



User Guide

Table of Contents

Chapter 1 - Getting Started	1
New Features	1
System Requirements	1
Uninstalling Other Firewalls	2
Downloading and Installing Personal Firewall	2
Testing Personal Firewall	3
Using McAfee SecurityCenter	3
Chapter 2 - Configuring Your Firewall Options	4
Security	5
Setting the Security Level	5
Application Recommendations.....	5
Event Logging.....	6
Accept ICMP Ping Requests.....	6
General	7
When an inbound event is detected	7
Use the following Visual Trace program	8
Set home location	8
Using sound effects during trace	9
Clear Visual Trace caches	9
Banned IPs	10
Trusted IPs	11
System Services	12
Updates	13
Chapter 3 - Using Personal Firewall	14
About the Summary	14
About Internet Applications	15
Changing Permissions	15
Changing Applications.....	16
About Events	16
Understanding Events	17
Showing Events in the Event Log.....	19
Responding to Events	20
Managing the Event Log	21
About Alerts	23
Connection Attempt Blocked	23
Application Requests Internet Access	24
Application Has Been Modified.....	25
Application Requests Server Access	25
New Application Allowed.....	26
Chapter 4 - Troubleshooting	27
Appendix A - Frequently Asked Questions	31
Glossary	35
Index	42

Chapter 1 - Getting Started

Welcome to McAfee Personal Firewall.

McAfee Personal Firewall is an online subscription service offering advanced protection for your computer and your personal data. Personal Firewall establishes a barrier between your computer and the Internet, silently monitoring Internet traffic for suspicious activities.

With it, you get the following features:

- Defends against potential hacker probes and attacks
- Complements anti-virus defenses
- Monitors Internet and network activity
- Alerts you to potentially hostile events
- Provides detailed information on suspicious Internet traffic
- Integrates Hackerwatch.org functionality, including event reporting, self-testing tools and the ability to email reported events to other online authorities
- Provides detailed tracing and event research features (Plus edition only)

New Features

Summary page

Personal Firewall now has a more informative and easy-to-understand summary page. The new page provides a simple event summary, easier access to Hackerwatch.org, a graph of port activity on your local computer, and direct access to a Worldwide Hacker Activity Map.

Intelligent application handling

When an application seeks Internet access, Personal Firewall first checks whether it recognizes the application as trusted or malicious. If the application is recognized as trusted, Personal Firewall automatically allows it access to the Internet so you don't have to.

Hackerwatch.org integration

Personal Firewall users no longer have to create a Hackerwatch.org ID before they can submit malicious events to Hackerwatch.org. The firewall automatically generates an ID during the installation, and users can report events with one click.

Enhanced alerting

To support these new features, McAfee has also updated its user interface and alert mechanism. See "About Alerts" for details about the types of alerts that can appear and the possible responses you can choose.

System Requirements

- Microsoft® Windows 95, 98, Me, 2000, or XP
- Personal computer with 486 or higher processor (Pentium recommended)
- 8 MB of free hard disk space for installation
- Microsoft® Internet Explorer 5.0 or later

Note: To upgrade to the latest version of Internet Explorer, visit the Microsoft Web site at <http://www.microsoft.com/>.

Windows 95 users need the Winsock2 upgrade from Microsoft to use McAfee Personal Firewall. To upgrade to the latest version of Winsock, visit the Microsoft Web site at <http://www.microsoft.com/>.

Uninstalling Other Firewalls

Before you install McAfee Personal Firewall, you must uninstall any other firewall programs on your computer. Please follow your firewall program's uninstallation instructions to do so.

Note: If you use Windows XP, you do not need to disable the built-in firewall feature before installing Personal Firewall.

Downloading and Installing Personal Firewall

Before you can download and install Personal Firewall, you must purchase a subscription. To do so, go to the McAfee.com Web site, and create an account with a password and billing information to sign up for the service.

Before installing Personal Firewall, save all of your work and close any open applications before you continue with the following installation steps. You must restart your computer as part of the installation process.

To install Personal Firewall:

1. Go to <http://www.mcafee.com/> and click the **My Account Info** link at the top right-hand of the homepage.
2. If prompted, enter your subscribing email address and password, and click **Log In**. If you selected the **Remember me** check box when you last logged in, you will automatically see your Account Info page. Click the **Update/Download** link to begin downloading Personal Firewall.
3. The Installation Wizard appears. If it does not appear automatically, click **Start**.
Note: If you are upgrading from a previous version of Personal Firewall, Personal Firewall will automatically uninstall the previous version before it installs the current version. You must restart your computer when the Installation Wizard prompts you. After your computer restarts, the current version of Personal Firewall will install.
4. When your computer restarts, the Installation Wizard dialog box appears again, prompting you to continue the installation. Click **Continue** to continue installing Personal Firewall.
5. When the Installation Wizard prompts you, click **OK** to restart your computer.
6. A welcome dialog box appears when your computer restarts. When you are finished reading its message, we recommend you click **What's New?** to read about its new features. Otherwise, click **OK** to close the welcome dialog box (see Figure 1).



Figure 1

Testing Personal Firewall

To test Personal Firewall:

1. Right-click the McAfee icon, point to **Personal Firewall**, and then click **Test Firewall**.
2. Personal Firewall opens Internet Explorer and goes to <http://www.hackerwatch.org/>, a Web site maintained by McAfee. Please follow the directions on the Hackerwatch.org Probe page to test Personal Firewall.


Note: If you connect to the Internet through a proxy server or Network Address Translation server, as is the case in most office networks (LANs), you will not get a proper reading. Hackerwatch.org's firewall tester looks for which computer asked for the firewall test and tests that computer. If you connect through a proxy or NAT server, it simply relays your computer's request for the firewall test, and Hackerwatch.org will test the wrong computer. The results that you get belong to the proxy server—not to your computer.


Using McAfee SecurityCenter

The McAfee SecurityCenter is your one-stop security shop, accessible from its icon in your Windows system tray or from your Windows desktop. With it, you can perform these useful tasks:

- Get free security analysis for your computer.
- Launch, manage, and configure all your McAfee.com subscriptions from one icon.
- See continuously updated virus alerts and the latest product information.
- Receive free trial subscriptions to download and install trial versions directly from McAfee.com using our patented software delivery process.
- Get quick links to frequently asked questions and account details at the McAfee.com Web site.

Note: For more information about its features, please click **Help** in the SecurityCenter dialog box.


While the SecurityCenter is running and all of the McAfee.com features installed on your computer are enabled, a red M icon  appears in the Windows system tray. This area is usually in the lower-right corner of the Windows desktop and contains the clock.

If one or more of the McAfee.com applications installed on your computer are disabled, the McAfee icon changes to black .

To open the McAfee SecurityCenter:

1. Right-click the McAfee icon .
2. Click **Open SecurityCenter**.

To access a Personal Firewall feature:

1. Right-click the McAfee icon .
2. Point to **Personal Firewall**, and then click the feature you want to use.

Chapter 2 - Configuring Your Firewall Options

Use the Options dialog box to set Personal Firewall's protection level.

To set Personal Firewall's options automatically:

1. Right-click the McAfee icon, point to **Personal Firewall**, and then click **Options**.
2. Click each tab (**Security**, **General**, **Banned IPs**, etc.), and then click **Default** or **Recommend** (if they are available) to let Personal Firewall automatically set the options for each page (see Figure 2).
3. Click **Yes** to make the changes, or click **No** to cancel the changes.
4. Click **OK** on the Options dialog box if you are finished making changes.

Note: The Default settings are for novice firewall users, and the Recommend settings are for experienced firewall users.

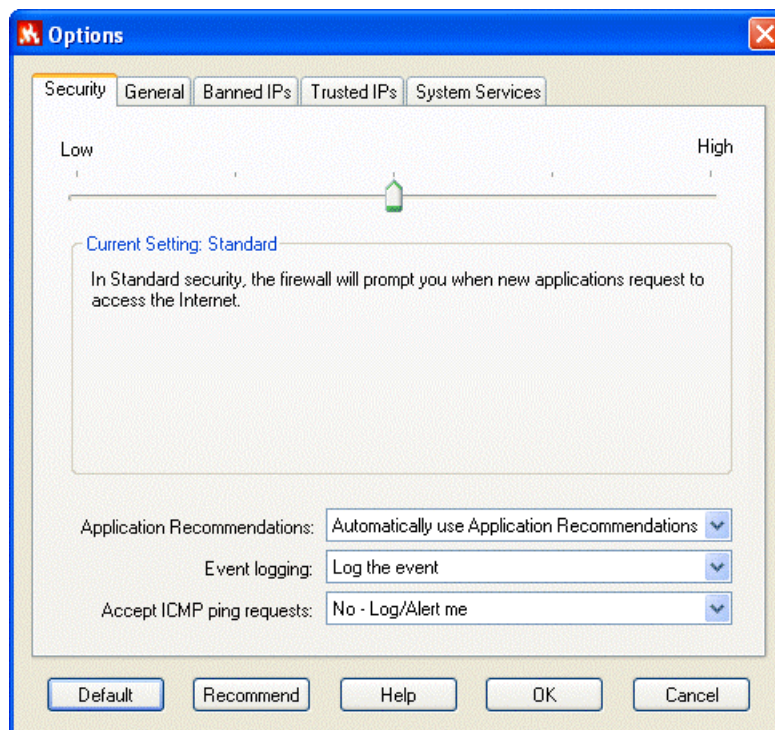


Figure 2

Security

You can configure security options for how the firewall responds when it detects unwanted traffic. By default, the **Standard** security level is enabled, so an application requests only once for access to the Internet. If you are an experienced firewall user, you can use other settings.

Note: With **Standard** and **Tight** Security, you cannot turn off application alerts.

Setting the Security Level

1. Right-click the McAfee icon, point to **Personal Firewall**, and then click **Options**.
2. Click the **Security** tab (see Figure 2).
3. Set the security level by moving the slider to the desired level. If you are a novice firewall user, accept the default **Standard** setting. The security level ranges from **Low** (Open) to **High** (Lockdown):

Setting	Description
High (Lockdown)	All traffic is stopped. This is essentially the same as unplugging your Internet connection. You can use this setting to block ports you configured to be open under the System Services tab.
Tight	An application requests only the type of access to the Internet that it explicitly needs (for example, Outbound Only Access), and you either grant access or block it. If the application later requests Full Access, you either grant Full Access or keep it limited to Outbound Only Access. Use this setting if you are an experienced firewall user.
Standard	(Recommended) An application requests only once for access to the Internet, and you either grant access or block it. If you grant access, the application can both send data and receive unsolicited data on non-system ports. Use this setting if you are a novice firewall user.
Trusting	All applications are automatically trusted when they first attempt to access the Internet. However, you can choose to be notified about new applications on your computer with alerts. Use this setting if you find that some games or streaming media do not work.
Low (Open/No Filtering)	Your firewall is effectively disabled. This setting allows all traffic through Personal Firewall with no filtering.

4. Click **OK** if you are finished making changes.

Application Recommendations

You can choose whether to automatically use, ignore, or only view application recommendations that Personal Firewall provides to help you handle application alerts:

1. Right-click the McAfee icon, point to **Personal Firewall**, and then click **Options**.
2. Click the **Security** tab.
3. Select either **Ignore** or **Show** in the **Application recommendations** list. By default, Personal Firewall is set to **Auto-use** and will automatically use its recommendations and then show the results to you.
4. Click **OK** if you are finished making changes.

If you choose to show recommendations, Personal Firewall displays the recommendations on the application alerts.

Event Logging

You can choose whether or not to log any events (inbound traffic) that Personal Firewall reports:

1. Right-click the McAfee icon, point to **Personal Firewall**, and then click **Options**.
2. Click the **Security** tab.
3. Select either **Log the event** or **Do not log the event** in the **Event logging** list.
4. Click **OK** if you are finished making changes.

If you choose to log events, Personal Firewall displays the events on the Events page of the main window.

Accept ICMP Ping Requests

You can set the behavior of blocking and logging for ICMP traffic. ICMP traffic is used mainly for performing traces and pings. Pinging is frequently used to perform a quick test before attempting to initiate communications. If you are using or have used a peer-to-peer file-sharing program, you might find yourself being pinged a lot.

1. Right-click the McAfee icon, point to **Personal Firewall**, and then click **Options**.
2. Click the **Security** tab.
3. Select a setting in the **Accept ICMP ping requests** list:
 - **No-Log/Alert me** blocks the ping request and logs it as an event. *
 - **No-Ignore** blocks the ping request, but it does not log it.
 - **Yes** allows all ping requests without logging them.
4. Click **OK** if you are finished making changes.

* You must select **Log the event** from the **Event logging** list before Personal Firewall logs any ping requests.

General

You can configure general logging and alerting options for how the firewall responds when it detects unwanted traffic (see Figure 3). By default, an alert message appears when events occur. When you are used to the operation of the firewall on your computer, you might want to turn this off.

Note: With **Standard** and **Tight** Security, you cannot turn off application alerts.

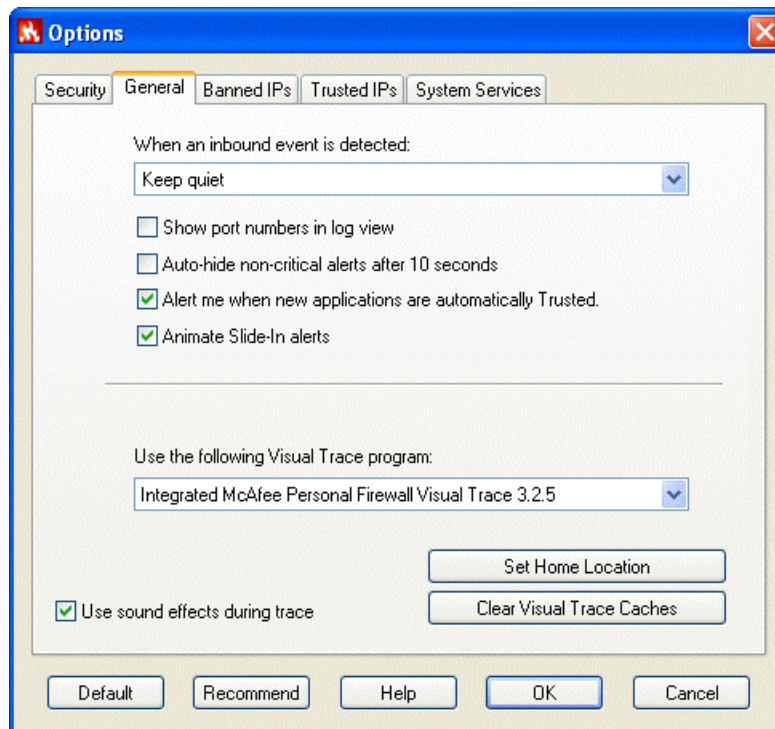


Figure 3

When an inbound event is detected

You can configure how Personal Firewall responds when it detects an event:

1. Right-click the McAfee icon, point to **Personal Firewall**, and then click **Options**.
2. Click the **General** tab.
3. Select one of the options from the **When an inbound event is detected** list:
 - **Flash the tray icon:** Select this option for Personal Firewall to flash the system tray icon.
 - **Display an alert:** Select this option for Personal Firewall to display an alert dialog box and flash the system tray icon.
 - **Keep quiet** (default setting): Select this option for Personal Firewall to silently log events.
4. Configure additional response options:
 - **Show port numbers in log view:** Select this check box to show the source and destination ports of an event in the Events page, along with the source and destination IP addresses, and other event information.
 - **Auto-hide non-critical alerts after 10 seconds:** Select this check box to hide an alert ten seconds after it alerts you about an event. Otherwise, clear this check box to keep alerts visible until you choose a course of action.

- **Alert me when new applications are automatically Trusted:** Select this check box (default setting) to display an alert for new applications when you are using the Trusting Security setting. Otherwise, clear the check box to stop the notifications.
- **Animate slide-in alerts:** Select this check box (default setting) to activate the slide-in alert feature on your Windows desktop. Otherwise, clear the check box to receive standard popup alerts.

5. Click **OK** if you are finished making changes.

Use the following Visual Trace program

You can select which available visual tracing application to use for tracing events. *

1. Right-click the McAfee icon, point to **Personal Firewall**, and then click **Options**.
2. Click the **General** tab.
3. Select the Visual Trace program that you want to use from the list.

By default, Personal Firewall uses the built-in visual tracing feature of Personal Firewall Plus. If you also own a copy of McAfee Visual Trace or NeoTrace, you can select it to trace events.

* Only available in McAfee Personal Firewall Plus.

Set home location

Click this button to change or set your home location in McAfee Visual Trace. *

Setting Your Home Location

The first time you perform a Visual Trace, Personal Firewall prompts you to set your home location.

Setting your home location is not vital to performing a Visual Trace. Click **Cancel** if you do not want to set your home location. You can set it or change it at any time on the Options dialog box.

1. Right-click the McAfee icon, point to **Personal Firewall**, and then click **Options**.
2. Click the **General** tab, and then click **Set Home Location**.
3. Click **Next** on the **Set Home Location** dialog box.
4. Select your country from the **Select Your Country** list.
5. Enter your ZIP or postal code.
6. Click **Next**, and then click **Finish**.

If the **Invalid Location** message appears:

1. Click **OK**.
2. Ensure that you entered your location information correctly.
3. Click **Next**.

If the information is correct and the Invalid Location message appears again, click **Advanced** to enter your latitude and longitude.

Setting Your Home Location – Advanced

1. From **Set Home Location**, click **Advanced**.
2. Click **Yes** to **Advanced View Confirmation**.
3. Enter the **Latitude** of your home location and click **North** or **South**.
4. Enter the **Longitude** of your home location and click **East** or **West**.
5. Click **OK**.

Tip: If you don't know your latitude and/or longitude, enter a number between or including 0 and 90 for latitude, and between or including 0 and 180 for longitude. Note that the red "crosshairs" move as you enter numbers. Adjust the numbers until you are on or near your home location.

* Only available in McAfee Personal Firewall Plus.

Using sound effects during trace

This option turns sound effects on or off in McAfee Visual Trace. *

1. Right-click the McAfee icon, point to **Personal Firewall**, and then click **Options**.
2. Click the **General** tab.
3. Select the **Use sound effects during trace** check box. Clear the check box if you do not want sound effects.

* Only available in McAfee Personal Firewall Plus.

Clear Visual Trace caches

Clearing the Trace caches deletes all information regarding event traces that McAfee Visual Trace stores. *

Warning: Do not click this button unless you want to clear your Visual Trace caches. The caches delete immediately upon pressing the button. Normally, you will only use this option at the request of our Technical Support staff.

* Only available in McAfee Personal Firewall Plus.

Banned IPs

The Banned IPs address list gives you a convenient mechanism to completely block traffic from a specific computer. You are invisible to a computer at that IP address regardless of your other settings. If Personal Firewall detects an event from a banned IP address, it alerts you via the method you selected from the **When an event is detected** list.

To add an IP address to the Banned IPs list:

1. Right-click the McAfee icon, point to **Personal Firewall**, and then click **Options**.
2. Click the **Banned IPs** tab (see Figure 4).
3. Click **Add**.
4. Enter the IP address you want to ban and click **OK**. The IP address appears in the **Banned IPs** list.
5. Click **OK** if you are finished making changes.

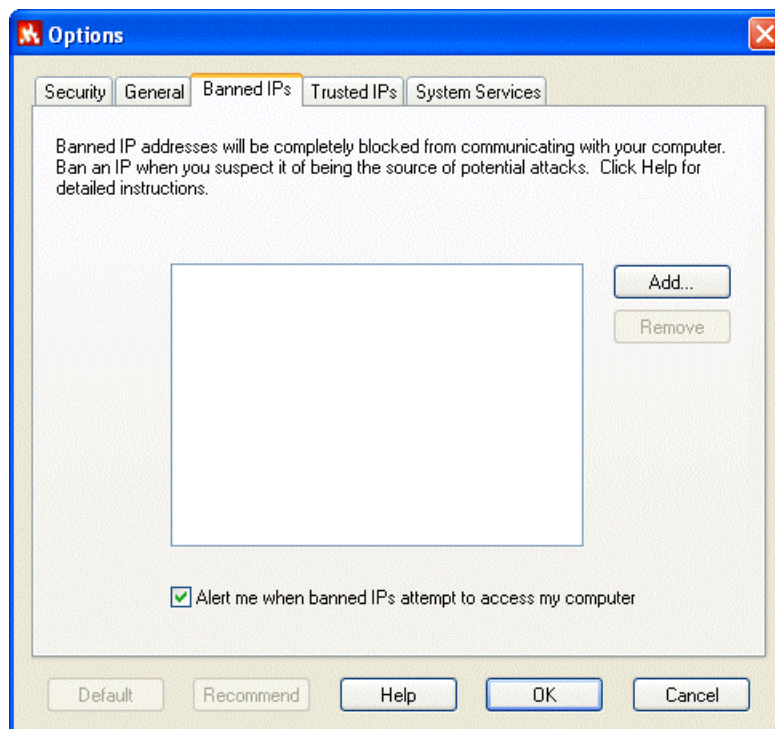


Figure 4

You can also add an IP address to the Banned IPs list by doing the following:

1. Right-click the McAfee icon, point to **Personal Firewall**, and click **View Events**.
2. Find the event containing the IP address that you want to ban and right-click it.
3. Click **Ban the Source IP Address**.
4. Verify that the IP address is the correct one on the **Ban This Address** message, and click **OK**. The IP address is now banned.
5. To verify that it is banned, open the Options dialog box again, and click the **Banned IPs** tab. The IP address should be in the Banned IPs list.

To remove an IP address from the Banned IPs list:

1. Right-click the McAfee icon, point to **Personal Firewall**, and then click **Options**.
2. Click the **Banned IPs** tab (see Figure 4).
3. Click the IP address you want to remove, and then click **Remove**. The IP address disappears from the Banned IPs list.
4. Click **OK** if you are finished making changes.

Trusted IPs

The Trusted IPs list lets you allow all traffic from a specific computer to reach your computer. For the computer at the IP address that you trust, it is like there is no firewall on your computer. Personal Firewall does not log traffic or generate event alerts from IP addresses in the Trusted IP list.

To add an IP address to the Trusted IPs list:

1. Right-click the McAfee icon, point to **Personal Firewall**, and then click **Options**.
2. Click the **Trusted IPs** tab (see Figure 5) and click **Add**.
3. Enter the IP address that you want Personal Firewall to trust at all times, and then click **OK**. The IP address appears in the **Trusted IPs** list.
4. Click **OK** if you are finished making changes.

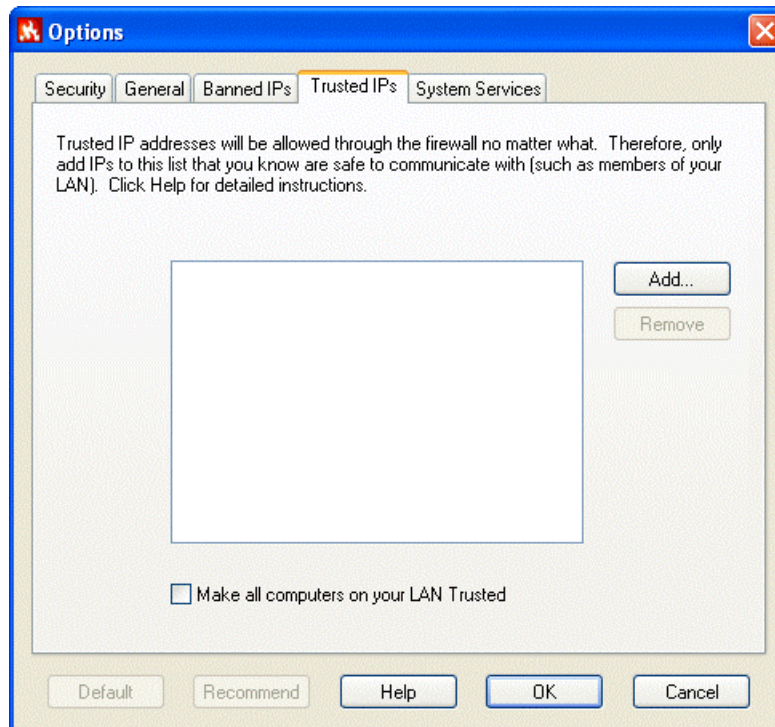


Figure 5

You can also add an IP address to the Trusted IPs list by doing the following:

1. Right-click the McAfee icon, point to **Personal Firewall**, and click **View Events**.
2. Find the event containing the IP address that you want to trust and right-click it.
3. Click **Trust the Source IP Address**.
4. Verify that the IP address is the correct one on the **Trust This Address** message, and click **OK**. The IP address is now trusted.
5. To verify that it is trusted, open the Options dialog box again, and click the **Trusted IPs** tab. The IP address should be in the **Trusted IPs** list.

To remove an IP address from the Trusted IPs list:

1. Right-click the McAfee icon, point to **Personal Firewall**, and then click **Options**.
2. Click the **Trusted IPs** tab.
3. Click the IP address that you want to remove, and then click **Remove**.
4. Click **OK** if you are finished making changes.

If you are using your computer on an office LAN, and you have no reason to block traffic from other computers on that LAN, you can instruct Personal Firewall to trust all computers on the LAN:

1. Right-click the McAfee icon, point to **Personal Firewall**, and then click **Options**.
2. Click the **Trusted IPs** tab.
3. Select the **Make all computers on your LAN Trusted** check box.
Note: If a LAN is not detected, this option will not be available.
4. Click **OK** if you are finished making changes.

System Services

Some applications, such as Web site host or file-sharing server programs, must accept unsolicited connections from other computers to work.

Here are some examples of when you must open ports by selecting them in the **System Services** list:

Mail server. You do not need to open a Mail Server port to receive email. You only need to open a port if the computer protected by Personal Firewall acts as an email server.

Web server. You do not need to open a Web Server port to run a Web browser. You only need to open a port if the computer protected by Personal Firewall acts as a Web server.

Note: Opening a system service port that does not have an application running on it poses no security threat. For example, if you open the Web Server port and then perform a firewall test scan, Port 80 will be in stealth mode and not be detected as listening during a port scan.

Warning: Only select a port in the **System Services** list if you are certain it must be open. You will rarely need to open a port.

If you need to add ports that are not already configured, you can add them easily through the Options dialog box or by simply clicking an event in the log view and creating a rule based on that event.

Following is a list of service ports that your operating system or other system applications might attempt to open. Because these ports represent the most likely source of insecurities in your system, they must be explicitly allowed in this list to enable access by outside computers. To allow your system to expose these ports to the outside world, make sure the check box next to the port description is selected.

System Services

File Transfer Protocol (FTP) Ports 20-21
Mail Server (IMAP) Port 143
Mail Server (POP3) Port 110
Mail Server (SMTP) Port 25
Microsoft Directory Server (MSFT DS) Port 445
Microsoft SQL Server (MSFT SQL) Port 1433
Remote Assistance / Terminal Server (RDP) Port 3389
Remote Procedure Calls (RPC) Port 135
Secure Web Server (HTTPS) Port 443
Universal Plug and Play (UPNP) Port 5000
Web Server (HTTP) Port 80
Windows File Sharing (NETBIOS) Ports 137-139

To allow applications to communicate freely across the Internet or LAN:

1. Right-click the McAfee icon, point to **Personal Firewall**, and then click **Options**.
2. Click the **System Services** tab (see Figure 6).
3. Select the check box next to one of the applications in the **Program** list.
4. Click **OK** if you are finished making changes.

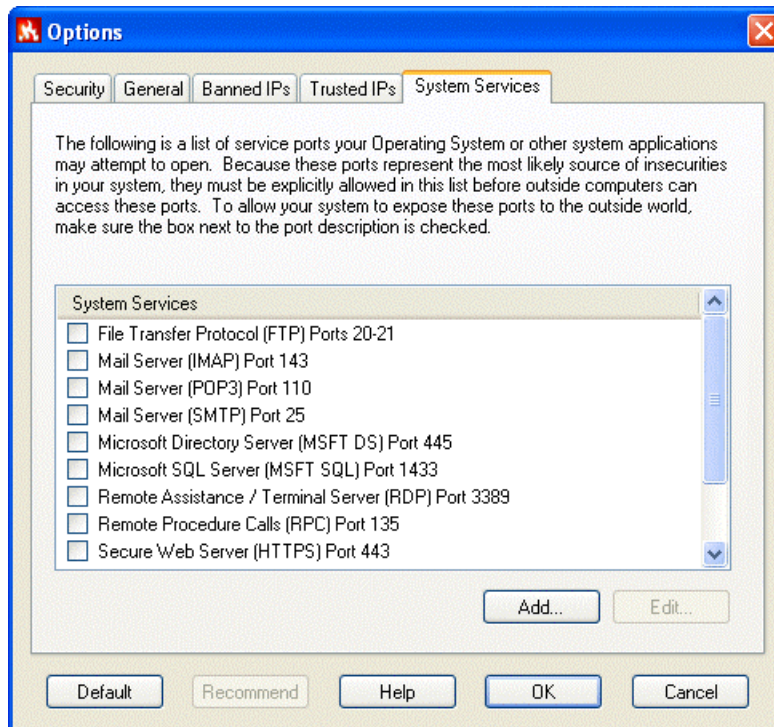


Figure 6

If the Program list does not have the application that needs access to the Internet, you will need to add it to the list manually:

1. Right-click the McAfee icon, point to **Personal Firewall**, and then click **Options**.
2. Click the **System Services** tab, and then click **Add**.
3. Enter the incoming and outgoing TCP/IP and UDP port information in the **Add Port Configuration** dialog box, and then click **OK**.
4. Click **OK** if you are finished making changes.

Updates

The McAfee SecurityCenter checks for updates to Personal Firewall every two hours while your computer is running and connected to the Internet. This ensures that you have the most up-to-date software components for Personal Firewall.

Chapter 3 – Using Personal Firewall

To open Personal Firewall:

- Right-click the McAfee icon, point to **Personal Firewall**, and click **View Summary**, **View Applications**, or **View Events**.

About the Summary

Use the Summary page to get an overview of blocked traffic and attacks on your computer and on computers worldwide:

- Right-click the McAfee icon, point to **Personal Firewall**, and then click **View Summary**. The Summary page opens (see Figure 7).

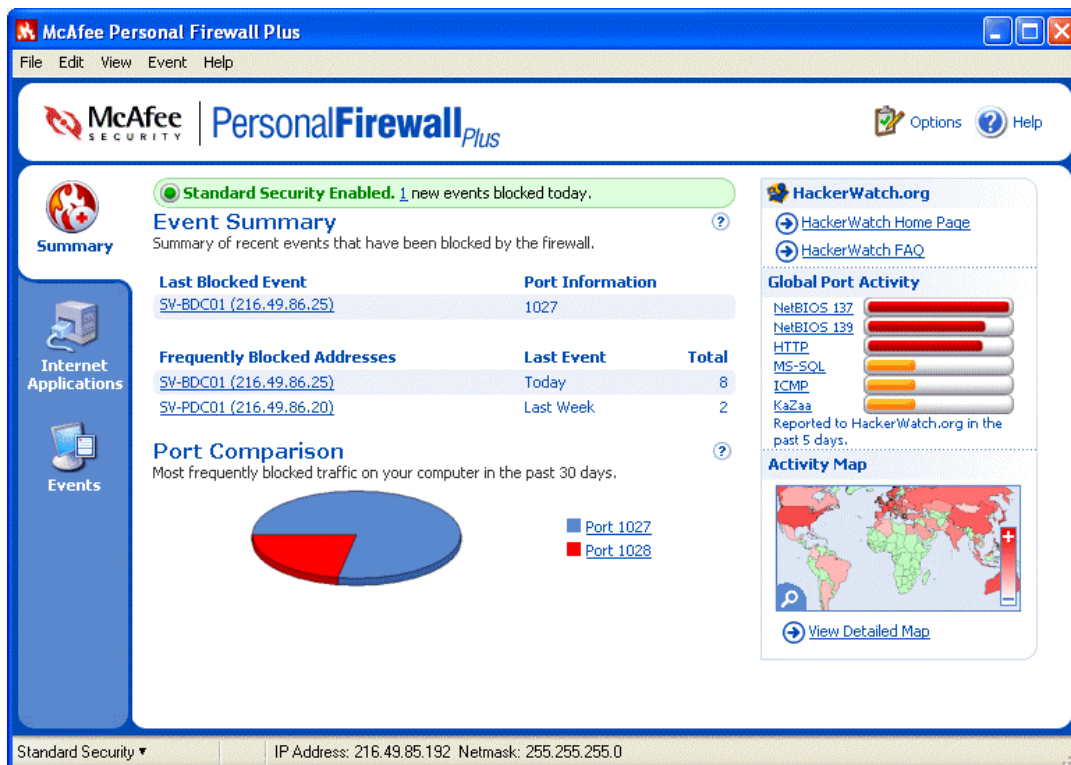


Figure 7

The Summary page provides the following information:

- The status bar at the top shows which security level is currently enabled and how many new events were blocked today.
- The Event Summary area shows the number of [events](#) logged today and last week, the last blocked event, and the most frequently blocked [addresses](#). You can click an event to view details in the Event Log.
- The Port Comparison area shows a pie chart of the most frequently attempted [ports](#) on your computer during the past 30 days. You can click a port name to view details at the [HackerWatch.org](#) Web site.
- The right pane contains links to the [Hackerwatch.org](#) Web site, a bar chart of global port activity during the past five days, and an activity map of worldwide traffic.

About Internet Applications

Use the Internet Applications page to view the list of allowed and blocked applications:

- Right-click the McAfee icon, point to **Personal Firewall**, and then click **View Applications**. The Internet Applications page opens (see Figure 8).



Figure 8

The Internet Applications page provides the following information:

- Application names
- File names
- Current permission levels
- Application details: pathnames, permission timestamps, and explanations of permission types

Changing Permissions

Personal Firewall lets you set the permission level for each application that requests Internet access.

To change a permission level:

1. Right-click the McAfee icon, point to **Personal Firewall**, and then click **View Applications**.
2. In the **Permissions** list, right-click the permission level for an application, and choose a different level:
 - Click **Allow Full Access** to allow the application to both send and receive data.
 - Click **Outbound Access Only** to prevent the application from receiving data.
 - Click **Block This Application** to prevent the application from sending or receiving data.

To delete a permission level:

1. Right-click the McAfee icon, point to **Personal Firewall**, and then click **View Applications**.
2. In the **Permissions** list, right-click the permission level for an application, and click **Delete Application Rule**. The next time the application requests Internet access, you can set its permission level to re-add it to the list.

Changing Applications

To change the list of allowed and blocked Internet applications:

1. Right-click the McAfee icon, point to **Personal Firewall**, and then click **View Applications**.
2. Add or remove applications from the **Application Name** list:
 - To add a new "Allowed" application, click **New Allowed Application**, select the application to allow, and then click **Open**.
 - To add a new "Blocked" application, click **New Blocked Application**, select the application to block, and then click **Open**.
 - To remove an application from the list, click **Delete Application Rule**.

About Events

Use the Events page to view the Event Log generated when Personal Firewall blocks unsolicited Internet traffic:

- Right-click the McAfee icon, point to **Personal Firewall**, and then click **View Events**. The Events page opens (see Figure 9).

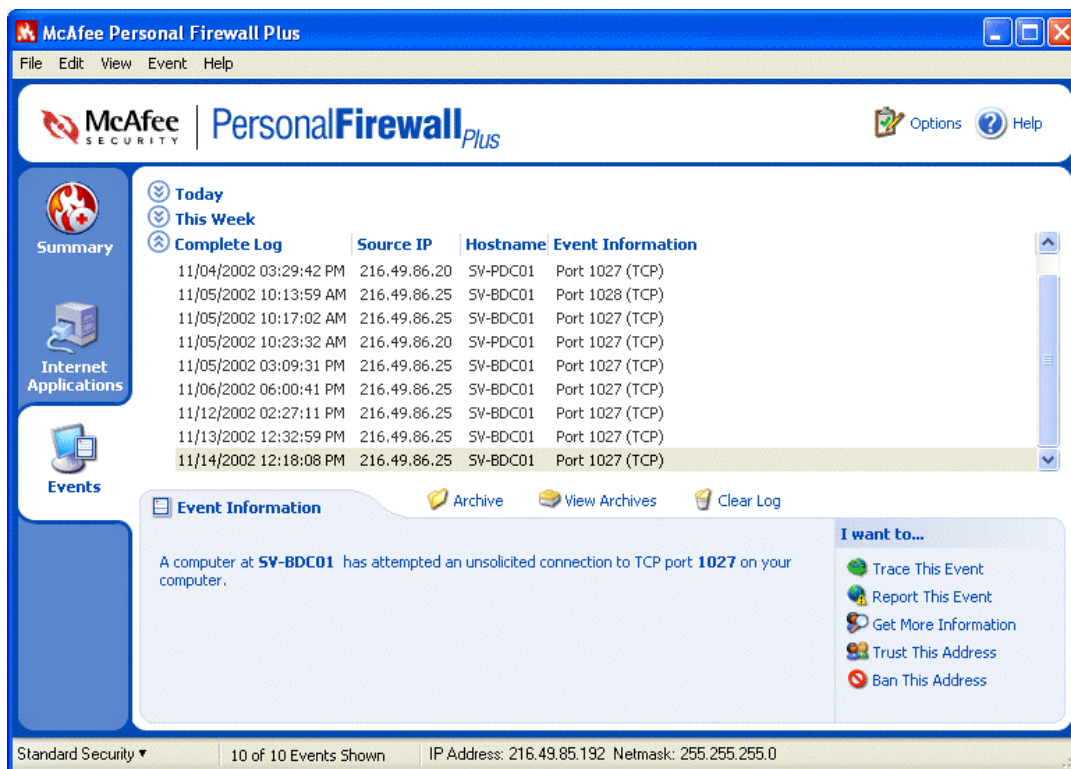


Figure 9

The Events page provides the following information:

- Timestamps
- Source IPs
- Hostnames
- Service or application names
- Event details: connection types, connection ports, and explanations of port events

Understanding Events

About IP Addresses

IP addresses are just numbers: four numbers between 0 and 255 to be precise. These numbers identify a specific place that traffic can be directed to on the Internet.

Special IP Addresses

Several IP addresses are unusual for various reasons:

- **Non-routable IP addresses:** These are also referred to as "Private IP Space." These IP addresses cannot be used on the Internet. Private IP blocks are **10.x.x.x**, **172.x.x.x**, and **192.168.x.x**.
- **Loop-back IP addresses:** Loop-back addresses are used for testing purposes. Traffic sent to this block of IP addresses comes right back to the device generating the packet. It never leaves the device, and is primarily used for hardware and software testing. The Loop-Back IP block is **127.x.x.x**.
- **Null IP address:** This is an invalid address. When it is seen, it indicates that the traffic had a blank IP address. This is obviously not normal, and frequently it indicates that the sender is deliberately obscuring the origin of the traffic. The sender will not be able to receive any replies to their traffic unless the packet is received by an application that understands the contents of the packet that will include instructions specific to that application. A Null IP Address is simply **0.0.0.0**.

Events from 0.0.0.0

If you see events from IP address 0.0.0.0, there are two likely causes. The first, and most common, is that for some reason your computer received a badly formed packet. The Internet isn't always 100% reliable, and bad packets can occur. Since Personal Firewall sees the packets before TCP/IP can validate them, it might report these packets as an event.

The other situation occurs when the source IP is *spoofed*, or faked. Spoofed packets might be a sign that someone is scanning around looking for Trojans, and they happened to try your computer. It's important to remember that Personal Firewall blocked this attempt, so your computer is safe.

Events from 127.0.0.1

Events will sometimes list their source IP as 127.0.0.1. It's important to note that this IP is special, and is referred to as the *loopback address*.

Basically, no matter what computer you're on, 127.0.0.1 always refers to yourself. This address is also referred to as *localhost*, as the computer name localhost will always resolve back to the IP address 127.0.0.1.

Does this mean that your computer is attempting to hack itself? Is some Trojan or spyware taking over your computer? Not likely. Many legitimate programs use the loopback address for communication between components. For example, many personal mail or Web servers let you configure them via a Web interface that is usually accessible through something like <http://localhost/>.

However, Personal Firewall allows traffic from these programs, so if you see events from 127.0.0.1, it most likely means that the source IP address is *spoofed*, or faked. Spoofed packets are usually signs of someone scanning for Trojans. It's important to remember that Personal Firewall blocked this attempt, so your computer is safe. Obviously, reporting events from 127.0.0.1 won't do any good, so there's no need to do so.

With that said, there are some programs, most notably Netscape 6.2 and higher, that requires you to add 127.0.0.1 to the trusted IP list. These programs' components communicate between each other in such a manner that Personal Firewall cannot determine if the traffic is local or not.

In the example of Netscape 6.2, if you do not trust 127.0.0.1, then you will not be able to use your buddy list. Therefore, if you see traffic from 127.0.0.1 and all of the applications on your computer work normally, then it is safe to block this traffic. However, if a program (like Netscape) is having problems, place 127.0.0.1 in Personal Firewall's trusted IP list, and then find out if the problem is resolved.

If placing 127.0.0.1 in the trusted IP list fixes the problem, then you need to weigh your options: if you trust 127.0.0.1, your program will work, but you will be more open to spoofed attacks. If you do not trust the address, then your program will not work, but you will remain protected against such malicious traffic.

Events from Computers on Your LAN

Events can be generated from computers on your local area network (LAN). To show that these events are coming from somewhere "close to home," Personal Firewall displays them in green.

In most corporate LAN settings, you'll want to check "Make all computers on your LAN Trusted" in the Trusted IPs options.

However, it's important to note that in some situations, your 'local' network can be as dangerous, or even more dangerous, than the outside network. This is especially true if you are on a high-bandwidth public network, such as DSL or cable modems. In such a scenario, it's best **not** to check the "Make all computers on your LAN Trusted" option.

If you are on a home network connected to broadband, you should instead manually add the IP addresses of your local computers to the Trusted IP list. Remember, you can use .255 style addresses to trust an entire block. For example, you can trust your entire ICS (Internet Connection Sharing) network by trusting the IP 192.168.255.255.

Events from Private IP Addresses

IP addresses of the format 192.168.xxx.xxx or 10.xxx.xxx.xxx are referred to as *non-routable* or *private* IP addresses. These IP addresses should never leave your network, and can be trusted most of the time.

The 192.168 block is used with Microsoft Internet Connection Sharing (ICS). If you are using ICS, and see events from this IP block, you might want to add the IP address 192.168.255.255 to your trusted IP list. This will trust the entire 192.168.xxx.xxx block.

If you are not on a private network, and see events from these IP ranges, the source IP address might be *spoofed*, or faked. Spoofed packets are usually signs that someone is scanning for Trojans. It's important to remember that Personal Firewall blocked this attempt, so your computer is safe.

Since private IP addresses refer to different computers depending on what network you are on, reporting these events will have no effect, so there's no need to do so.

Showing Events in the Event Log

The Event Log sorts events by events occurring on the current day, the past week, and the complete log. Personal Firewall lets you view them on the Events page in one of those three ways at a time. Personal Firewall also lets you display events from specific days, from specific Internet addresses (IP addresses), or events that contain the same event information.

For information about an event, click the event, and the information appears in the **Event Information** area at the bottom of the Events page.

Showing Today's Events

To show only events occurring today:

1. Right-click the McAfee icon, point to **Personal Firewall**, and then click **View Events**.
2. From the **View** menu, click **Show Today's Events**. The Events page displays only events occurring today from the Event Log.

Showing This Week's Events

To show events occurring in the past week:

1. Right-click the McAfee icon, point to **Personal Firewall**, and click **View Events**.
2. From the **View** menu, click **Show This Week's Events**. The Events page displays only events occurring this week from the Event Log.

Showing the Complete Event Log

To show all of the events in the Event Log:

1. Right-click the McAfee icon, point to **Personal Firewall**, and click **View Events**.
2. From the **View** menu, click **Show Complete Log**. The Events page displays all events, not including archives, from the Event Log.

Showing Only Events from the Selected Day

This is useful when you just want to look events from a specific day. All events not occurring on that day are hidden.

1. Right-click the McAfee icon, point to **Personal Firewall**, and click **View Events**.
2. From the **View** menu, click **Show Only Events from Selected Day**. Today's events appear on the Events page.

Showing Only Events from the Selected Internet Address

This is useful when you need to see other events originating from a specific Internet address. All other events are hidden.

1. Right-click the McAfee icon, point to **Personal Firewall**, and click **View Events**.
2. From the **View** menu, click **Show Only Events from Selected Internet Address**. Events originating from the selected Internet address appear on the Events page.

Showing Only Events with the Same Event Information

This is useful when you need to see if there are other events in the Event Log that have the same information as the one you selected. You can find out how many times this happened, and if it is from the same source.

1. Right-click the McAfee icon, point to **Personal Firewall**, and click **View Events**.
2. From the **View** menu, click **Show Only Events with the Same Event Information**. Events with the same Event Information appear on the Events page.

Responding to Events

Tracing the Selected Event

You can try to perform a visual trace of the IP addresses for an event in the Event Log. *

1. Right-click the McAfee icon, point to **Personal Firewall**, and click **View Events**.
2. Right-click the event you want to trace, and then click **Trace Selected Event**.
By default, Personal Firewall begins a visual trace using the integrated Personal Firewall Visual Trace program. However, you can select another visual trace program in the **General** tab of the Options dialog box.

Note: The first time you perform a Visual Trace, Personal Firewall prompts you to set your home location. See "Setting Your Home Location" for details.

You can also try to get advice at the anti-hacker online community HackerWatch.org Web site.

When you get enough information, you can then decide whether to report the event to HackerWatch.org, or to trust or ban the IP addresses involved in the event. However, be sure to understand events and IP addresses before taking any action.

* Only available in McAfee Personal Firewall Plus.

Getting Advice from HackerWatch.org

You can get more information about an event from the anti-hacker online community [HackerWatch.org](http://www.hackerwatch.org) by doing the following:

1. Right-click the McAfee icon, point to **Personal Firewall**, and click **View Events**.
2. Locate and click the event about which you want more information.
3. From the **Event** menu, click **More Information on Event**.
Your Web browser opens and goes to the HackerWatch.org Web site at <http://www.hackerwatch.org/> to get details about the event type and advice about whether to report the event.

Reporting an Event

To report an event that you think was an attack on your computer, please do the following:

1. Right-click the McAfee icon, point to **Personal Firewall**, and click **View Events**.
2. Click the event you want to report, and then click **Report This Event** in the lower right pane.
Personal Firewall reports the event to the HackerWatch.org Web site using your unique ID.

Signing Up for HackerWatch.org

When you first open the Personal Firewall Summary page, Personal Firewall contacts HackerWatch.org to generate your unique user ID. If you are an existing user, your sign-up is automatically validated. If you are a new user, you must enter a nickname and email, and then click the validation link in the confirmation email from HackerWatch.org to be able to use the event filtering/emailing features at its Web site.

You can report events to HackerWatch.org without validating your user ID. However, to filter and email events to a friend, you must sign up for the service.

Signing up for the service allows your submissions to be tracked and lets us notify you if HackerWatch.org needs more information or further action from you. We also require you to sign up because we must confirm any information we receive for that information to be useful.

All email addresses provided to HackerWatch.org are kept confidential. If a request for additional information is made by an ISP, that request is routed through HackerWatch.org; your email address is never exposed.

Trusting an Address

If you see an event in the Event Log that contains an IP address that you need to allow, you can have Personal Firewall allow connections from it at all times:

1. Right-click the McAfee icon, point to **Personal Firewall**, and click **View Events**.
2. Right-click the event whose IP address you want trusted, and click **Trust the Source IP Address**.
3. Verify that the IP address displayed in the **Trust This Address** confirmation message is correct, and click **OK**. The IP address is added to the Trusted IPs list.

To verify that the IP address was added:

1. Click **Options** in the top right of the main window.
2. Click the **Trusted IPs** tab. The IP address that you just set Personal Firewall to trust should be in the list.

Banning an Address

If an IP address appears in your Event Log, this indicates that traffic from that address was blocked. Therefore, banning an address adds no additional protection unless your computer has ports that are deliberately opened through the System Services feature, or unless your computer has an application that has permission to receive traffic.

Add an IP address to your banned list only if you have one or more ports that are deliberately open and if you have reason to believe that you must block that address from accessing the open port(s).

If you see an event in the Event Log that contains an IP address that you want to ban, you can have Personal Firewall prevent connections from it at all times:

1. Right-click the McAfee icon, point to **Personal Firewall**, and click **View Events**.
2. Right-click the event whose IP address you want to ban, and click **Ban the Source IP Address**.
3. Verify that the IP address displayed in the **Ban This Address** confirmation message is correct, and click **OK**. The IP address is added to the Banned IPs list.

To verify that the IP address was added:

1. Click **Options** in the top right of the main window.
2. Click the **Banned IPs** tab. The IP address that you just set Personal Firewall to ban should be in the list.

Managing the Event Log

You can use the Events page to manage the events in the Event Log generated when Personal Firewall blocks unsolicited Internet traffic.

Archiving the Event Log

You can archive the current Event Log in a file on your hard drive. We recommend that you archive your Event Log periodically because the Event Log can get quite large.

To archive the Event Log:

1. Right-click the McAfee icon, point to **Personal Firewall**, and then click **View Events**.
2. From the **File** menu, click **Archive Log**.
3. Click **Yes** on the confirmation message.
4. Click **Save** to save the archive in the default location, or browse to a location where you want to save the archive.

Viewing Archived Event Logs

You can view any Event Logs that you previously archived.

Caution: Before you view your archives, you must archive your current Event Log. Failure to do so will clear your current Event Log when you view an archive.

1. Right-click the McAfee icon, point to **Personal Firewall**, and then click **View Events**.
2. From the **File** menu, click **View Archived Logs**.
3. Click the archive file name (you might have to browse to it) and click **Open**. The archive displays where the Event Log normally displays.

Clearing the Event Log

You can clear all information from the Event Log.

Warning: Once you clear the Event Log, you cannot recover it. If you think you will need the Event Log in the future, you should [archive](#) it instead.

1. Right-click the McAfee icon, point to **Personal Firewall**, and then click **View Events**.
2. From the **File** menu, click **Clear Log**.
3. Click **Yes** on the confirmation box to clear the log. The Event Log clears from the Personal Firewall window.

Exporting Displayed Events

You can export your Event Log to a text file in case you need to share it with your ISP, technical support, or law enforcement officials.

1. Right-click the McAfee icon, point to **Personal Firewall**, and then click **View Events**.
2. From the **File** menu, click **Export Displayed Events**.
3. Browse to the location to which you want to save the events.
4. Rename the file if necessary, and then click **Save**. Your events are saved to a .txt file in the location you chose.

Copying an Event to the Clipboard

You can copy an event to the clipboard so that you can paste it in a text file using Notepad.

1. Right-click the McAfee icon, point to **Personal Firewall**, and then click **View Events**.
2. Click the event in the Event Log that you need to export.
3. From the **Edit** menu, click **Copy Selected Event to Clipboard**.
4. Open Notepad:
 - Click the Windows **Start** button, point to **Programs**, then **Accessories**, and then click **Notepad**.
5. Click **Edit**, and then click **Paste**. The event appears in Notepad. Repeat this step until you have all of the necessary events.
6. Save the Notepad file in a safe place.

Deleting the Selected Event

You can delete events from the Event Log.

1. Right-click the McAfee icon, point to **Personal Firewall**, and then click **View Events**.
2. Click the event in the Event Log that you want to delete.
3. Click **Edit**, and then click **Delete Selected Event**. This deletes the event you selected.

About Alerts

Personal Firewall features five types of alerts:

- **Connection Attempt Blocked** - This alert appears when Personal Firewall blocks unwanted Internet or network traffic. This alert will only appear if you have chosen **Display an alert** on the General tab of the Options dialog box. (Trusting, Standard, or Tight Security)
- **Application Requests Internet Access** - This alert appears when Personal Firewall detects Internet or network traffic for new applications. (Standard or Tight Security)
- **Application Has Been Modified** - This alert appears when Personal Firewall detects that an application you have previously allowed to access the Internet has changed. If you have not recently upgraded the application in question, you should be careful about granting the modified application access to the Internet. (Trusting, Standard, or Tight Security)
- **Application Requests Server Access** - This alert appears when Personal Firewall detects that an application you have previously allowed to access the Internet has requested Internet access as a server. (Tight Security)
- **New Application Allowed** - This alert appears when Personal Firewall automatically grants Internet access for all new or modified applications, then notifies you. (Trusting Security)

Note: To view recommendations to help you handle application alerts, you must first select either **Auto-use** (the default) or **Show** in the **Application recommendations** list of the Options dialog box. Personal Firewall will then show application recommendations on its alerts (see "Application Recommendations" for details).

Important: We strongly recommend that you become familiar with the types of alerts you will encounter while using Personal Firewall. Review the following types of alerts that can appear and the possible responses you can choose, so that you can confidently respond to an alert.

Connection Attempt Blocked

If you selected **Display an alert** in the Options dialog box and **Trusting, Standard, or Tight Security**, Personal Firewall displays an alert (like Figure 10) when it blocks unwanted Internet or network traffic. If a Trojan program alert appears (like Figure 11), McAfee automatically denies this program access the Internet and recommends that you scan your computer for viruses.

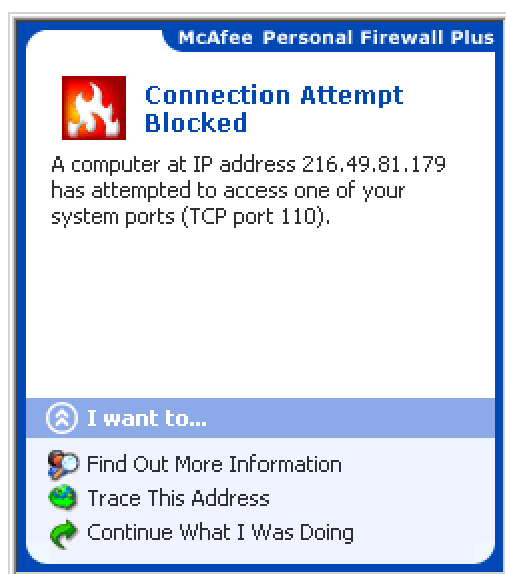


Figure 10

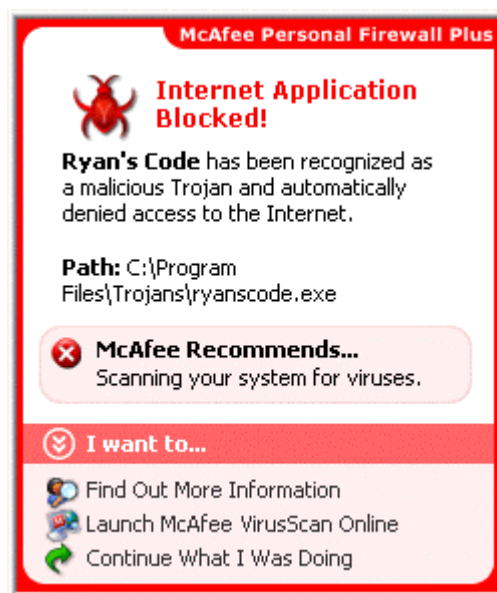


Figure 11

View a brief description of the event, then choose from these options:

- Click **Find Out More Information** to get details about the event through the Personal Firewall Event Log (see "About Events" for details).
- Click **Trace This Address** to perform a visual trace of the IP addresses for this event (Figure 10). *
- or -
Click **Launch McAfee VirusScan Online** to scan your computer for viruses (Figure 11).
- Click **Continue What I Was Doing** if you do not want to take action beyond what Personal Firewall has already done.

* Only available in McAfee Personal Firewall Plus.

Application Requests Internet Access

If you selected **Standard** or **Tight** in the Firewall Options, Personal Firewall displays an alert (like Figure 12) when it detects Internet or network traffic for new or modified applications. If a spyware program alert appears (like Figure 13), McAfee recommends that you use caution in allowing this program to access the Internet. You can click the "learn more" link to get advice.

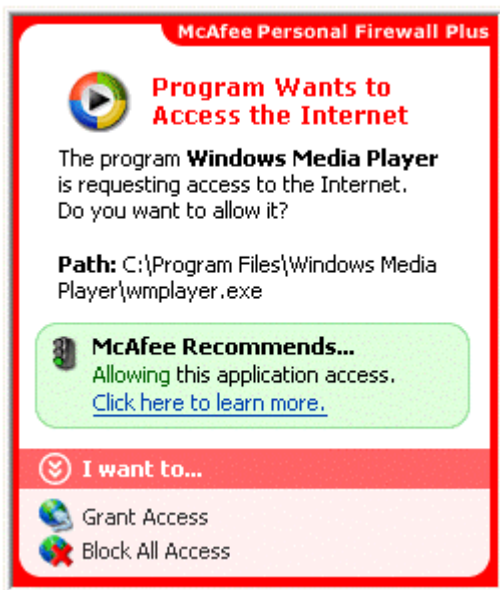


Figure 12

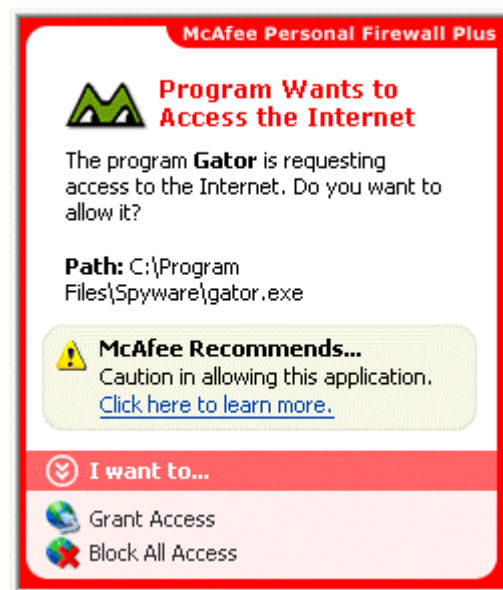


Figure 13

View a brief description of the event, then choose from these options:

- Click **Grant Access** to allow the application to both send data and receive unsolicited data on non-system ports.
- Click **Block All Access** to prevent the application from sending or receiving data.

Important: You must grant access to applications that require Internet access for online product updates (such as McAfee.com security services) to keep them up-to-date. Check the pathname shown in the alert (for example, "C:\Program Files\McAfee.com\...") to verify whether an application needs to have Internet access.

Application Has Been Modified

If you selected **Trusting**, **Standard**, or **Tight** Security in the Firewall Options, Personal Firewall displays an alert (like Figure 12) when Personal Firewall detects that an application you have previously allowed to access the Internet has changed. If you have not recently upgraded the application in question, be careful about granting the modified application access to the Internet.

View a brief description of the event, then choose from these options:

- Click **Grant Access** to allow the application to both send data and receive unsolicited data on non-system ports.
- Click **Block All Access** to prevent the application from sending or receiving data.

Application Requests Server Access

If you selected **Tight** Security in the Firewall Options, Personal Firewall displays an alert (like Figure 14) when it detects that an application you have previously allowed to access the Internet has requested Internet access as a server. For example, an alert appears when MSN Messenger requests server access to send a file during a chat.

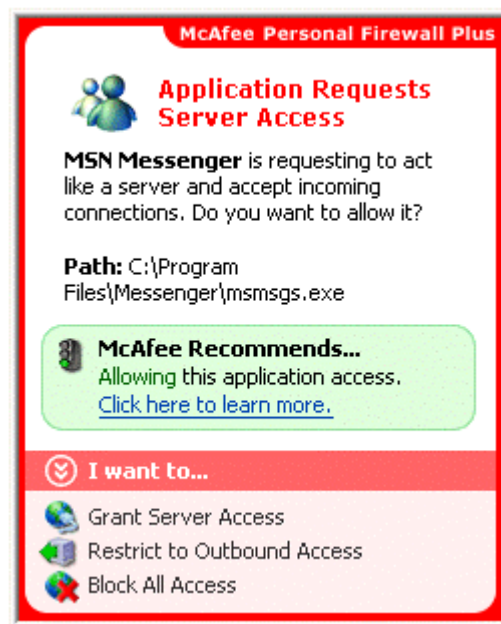


Figure 14

View a brief description of the event, then choose from these options:

- Click **Grant Server Access** to allow the application to both send and receive data.
- Click **Restrict to Outbound Access** to prevent the application from receiving data.
- Click **Block All Access** to prevent the application from sending or receiving data.

New Application Allowed

If you selected **Trusting** Security in the Firewall Options, Personal Firewall automatically grants Internet access for all new or modified applications, then notifies you with an alert (like Figure 15).

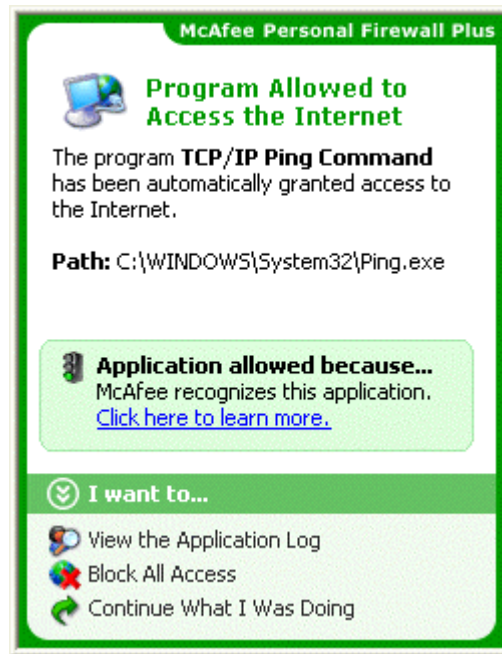


Figure 15

View a brief description of the event, then choose from these options:

- Click **View the Application Log** to get details about the event through the Personal Firewall Internet Applications Log (see "About Internet Applications" for details).
- Click **Turn Off This Alert Type** to prevent these types of alerts from appearing.
- Click **Continue What I Was Doing** if you do not want to take action beyond what Personal Firewall has already done.

Chapter 4 - Troubleshooting

Help! My computer has been hacked!

The most important thing for you to remember is that your computer is behind a firewall. If you haven't opened any malicious programs, if you are being careful, and if your computer was not already compromised before you installed Personal Firewall, then you should be safe.

When you see an event in the log, it does not necessarily mean that someone tried to hack into your computer. All it means is that a certain type of packet came to the IP address you are currently using and Personal Firewall determined you didn't need it, so it blocked the packet.

Warnings from Personal Firewall are broken down into three categories:

- **Application Driven**

These are the most common. An application you are using caused the firewall to be triggered. Look at the information provided about the event in the log view. If it mentions an application you are using, then most likely, you can configure settings in **Options** to prevent this warning from happening again.

- **Random Probes**

Even if a warning is created that has nothing to do with an application you are using, you still might not be a specific target. Many would-be hackers configure scanners to attempt to access random IP addresses over time. Due to the sheer number of 'script-kiddies' running these scanners, you can expect to be hit by one almost daily.

There are two important things to remember:

1. These probes are at random; they were not specifically targeted at you.
2. Personal Firewall STOPPED these probes from reporting to the 'script-kiddie.' As far as the probing program knows, your computer doesn't exist, so the script-kiddie won't know either.

- **True Attempts**

If you receive multiple hits over time from a similar address, then there's a chance someone is actually trying to hack into your computer. However, the key is to err on the side of reason.

Don't go reporting every little probe that hits your computer. Remember the boy who cried "wolf." If someone persistently pesters you, ban their IP, or collect as much data as possible before reporting them.

Open NetBIOS port

"When I connect to www.grc.com, an alert says my NetBIOS port is open."

When you are using the 2nd and 3rd levels (Trusting, Standard) of security in Personal Firewall, your computer accepts all UDP communication with computers that you initiate traffic with. Because you initiated the connection to the GRC site, Personal Firewall allows the NetBIOS query, which comes over UDP.

This is not dangerous unless you are in the habit of initiating communication with computers or people you do not trust. This might occur in peer-to-peer programs such as Kazaa or AIM. To prevent this from being a problem, either disable NetBIOS over TCP/IP in your Windows protocol settings or use security level 4 on the **Security** tab of Personal Firewall options (Tight).

Unknown event type code

"The event type code being reported is unknown. This should not happen. Please contact technical support."

If someone is pinging you with an unknown address, then he or she is spoofing his or her IP address. The bad news is that we can't track that down, since the IP is wrong. The good news is that they can't learn anything about your computer or its contents.

Pings work kind of like the old "Self Address Stamped Envelopes" used by catalog companies. Think of the source IP as a "Return Address" on an envelope. When they ping, they're sending you an envelope with a return address in it, and they're asking you to put a piece of paper in the envelope saying that you exist and to send it back. However, since they didn't put a real return address, even if Personal Firewall hadn't blocked it, your computer would have sent the return to an invalid address. So, in other words, don't worry about it.

Installation issues in Windows 2000

The event viewer in Windows 2000 can provide useful details about a Personal Firewall install if technical support is needed.

Note that this option is only available in Windows 2000, not in Windows 95, 98, or ME. Also note that we are referring to the Event Viewer built into Windows 2000, **not** the Personal Firewall Event Log. To open the Event Viewer and look for Personal Firewall Warnings or Errors:

1. Open Start | Programs | Administrative Tools | Event Viewer
2. Click on Application Log
3. Click on the "Source" Column to sort by source
4. Look for events with a Source of "MpfService"

If you see any events from Source "MpfService" with Type "Error", double-click on them. To copy the contents, press the button that has two pieces of paper on it in the Event Properties window. Then, if needed for technical support, paste these events into an email. The result should look something like:

```
Event Type: Error
Event Source:      MpfService
Event Category:   None
Event ID:         2
Date:             4/17/2001
Time:             3:44:22 PM
User:             NT AUTHORITY\SYSTEM
Computer:        CIVIC
Description:
Filter Device I/O Proxy Thread could not open a vital shared memory resource.
This is a fatal error. Ensure multiple copies of application are not
installed. If error persists, reinstall is suggested.
```

"Track an Attack" error messages

If you enter an invalid address in the **Track an Attack** dialog box *, an error message appears. Here are possible errors and solutions.

- **An invalid hostname is entered as the target location.**
- **The target name entered is too long to be a valid target.**

These errors appear when either the item you entered as a target is invalid or you are not connected to the Internet.

Valid trace targets are IP addresses or computer names that can be resolved to an IP address.

You can also enter an email address as a trace target. Be sure to enter the email address only, without spaces or punctuation. When an email address is entered as the target, Visual Trace determines the MX record IP address. This might be different from the IP address associated with that machine name for other purposes.

Examples of valid targets are:

- 207.90.69.200
- www.mcafee.com
- localhost
- support@mcafee.com

* Only available in McAfee Personal Firewall Plus.

Configuring Microsoft® Internet Explorer

McAfee.com uses ActiveX controls and cookies in its applications. These technologies require specific Internet browser configurations to ensure the applications are installed correctly and work properly on your computer.

Most Web browsers will already have the proper settings to install Personal Firewall. To avoid any problems with the installation, we suggest that you verify that the Internet Explorer settings are correct before you try to install Personal Firewall.

First, determine which version of Internet Explorer you are using:

1. Open Internet Explorer.
2. On the Internet Explorer menu bar, click **Help**, and then click **About Internet Explorer**.
3. Look for the line labeled Version: and note the first three numbers.

Example: Version: **5.50**.4807.2300. The bold numbers indicate where you should look. This version of Internet Explorer is 5.50, so you would follow the steps in the "Configuring Internet Explorer 5.x" section.

Configuring Internet Explorer 5.x

1. Open Internet Explorer. On the **Tools** menu, click **Internet Options**.
2. Click the **Security** tab (see Figure 16). Make sure that you are in the **Internet** Web content zone and that **Security level for this zone** is set to **Medium** or lower.
3. Click **Custom Level**. Select **Enable** for these ActiveX controls and plug-ins options:
 - Download signed ActiveX controls
 - Run ActiveX controls and plug-ins
 - Script ActiveX controls marked safe for scripting
4. Select **Enable** for the Active scripting option under the **Scripting** settings. You will need to scroll down the list to find it.
5. Click **OK**, and then click **Yes** to confirm the changes.
6. Click **Apply**, and then click **OK** to close the Internet Options dialog box.
7. Quit Internet Explorer.

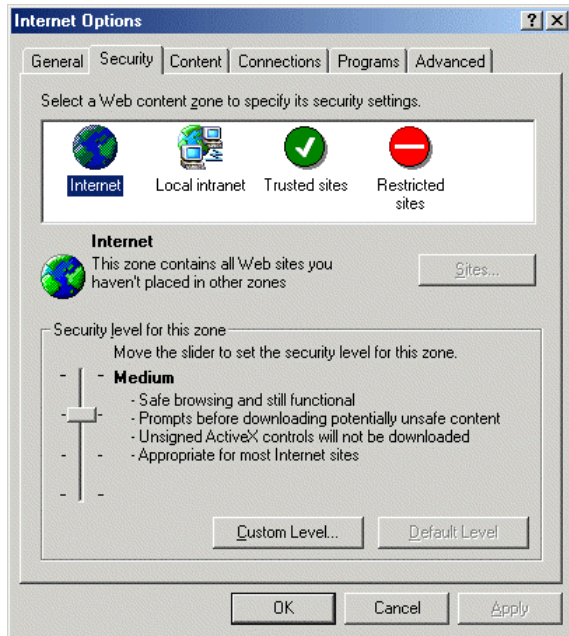


Figure 16

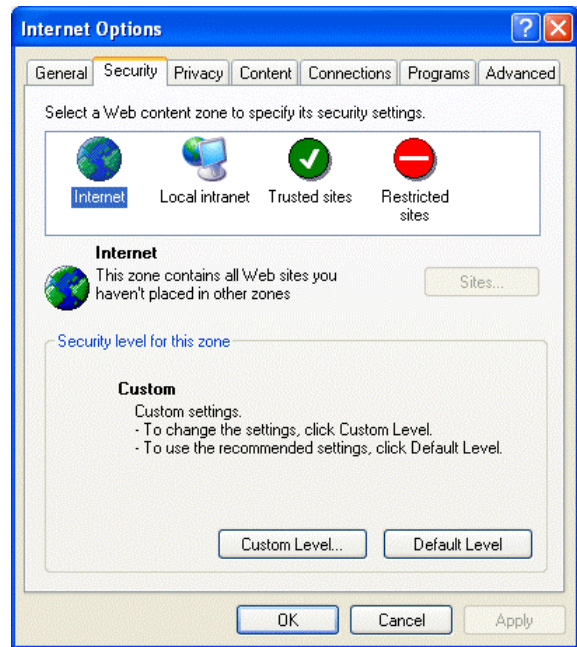


Figure 17

Configuring Internet Explorer 6.x

1. Open Internet Explorer. On the **Tools** menu, click **Internet Options**.
2. Click the **Security** tab (see Figure 17). Make sure that you are in the **Internet** Web content zone and that the security level for this zone is set to **Medium** or lower.
3. Click **Default Level** to use the recommended settings.
4. Click **Custom Level**. Select **Enable** for these ActiveX controls and plug-ins options:
 - Download signed ActiveX controls
 - Run ActiveX controls and plug-ins
 - Script ActiveX controls marked safe for scripting
5. Select **Enable** for the **Active scripting** option under the **Scripting** settings. You will need to scroll down the list to find it.
6. When you are done, click **OK**, and then click **Yes** to confirm the changes.
7. Click the **Privacy** tab (see Figure 18), and then click **Advanced**.
8. Make sure that **Override automatic cookie handling** and **Always allow session cookies** are selected, and then click **OK**. Click **OK** again.
9. Quit Internet Explorer.



Figure 18

Appendix A - Frequently Asked Questions

What's new in McAfee Personal Firewall?

McAfee has added several key functional enhancements to its firewall technology. To strengthen the security and control that you have over how your computer accesses the Internet, Personal Firewall now features application fingerprinting and outbound filtering. These features help you control programmatic access to the Internet by allowing you to securely fingerprint trusted applications. Together, application fingerprinting and outbound filtering help to prevent malicious spyware and Trojans from sending data out of your computer to a hacker. To support these new features, McAfee has also updated its user interface and alert mechanism.

What should I expect when I first run Personal Firewall?

When you first run Personal Firewall, you will notice that many applications that you have installed on your computer are asking for access to the Internet. If you recognize and trust these applications, you should grant them access to the Internet. You will only see one alert per application, so Personal Firewall will alert you less frequently about new applications after a short period of time. To view which applications you have trusted, simply open Personal Firewall and click the **Internet Applications** tab.

Why is a program requesting access to the Internet?

Here are some of the many reasons why an application might seek Internet access:

- A program might need to check for automatic updates.
- A program might need to retrieve information such as email, news, or music.
- A program might need to communicate with a licensing server to verify your right to use the program.
- A program (e.g., explorer.exe, rundll.exe, svchost.exe) might be called by another program to communicate with the Internet.

Why is a program requesting server access?

A program might request server access if it expects to receive anonymous connections from the Internet. Some examples of this might include online games, messenger applications, and file-sharing applications. Only grant an application server access if you recognize and trust the application and if you want it to be able to receive anonymous connections.

Why is explorer.exe requesting access to the Internet?

Explorer.exe is used by Internet Explorer to display "tree" diagrams of FTP sites. If you are using **Tight Security**, explorer.exe should be granted outbound access only—do not grant server access to explorer.exe.

What is the difference between "Outbound" and "Full" access?

"Outbound" access permits an application to communicate with other systems but not receive communications it did not initiate. "Full" access permits an application to not only make any connections it wants, but also permits the application to receive connections from other users. When you grant an application the ability to receive Internet connections, you need to be very careful with security packages.

Why am I seeing an “Application Has Been Modified” alert?

This alert indicates that an application has somehow changed since the firewall last let the application run. Typical changes might include:

- **W AOL.exe**
If you just ran AOL and noticed that a TOD update was downloaded, you will see a modified application alert the next time AOL starts.
- **I explorer.exe**
If you just applied an automatic update or upgraded to your version, you will see a modified application alert.
- **I netinfo.exe**
If you use IIS, you will see a modified application alert as each new patch is applied.

Important: In the aforementioned cases, you should grant Internet access to the application if you continue to trust it. If you cannot think of a reason that the application has changed, then block Internet access from the application. Next, update your virus signature files for your anti-virus services, and scan of all your hard disks for viruses. If the anti-virus scan comes up clean, then you should grant Internet access to the application.

What are “Security Levels”?

Security levels are used to let users control how trusting their firewall should be of inbound and outbound traffic:

Setting	Description
High (Lockdown)	All traffic is stopped. This is essentially the same as unplugging your Internet connection. You can use this setting to block ports you configured to be open under the System Services tab.
Tight	An application requests only the type of access to the Internet that it explicitly needs (for example, Outbound Only Access), and you either grant access or block it. If the application later requests Full Access, you either grant Full Access or keep it limited to Outbound Only Access. Use this setting if you are an experienced firewall user.
Standard	(Recommended) An application requests only once for access to the Internet, and you either grant access or block it. If you grant access, the application can both send data and receive unsolicited data on non-system ports. Use this setting if you are a novice firewall user.
Trusting	All applications are automatically trusted when they first attempt to access the Internet. However, you can choose to be notified about new applications on your computer with alerts. Use this setting if you find that some games or streaming media do not work.
Low (Open/No Filtering)	Your firewall is effectively disabled. This setting allows all traffic through Personal Firewall with no filtering.

When do I need to open ports using System Services?

You only need to open ports using System Services if the application must accept unsolicited connections from other computers to work. Examples of this include:

- Mail Server: You do not need to open a Mail Server port to receive email. You only need to open a port if the computer protected by Personal Firewall acts as an email server.
- Web Server: You do not need to open a Web Server port in order to run a Web browser. You only need to open a port if the computer protected by Personal Firewall acts as a Web server.

When I submit events to HackerWatch, why do they not appear immediately in my submitted events list?

Data streaming into the HackerWatch servers is not immediately available for summary viewing. It must first be filtered and integrated with the other millions of events the system processes every day. The delay between your submitting the event and being able to manipulate the data on your personal screens at HackerWatch will vary from a few minutes to several hours depending upon the time of day and the total volume of traffic.

What do the color-coded events mean in the Personal Firewall Log?

- **Green** entries are from a local IP or non-routable IP (e.g. 192.168.X.X).
- **Gray** entries are from a possibly spoofed IP address, such as the loopback adapter (127.0.0.1) or an invalid IP (0.0.0.0).
- **Red** entries are from banned IP addresses.

Help links are also included in the event description areas, which will further describe why you might be seeing events from these sources.

Does Personal Firewall work with Internet Connection Sharing?

All issues with ICS on all versions of Windows are corrected. There are no known conflicts with Personal Firewall and ICS.

How does Personal Firewall impact system performance and traffic?

There is very little performance impact. Potential resource consumption or slowdown occurs in two areas; CPU usage by the filter in inspecting the traffic, and additional latency added by the time it takes the filter to inspect the packet before blocking or allowing it.

The CPU overhead is negligible. Even on a heavily loaded system it is difficult to measure. On older computers under 120 MHz, there might be some measurable overhead.

Added packet latency is under 1 ms, and is effectively zero.

What is a Trojan?

A large portion of the mischief and malice done to personal computers across the Internet is performed through Remote Access Trojan programs, or RATs.

All Trojans are programs that contain a malicious payload. Frequently they appear to do something benign or beneficial. They might display a pretty animation or appear to be a utility of some sort (a famous Trojan of several years ago was an email client).

How do Trojans get on your computer? You put them there; therefore, it is very important that you exercise caution in where you obtain software. Never take software from someone you meet in a chat room, for example. This is the #1 place where people get stuck with Trojans. Often people are tricked into thinking the program they are obtaining will do something for them, like help them play a game.

Many Trojans can do destructive things to your computer regardless of whether you are connected to the Internet or not. The bottom line is that if a bad person can get you to run his or her program, it is no longer your computer.

Only you can protect yourself completely. Putting too much faith in virus scanners, firewalls and other software only makes you less careful. Would you put on a 'bullet-proof' vest and then never worry about walking around where people were shooting? Always think it through.

Remember these key facts:

- If you run a program that is a Trojan, it will get on your system unless it is blocked by an anti-virus program such as McAfee VirusScan Online.
- The only way to not be hit by Trojans is not to download software from un-trusted sources. Someone you met online is **never** a trusted source.

How do I uninstall Personal Firewall?

1. Click **Start** on your Windows taskbar, point to **Programs**, then **McAfee**, then **McAfee Personal Firewall**, and then click **Uninstall McAfee Personal Firewall**.
2. Click **Uninstall** to start uninstalling Personal Firewall.

Does Personal Firewall support Microsoft® Internet Information Services (IIS)?

Personal Firewall is not intended for server-side use. Therefore, it does not include protection from IIS exploits. Personal Firewall users who run IIS put themselves at risk if they allow access to IIS and do not keep IIS security patches up-to-date.

Glossary

A

ActiveX controls

ActiveX controls are software modules based on Microsoft's Component Object Model (COM) architecture. They add functionality to software applications by seamlessly incorporating pre-made modules with the basic software package. Modules can be interchanged but still appear as parts of the original software.

ARP

ARP stands for Address Resolution Protocol and is used for communication over the Ethernet networks found in most offices. ARP converts the protocol Internet traffic uses for Web pages and email to the protocol the Ethernet card in your computer uses. If this is blocked, your computer will not understand the traffic coming from the network. The result is you cannot use email, the Internet, nor can you print on a network printer.

B

BPS

The speed at which data is transmitted in bits-per-second. A 28.8 modem can move 28,800 bits per second.

browser

A client program that uses the Hypertext Transfer Protocol (HTTP) to make requests of Web servers throughout the Internet. A Web browser graphically displays content for the browser user.

C

cookie

A cookie most commonly refers to a piece of information sent by a Web server to a user's Web browser. The browser software sends it back to the server whenever the browser makes additional requests from the server. When you visit a site that you previously visited, and were welcomed by name, thank (or blame) a cookie that told them who you are.

country code

In the course of tracing intrusion attempts you will eventually encounter a country code. The country code is a two-letter tag at the end of a site URL that identifies the country where the site is located. See the on-line help for a detailed list of country codes.

D

DHCP

DHCP stands for Dynamic Host Configuration Protocol. It is a protocol used on many networks and by DSL and Cable providers to assign IP addresses to computers automatically (dynamic IP address). Every computer on an office network needs an IP address so it can log on to the network, get email, and connect to the Internet.

domain name system (DNS)

The Domain Name System simplifies Internet navigation. Computers on the Internet can only be found at their numerical IP address (e.g., 206.216.115.4). An address like "McAfee.com" makes sense to a human but a DNS server must match it up to its real IP address. The DNS server databases are updated regularly as new domain names are registered.

domain name

An Internet site's unique name, which can consist of two or more parts separated by dots (McAfee.com, whitehouse.gov, www.chubu.ac.jp).

DSL

DSL or Digital Subscriber Line is an increasingly popular method of connecting to the Internet over regular phone lines. DSL offers the advantage of a relatively high-speed connection at prices substantially lower than ISDN connections. In theory, DSL has a download speed limit of 9 megabits per second and an upload limit of 640 kilobits per second. In reality, and dependent of your provider's equipment as well as your computer equipment, you can expect anything from about 1.5 megabit download/128 kilobit upload (Asymmetric DSL) to 384 kilobits in both directions (Symmetric DSL).

E**email**

Electronic Mail, messages sent via the Internet or within a company LAN or WAN. Email attachments in the form of EXE (executable) files or VBS (Visual Basic script) files have become increasingly popular as a means of transmitting viruses and Trojans.

F**finger**

Software that allows you find out more information about an Internet user such as their real name and if they are logged on to a network or the Internet.

firewall

Hardware and/or software designed to keep unauthorized outsiders from tampering with a computer system or network. That system can be a standalone computer, a small LAN, or a company-wide network or WAN with thousands of users. Personal Firewall is a software firewall effective in protecting standalone computers and small networks.

FTP

FTP or File Transfer Protocol is used to move files between Internet sites. When you "download" a file from a site, e.g. a virus program update, you are using FTP. Public FTP sites from which you can download program or driver updates are usually anonymous FTP servers that permit anonymous logins. Private FTP sites normally require a Login name as well as a password and those who use them regularly, usually make use of specialized FTP programs.

H**hit**

A "hit" is a single request from a web browser for a single item from a web server. A single web page with text and graphics will require multiple hits in order to acquire the complete page. The number of hits required to get the entire page, the size of graphic files, the speed of your connection and the transfer speed of all the various nodes between your browser and the web site all add up to a page that appears in seconds or one that comes in very slowly.

HTTP

Hypertext Transfer Protocol moves hypertext (HTML) files on the Internet from the server you are visiting to the browser you are viewing with.

I

ICMP

ICMP stands for Internet Control Message Protocol. It is a troubleshooting tool used by technicians to find errors on a network, and it communicates errors on a network as they occur. Unfortunately, hackers can also use it to interfere with and redirect communications. Hackers do this to get information such as account numbers, credit card numbers, and other information. Thankfully, ICMP is usually not necessary, and it can be blocked without causing problems.

Internet

The Internet consists of a huge number of inter-connected networks that use the TCP/IP protocols for the location and transfer of data. The Internet evolved from a linking of university and college computers (in the late 1960s and early 1970s) funded by the U.S. Department of Defense and called the ARPANET. The Internet today is a global network of almost 100,000 independent networks.

intranet

A private network, usually inside an organization, that functions very much like the Internet. It has become common practice to permit access to such Intranets from standalone computers used by students or employees off-campus or off-site. Firewalls, login procedures and passwords are designed to provide security.

IP number

The Internet Protocol Number or IP address is a unique number consisting of four parts separated by dots (e.g. 63.227.89.66). Every computer of the Internet from the largest server to a laptop communicating through a cell phone has a unique IP number. Not every computer has a domain name, but everyone has an IP.

ISDN

Integrated Services Digital Network is yet another way of moving data at high speed over existing phone lines (see DSL). ISDN is widely available and with increasing pressure from DSL providers, cost is coming down. While a 128,000 Bps rate is theoretically possible, most users find that reality is in the 56,000 to 64,000 Bps range.

ISP

Internet Service Provider. This is the service you subscribe to in order to connect with the Internet. It can be a small local company with a few thousand subscribers, a regional company (e.g. uswest.net) or a nationwide mega-provider like A.O.L. or AT&T WorldNet. Most ISPs sell you a connection, nothing more. They provide no security whatsoever and if your computer is hacked and subsequently damaged or destroyed, they don't owe you the time of day. On the other hand if you are a hacker or violate any of the fine print in your ISP service agreement, they can cut off your Internet access before you can say World Wide Web.

L

LAN

Local Area Network. Two or more computers that are linked together and able to share programs, data and/or peripherals

M

MIME

Multipurpose Internet Mail Extensions, MIME, is the standard format used for transmitting files attached to email messages (pictures, sound files, video files, executables, etc.). The attachment is encoded when it leaves your computer and is decoded and restored to its original form at the receiving end. The specific encoding/decoding format for a given file varies with the file type. Once in a great while you might receive a MIME format attachment, essentially an attachment that was not properly encoded or decoded. If you open it and look at it, it will appear to be indecipherable gobbledygook.

modem

MOdulator/DEModulator. Your modem takes data you are sending and modulates it so that it can be transmitted over an analog voice phone line. Your modem accepts incoming modulated data and demodulates it so that it is usable by your computer. The earliest modems required the user to place the telephone handset into a cradle with padded apertures for the two ends of the handset. Speeds were in the range of 300 to 1,200 Bps. With improvements in error correction, modems today under ideal conditions can transmit data at over 50,000 Bps. over a single phone line. DSL and ISDN connections offer even higher speeds. These days the term modem is frequently used to describe external network connection devices that don't actually perform any modulation or demodulation, such as DSL and Cable modems which are actually digital end-to-end.

N

NAT

Network Address Translation. The process of converting between IP addresses used within an intranet or other private network and Internet IP addresses. This makes it possible to use a large number of addresses within the private network without depleting the limited number of available numeric Internet IP addresses.

network

When you connect two or more computers, you create a network. When you connect two or more networks you create an internet (lower case "i").

node

A single computer connected to a network. When you ask Personal Firewall to perform a trace, the Visual Trace Express trace list shows you all of the nodes between your computer and the source of your intrusion event. The nodes simply served as connection points in passing along the data.

P

packet switching

This is the method used to move data on the Internet. The data you are sending or receiving is broken up into pieces, each piece carrying the IP address of where it is going and where it is coming from. Billions of these pieces are passing through the Internet at any given time and the major node servers are sorting these pieces and routing them at incredible speeds. The email you are reading or the web page you are looking at has been reassembled and delivered to your monitor after traveling across town or around the world and, best of all, you don't have to give it a moments thought.

password

A code (usually alphanumeric) you use to gain access to your computer, to a given program, or to a Web site.

PING

Packet Internet Groper is a program used to determine whether a specific IP address is accessible. A packet is sent to the specified address and the program waits for a reply. Programs like Visual Trace and Visual Trace Express use PING to identify and/or troubleshoot Internet connections. In addition to identifying the target site, these programs also note all of the nodes the data passed through between the two ends of the connection. The most popular shareware PING utility is the full-featured version of Visual Trace.

port

A place where information goes into and/or out of a computer, e.g. a conventional analog modem is connected to a serial port. The port numbers in TCP/IP communications are virtual values used to separate traffic into application-specific streams. The ports (destination and source) captured in the Personal Firewall Event Log are significant because different applications listen and transmit on different ports. Ports are assigned to standard protocols like SMTP or HTTP so that programs know what port to try a connection on. The destination port for TCP packets indicates the application or server being looked for. In the case of UDP packets the source port has more significance.

PPP

Point to Point Protocol allows a computer to use a regular phone line and modem to make TCP/IP connections to the Internet.

proxy

A computer (or the software that runs on it) that acts as a barrier between a network and the Internet by presenting only a single network address to external sites. By acting as a go-between representing all internal computers, the proxy protects network identities while still providing access to the Internet. *See also* proxy server.

proxy server

A firewall component that manages Internet traffic to and from a local area network (LAN). A proxy server can improve performance by supplying frequently requested data, such as a popular Web page, and can filter and discard requests that the owner does not consider appropriate, such as requests for unauthorized access to proprietary files.

S**server**

A computer or software that provides specific services to software running on other computers. The "mail server" at your ISP is software that handles all of the incoming and outgoing mail for all of your ISP's users. A server on a LAN is hardware that constitutes the primary node on the network. It can also have software that provides specific services, data or other capabilities to all of the client computers attached to it.

SLIP

Serial Line Internet Protocol used to connect a computer to the Internet by way of a phone line. PPP is replacing SLIP because it is more efficient.

SMTP

Simple Mail Transfer Protocol is a set of rules governing the sending and receiving of email on the Internet.

SNMP

Simple Network Management Protocol is a set of standards governing communication with devices connected to a TCP/IP network. This communication takes the form of Protocol Data Units (PDUs).

SSL

Secure Sockets Layer, a protocol created by Netscape Communications to enable encrypted, secure communications across the Internet. Internet banking, securities and e-commerce sites commonly use SSL.

T

TCP/IP

Transmission Control Protocol/Internet Protocol, the protocols that make the Internet possible and that make it possible for your computer to be part of the Internet.

top-level domain

Top-level domains (TLDs) are the most common domain name extensions. The most familiar of these is the ubiquitous "dot com" but there are others in common usage:

- .com (US Commercial)
- .edu (US Educational)
- .gov (US Government)
- .int (International)
- .mil (US Military)
- .net (Network)
- .org (Non-Profit Organization)

Trojan Horse

A type of computer worm or virus that comes to you disguised as a desirable program. The name is based on the famous Trojan Horse that was left outside the walls of Troy by a departing army that appeared to have given up its plans of conquest. The horse, which concealed a band of soldiers, was brought into the walled city by its unwary inhabitants. The soldiers opened the gates of the city in the middle of the night and Troy was destroyed by the returning troops.

U

UDP

User Datagram Protocol. UDP converts data messages generated by an application into packets to be sent via IP.

URL

Uniform Resource Locator, the standard format for Internet addresses.

USENET

More commonly called Newsgroups, USENET is a decentralized worldwide community made up of almost 20,000 discussion groups covering almost every conceivable area of interest. Rule of thumb: don't accept software from someone you meet in a newsgroup or chat room!

V

Visual Trace

Powerful geographical Internet tracing program. Visual Trace uses a proprietary database system maintained by McAfee.com to determine and provide location information on routes and IP addresses.

VPN

Virtual Private Network. A network that makes use of the Internet to connect computers that are in different locations. Communication is encrypted for security.

W

WAN

Wide Area Network, a network of computers that covers an area larger than a single building or campus. In the past WANs have been private networks connecting geographically separated offices of the same organization. WANs are rapidly being replaced by the Internet and the wide use of VPNs.

WWW

The World Wide Web or just "The Web." Many people think of this in terms of what is accessible to their browser but in reality the web now encompasses all of the resources that make up the Internet including such things as FTP sites, USENET, and much more.

Index

ActiveX controls	35	understanding	16-18
alerts	23	viewing archived Event Logs	22
Application Has Been Modified	25	finger	36
Application Requests Internet Access.....	24	firewall.....	36
Application Requests Server Access.....	25	Frequently Asked Questions	31-34
Connection Attempt Blocked	23	FTP.....	36
New Application Allowed	26	getting started	2-3
application recommendations.....	5	glossary	35-41
ARP.....	35	HackerWatch.org	
Banned IPs list.....	10	advice	20
adding an IP address	10	reporting an event to.....	20
removing an IP address.....	10	signing up.....	20
banning an IP address	21	Help! My computer has been hacked!	26
BPS.....	35	hit	36
browser	35	HTTP.....	36
configuring		ICMP.....	6, 37
Internet Explorer.....	28-30	installing Personal Firewall	2
Personal Firewall	4-13	Internet	37
cookie	35	Internet applications	
country code	35	about	15
DHCP	35	changing applications	16
DNS	35	changing permissions	15
domain name	36	Internet Explorer	
domain name system.....	35	configuring version 5.x	29
downloading Personal Firewall.....	2	configuring version 6.x	30
DSL.....	36	intranet.....	37
email.....	36	IP addresses	
Event Log		about	17
about	16-18	banning	21
managing.....	18-19	trusting	21
viewing.....	19	IP number	37
events		ISDN	37
about	16-18	ISP	37
archiving the Event Log.....	21	LAN	37
clearing the Event Log.....	22	logging events.....	6
copying.....	22	McAfee.com SecurityCenter.....	3
deleting	22	Microsoft Internet Explorer.....	29
exporting	22	MIME	38
from 0.0.0.0	17	modem	38
from 127.0.0.1.....	17	NAT	38
from computers on your LAN.....	18	network.....	38
from private IP addresses.....	18	new features.....	1
HackerWatch.org advice	20	node	38
logging	6	options	
loopback	17	configuring.....	4-13
more information	19-20	General tab.....	6-9
reporting.....	20	inbound events	7
responding to	20	animating alerts	8
showing	19	auto-hiding alerts	7
all	19	showing port numbers.....	7
from one address.....	19	Trusted Security alerts	8
one day's	19	visual trace	
this week's	19	clear caches.....	9
today's.....	19	home location	8
with same event info.....	19	program.....	8
tracing.....	20	sound effects	9

Security tab.....	4–6	system requirements.....	1
application recommendations	5	System Services list.....	12–13
event logging	6	TCP/IP	40
ICMP traffic.....	6	testing Personal Firewall	3
security level	5	top-level domain.....	40
packet switching	38	tracing an event	20
password	38	Trojan Horse	34, 40
Personal Firewall		troubleshooting	27
installing	2	‘Track an Attack’ error messages.....	28
opening	14	configuring Internet Explorer	29
testing	3	Help! My computer has been hacked!	27
uninstalling.....	34	installation in Windows 2000	28
updating	13	open NetBIOS port.....	27
using	14–26	unknown event type code.....	28
PING	39	Trusted IPs list	11
port	39	adding an IP address	11
PPP	39	removing an IP address	11
proxy	39	trust all computers on the LAN	12
proxy server.....	39	trusting an IP address	21
reporting an event.....	20	UDP	40
security level.....	5	uninstalling	
server	39	other firewalls	2
setting your home location		Personal Firewall.....	34
advanced	8	updates.....	13
basic	8	URL	40
showing events in the Event Log	19	USENET.....	40
SLIP.....	39	Visual Trace	20, 40
SMTP.....	39	VPN	40
SNMP	39	WAN	41
SSL.....	39	WWW.....	41
Summary page	14		