or network. In these instances, simply close down the browser and then re-luanch it.

If you are receiving a "page not displayed error", a quick fix is (from the

Programs panel) to right-click beside the application and click on "Remove [application]." Then re-launch the browser and allow ZoneAlarm to recognize it.

If you are using Windows 2000, you will need to allow Internet access rights to Services and Controller App. Versions of Netscape above 4.73 have no problem browsing with ZoneAlarm active.

If you are already using Navigator above 4.73 and are still experiencing difficulty accessing the Web with ZoneAlarm active, check the browser Preferences to make sure you are not configured for proxy access.

Internet Explorer may run in the same process as Windows Explorer by default. Here is a Microsoft article that explains this phenomena:

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.

Adaptec CD Creator

If you have Adaptec CD Creator on your system, we suggest configuring it so that it does not launch itself as a service at startup. Upon installation, Adaptec CD Creator establishes itself with an icon in the system tray. There can be a tendency for ZoneAlarm to conflict with other items at bootup so it is strongly advised to only have what you need to start at bootup, do so. One option is to configure your registry settings to arrange the order of bootup so that Adaptec CD Creator starts up after ZoneAlarm. This option would require specialized knowledge of the registry to accomplish. Another option is to disable Adaptec CD Creator's system tray icon. You can launch CD Creator manually without any difficulty or effect to the purpose of the software.

FTP & Telnet

If you are having difficulties with your FTP and Telnet program, make sure that the program is on your Programs List. Also, make sure the FTP or telnet location is in your Local Zone.

FTP and Telnet programs may require server rights. For FTP programs, make sure you have Passive or PASV mode enabled, which tells the client to use the same port for communication in both directions. Enable that option in your FTP program.

Music File Sharing

Music file sharing tools such as Napster require that you let the application accept incoming connections in order to share files. To assign server rights, go to the Programs Panel in ZoneAlarm. Make sure the program has a checkmark in the area that says *Allow Server*.

Streaming Media

Applications that stream multimedia such as RealPlayer, Windows Media Player, etc. must have server rights to work with ZoneAlarm. Go to the Programs panel to set *allow server* permissions.

Always launch applications after ZoneAlarm is active.

Anti-Virus Scanner

Zone Labs recommends the use of ZoneAlarm and a virus scanner.

Anti-Virus software will require server privileges to function properly. You can assign these privileges in the Programs Panel. In the "Allow Server" column, make sure there is a green check mark next to the McAfee entry in the Program List. To receive updates, you need to enter your anti-virus vendor's domain (i.e. updates.mcafee.com) into the trusted Local Zone.

We are aware of a potential conflict between the MailSafe feature ZoneAlarm uses and anti-virus scanner mail protection. The workaround is to disable either MailSafe (via the Security Panel) or disabling your anti-virus software's mail checker.

There is also a conflict between ZoneAlarm's deskband and McAfee's VShield. To resolve this conflict:

1. Exit McAfee's VShield from the system tray
2. Right click on the task bar to launch the zone alarm desk band
3. Load Mcafee's Vshield from the Mcafee anti-virus's options --->V shields properties ------->clicking OK and clicking "yes " when promoted "Do you want to load V shield now?"

Mcafee's Vshield and ZA/ZAP should now function together.

Chat Programs

AOL Instant Messenger, Yahoo Messenger, MSN Messenger, ICQ and mIRC (Internet Relay Chat) are all popular free chat software programs that allow real time conversations and file transfers. To use with ZonerAlarm active, all chat software requires server rights. You assign these rights in the Programs panel.

It is strongly advised to check your chat software options to deny file transfers without prompting first. File transfer within chat programs is a means to distribute malware such as worms, viruses, nukes and trojan horses. Check with your chat software vendor's help files for configuration options to maximize security.

mIRC and ICQ especially will be portscanned. mIRC and ICQ channels are breeding grounds for adventurous hackers seeking to harvest IP addresses. What they hope to determine is if you have a Trojan listening on a Windows port that can be proxied through. This process is what is known as a "staging area" to launch denial of service attacks anonymously. The pitfall for good net citizens is not realizing their machines are being used as part of the staging area. Using Chat software wisely in conjunction with ZoneAlarm will prevent this type of activity from breaching your computing environment.

By specifying that you trust an application within ZoneAlarm, you are giving that application the ability to communicate with the Internet. Therefore the onus is on users of chat software and public message forums to learn responsible web habits. Understanding the vulnerabilities of the software you use is the first step in protecting your technology investment.

A tip for enabling mIRC to work with ZoneAlarm, we suggest disabling the IDENT feature located in the IDENT tab within mIRC.

BACK HOME NEXT

Copyright © 1999-2001 Zone Labs, Inc.

All rights reserved. ZoneAlarm and ZoneAlarm Pro include TrueVector Technology, covered by U.S. Patent No. 5,987,611. Zone Labs, ZoneAlarm, ZoneAlarm Pro, and TrueVector are registered trademarks of Zone Labs, Inc.

Computer Games and ZoneAlarm

Server-Based Games
Website-Based Games

Server-Based Games

Depending on the game software, the program might need to be added to the Programs List and given server rights. When you are connected to a server with other gamers, the easiest method to be assured of functionality is to add the game server's IP address into your Local Zone. Sometimes this is not available so the next best measure is to reduce Internet security settings to medium. At medium security you do not lose application control functionality. Keep in mind, in order to play the game, you need to trust the server you are attached to. Therefore, ZoneAlarm does not prevent vulnerabilities instigated by fellow gamers in this environment.

If you are using games with Direct X, make sure you have the latest version and make sure that you have researched the vulnerabilities associated with this feature.

Many games run in "exclusive" full screen mode. This prevents the display of ZoneAlarm alerts as well as normal Windows error messages on your screen.

If you are not able to see ZoneAlarm alerts while you are playing a full screen game, you can try the following procedures to rectify the problem.

Set your game to run in a window

Setting your game to run in a window allows you to see the alert if the game is running in a resolution lower than your desktop.

If your mouse is locked to the game, try pressing the Windows key. You should then be able to use the mouse to click on the alert. After allowing the game Internet access, reset the game to run in full screen mode.

Change your rendering mode to Software Rendering

Changing the rendering mode to *Software Rendering* will allow Windows to overlay the ZoneAlarm Alert on top of your game screen.

After allowing Internet access, you can change back to your preferred rendering device.

Press Alt+Tab to toggle back into Windows

Pressing Alt + Tab to toggle back into windows will allow the game to run while allowing you to respond to the alert.

Once you have allowed Internet access you press Alt + Tab again to restore your game. This 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.

Website-Based Games

For games that make use of java, applets or other web-based portal functionality, you might need to reduce Internet security settings to medium. At medium security you do not lose application control functionality. Keep in mind, in order to play the game, you need to trust the server you are attached to. Therefore, ZoneAlarm does not prevent vulnerabilities instigated by fellow gamers in this 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.

BACK HOME NEXT

Copyright © 1999-2001 Zone Labs, Inc.

All rights reserved. ZoneAlarm and ZoneAlarm Pro include TrueVector Technology, covered by U.S. Patent No. 5,987,611. Zone Labs, ZoneAlarm, ZoneAlarm Pro, and TrueVector are registered trademarks of Zone Labs, Inc.

Trojan Horses & Portscanning

"Why would hackers single me out of all the computers attached to the Internet?"

Unfortunately, it's not usually a matter of choice when a hacker comes calling, especially if you are using a broadband connection that is "always on." One method used to identify potential hack targets is through the widespread practice of portscanning.

In a nutshell, portscanning is a tool that allows for information gathering on computers attached to a network. Online vandals will regularly portscan vast blocks of IP addresses. By doing so, they are able to determine what services are currently listening for connections on a computer and what specific ports they are listening on. Thus, providing clues to form an attack strategy.

How ZoneAlarm & ZoneAlarm Pro Handle Portscans

ZoneAlarm & ZoneAlarm Pro handle portscans by simply dropping the packets as they hit your machine. You might see a string of alerts, letting you know there have been X attempts to access your computer and the alerts run sequentially by port number. That is a portscan in progress. ZoneAlarm/ZoneAlarm Pro will log up to 500 alerts and will not report the scans after that point. However, ZoneAlarm/ZoneAlarm Pro does continue to block the scans. The 500 alert maximum is in effect because there are over 65,000 ports on a Windows Operating System, it would not make sense to consume such a large quantity of disk space to report blocked scans so that is why ZoneAlarm/ZoneAlarm Pro stops at 500.

You can break a portscan just by shutting off your Internet connection but bear in mind, most portscans are run by automated commands so there is no predicting when they could return.

What Happens If I Don't Have ZoneAlarm or ZoneAlarm Pro Protecting My Computer?

Once an unprotected computer is singled out as worthy of an attack, a common means to gain control of the computer is via a Trojan Horse - also known as a Remote Administration Tool (RAT). Trojan Horses are easy for even the most rudimentary of programmers to create and are therefore very common on the Internet. If installed correctly, Trojans can be highly intrusive because they 1) can cause consternation and mayhem, 2) can establish a direct mechanism for stealing data stored on the PC and 3) can serve as a launching pad for attacks directed elsewhere on the Internet.

How do Trojan Horses get distributed?

Trojan Horses can come from seemingly innocent sources, typically as e-mail attachments, file transfers or downloads. Since Trojans can be bundled with a legitimate file, there is no obvious tip-off of a bundled Trojan but such a file must retain an .exe or .scr extension. The objective is for the victim to unwittingly launch the file believing it to be legitimate. In this manner, a Trojan will extract in stealth and attempt to take over your machine at a later time when you least expect it. Thus, you can see why the Trojan Horse analogy is used to describe the phenomena.

The best bet to avoid Trojan Horses in the first place is to not launch .exe or .scr files from an untrusted source. ZoneAlarm Pro users can configure MailSafe to catch files with these extensions coming through e-mail.

There is another dimension to acquiring Trojan Horses and it involves safe surfing habits. It is possible to acquire Trojans through a browser but only if you are tricked into clicking on a self-extracting payload. Pop-up banners and similar enticements can be Trojans so be careful! Use good judgment in deciphering what is a legitimate click-through and what falls under the category of suspicious.

How ZoneAlarm & ZoneAlarm Pro Recognize Trojan Horses

Once installed on the target machine, a Trojan Horse can be difficult to identify because it can have cryptic a file name or even masquerade as a legitimate file name.

You'll be able to recognize a cryptic application trying to access the Internet simply by examining your Programs List. ZoneAlarm & ZoneAlarm Pro will detect and prevent Trojans re-named as legitimate applications from accessing the Internet.

Many of the other firewalls today, do their application verification process through name recognition. Hackers can easily exploit this weakness by creating a Trojan Horse that has the same name or properties as a legitimate application, enabling it to bypass a firewall. With ZoneAlarm and ZoneAlarm Pro, even if a hacker changes the name of an application to make it look legitimate, it will still be stopped because of an MD5 Checksum verification process.

BACK HOME NEXT

Copyright © 1999-2001 Zone Labs, Inc.

All rights reserved. ZoneAlarm and ZoneAlarm Pro include TrueVector Technology, covered by U.S. Patent No. 5,987,611. Zone Labs, ZoneAlarm, ZoneAlarm Pro, and TrueVector are registered trademarks of Zone Labs, Inc.

ZoneAlarm for Business Use

The mobile workforce and telecommuters have unique requirements for desktop protection. For these users, the primary objective of ZoneAlarm is to protect their computer from malicious activity when a secure tunnel is established from a VPN client to a corporate network. An equally important objective is to meet the desktop firewall protection needs of end-users when the VPN is not active. If you are a business user making use of ZoneAlarm for VPN protection, please read our license agreement.

ZoneAlarm, though robust for the desktop, is not designed to function on a server. A more flexible option for server protection would be ZoneAlarm Pro. You might also be interested in checking our web site for other enterprise-level products.

Some circumstances may be suitable for running ZoneAlarm on a server. This section describes best practices for server installation and VPN protection.

If you are using ZoneAlarm on a LAN then make sure you read the section on networking in conjunction with this article.

Installing ZoneAlarm on a Server

Allowing trusted users and applications into the server requires configuring the Local Zone. Installing ZoneAlarm on a server must take into account the possibility of multiple subnets, DNS, domain controllers, any software that requires access to the Internet as well as specialized services such as VPN.

Open ZoneAlarm, and click the Security Panel. Click on the advanced button. Click the add button and enter the following information into the Local Zone:

- All of your internal LAN/WAN subnets that interact with this server. These can be Class A, B, or C networks, such as 10.0.0.0, subnet 255.0.0.0
- DNS servers if they are not on your internal network
- Any Gateways or VPN's that are not part of your internal network
- Any trusted static external IP addresses

Adding trusted IP sources to your Local Zone will ensure that normal internal network traffic will proceed unhindered, while at the same time protecting the server from any requests that come in from the Internet.

There is one other very important point that you must address. When a Program Alert pop-up appears from ZoneAlarm asking for permission for an application to access the Internet, all network traffic is halted. When traffic is halted, computers attached to the server risk being disconnected from the LAN. This situation can be dealt with by defining the default application privileges.

Setting Application Permissions

In the Programs Panel and make sure no options are set to ask for permissions to access the network or you will be risking a loss of network connectivity due to a Program Alert popup. To use ZoneAlarm on a server requires knowledge of all applications and components that require access to the network and the Internet. Initially it will be best to allow all applications access and after running the server for a while you will be able to review your program list and either change the permissions for individual applications, or wholly revoke permission for any further new applications from accessing the Internet. In either case, make sure your Program List is defined before changing the default behavior.

Server rights are for applications which listen to incoming connections but do not initiate them. Applications such as IIS and FTP servers work in this way. When an application is granted server rights it is allowed to receive anonymous incoming requests intended for that application. An application that is granted server rights can be probed with a port scan. Unfortunately this cannot be avoided as these are usually public servers and intended for others to contact. Ports that are not in use by the server application will continue to be stealthed.

Configuring ZoneAlarm to Work with a VPN

There are many different varieties of VPN software and configurations. As a result, you might need to check with your network administrator for clarification on ensuring functionality with the systems, services and protocols described in this section.

ZoneAlarm is compatible with:

- The IPSec security protocol standard
- Microsoft's Point to Point Tunneling Protocol (PPTP)
- L2F and L2TP
- DES (56 bit) and 3DES (168 bit), authentication with digital certificates, one-time password tokens, pre-shared keys, the H.323 RAS protocol which supports Voice over IP implementation, Extended Authentication (Xauth), IKE, RADIUS, TACACS+, PKI, LDAP and PGP

When you have your VPN client software installed, you will then need to make sure the adapter is recognized by ZoneAlarm. Follow the guidelines for networking requirements.

Populate your Local Zone with:

- VPN server or concentrator IP address
- Remote PC that acts as a gateway (i.e. 10.0.0.10)
- All of the LAN/WAN subnets that interact with the internal network. These can be Class A, B, or C networks, such as 10.0.0.0, subnet 255.0.0.0
- RADIUS or TACACS+ server IP address (if applicable)
- DNS servers used that are not on your internal network
- Depending on the operating system the VPN client is installed on, it may be necessary to add the local host address (NIC loopback): 127.0.0.1 Note: Make sure there is no proxy software running on the local host if the loopback address needs to be added.

ZoneAlarm will recognize services and applications on the machine when they are launched or a related service is invoked.

Check here for information on applying program permissions

BACK HOME NEXT

Copyright © 1999-2001 Zone Labs, Inc.

All rights reserved. ZoneAlarm and ZoneAlarm Pro include TrueVector Technology, covered by U.S. Patent No. 5,987,611. Zone Labs, ZoneAlarm, ZoneAlarm Pro, and TrueVector are registered trademarks of Zone Labs, Inc.

ZONE LABS

For our partners Select One... Site Search go

Products & Solutions | Download & Buy | Service & Support | About Zone Labs, Inc.

Zone Labs strives to provide you with the best software

Service & Support

> Support

Welcome to the Zone Labs Web-Based Technical Support for ZoneAlarm and ZoneAlarm Pro.

Zone Labs is committed to satisfying the needs of our customers. The technical support group at Zone Labs provides expertise in technical support to help ensure that our customers' technical questions and issues are quickly addressed.

- **To Solve a Technical Issue**

  ZoneAlarm Technical Support

  ZoneAlarm Pro Technical Support
  Users of ZoneAlarm and ZoneAlarm Pro who need to solve a technical issue, or have questions about setting up and properly using ZoneAlarm and ZoneAlarm Pro.

- **To Address a Customer Service Issue**

  Web-Based Customer Service
  Please select this option for all other service related issues such as purchasing and successfully downloading our products, billing, refunds, and general questions about ZoneAlarm and ZoneAlarm Pro.

- **To Obtain Corporate Customer Support**

  Corporate customers may directly contact their designated support representative.

Customer Service

Information

Technical Support FAQ's

ZoneAlarm

ZoneAlarm Pro

Common Questions

Technical Support

Web-based Support Form

Additional Information

Enterprise Sales

Privacy & Legal

About Zone Labs

● Press Room ● Careers ● Volume Sales ● Contact Us ● Site Map ● News & Articles
● Affiliates

Copyright ©1999-2001 Zone Labs, Inc., 1060 Howard Street, San Francisco, CA 94103, USA.
All rights reserved. All other trademarks are the property of their respective owners.

Zone Labs strives to provide you with the best software

Customer Service

Information

Technical Support FAQ's

ZoneAlarm

How It Works

Installation and Uninstallation

Configuration

Operation

Registration

LAN Topics

ICS Topics

ISP Topics

OS Topics

Full List of FAQ's

ZA Release History & Updates

ZoneAlarm Pro

Common Questions

Technical Support

Web-based Support Form

Additional Information

Service & Support

Support > Support Info: ZoneAlarm > **Installation and Uninstallation**

Installation and Uninstallation

If you want to double-check the work of the uninstaller, or if you suspect you may have a broken installation/uninstallation, this document contains the complete list of files and registry entries to check.

The uninstaller should remove all of the ZoneAlarm program files. If ZoneAlarm is your only client of the TrueVector Internet monitoring service (this is usually the case, unless you installed Internet Access Monitor), the uninstaller should remove the TrueVector service files also.

The uninstaller does not remove the program information files.

1. Uninstalling ZoneAlarm
2. Files installed with ZoneAlarm
3. Files created when using...
4. Registry entries
5. Other changes to your system
6. What is the most troublefree way to uninstall or upgrade ZoneAlarm?
7. Missing the "Install.log" file

1.Uninstalling ZoneAlarm

If you want to uninstall ZoneAlarm, first run the Uninstaller program: click on the Start menu|Programs|ZoneAlarm|Uninstall ZoneAlarm menu item.

You can uninstall the program manually by removing the following files and registry entries.

2.Files installed with ZoneAlarm:

Installing ZoneAlarm places program files in three places:

The c:\Program Files\Zone Labs\ZoneAlarm folder contains these files (unless manually installed elsewhere):

zonealarm.exe
zoneband.dll
license.txt
readme.txt
unwise.exe
install.log
\Help folder containing a number of files

The c:\windows\system (for Windows 95, 98, and Me) or c:\windows\system32 (for Windows NT and 2000) folder contains these files (unless manually installed elsewhere):

vsutil.dll
vspubapi.dll
vsmonapi.dll
vsdata.dll
vsdata95.vxd—if computer runs Windows 95, 98, Me
vsdatant.sys—if the computer runs Windows NT or 2000

Enterprise Sales

Privacy & Legal

About Zone Labs

The c:\windows\system\zonelabs (for Windows 95, 98, and Me) or c:\windows\system32\zonelabs (for Windows NT and 2000) folder contains these files (unless manually installed elsewhere):
vsdb.dll
minilog.exe
html.tdr
vsmon.exe
vsruledb.dll

Installing also creates a shortcut called "ZoneAlarm.lnk" in the c:\Windows\Start Menu\All Users\Programs\StartUp (for Windows 95, 98, and Me) or c:\Windows\Profiles\All Users\Start Menu\Programs\Startup (for Windows NT and 2000) folder (unless manually installed elsewhere).

3. Files created by ZoneAlarm as it runs
When running ZoneAlarm, the following files are created:

In the c:\windows\internet logs folder:
ZALog.txt
iamdb.rdb
<mycomputer>.ldb (where the <mycomputer> is your computer name)

Note: The uninstaller does not normally remove these files, so that your settings are retained when you upgrade to a new version.

4. Registry Entries
Important Advisory : Deleting registry entries incorrectly may cause serious problems to your operating system (OS) which may necessitate the need to reinstall the OS. Please make sure you are able to perform these deletions correctly before you decide to edit the entries.

For information about how to edit the registry in Windows 95, 98, and Me, type regedit.exe from a command prompt. Click "Help," then "Help Topic." Click "Changing Keys and Values."

If you are running Windows NT or 2000, type "regedt32.exe" from a command prompt. Click Help, then Contents. Click the "Add and Delete Information in the Registry" and "Edit Registry Information."

Note that you should back up the registry before you edit it. If you are running Windows NT or Windows 2000, you should also update your Emergency Repair Disk (ERD).

Installing and running ZoneAlarm creates the following registry entries:

Key: HKEY_LOCAL_MACHINE\Software\Zone Labs and all its subkeys and values.

Key:
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\ZoneAlarm.

If your system is running Windows 95, Windows 98, or Windows Me these registry items starts the services required for ZoneAlarm.

Key: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices

Value: MiniLog and Value: TrueVector

Under Windows NT and Windows 2000, these two registry keys, and all their subkeys, denote the TrueVector service and the TrueVector device driver:

Key: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\vsmon

Key: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\vsdatant

Under Windows NT and Windows 2000, this registry key and its subkeys denote ZoneAlarm's alert logging service:

Key: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\minilog

Under all versions of Windows, these values are added to the Shared DLLs database:

This is a database that contains a long list of values, but only these values are related to ZoneAlarm and TrueVector:

Key: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\SharedDLLs

Values:
C:\Windows\System\vsdata.dll
C:\Windows\System\vsdata95.vxd (if you are running Windows NT or Windows 2000, this will be vsdatant.sys)
C:\Windows\System\vsmonapi.dll
C:\Windows\System\vsnetutils.dll
C:\Windows\System\vspubapi.dll
C:\Windows\System\vsutil.dll
C:\Windows\System\Zone Labs\html.tdr
C:\Windows\System\Zone Labs\vsdb.dll
C:\Windows\System\Zone Labs\minilog.exe
C:\Windows\System\Zone Labs\vsmon.exe
C:\Windows\System\Zone Labs\vsruledb.dll

For each user who has run ZoneAlarm, there are registry keys in:
Key: HKEY_CURRENT_USER\Software\Zone Labs

Users who have run ZoneAlarm versions prior to 1.8.2 may find entries in:
Key: HKEY_CURRENT_USER\Software\Zone Labs\Monitor

The following keys allow the user to modify the sound that is played when there is an alert through use of the Control Panel Sounds applet:
Key: HKEY_CURRENT_USER\AppEvents\EventLabels\InternetAlert
Key: HKEY_CURRENT_USER\AppEvents\Schemes\Apps\.Default\InternetAlert\.current

On Windows95/98/Me systems, the following keys tell Windows the ZoneAlarm Desk Band is a part of ZoneAlarm:
Key: HKEY_CLASSES_ROOT\CLSID\{long string of characters}\InprocServer32
Value: C:\Program Files\Zone Labs\ZoneAlarm\zoneband.dll

The string of characters will vary from system to system

5. Other changes to your computer when installing
Installing ZoneAlarm also **upgrades** a few system files on your computer, if your computer does not currently have them or if the current version on your computer was older when you installed ZoneAlarm.

These files are published by Microsoft as part of your operating system, and are critical to keeping your system running, so they should **not** be removed if you uninstall ZoneAlarm.

On a Windows 95 or Windows Me system:

c:\windows\system\comctl32.dll is upgraded to version 4.71, only if the previous version on your machine was prior to 4.71. This should only ever be the case if you've never installed Internet Explorer on your Win95 system.

c:\windows\system\msvcrt.dll is upgraded to version 5.00.7128, if it is older.

On a Windows NT 4.0 system:

c:\winnt\system32\psapi.dll is upgraded to version 5.00.1641.1, or copied there if it was not present before. Early versions of NT 4 did not ship with PSAPI.DLL, but later versions, especially those with Internet Explorer installed, should have a newer version of PSAPI.DLL already.

6. What is the most troublefree way to uninstall or upgrade ZoneAlarm?
The most important step in uninstalling or upgrading is to make sure that ZoneAlarm and its underlying TrueVector service are not running. If TrueVector is left running, certain files may not be removed or replaced. Also, if you use the Desk Band feature, this should be disabled before uninstalling or upgrading ZoneAlarm.

Note that shutting down ZoneAlarm from the tray icon only shuts down the user interface. It may or may not unload TrueVector, depending on how ZoneAlarm was started.

To unload the TrueVector Service and disable the Desk Band:
1. Go to the Configure panel and uncheck the box labeled, "Load ZoneAlarm at Windows startup" (or "Load ZoneAlarm Pro at startup").
2. Right click any unused portion of the task bar at the bottom of the screen, select "Toolbars", and uncheck "ZoneAlarm Desk Band" (or ZoneAlarm Pro Desk Band").
3. REBOOT WINDOWS (very important).

AFTER UNLOADING TRUEVECTOR AND REBOOTING:

To uninstall ZoneAlarm: Click Start | Programs | Zone Labs | Uninstall ZoneAlarm

To clear your configuration settings in ZoneAlarm or ZoneAlarm Pro:
1. For Windows9x, remove the files in \windows\internet logs.
2. For WindowsNT and Windows2000, remove the files in \winnt\internet logs
Note that these files are not deleted by the uninstallation process.

To upgrade ZoneAlarm:
1. It is usually not necessary to uninstall your current version of ZoneAlarm to upgrade to a newer version or to ZoneAlarm Pro. Just double-click on the self-installing executable file, zonealmxx.exe or zaproxx.exe. Your configuration settings are saved from your previous installation.
2. If you are upgrading from a very old version of ZoneAlarm (especially from version 2.0 or earlier), you should uninstall ZoneAlarm and clear your configuration settings in the internet logs directory, as described above. You may also with to consider doing this if you are upgrading from a beta release of ZoneAlarm.
3. If you encounter problems, please refer to this ZoneAlarm uninstall FAQ page.

Due to significant differences between ZoneAlarm and ZoneAlarm Pro, it is particularly important to uninstall ZoneAlarm Pro completely if you wish to go back to using regular ZoneAlarm.

To revert back to ZoneAlarm from ZoneAlarm Pro:
1. Unload TrueVector and disable the Desk Band, as described above
2. Uninstall ZoneAlarm Pro, as described above
3. Remove the files in the internet logs directory, as described above
4. Check for completeness of the uninstallation
5. Install ZoneAlarm by double-clicking on zonealmxx.exe

7. Missing INSTALL.LOG file?
If the uninstaller displays the message "Could not open INSTALL.LOG file" or prompts you for an Install.log file but you can't find one in the ZoneAlarm directory, this usually indicates that original installation was incomplete. This can occur if you canceled the installation program after it installed product.

Back to Top

● Press Room ● Careers ● Volume Sales ● Contact Us ● Site Map ● News & Articles
● Affiliates

Copyright ©1999-2001 Zone Labs, Inc., 1060 Howard Street, San Francisco, CA 94103, USA.
All rights reserved. All other trademarks are the property of their respective owners.

Internet Components

This page provides an introduction to the basics of the Internet and how ZoneAlarm and ZoneAlarm Pro serve as protectors of individual machines.

The Internet

The Internet is a worldwide infrastructure that allows millions of computers, each of which is part of a smaller network, to communicate with each other. Participants on the Internet include individual users, corporations, government agencies, universities, ISPs and various online services.

Data traffic between networks is managed by routers. The primary function of a router is to make sure that data traffic, in the form of packets, arrives at its destination.

The concept of a firewall is to be a sentry, allowing authorized network traffic while blocking unauthorized network traffic through the network. However, many threats and vulnerabilities exist on the Internet which makes protection only on the network impractical. Since time and experience have proven that unseen threats can penetrate a network, additional protection has become a necessity at the desktop, especially for users with "always on" connections to the Internet.

ZoneAlarm and ZoneAlarm Pro are desktop firewalls, ensuring a secure environment while connected to the Internet by allowing the user to dynamically control traffic in and out of the PC. Unseen threats to the desktop include viruses, worms, Trojan horses, denial of service attacks, various direct intrusion methods and many other forms of privacy invasion. ZoneAlarm and ZoneAlarm Pro are equipped with sophisticated means of reporting suspicious activity to log files as well as alert notifications. Since Internet activity is unpredictable, ZoneAlarm and ZoneAlarm Pro arm users with the ability to protect their PCs from unwanted and potentially damaging occurrences.

Connections

Networks can be connected by a variety of transports. The most common examples of Internet access include ordinary telephone lines (dial-up), broadband services such as DSL and cable, ISDN, T1 and T3 lines. Modems and leased lines are the most common methods of transport.

- Traditional dial-up modems provide Internet access via the public telephone network at up to 56 Kbps.
- ISDN modems are capable of speeds up to 10 Mbps.
- DSL modems transmit and receive data digitally with a capacity of 1.544 Mbps.
- Cable modems provide high-speed Internet access through a cable

television network at more than 1 Mbps. This is approximately 20 times faster than dial-up modems.

- T1 lines don't require a modem and can transmit and receive data with a capacity of 1.544 Mbps.
- T3 lines don't require a modem and can transmit and receive data with a capacity of 45 Mbps.

TCP/IP

TCP/IP is the standard protocol for data traffic on the Internet. All data moving through the Internet constitute segmented packets. Routers read the IP packet headers to determine their appropriate destination for the traffic. Once the packets reach their destination, they are reassembled and read by the receiving computer.

An IP address is a unique identifier for each computer or device on the Internet and any TCP/IP network. An example of an IP address would be *127.0.0.1*.

The known and verifiable IP addresses of computers that you trust can be input into the Local Zone so that ZoneAlarm and ZoneAlarm Pro recognize them.

If you are on a network, please click here for instructions on adding your subnet adapter to the Local Zone.

Firewall Protection

Many firewalls use a packet filtering method for distinguishing permissible traffic. This type of protection only examines the IP packet headers. A packet filtering firewall does not protect against attacks directed at the application layer. For instance, if a packet filtering firewall was set to allow incoming e-mail from the Internet, then an attack on the SMTP service would pass through the firewall without a problem. In other words, as long as the rule set is passed, a connection is made directly from outside the firewall to inside the firewall.

One step up from packet filtering is the Stateful Inspection model of firewall. This type of firewall will analyze incoming packets until it has enough information (using information such as TCP sequence numbers) to determine the state of the connection. Then, if the packets pass the rules set, they're forwarded to the correct interface. Using this information, the firewall builds dynamic state tables. It uses these tables to keep track of the connections that go through the firewall. Rather than allowing all packets that meet the rule set's requirements to pass, it allows only those packets which are part of a valid, established connection.

Like packet filtering, a Stateful Inspection does not guard the application layer where many types of attacks are focused.

A core feature of ZoneAlarm is providing protection at the application layer, ensuring nefarious applications such as Trojan horses and spyware are unable to achieve their purpose of reaching the Internet from your computer.

BACK HOME NEXT

Copyright © 1999-2001 Zone Labs, Inc.

All rights reserved. ZoneAlarm and ZoneAlarm Pro include TrueVector Technology, covered by U.S. Patent

No. 5,987,611. Zone Labs, ZoneAlarm, ZoneAlarm Pro, and TrueVector are registered trademarks of Zone Labs, Inc.

Search Engines

This page lists brief descriptions of Search Engines and their uses on the Internet.

Search Engines

There are many search engines on the Internet and if you have spent time at portals such as Yahoo, Excite, HotBot and Alta Vista for instance, you have undoubtedly already made use of their respective search utilities. Using a search engine is a first step in conducting research on the Internet. Essentially, search engines cull "hits" of links to web sites based on keyword searching. Using a search engine will enable you to locate information in a targeted fashion. Use these services for troubleshooting desktop problems and notice how quickly you can learn about understanding operability of your computer.

For dependable results, run variations of syntax in your queries. For example, using Boolean operators (and, or, not) will help narrow search results. Check the help section of the search utility you are using for more tips on enhanced search methods.

BACK HOME NEXT

Copyright © 1999-2001 Zone Labs, Inc.

All rights reserved. ZoneAlarm and ZoneAlarm Pro include TrueVector Technology, covered by U.S. Patent No. 5,987,611. Zone Labs, ZoneAlarm, ZoneAlarm Pro, and TrueVector are registered trademarks of Zone Labs, Inc.

Surfing the Web

Use the links below to review basic concepts about the World Wide Web.

Web Browsers

There are several varieties of web browsers, though the most commonly used on the Internet are Netscape Navigator and Internet Explorer. All browsers use the same principle of retrieving content from the web. HTTP (Hyper Text Transfer Protocol) is the standard protocol for retrieving text and images and serving them through a browser. HTML (Hyper Text Markup Language) is the current standard for formatting web content so that it is readable by browsers.

When a URL is typed into a browser, it looks up the associated web server, which in turn sends back a web page.

Many web pages contain portions written in languages other than HTML. Language such as Java, ActiveX, JavaScript and other scripting languages are utilized by enterprising webmasters. It is commonplace for sound and animation files to be incorporated into web pages, requiring plug-ins or even third party software to be downloaded. Therefore, multiple components are working in synchronization to deliver content through the browser.

Web Pages

At its simplest, a web page is a document written in Hypertext Markup Language (HTML). HTML is a kind of text markup that Web browsers understand.

When you click on a link within a web site or from an e-mail, you are issuing a request from a web server to display a web page.

Web Sites

Web sites are organized groups of web pages that are linked and presented together by one or more web servers located at an enterprise or other organization.

URL Addresses

URL stands for Uniform Resource Locator, a series of letters separated by periods that represents a web IP address. (For example: www.cnn.com.) URLs exist so that we can remember the names of web sites, rather than having to remember a series of digits that make up an IP address, such as 123.12.123.143.

Your web browser sends URL requests to a name service site, where the URL is translated to the IP address. When the server is located, it further resolves the name of the page (or other document) and sends it to your web browser. The result (what you see inside your browser) is the browser's interpretation of the target site's HTML.

Web Servers

Web servers are computers that send you a web page when you request an URL in your browser. Each web server on the Internet has an IP address and could be hosting a domain. When you enter this URL in your browser-

```
    http://www.fastasticvoyage.com/helppage.html
```

-the web server whose domain name is fastasticvoyage.com receives the request from your browser. In response, the web server fetches a web page named helppage.html, which sends it to your browser.

Any computer can act as a Web server. All that is required is server software and a live connection to the Internet.

Internet Explorer Browser

Browsers are used to locate and display Web pages, displaying graphics, text, and multimedia such as sound and video. Internet Explorer, Microsoft's web browser, is integrated with the Windows operating system. You can place web links directly as icons on the desktop. These icons can be clicked on in order to directly open a specific web site inside Internet Explorer. With the Active Desktop, applications loading directly from the Internet can be running as minimized icons on the desktop.

Netscape Communicator

Netscape Communicator, like Internet Explorer, is a web browser used to locate and display Web pages. It displays graphics and text in addition to multimedia such as sound and video. Plug-ins are required for some video and audio formats.

Audio

Web pages can link to audio files that you can listen to if you have the right software. To listen to audio from a Web page that includes a RealAudio sound file, you need a RealAudio player or plug-in, a program that is freely available from a number of sites. It's also included in current versions of both Netscape Navigator and Microsoft Internet Explorer.

Video

The ability to present video, animation and graphics together in an integrated fashion is often termed multimedia.

Video transmission is possible with high speed connections to the Internet. However, the quality of video resolution depends on the power of the computer's video card and CPU.

Streaming Content

Streaming refers to presentation of any form of multimedia such as audio and video *as it is transmitted* by the host website.

When streaming is used, the streamed data can start the display in your browser before the whole file has been received. In other words, you are viewing before data transmission is complete.

If your machine receives streamed data more quickly than it can be presented, the excess data is saved in a buffer. However, if the streamed data comes to your machine too slowly, the quality of the presentation degrades. Therefore, the speed of your connection is important.

Push Technology

Push technology uses a *continuously open connection* to deliver ("push") HTML pages, Java applets, multimedia objects, and ActiveX components to your browser. This sort of service is designed to deliver customized information to users, for instance, stocks updates and sports tickers.

BACK HOME NEXT

Copyright © 1999-2001 Zone Labs, Inc.

All rights reserved. ZoneAlarm and ZoneAlarm Pro include TrueVector Technology, covered by U.S. Patent No. 5,987,611. Zone Labs, ZoneAlarm, ZoneAlarm Pro, and TrueVector are registered trademarks of Zone Labs, Inc.

ZONE LABS

About E-mail

This section talks about how e-mail works within the infrastructure of the Internet and your desktop. For help setting up your mail software to work with ZoneAlarm, check here.

(Many e-mail programs require server rights. You assign these rights in the Programs panel. For many e-mail programs to work efficiently, set the Allow Server option for the e-mail software you use.)

How E-mail Works

An e-mail message consists of binary data. Most e-mail messages are in the ASCII text format which is a standard that allows any computer to read it.

E-mail messages are sent in the same way as most other data is sent over the Internet, via TCP. TCP separates outgoing e-mail messages into IP packets, then delivers those packets to the destination indicated in the address header. Upon receipt at its destination, the packets are reassembled.

Most files such as pictures, audio and programs, can be attached to an e-mail message. When these files are sent over the Internet, an encoding scheme, such a MIME or uuencode is used to encode the attachment, which will be decoded by the e-mail system at the destination. Most e-mail packages automatically and transparently decode attachments.

ZoneAlarm's MailSafe feature protects your e-mailbox by allowing you to decide which kinds of e-mail attachments you are going to allow to be opened without protective intervention.

When an e-mail message is sent, it usually has to be sent through a number of networks before reaching its destination. Some of these use different e-mail formats. When this is the case, the network gateway will perform the task of translating from one e-mail format to another. This allows the message to make its way to the recipient.

E-mail Software

In order to send and receive e-mail, you need a software package.

E-mail that is sent to you is usually delivered to your company's or Internet provider's e-mail server. When you want to check for new mail or open mail, your e-mail software logs on to the e-mail server to find out if there are messages addressed to you.

When you have new mail, you click a button or icon to display the list of unread mail in your mailbox. To read a specific message, you click on the mail item, which tells your e-mail software to open it.

How E-mail Reaches Its Destination

You've just sent an e-mail message from Netscape Messenger or Outlook Express. What happens next?

First, TCP breaks the e-mail message up into IP packets. Next, the packets go to a router on your Local Area Network (LAN) where the destination address is examined. If your e-mail is going to someone whose computer is on your LAN, the packets are reassembled into the original message and the e-mail is delivered without any further steps.

If the e-mail is going outside your LAN, it will go through whatever firewall may be set up on your LAN. Next, the e-mail message moves on to a router located outside your LAN, somewhere on the Internet. That router determines the destination from the address, then sends the e-mail on its way there.

When the e-mail arrives at its destination, the gateway receives it. The gateway first reassembles all the packets that make up the e-mail using the TCP protocol. The result is that the separate packets have become an actual message again.

Next, the gateway translates the reassembled e-mail message into the e-mail protocol that is used on the network. Finally, the gateway sends the message, in its reassembled and translated format, into the network where it may pass through another firewall before getting to its final destination inside your e-mail software.

E-mail Security

The basic security problem surrounding e-mail is the same problem that exists with any Internet communication; being, data communications can be intercepted. E-mail piracy is rare and usually is either of two extremes: one, an interception is confined to a specific personal attack, or two, the attack is traced to a widespread intrusion involving one or more Internet Service Providers (ISPs).

Besides the e-mail message itself, by searching around on the Internet (chatrooms, etc.) snoopers might be able to find your e-mail address. In the past, if an Internet snooper only had your name, he or she might not be able to get retrieve your e-mail address. These days, many directories and query servers exist to trace e-mail addresses.

Encryption can be used to scramble mail so that only people with the proper encryption keys are able to descramble e-mail. However, this is an arduous task and usually not worth the time to invest. The basic rule of thumb is to be careful who you communicate with and where you divulge your e-mail address on the Internet.

E-mail Mailing Lists

The purpose of e-mail mailing lists is to connect people who share some kind of common interest. Once you are a member of an e-mail list, whenever you send an e-mail to the mailing list, it is automatically sent to everyone on the list.

You join a list by subscribing to it. You do this by sending an e-mail to the mail list administrator or to a list server. If you send your request to a list server, a computer will read your request without any human intervention and will automatically put you on the list. You can also cancel your subscription to the list by sending the same type of e-mail.

A database resides on the computer where the mailing list is administered. When you send a subscription request, the e-mail list database will send your message to every address already on the mailing list.

BACK HOME

Copyright © 1999-2001 Zone Labs, Inc.

All rights reserved. ZoneAlarm and ZoneAlarm Pro include TrueVector Technology, covered by U.S. Patent No. 5,987,611. Zone Labs, ZoneAlarm, ZoneAlarm Pro, and TrueVector are registered trademarks of Zone Labs, Inc.

Repeat program

Do you want to allow a specific program to access the Internet?

What is a repeat program?

A repeat program is a program that has previously asked you for permission to access the Internet or the local network. When it did, you either allowed or denied the program access for that instance only.

If you would like to allow or deny this program access for every future instance, check the box, "Remember this answer each time," before you click "Yes" or "No" . Some people like to make their programs ask permission every time they try to access the network. That way, for example, they will know when some other application is launching their browser. You don't have to do anything special to be asked each time. Asking is ZoneAlarm's default behavior.

How should I answer?

Follow the rules below and you'll be able to answer program alerts with confidence.

The rule of expectancy: If you're using a program for the first time that requires Internet access, you should expect to receive a pop-up alert as soon as the program tries to initiate Internet access. In this case, it's probably safe to grant the program access rights.

- Example: You've just opened your Web browser to surf the Internet, and you immediately receive a pop-up alert asking if your Internet browser may access the Internet.

The rule of logic: For some programs such as Web browsers and e-mail clients, it's only logical that they need Internet access. But for other programs, it's not always so obvious. Take your word processor, for example. There are times when it's logical for it to access the Internet, and other times when it is not:

- You're not even using your word processor and it suddenly asks for Internet access. Logic: Why would it need Internet access? Be suspicious.
- You're doing nothing more than typing a document and your word processor asks for access. Logic: Why would it need Internet access? Be suspicious.
- You've just clicked a link to the Internet within your document, or you've told your word processor to import a graphic from the Internet. Logic: It now makes sense for it to need Internet access. It's probably safe.
- You've just cut and pasted formatted text from a web page into your document, and your word processor asks for Internet access. Logic: Your word processor may be trying to get the formatting information from the Internet. It makes sense for it to need access. It's probably safe.

The rule of caution: If you're not sure whether a program should have access rights, start by denying it access rights. Then, investigate the program by asking

- Is the program you've denied access to one you recognize? If not, you may want to research the program to try and identify it as legitimate or illegitimate.
- Is it reasonable this program needs Internet access to perform its funtions?
- Is the program you've denied access to still able to perform the functions you want it to without Internet access? Consider all of the above questions before deciding if your decision was right. You may change your decision at any time in the Programs panel.

How do I know what program is trying to gain access?

Sometimes you can tell what a program is by its name; other times you may not. An unfamiliar program may be an important component of a known program, and may be needed by the known program in order to function:

- "Services and controller app" is a Windows component used by Microsoft Internet Explorer(TM) to access the Internet.
- "Microsoft Windows(TM) Messaging Subsystem Spooler" is a component of Microsoft Outlook(TM), used to get e-mail.

Therefore, some unfamiliar programs do need Internet access. Other unfamiliar programs, however, may be potentially harmful. If you don't recognize a program, start by reading our FAQ for a list of commonly unrecognized programs. If you can't find your answer there, try entering the program name into a search engine.

What else should I know?

There are a few ways you may answer a pop-up:

- Answer, "Yes," to give a program access rights just this one time. The next time the program needs to access the Internet , it will ask again.
- Answer, "No," to deny access rights just this one time. The next time the program needs to access the Internet, it will ask again.
- If you check, "Remember this answer the next time I use this program," before you click "Yes," or "No," the program will NOT ask you again. Your answer will be saved and applied each time the program tries to access the local network or the Internet.

You may change your answer any time in the Programs panel for any program by clicking on the interface.

A red X = deny access, a green checkmark = allow access, a black ? means ask me every time.

For further information

Knowledgebase Main Page
Zone Labs Home Page
Zone Labs Support Page

BACK HOME NEXT

Copyright © 1999-2001 Zone Labs, Inc.

All rights reserved. ZoneAlarm and ZoneAlarm Pro include TrueVector Technology, covered by U.S. Patent No. 5,987,611. Zone Labs, ZoneAlarm, ZoneAlarm Pro, and TrueVector are registered trademarks of Zone Labs, Inc.

Current Alerts Display Area

The Current Alerts Display Area displays information about connection alerts on your machine.

The Display Area

The large display area on the Alerts panel is Current Alerts. It displays the following information about current connection alerts on your machine:

- the IP address
- the port
- the protocol
- the time and date of the connection attempt
- whether the connection attempt was incoming or outgoing
- possibly, but not always, the name of the application causing the alert

You can submit a request to the Zone Labs Alert Analyzer to get detailed information about the block by clicking the More Info button. Clicking More Info sends information about the alert to the Alert Analyzer web site. It launches the user's browser and displays a page with the following information:

- A synopsis of the source and destination IP addresses and ports, the program name and file name of the program associated with the alert, if known
- A link to query the ARIN *whois* database for the source or destination IP address. This provides administrative contact information about the upstream provider for the IP address. It does NOT identify the computer
- For the most common alerts, a brief article explaining what might be causing the alert
- Links to FAQ articles on the Zone Labs web site

Alert Logs

Click here to view the help article on Zone Alarm Logs

Click the links below to view information about common log entries:

- FWIN Sample: An incoming request was blocked
- FWOUT Sample: An outbound request was blocked
- PE Sample: One of your applications tried to connect

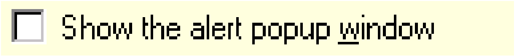
BACK HOME NEXT

Copyright © 1999-2001 Zone Labs, Inc.

All rights reserved. ZoneAlarm and ZoneAlarm Pro include TrueVector Technology, covered by U.S. Patent No. 5,987,611. Zone Labs, ZoneAlarm, ZoneAlarm Pro, and TrueVector are registered trademarks of Zone Labs, Inc.

Firewall Alerts

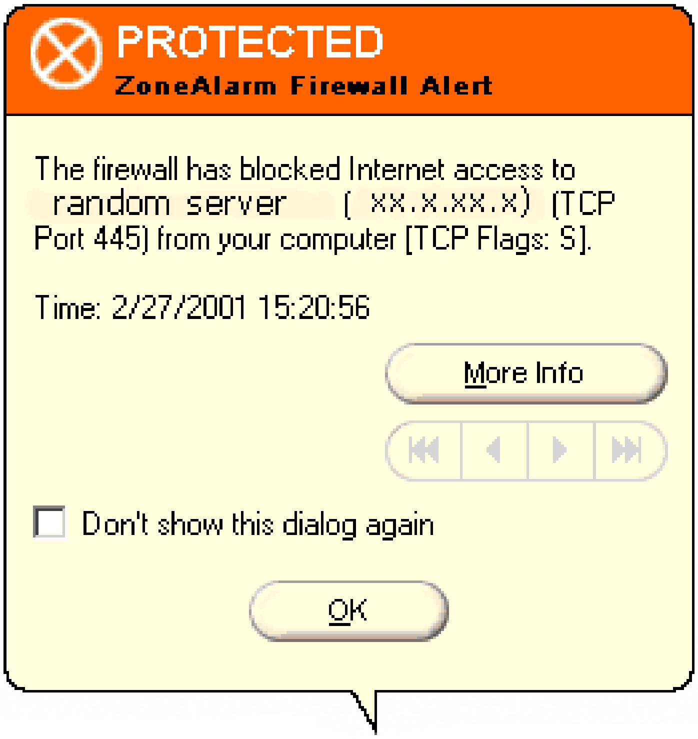
The checkbox shown here controls whether Internet alerts are displayed on your computer screen. You can find this checkbox at the bottom of the Alerts panel in the "Alert Settings" section. Unless you select this checkbox, you will not receive a popup display for Internet alerts.



□ Show the alert popup window

When the checkbox is checked, ZoneAlarm displays an alert popup whenever it blocks an Internet communication.

There are two types of firewall alerts: Cautious and Urgent, each displayed with a color code to identify severity. An orange title band means the alert of a cautious nature.



PROTECTED

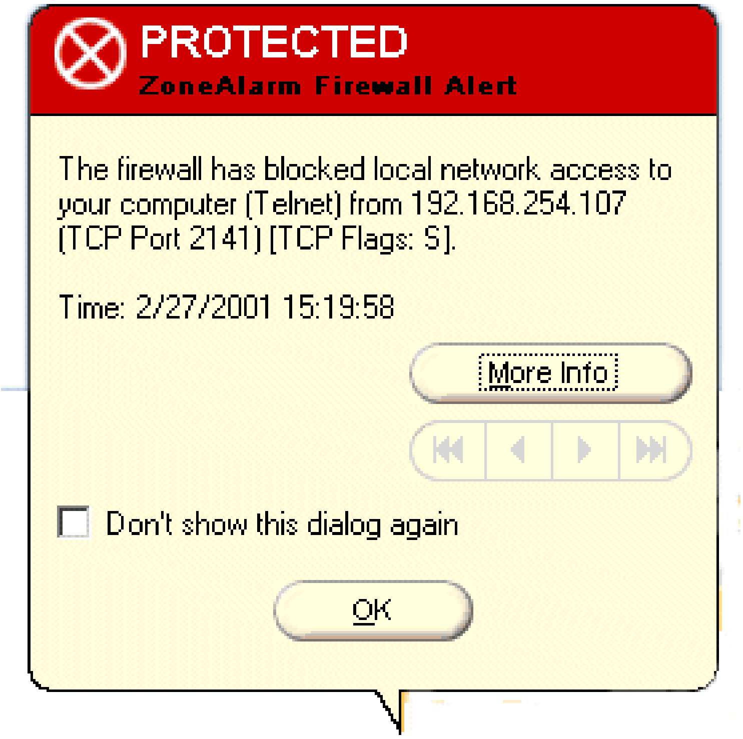
ZoneAlarm Firewall Alert

The firewall has blocked Internet access to random server (xx.x.xx.x) (TCP Port 445) from your computer [TCP Flags: S].

Time: 2/27/2001 15:20:56

□ Don't show this dialog again

Alerts generated by a potentially problematic source are identified by a red title band.



PROTECTED

ZoneAlarm Firewall Alert

The firewall has blocked local network access to your computer [Telnet] from 192.168.254.107 [TCP Port 2141] [TCP Flags: S].

Time: 2/27/2001 15:19:58

In the example above, this was a telnet attempt from an unknown source.

Learn More About:
Alert Settings
Current Alerts
Understanding Alerts
Alert Logs — See samples of the three types of alerts in the log file.

BACK HOME

Copyright © 1999-2001 Zone Labs, Inc.

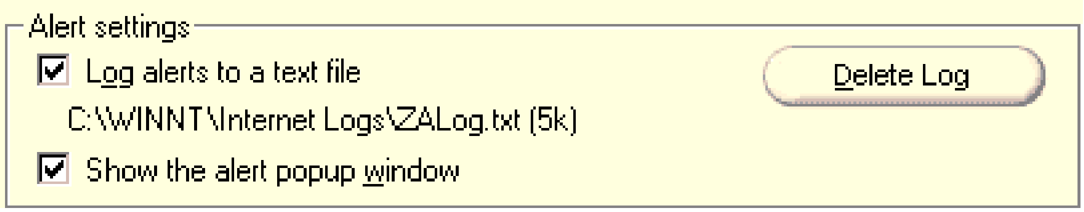
All rights reserved. ZoneAlarm and ZoneAlarm Pro include TrueVector Technology, covered by U.S. Patent No. 5,987,611. Zone Labs, ZoneAlarm, ZoneAlarm Pro, and TrueVector are registered trademarks of Zone Labs, Inc.

Alert Settings Section

The Alert settings section of the Alerts panel lets you determine if alerts are sent to the Alert Log, to a popup window or both.

About the Alerts Section

Important: A popup may block network traffic until the alert is OK'd in the popup window. If you are not monitoring traffic at the workstation, it is advised to not use the popup option.


Alert settings

☑ Log alerts to a text file

C:\WINNT\Internet Logs\ZALog.txt (5k)

☑ Show the alert popup window

Check the Log Alerts to a text file checkbox to save alerts to a text file in CSV format (most spreadsheet and database applications can import this file format).

Check the Show the Alerts Popup window checkbox to either display the Visual Alert window or to turn it off altogether.

Delete Logs

ZoneAlarm logs can be deleted at your discretion so they do not become excessively large. You can back up your logs by renaming the file using whatever naming scheme you prefer. Please refer to the section on Alert Logs for additional information.

Learn More About:

Current Alerts

Understanding Alerts

Alerts Panel

BACK HOME

Copyright © 1999-2001 Zone Labs, Inc.

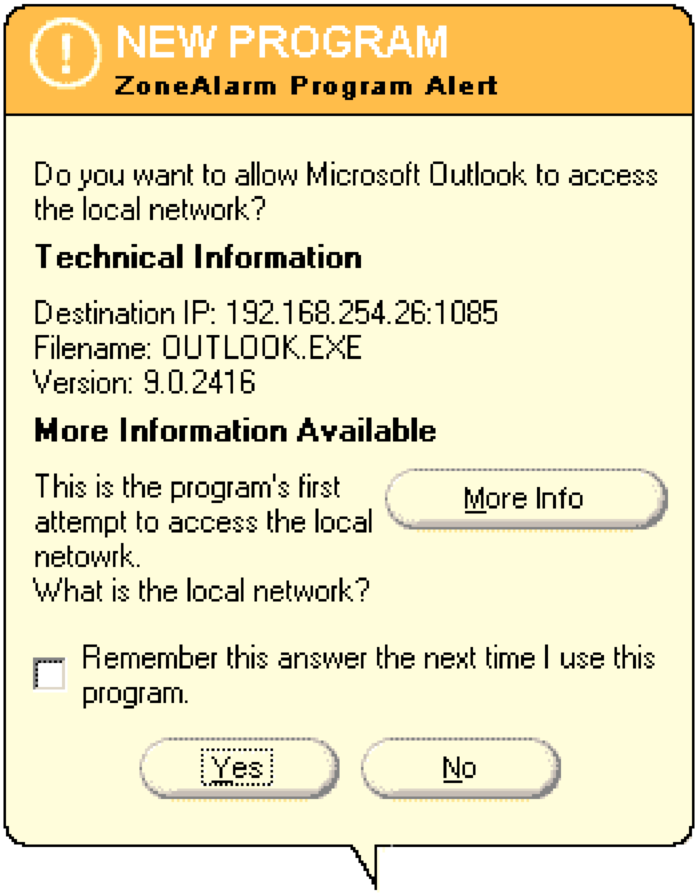
All rights reserved. ZoneAlarm and ZoneAlarm Pro include TrueVector Technology, covered by U.S. Patent No. 5,987,611. Zone Labs, ZoneAlarm, ZoneAlarm Pro, and TrueVector are registered trademarks of Zone Labs, Inc.

Program Alerts

There are four types of program alerts: New, Changed, Repeat and Server.

When a program asks for permission either to access the Internet (or private LAN) or to act as a server for the first time (i.e. it is not listed in the Programs Panel), it will be labeled as "New Program." Once the program either has been accepted or denied access, it is no longer a new program.

The "New Program" alert will be displayed whenever one of the applications on your computer attempts to access the Internet. The example shown below indicates that Microsoft Outlook, which has never accessed the Internet from the the user's machine before, is attempting to reach an IP address on the Internet.



NEW PROGRAM

ZoneAlarm Program Alert

Do you want to allow Microsoft Outlook to access the local network?

Technical Information

Destination IP: 192.168.254.26:1085
Filename: OUTLOOK.EXE
Version: 9.0.2416

More Information Available

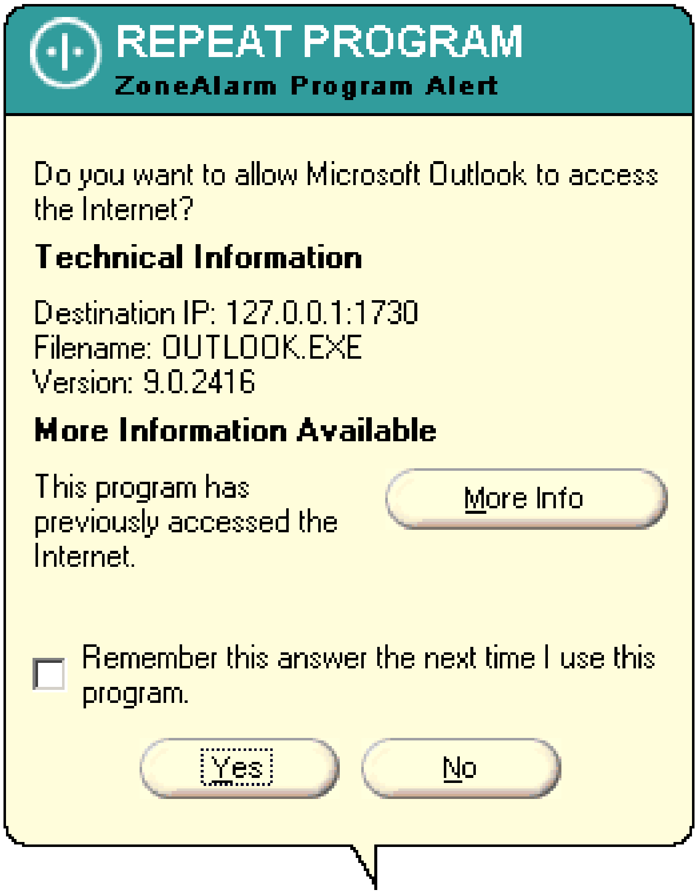
This is the program's first attempt to access the local netowrk.
What is the local network?

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

By selecting *Yes* on this pop-up, you are indicating that the application is allowed to contact the Internet destination indicated under Technical Information in the pop-up.

At the time you receive a pop-up message like the one above, you can easily instruct ZoneAlarm not to invoke pop-up alerts for that particular application. You can accomplish this by selecting the *"Remember this answer the next time I use this program"* box, located at the bottom of the pop-up message.

If you do not select the *"Remember this answer the next time I use this program"* box, you will receive a message like the one shown below the next time Microsoft Outlook tries to reach an Internet destination:


REPEAT PROGRAM
ZoneAlarm Program Alert

Do you want to allow Microsoft Outlook to access the Internet?

Technical Information

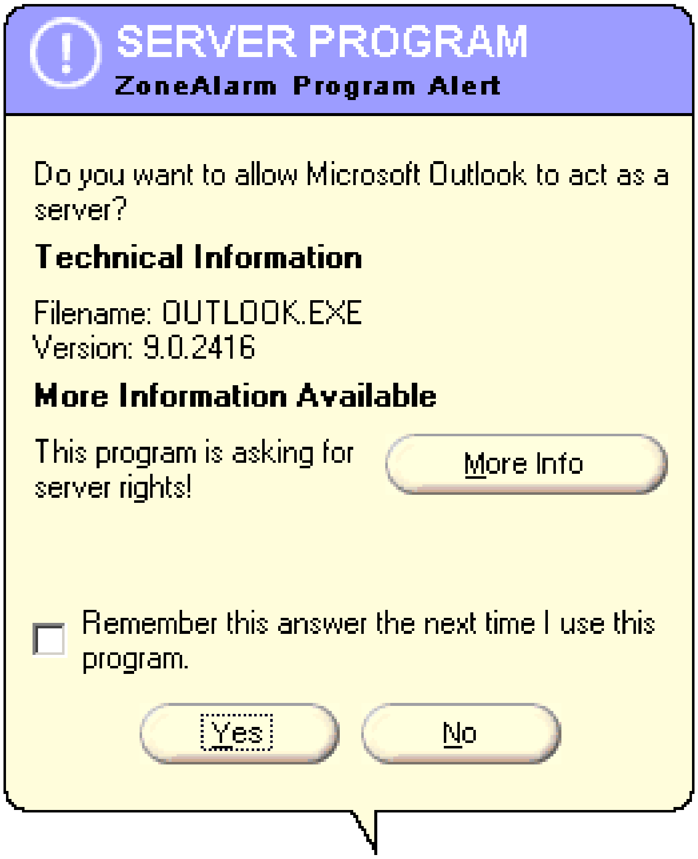
Destination IP: 127.0.0.1:1730
Filename: OUTLOOK.EXE
Version: 9.0.2416

More Information Available

This program has previously accessed the Internet.

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

If the application is already in your Programs List and has server rights, you will receive a Server Program Alert.


SERVER PROGRAM
ZoneAlarm Program Alert

Do you want to allow Microsoft Outlook to act as a server?

Technical Information

Filename: OUTLOOK.EXE
Version: 9.0.2416

More Information Available

This program is asking for server rights!

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

If you do not mark the *"Remember this answer the next time I use this program"* box, then ZoneAlarm will still recognize the application and put it into your Programs List. It will not however, have access to the Internet (allow connect will not be checked). Once in your Programs List, you can either allow it access or remove it.

Changed Program

If a program that already has a rule listed in the programs panel tries to 1) access the Internet or LAN, and/or 2) act as a server, the alert will be labeled "changed program."

- The MD5 or CRC checksum has changed
- The version number of the program has changed
- The name of the program has changed
- The name of the executable has changed
- The path/directory of the program has changed
- The file size has changed
- The certificate has changed

For additional information on MD5 Checksum, go here.

Program Alert Content

ZoneAlarm program alerts will contain the following information:

- the IP address
- the port
- the protocol
- the time and date of the connection attempt
- whether the connection attempt was incoming or outgoing
- possibly, but not always, the name of the application causing the alert

More Info Button

The More Info button is the way to find out additional information about the meaning of a specific Program alert pop-up you have received. The information displayed when you click on the More Info button comes from the Zone Labs KnowledgeBase located on our web site.

BACK HOME NEXT

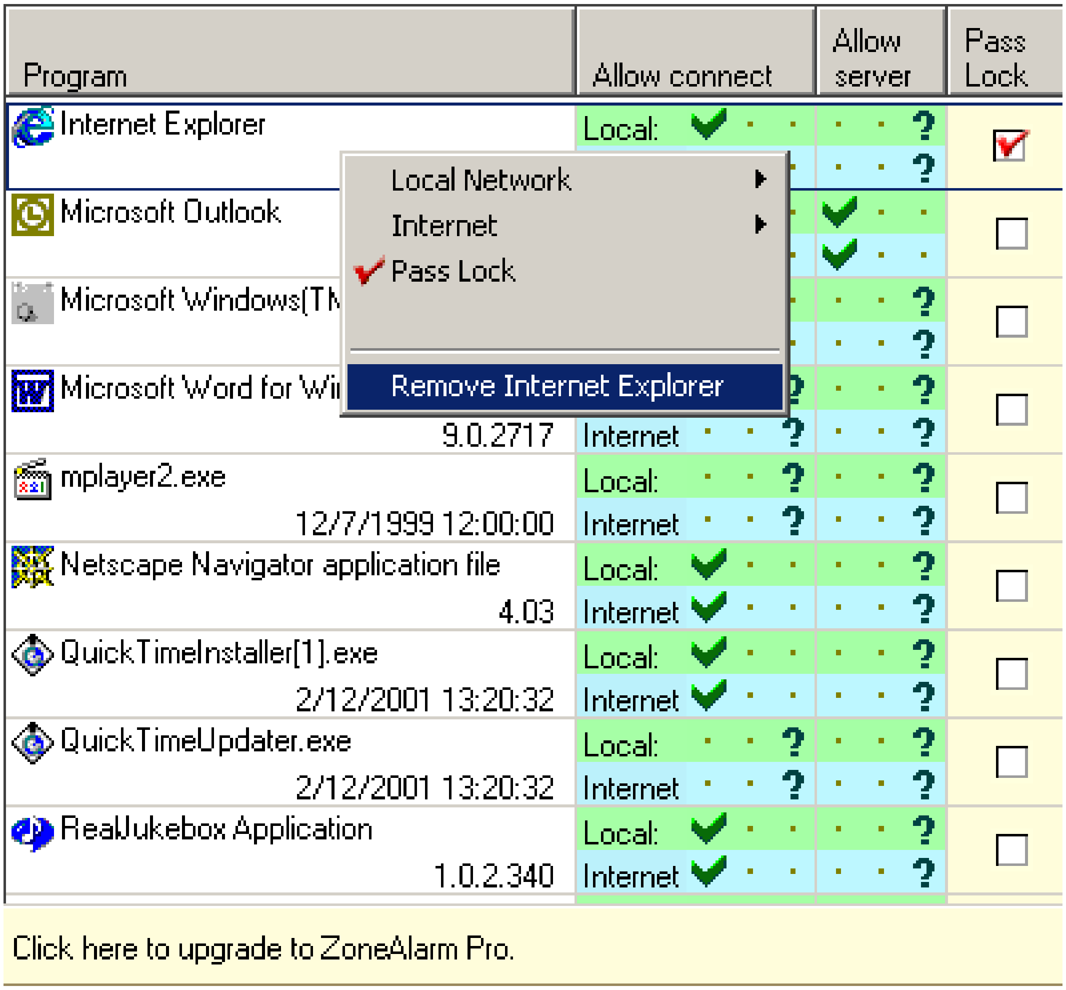
Copyright © 1999-2001 Zone Labs, Inc.

All rights reserved. ZoneAlarm and ZoneAlarm Pro include TrueVector Technology, covered by U.S. Patent No. 5,987,611. Zone Labs, ZoneAlarm, ZoneAlarm Pro, and TrueVector are registered trademarks of Zone Labs, Inc.

Removing a Program from the Programs List

To remove a program from the list, right-click on the program entry then select Remove from the popup menu. Removing a program from the list does not prevent ZoneAlarm from monitoring the application. ZoneAlarm will detect the program next time it attempts to access the Internet.

(You can also change a program's Internet access rights using the right-click menu.)



Program		Allow connect		Allow server	Pass Lock
Internet Explorer		Local:	✓ · ·	· · ?	☑
			·	· · ?	
Microsoft Outlook			·	✓ · ·	☐
			·	✓ · ·	
Microsoft Windows(TM			·	· · ?	☐
			·	· · ?	
Microsoft Word for Wi			?	· · ?	☐
	9.0.2717	Internet	· · ?	· · ?	
mplayer2.exe		Local:	· · ?	· · ?	☐
	12/7/1999 12:00:00	Internet	· · ?	· · ?	
Netscape Navigator application file		Local:	✓ · ·	· · ?	☐
	4.03	Internet	✓ · ·	· · ?	
QuickTimeInstaller[1].exe		Local:	✓ · ·	· · ?	☐
	2/12/2001 13:20:32	Internet	✓ · ·	· · ?	
QuickTimeUpdater.exe		Local:	· · ?	· · ?	☐
	2/12/2001 13:20:32	Internet	· · ?	· · ?	
RealJukebox Application		Local:	✓ · ·	· · ?	☐
	1.0.2.340	Internet	✓ · ·	· · ?	

Click here to upgrade to ZoneAlarm Pro.

BACK HOME

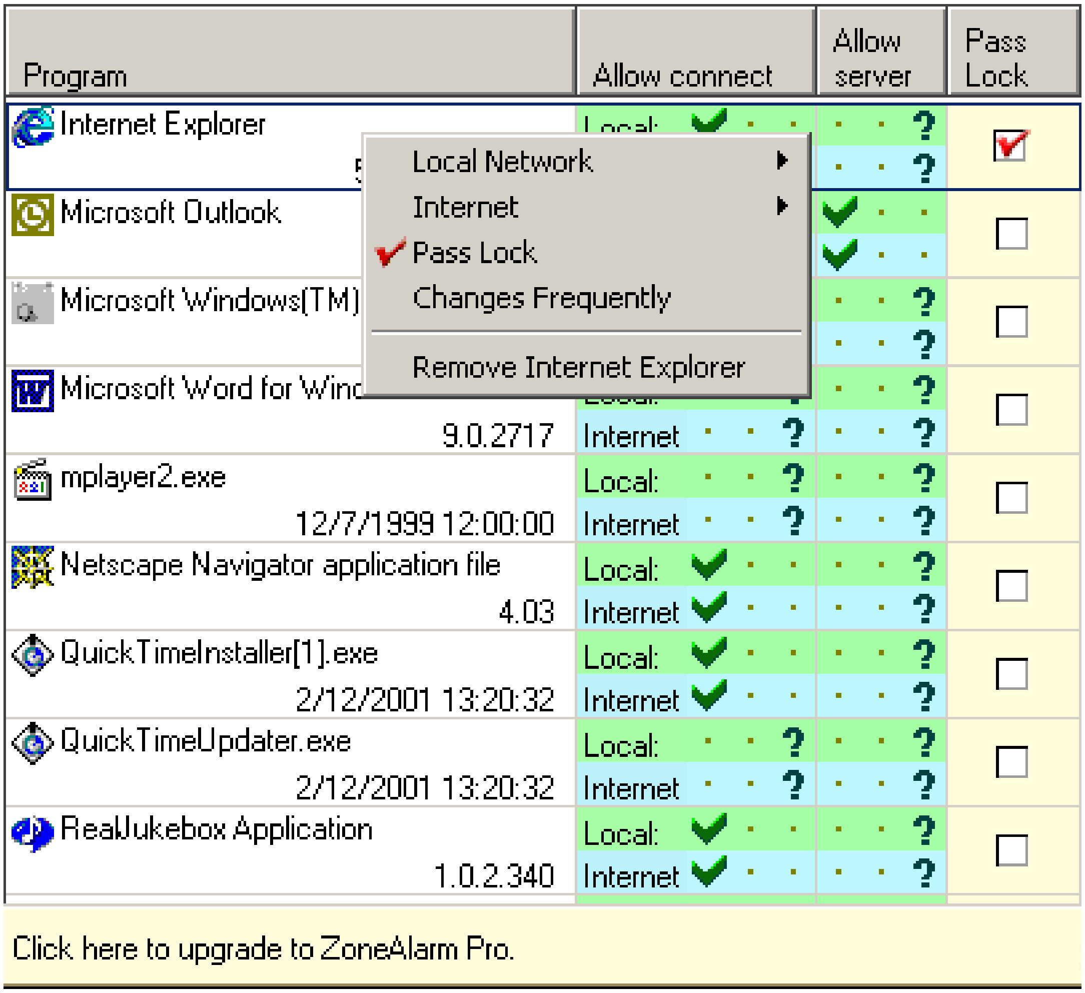
Copyright © 1999-2001 Zone Labs, Inc.

All rights reserved. ZoneAlarm and ZoneAlarm Pro include TrueVector Technology, covered by U.S. Patent No. 5,987,611. Zone Labs, ZoneAlarm, ZoneAlarm Pro, and TrueVector are registered trademarks of Zone Labs, Inc.

Pass Lock Feature

The Pass Lock feature enables you to select applications that are allowed to connect to the Internet when the Automatic Lock is engaged.

Select Pass Lock from the popup menu to allow the program on which you right-clicked to bypass the Automatic Lock. You can use this feature to allow a program such as your e-mail client to check for mail when access to all zones is locked.



Program	Allow connect	Allow server	Pass Lock
Internet Explorer	Local: ✓ · ·	· · ?	☑
5		· · ?	
Microsoft Outlook		✓ · ·	☐
		✓ · ·	
Microsoft Windows(TM)		· · ?	☐
		· · ?	
Microsoft Word for Wind	Local:	· · ?	☐
9.0.2717	Internet · · ?	· · ?	
mplayer2.exe	Local: · · ?	· · ?	☐
12/7/1999 12:00:00	Internet · · ?	· · ?	
Netscape Navigator application file	Local: ✓ · ·	· · ?	☐
4.03	Internet ✓ · ·	· · ?	
QuickTimeInstaller[1].exe	Local: ✓ · ·	· · ?	☐
2/12/2001 13:20:32	Internet ✓ · ·	· · ?	
QuickTimeUpdater.exe	Local: · · ?	· · ?	☐
2/12/2001 13:20:32	Internet · · ?	· · ?	
RealJukebox Application	Local: ✓ · ·	· · ?	☐
1.0.2.340	Internet ✓ · ·	· · ?	

Click here to upgrade to ZoneAlarm Pro.

You can also use this feature to allow server applications to bypass the Automatic Lock. If an FTP or Web server application is running on your computer, checking the Pass Lock checkbox will allow the application to remain connected to the Internet.

If one of your programs generates errors regarding an Internet connection, it is possible that it attempted to access the Internet when the Automatic Lock was engaged. To allow the program access, check the Pass Lock checkbox.

BACK HOME

Copyright © 1999-2001 Zone Labs, Inc.

All rights reserved. ZoneAlarm and ZoneAlarm Pro include TrueVector Technology, covered by U.S. Patent No. 5,987,611. Zone Labs, ZoneAlarm, ZoneAlarm Pro, and TrueVector are registered trademarks of Zone Labs, Inc.

About Zone Alarm Logs

This page presents information about the ZoneAlarm event logs.

`ZAlog.txt` contains information on ZoneAlarm Alerts. If you are using Windows95, Windows98 or Windows Me, the file is located in the folder `(x):\Windows\Internet Logs`.

If you are using WindowsNT or Windows2000, the file is located in the folder `(x):\Winnt\Internet Logs`.

ZoneAlarm logs the following information:

> FWIN: indicates that the firewall blocked an incoming request to connect to your computer.
>
> FWOUT: indicates that the firewall blocked an outbound request from your computer.
>
> PE: indicates that an application on your computer attempted to access the Internet.

TCPFlags

There are six TCP flags. They are:

> URG - urgent pointer is valid
> ACK - acknowledge data received (set in all packets but first)
> PSH - push data to app
> RST - reset connection (hard close)
> SYN - connection request (& returned by server w/ ack to accept)
> FIN - end connection (normal close)

The flag as noted in the log file is the first letter of the flag abbreviation. Therefore, "AP" means ACK plus PSH, "S" means SYN.

Click the links below to view information about common log entries:

- FWIN Sample: An incoming request was blocked
- FWOUT Sample: An outbound request was blocked
- PE Sample: One of your applications tried to connect

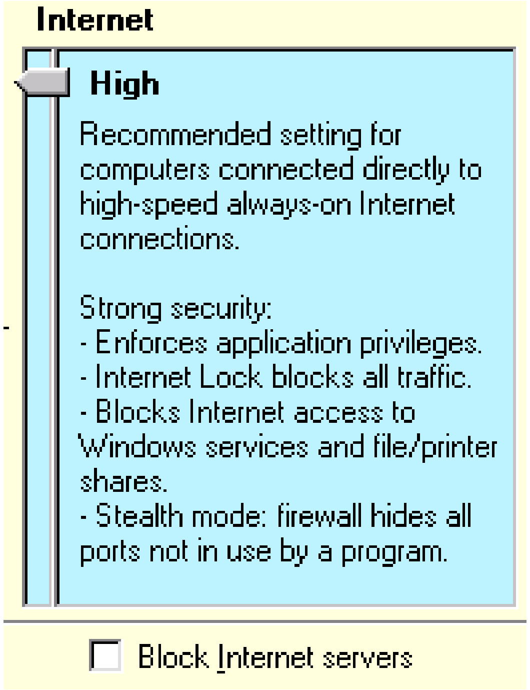
BACK HOME

Copyright © 1999-2001 Zone Labs, Inc.

All rights reserved. ZoneAlarm and ZoneAlarm Pro include TrueVector Technology, covered by U.S. Patent No. 5,987,611. Zone Labs, ZoneAlarm, ZoneAlarm Pro, and TrueVector are registered trademarks of Zone Labs, Inc.

Internet Zone Security settings

Three levels of security are available. The default security setting for the Internet Zone is High.



Internet

High

Recommended setting for computers connected directly to high-speed always-on Internet connections.

Strong security:
- Enforces application privileges.
- Internet Lock blocks all traffic.
- Blocks Internet access to Windows services and file/printer shares.
- Stealth mode: firewall hides all ports not in use by a program.

☐ Block Internet servers

Low Security: *Low Security is not recommended for the Internet Zone.* Low security only enforces application privileges and Internet Lock settings, leaving your computer visible to other computers in the Internet Zone. The firewall does not block file or printer sharing, or traffic to and from the Internet Zone.

Medium Security: At this security level, file shares, printer shares and Windows services are allowed. When Medium security is set, the firewall blocks access from the Internet Zone to Windows (NetBIOS) services. Also, with security set at this level, the Automatic Lock is enhanced by the firewall and blocks all ports.

High Security: This is the default security setting for the Internet Zone. At High security, the firewall blocks access from the Internet Zone to Windows (NetBIOS) services and file and printer shares.

When High Security is set, your computer is in "Stealth Mode" — all ports not currently in use by a program are blocked and are not visible to the Internet Zone. High security opens ports only when an approved program requests them.

BACK HOME

Copyright © 1999-2001 Zone Labs, Inc.

All rights reserved. ZoneAlarm and ZoneAlarm Pro include TrueVector Technology, covered by U.S. Patent No. 5,987,611. Zone Labs, ZoneAlarm, ZoneAlarm Pro, and TrueVector are registered trademarks of Zone Labs, Inc.

Local Zone Properties

This page explains how to add Internet servers, IP addresses & subnets to your trusted local zone.

About the Panel

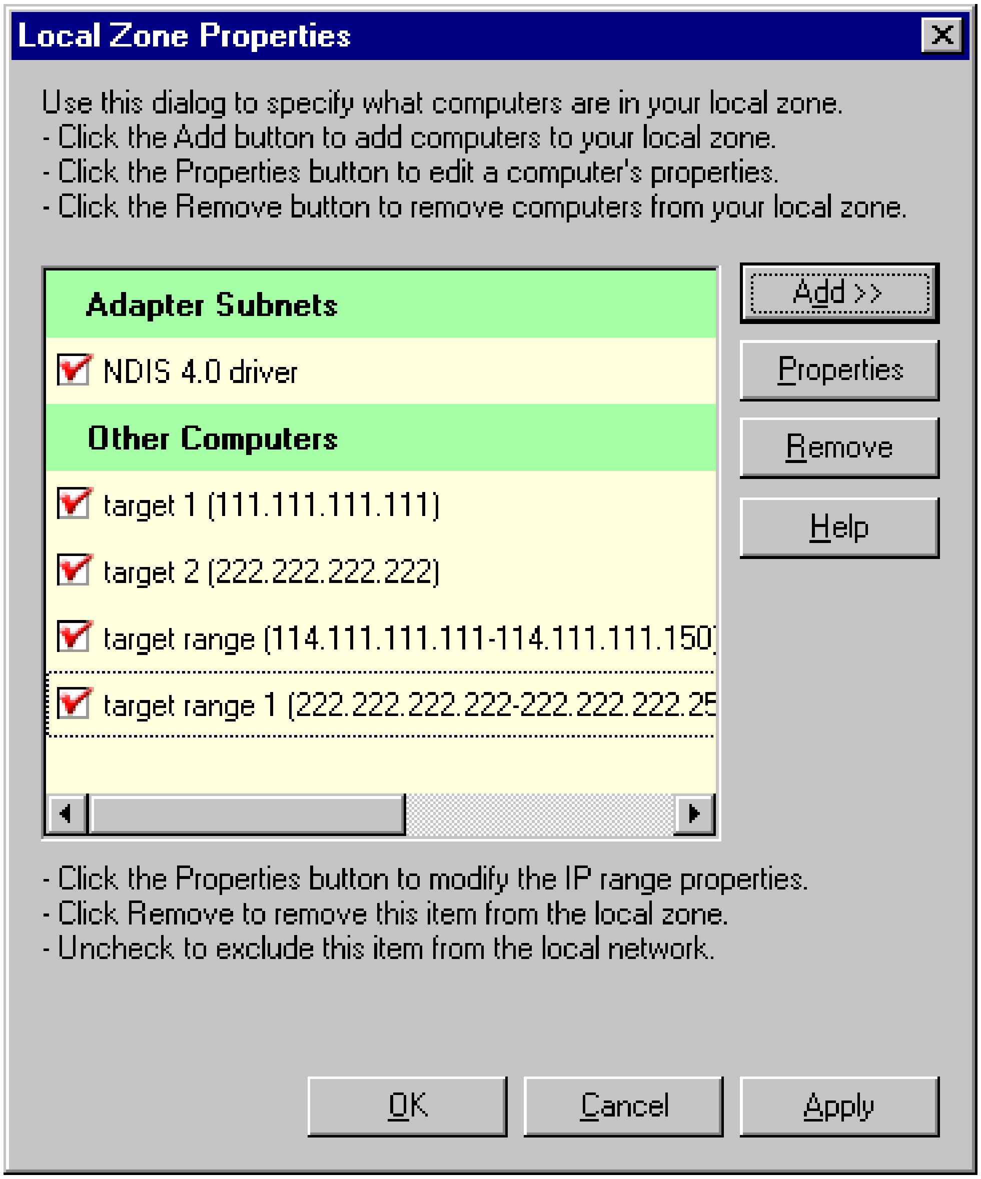
The Local Zone Properties dialog is displayed when you click the Advanced button in the Security panel. Use the Local Zone Properties to add trusted:

- Domains
- IP addresses or IP ranges
- Subnets

Click the Add button to add any of these elements and the Remove button to remove items from your Local Zone list. Click on the Properties button to modify the name or IP address of any element of your Local Zone properties.

The Adapter Subnets section lists all the Network Interface Cards (NICs) on your machine. Checking an adapter automatically adds the network adapter's local subnet to the Local Zone.

If you are on a local area network, checking an adapter automatically adds any computers and other devices such as printers using that subnet to your Local Zone. On a LAN using multiple subnets, you would need to add these individually.



Use this dialog to specify what computers are in your local zone.
- Click the Add button to add computers to your local zone.
- Click the Properties button to edit a computer's properties.
- Click the Remove button to remove computers from your local zone.

Adapter Subnets
☑ NDIS 4.0 driver
Other Computers
☑ target 1 (111.111.111.111)
☑ target 2 (222.222.222.222)
☑ target range (114.111.111.111-114.111.111.150)
☑ target range 1 (222.222.222.222-222.222.222.25

- Click the Properties button to modify the IP range properties.
- Click Remove to remove this item from the local zone.
- Uncheck to exclude this item from the local network.

Populating the Local Zone

To add a trusted Host/Site, IP Address, IP Range, or Subnet to your Local Zone:

1. In the Security panel, click the Advanced button. The Local Zone Properties dialog is displayed.
2. Click Add and select Host/Site (where you have the domain of the remote server rather than the IP address), IP address, IP Range or Subnet. Note: to add a subnet, you will need to know the subnet mask.
3. Under Description, enter a name for the entry. This description can be anything and has no bearing on functionality. It is intended to help you distinguish multiple entries in the Local Zone.
4. Enter the name of the Host/Site, IP Address, IP Range, or Subnet. Example: `update.myviruscanner.com` or `10.10.10.1`
5. Click Next
6. Click Finish

7. Click OK

Cable Modem Issues

If you use a network adapter card connected directly to a cable modem to connect to the Internet, you will want to leave the cable subnets unchecked, to prevent your neighbors from being able to access your computer.

BACK HOME

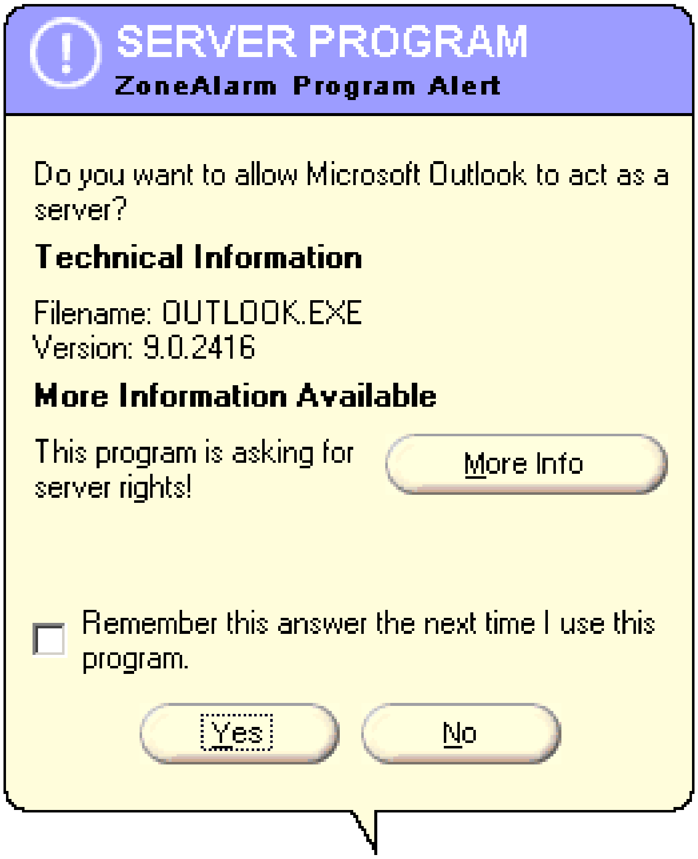
Copyright © 1999-2001 Zone Labs, Inc.

All rights reserved. ZoneAlarm and ZoneAlarm Pro include TrueVector Technology, covered by U.S. Patent No. 5,987,611. Zone Labs, ZoneAlarm, ZoneAlarm Pro, and TrueVector are registered trademarks of Zone Labs, Inc.

Allow Server

From within the Programs Panel, the Allow Server feature lets you control which applications can establish incoming connectivity from a server on the Internet

Some applications listen for incoming connection requests and need to respond to those requests in order to function correctly. Examples of application requiring server rights would include Microsoft Outlook and Real Player.



SERVER PROGRAM

ZoneAlarm Program Alert

Do you want to allow Microsoft Outlook to act as a server?

Technical Information

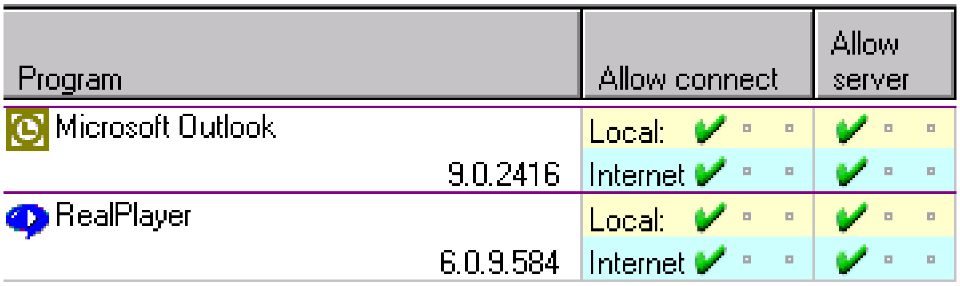
Filename: OUTLOOK.EXE
Version: 9.0.2416

More Information Available

This program is asking for server rights!

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

If you select Yes, ZoneAlarm identifies the application as having server rights. However, make sure you check the "Remember this answer the next time I use this program" box in order for it to show up as approved in the Allow Server column of the Programs List.



Program	Allow connect	Allow server
Microsoft Outlook	Local: ✓ ▫ ▫	✓ ▫ ▫
9.0.2416	Internet ✓ ▫ ▫	✓ ▫ ▫
RealPlayer	Local: ✓ ▫ ▫	✓ ▫ ▫
6.0.9.584	Internet ✓ ▫ ▫	✓ ▫ ▫

By assigning server rights to a program in the Program List, you designate it as a trusted application. However, some software may require additional configuration to pass through the Local Zone. For example, software that is updated online (such as virus scanners) may try to connect to an FTP server at periodic intervals.

Click here for information about adding specific Internet locations to your Local Zone.

Sometimes an application configured with server privileges may start before ZoneAlarm does, which causes the application not to be granted server privileges. To resolve this situation, quit the problem application and re-launch it after ZoneAlarm is running.

Note: Allowing incoming connections for server applications opens one or more ports on your computer. These ports will show as open ports when you test your computer with an online port probe test such as ShieldsUp or HackerWhacker.

Other Program Panel Options

- Allow Connect
- Pass Lock
- Remove Programs

BACK HOME

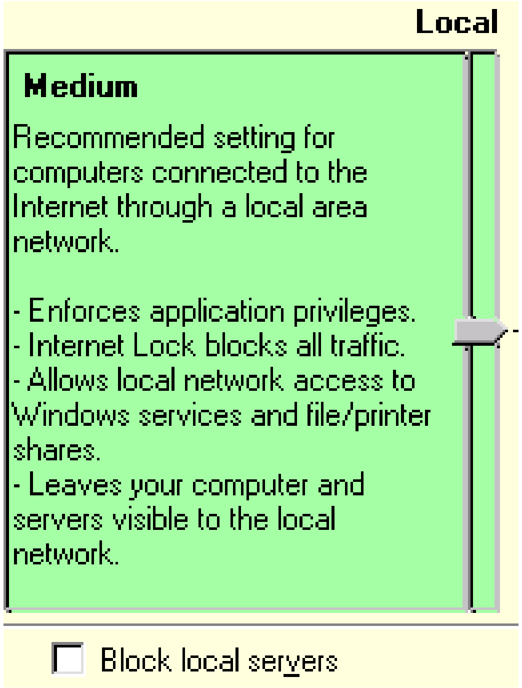
Copyright © 1999-2001 Zone Labs, Inc.

All rights reserved. ZoneAlarm and ZoneAlarm Pro include TrueVector Technology, covered by U.S. Patent No. 5,987,611. Zone Labs, ZoneAlarm, ZoneAlarm Pro, and TrueVector are registered trademarks of Zone Labs, Inc.

Local Zone Security Settings

The default security level for the Local Zone is Medium. The difference between Medium and High security levels is that High security blocks access to the network and system services.

Important: The access privileges you assign to specific programs in the Programs panel override the security levels you set in this panel. The same is true for your Internet Lock settings.



Local

Medium

Recommended setting for computers connected to the Internet through a local area network.

- Enforces application privileges.
- Internet Lock blocks all traffic.
- Allows local network access to Windows services and file/printer shares.
- Leaves your computer and servers visible to the local network.

□ Block local servers

Low Security: Low security only enforces application privileges and Internet Lock settings, leaving your computer visible to other computers in the Local Zone. The firewall does not block file or printer shares or traffic to and from the Local Zone.

Medium Security: This is the default Local Zone setting. At this security level, the computer is visible to the Local Zone. File shares, printer shares and Windows services are allowed for computers in the Local Zone. At Medium security, the Automatic Lock is enhanced by the firewall and blocks all ports.

High Security: This is the highest security level available providing strong application flexibility. At High security, the firewall blocks access from the Local Zone to Windows (NetBIOS) services and file and printer shares.

When High Security is set, your computer is in "Stealth Mode." — all ports not currently in use by a program are blocked and not visible to the Local Zone. High security opens ports only when an approved program needs them.

Note: By default, no computer belongs to the Local Zone. Please see the Local Zone Properties dialog for information on how to add computers to your trusted Local Zone.

BACK HOME

Copyright © 1999-2001 Zone Labs, Inc.

All rights reserved. ZoneAlarm and ZoneAlarm Pro include TrueVector Technology, covered by U.S. Patent No. 5,987,611. Zone Labs, ZoneAlarm, ZoneAlarm Pro, and TrueVector are registered trademarks of Zone Labs, Inc.

Pre-configuration of your Web Browser

As part of the installation process, you will be asked if you want to automatically give your default browser (and services and controller app for Windows 2000 users) Internet access.

If you choose Yes

If you choose Yes, your browser will have permission to access the Internet. If you choose No, you will be asked to give Internet access rights to your browser the first time you try to access the Internet. Note: If the installer cannot locate your default browser or if you've run ZoneAlarm previously, you will not see this feature.

What is the purpose of this feature?

By automatically giving your default browser Internet access rights in the installer, you won't have to do it yourself later. This feature, then, is for your convenience and ensures that you will have immediate Internet access after installing ZoneAlarm.

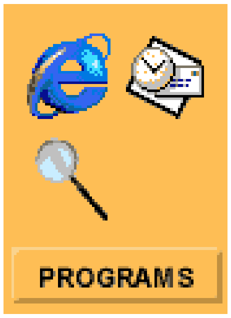
BACK HOME

Copyright © 1999-2001 Zone Labs, Inc.

All rights reserved. ZoneAlarm and ZoneAlarm Pro include TrueVector Technology, covered by U.S. Patent No. 5,987,611. Zone Labs, ZoneAlarm, ZoneAlarm Pro, and TrueVector are registered trademarks of Zone Labs, Inc.

Programs Icons

The Programs icon displays the applications within the Program List that are currently in use.



A blinking application icon means that the program is actively sending or receiving Internet data. A server application that has been listening for connections is displayed with a hand under the icon.

Learn more about the Programs Panel

- Allow Connect
- Allow Server
- Pass Lock
- Program Removal

BACK HOME

Copyright © 1999-2001 Zone Labs, Inc.

All rights reserved. ZoneAlarm and ZoneAlarm Pro include TrueVector Technology, covered by U.S. Patent No. 5,987,611. Zone Labs, ZoneAlarm, ZoneAlarm Pro, and TrueVector are registered trademarks of Zone Labs, Inc.

Keyboard Shortcuts

You can use a combination of keystrokes on your keyboard to access many features of ZoneAlarm. This provides an alternative to using your mouse.

A list of features you can activate with keystrokes is provided below. To perform most shortcuts, press either the Ctrl or the Alt key in conjunction with one of the letter keys on your keyboard:

Ctrl+L	Lock/Unlock
Ctrl+S	Emergency Stop
Ctrl+H	Zone Labs Information Overview
Alt+A	Expand/Close the Alerts Panel
Alt+L	Expand/Close the Lock Panel
Alt+S	Expand/Close the Security Panel
Alt+P	Expand/Close the Programs Panel
Alt+C	Expand/Close the Configure Panel
Alt+Z	Zoom/Unzoom - Expand/Close the current panel
ESC	Unzoom - Close the open panel
F1	Access the help file

In the alert popup dialog, these keys let you navigate multiple alerts:

PgUp	Previous Alert
PgDn	Next Alert
Home	First Alert
End	Last Alert

BACK HOME NEXT

Copyright © 1999-2001 Zone Labs, Inc.

All rights reserved. ZoneAlarm and ZoneAlarm Pro include TrueVector Technology, covered by U.S. Patent No. 5,987,611. Zone Labs, ZoneAlarm, ZoneAlarm Pro, and TrueVector are registered trademarks of Zone Labs, Inc.

How to manage File and Printer sharing

This page discusses security issues around file and printer sharing.

What Is File and Printer Sharing (FPS)?

The greatest security risk to Windows users in a network setting is caused by the improper use of file and printer sharing (FPS). File sharing is implemented when files in specific directories are shared between users across a network. This includes users on the Internet when the computers have a live Internet connection.

File and Printer Sharing (FPS) is a service that comes with Windows operating systems. It allows users to share files and printers over a network. To implement file sharing, certain drives, folders, files or a combination of these are selected to be shared.

With printer sharing, you have the option of sharing the printer(s) connected to your computer.

Why Implement File Sharing

File sharing allows easy collaboration because everyone in a group or network can share specific files on their computers with everyone else in their trusted group.

File sharing must be activated by your network administrator or in your operating system. ZoneAlarm can then provide the Internet security firewall that will protect the shared files from Internet intrusions from untrusted computers.

To take advantage of ZoneAlarm's protection, each computer that is sharing files must be included in the *Local Zone*.

NetBIOS: Example of the Risks of File Sharing

When all the files on your computer are shared, there is a major risk that an Internet intruder can get confidential system information from your computer. A good example is NetBIOS Names And Share Names.

The NetBIOS name table of your computer is available to anyone who wishes to query your system directly over the Internet using its IP address.

A utility exists on all Windows machines called NBTSTAT.EXE which performs these queries. If your name table discloses something you would rather keep secret, change its entries to something less informative. If you want anonymity, don't list your personal name or other identifying information in your NetBIOS name table.

If sharing is enabled via the Internet, the shared resources' names and descriptions are automatically available for anyone to see, regardless of passwords. To see what others see in your NetBIOS nametable, open a DOS window while online and type: `nbtstat -n`

Add Computers to the Local Zone for File Sharing

Once ZoneAlarm is installed on the computers in your network, each computer in the network has a *Local Zone*.

To set up ZoneAlarm's file sharing protection, the Local Zone on each computer must include all the other computers with which secure file sharing will take place. If you are a single user, you only need to include machines that you trust in your Local Zone. Once this is done, you can share files knowing that you are protected by the ZoneAlarm firewall.

At the same time, Internet Zone security should be set to *High* for maximum protection. Click on this link for directions:
Adding computers to your Local Zone.

BACK HOME

Copyright © 1999-2001 Zone Labs, Inc.

All rights reserved. ZoneAlarm and ZoneAlarm Pro include TrueVector Technology, covered by U.S. Patent No. 5,987,611. Zone Labs, ZoneAlarm, ZoneAlarm Pro, and TrueVector are registered trademarks of Zone Labs, Inc.

ZoneAlarm License Agreement

ZONE LABS INC.
END USER LICENSE AGREEMENT
ZONEALARM STANDARD VERSION

Software License Agreement for ZoneAlarm Standard Version

IMPORTANT- PLEASE READ CAREFULLY: BY INSTALLING THE SOFTWARE (AS DEFINED BELOW), COPYING THE SOFTWARE AND/OR CLICKING ON THE "ACCEPT" BUTTON BELOW, YOU (EITHER ON BEHALF OF YOURSELF AS AN INDIVIDUAL OR ON BEHALF OF AN ENTITY AS ITS AUTHORIZED REPRESENTATIVE) AGREE TO ALL OF THE TERMS OF THIS END USER LICENSE AGREEMENT ("AGREEMENT") REGARDING YOUR USE OF THE SOFTWARE. IF YOU DO NOT AGREE WITH ALL OF THE TERMS OF THIS AGREEMENT, CLICK ON THE "NO" BUTTON AND/OR DO NOT INSTALL, COPY OR OTHERWISE USE THE SOFTWARE.

1. GRANT OF LICENSE: Subject to the terms below, ZONE LABS, INC. ("ZONE LABS") hereby grants you a non-exclusive, non-transferable license to install and to use the downloadable, standard version of ZoneAlarm ("Software").

If you are licensing the Software as an individual or not-for-profit entity (excluding governmental entities and educational institutions) only, your license will be free to you for the term of the Agreement and you may: (i) install and use the Software on a single computer for your personal, internal use and in no event for the benefit of a company, for-profit entity, governmental entity, or educational institution; and (ii) copy the Software for back-up or archival purposes.

If you are licensing the Software on behalf of a for-profit entity, governmental entity, or educational institution, your license will be free for an introductory sixty (60) day period and, should you elect to purchase the full license, will continue perpetually. During the introductory period, or the full license term, if you elect to purchase it, you may: (i) install and use the Software for your internal use on the number of computers for which you have paid license fees; and
(ii) copy the Software for back-up or archival purposes.

Whether you are licensing the Software as an individual or on behalf of an entity, you may not:
(i) reverse engineer, decompile, or disassemble the Software;
(ii) modify, or create derivative works based upon, the Software in whole or in part;
(iii) distribute copies of the Software;
(iv) remove any proprietary notices or labels on the Software; or
(v) resell, lease, rent, transfer, sublicense, or otherwise transfer rights to the Software.

2. TITLE: You acknowledge that no title to the intellectual property in the Software is transferred to you. Title, ownership, rights, and intellectual property rights in and to the Software shall remain in ZONE LABS. The Software is protected by copyright and patent laws of the United States and international treaties.

3. UPDATES. From time to time, ZONE LABS may make available updates to the

software. You may download and install or otherwise use those updates to the software that are released by ZONE LABS within one year of software registration date. You must complete the product registration form during software installation to be notified of software updates. All updates to the Software are governed by this Agreement, unless other license terms are provided with the update.

4. DISCLAIMER OF WARRANTY: The Software is provided to you at no, or minimal charge. YOU AGREE THAT ZONE LABS HAS MADE NO EXPRESS WARRANTIES, ORAL OR WRITTEN, TO YOU REGARDING THE PRODUCTS AND THAT THE PRODUCTS ARE BEING PROVIDED TO YOU "AS IS" WITHOUT WARRANTY OF ANY KIND. ZONE LABS DISCLAIMS ANY AND ALL OTHER WARRANTIES, WHETHER EXPRESSED, IMPLIED, OR STATUTORY, INCLUDING, BUT WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF NONINFRINGEMENT OF THIRD PARTY RIGHTS, MERCHANTABILITY, AND FITNESS FOR A PARTICULAR PURPOSE. ZONE LABS SHALL NOT BE LIABLE FOR INDIRECT, INCIDENTAL, SPECIAL, COVER, RELIANCE, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, LOSS OF ANTICIPATED PROFIT) ARISING FROM ANY CAUSE UNDER OR RELATED TO THIS AGREEMENT.

5. LIMITATION OF LIABILITY: You must assume the entire risk of using the program. IN NO EVENT SHALL ZONE LABS BE LIABLE TO YOU FOR ANY DAMAGES, INCLUDING ANY LOST PROFITS, LOST SAVINGS, OR OTHER INCIDENTAL, INDIRECT OR CONSEQUENTIAL DAMAGES OF ANY KIND ARISING OUT OF THE USE OF THE ZONE LABS SOFTWARE, EVEN IF ZONE LABS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT WILL ZONE LABS' LIABILITY FOR ANY CLAIM, WHETHER IN CONTRACT, TORT, OR ANY OTHER THEORY OF LIABILITY, EXCEED THE LICENSE FEE PAID BY YOU, PROVIDED, HOWEVER, IF THE RELEVANT PRODUCT WAS PROVIDED TO YOU AT NO CHARGE YOU AGREE ZONE LABS SHALL NOT BE LIABLE TO YOU FOR ANY DAMAGES. THIS LIMITATION SHALL APPLY TO CLAIMS OF PERSONAL INJURY TO THE EXTENT PERMITTED BY LAW.

6. TERMINATION: This Agreement shall terminate automatically if you fail to comply with the limitations described in this Agreement, or if you are licensing the Software on behalf of an entity and do not elect to continue the license following the expiration of the introductory period or you do not renew any one (1) year license with ZONE LABS. No notice shall be required from ZONE LABS to effect such termination. Upon termination, except for failure to renew, you must uninstall and destroy all copies of the Software.

7. MISCELLANEOUS:

Severability.
In the event of invalidity of any provision of this Agreement, the parties agree that such invalidity shall not affect the validity of the remaining portions of this Agreement.

Export.
You agree that you will not export or re-export the Software outside of the jurisdiction in which you obtained it without the appropriate United States or foreign government licenses.

Governing Law.
This Agreement will be governed by the laws of the State of California as they are applied to agreements between California residents entered into and to be performed entirely within California. The United Nations Convention on Contracts for the International Sale of Goods is specifically disclaimed.

Entire Agreement.
You agree that this is the entire agreement between you and ZONE LABS, which supersedes any prior agreement, whether written or oral, and all other communications between ZONE LABS and you relating to the subject matter of this Agreement.

Reservation of rights.
All rights not expressly granted in this Agreement are reserved by ZONE LABS.

Copyright (c) 1999, 2000, 2001 ZONE LABS, Inc. 1060 Howard Street, San Francisco, CA, 94103. All rights reserved. Zone Labs, ZoneAlarm, ZoneAlarm Pro and TrueVector are trademarks of ZONE LABS, Inc.

BACK HOME NEXT

Copyright © 1999-2001 Zone Labs, Inc.

All rights reserved. ZoneAlarm and ZoneAlarm Pro include TrueVector Technology, covered by U.S. Patent No. 5,987,611. Zone Labs, ZoneAlarm, ZoneAlarm Pro, and TrueVector are registered trademarks of Zone Labs, Inc.

FWIN Sample Log Entry

ZoneAlarm blocked an incoming request

Example

```
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

BACK HOME

Copyright © 1999-2001 Zone Labs, Inc.

All rights reserved. ZoneAlarm and ZoneAlarm Pro include TrueVector Technology, covered by U.S. Patent No. 5,987,611. Zone Labs, ZoneAlarm, ZoneAlarm Pro, and TrueVector are registered trademarks of Zone Labs, Inc.

FWOUT Sample Log Entry

ZoneAlarm blocked an outbound request

Example

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

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

BACK HOME

Copyright © 1999-2001 Zone Labs, Inc.

All rights reserved. ZoneAlarm and ZoneAlarm Pro include TrueVector Technology, covered by U.S. Patent No. 5,987,611. Zone Labs, ZoneAlarm, ZoneAlarm Pro, and TrueVector are registered trademarks of Zone Labs, Inc.

PE Sample Log Entry

ZoneAlarm detected an application on your computer attempting to access the Internet.

Example

```
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

---

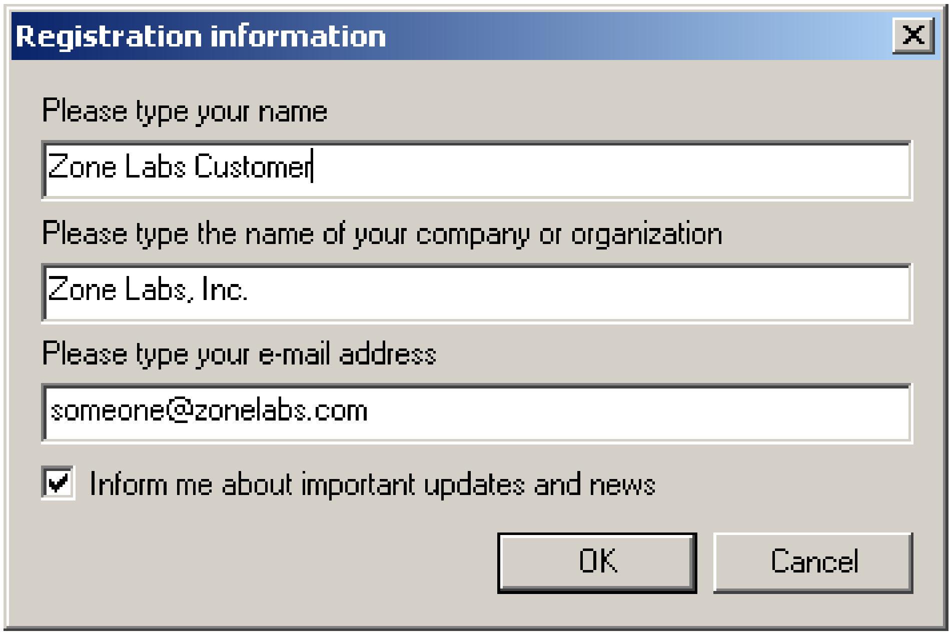
BACK HOME

Copyright © 1999-2001 Zone Labs, Inc.

All rights reserved. ZoneAlarm and ZoneAlarm Pro include TrueVector Technology, covered by U.S. Patent No. 5,987,611. Zone Labs, ZoneAlarm, ZoneAlarm Pro, and TrueVector are registered trademarks of Zone Labs, Inc.

The Change Registration Button

Click the Change Registration button to review or modify your ZoneAlarm registration information. Provide any new information, such as a new name, address, telephone number or e-mail address, in the Registration Information dialog, shown below:



Please type your name

Zone Labs Customer

Please type the name of your company or organization

Zone Labs, Inc.

Please type your e-mail address

someone@zonelabs.com

☑ Inform me about important updates and news

When changing the registration information, ZoneAlarm automatically records the update. ZoneAlarm displays the date and time of your last registration.

The Registration function has no impact on your ability to use ZoneAlarm. If you receive a "Registration Pending" message, that means Zone Labs servers have not yet acknowledged the change request but will do so at the earliest opportunity.

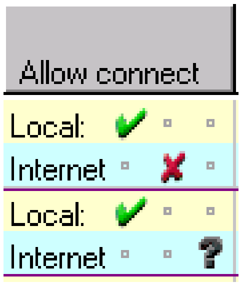
BACK HOME

Copyright © 1999-2001 Zone Labs, Inc.

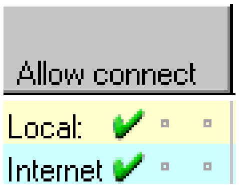
All rights reserved. ZoneAlarm and ZoneAlarm Pro include TrueVector Technology, covered by U.S. Patent No. 5,987,611. Zone Labs, ZoneAlarm, ZoneAlarm Pro, and TrueVector are registered trademarks of Zone Labs, Inc.

Allow Connect

Allow Connect controls the connection behavior of programs in the Programs List and specifies each program's access rights in the Local Zone and the Internet Zone.

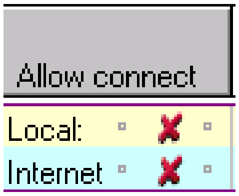


The row of dots in the Allow Connect column (. . .), allows you to select the connectivity permissions. A check mark indicates permission has been granted. An X indicates permission is not granted. A question mark (?) means ZoneAlarm will ask for permission each time the program seeks to establish connectivity.



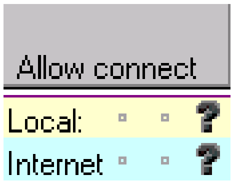
A check mark means that the program always has permission to connect without asking for your explicit permission.

When you grant a program permission to access the Internet Zone at this level, ZoneAlarm automatically allows the program to have the same access to the Local Zone. You will see this when a check mark is automatically added to the Local Zone area.



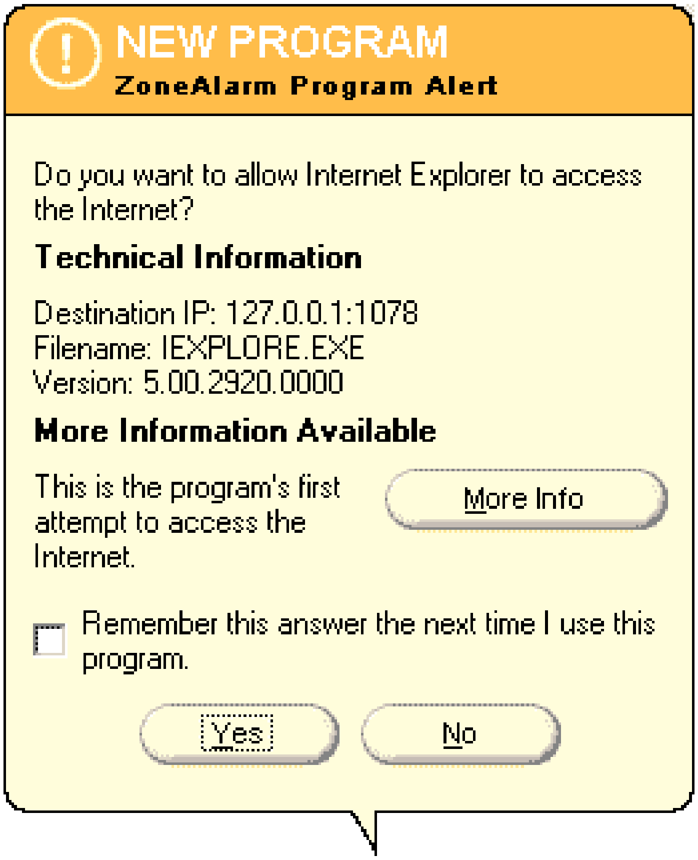
An X means that the selected program is denied connectivity access.

When Local Zone access permission is denied, the selected program will automatically inherit the same access restrictions to the Internet Zone. You will see this when an X is automatically placed in the Internet Zone area of the Program List. The reason for this is the Internet Zone cannot have greater access rights than the Local Zone.



A ? means that the program will ask permission each time it tries to connect. A question mark is the default setting for applications.

When a program permission request is initiated in a popup window, you decide whether or not to grant the requested permission by clicking on Yes or No.



NEW PROGRAM

ZoneAlarm Program Alert

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

Technical Information

Destination IP: 127.0.0.1:1078
Filename: IEXPLORE.EXE
Version: 5.00.2920.0000

More Information Available

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

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

By default, if you select "No", an entry for the application will be placed in the Programs List with the option set to ask. The reason the application is put in the Programs List even if you said "No" is because ZoneAlarm keeps track of all applications that request connectivity in order to provide the strongest level of protection. ZoneAlarm needs to remember what applications have asked for connectivity permissions and then leaves it up to the user to assign permissions (or not to) as appropriate. Check here for additional information on how ZoneAlarm protects. You can always Remove Programs from the Programs List as well.

Note: ZoneAlarm will not allow a check mark for Internet Zone access if a program's Local Zone access is set to ask.

Learn to use the Allow Server feature.

BACK HOME

Copyright © 1999-2001 Zone Labs, Inc.

All rights reserved. ZoneAlarm and ZoneAlarm Pro include TrueVector Technology, covered by U.S. Patent No. 5,987,611. Zone Labs, ZoneAlarm, ZoneAlarm Pro, and TrueVector are registered trademarks of Zone Labs, Inc.