McAfee.com Personal Firewall

User Guide

Table of Contents

Installing Personal Firewall

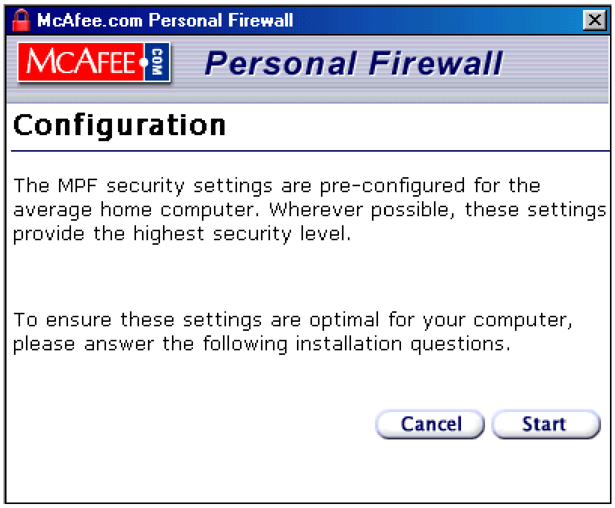
To install Personal Firewall on your computer, follow these instructions:

1. If this is your first time installing McAfee.com Personal Firewall, a Security Warning window may appear asking you if you want to install and run "McAfee.com Installer Control"… Click **Yes**. A second Security Warning may appear. Click **Yes** to proceed.
2. The Personal Firewall installation window will appear. Click the **Start Installation** button to install Personal Firewall, or click the **Reinstall McAfee.com Personal Firewall** link to reinstall Personal Firewall if necessary.
3. The Progress window will appear showing you the status of the Personal Firewall installation.
4. After the installation is complete, a series of Configuration windows with a question on each one will appear to help you configure Personal Firewall to best suit your computer's security needs.

Configuring Personal Firewall and Completing the Installation

Configuring Personal Firewall

1. Click **Start** in the first Configuration window (see Figure 1) to begin the installation questions.



Configuration

The MPF security settings are pre-configured for the average home computer. Wherever possible, these settings provide the highest security level.

To ensure these settings are optimal for your computer, please answer the following installation questions.

Figure 1

2. The first question asks if you want to allow other users to access your files and printer
   1. Select the check box next to **Yes, allow others to access my files** if you want to allow other users to access your files or to print on your printer.

   Note: You must be on a network to select this option. If you are not on a network, or if you are unsure, do not select the option.

   2. Click **Next** to continue.

3. The next question asks if you use DSL or a cable modem to connect to the Internet.
   1. Select the check box next to **Yes, I use DSL or a cable modem** if you use DSL or a cable modem to connect to the Internet**.** If you do not use DSL or a cable modem, do not select this option.
   2. Click **Next** to continue.

   Note: If you are working in an office environment, do not click Yes unless you know you use DSL or a cable modem. If you are unsure, please consult your network administrator.

4. The next window asks if you are connected to a Local Area Network (LAN) and/or a network printer.
   1. Select the check box next to **Yes, I am connected to a LAN** and/or a network printer.

      Note: If you are not connected to a LAN, or if you are unsure, do not select this option.

   2. Click **Next** to continue.

5. The next window asks if you want to protect your Personal Firewall settings with a password.
   1. Select the check box next to **Yes, I want a password** if you want to protect your settings with a password. If you do not want a password, just leave the check box clear, click next, and proceed to Step 6.
   2. Click **Next** to set your password.

   Note: If you select this option, you will be required to enter your password each time you attempt to change the settings on Personal Firewall.

   3. Enter your password in the **Enter Password** text box.
   4. Reenter your password in the **Confirm Password** text box. Your password can consist of letters and/or numbers and can be up to 50 characters.
   5. Click **Next** when you are finished entering and confirming your password.

6. Click **Reboot** on the installation progress window to restart your computer **if you are not using Windows NT**. If you are using Windows NT, please follow these instructions:

   Windows NT users: please install the Personal Firewall driver by doing the following:
   1. Open the Control Panel by clicking **Start,** selecting **Settings**, and then clicking **Control Panel.**
   2. Double-click **Network.**
   3. Click the **Services** tab.
   4. Click **Add.**
   5. Click **Have Disk.**
   6. Enter **"c:\program files\mcafee.com\mpf\drivers"** in the text box and click **OK.**
   7. Click **OK** again. If the driver is installed properly, it will appear in the **Network Services** list.
   8. Click **Close.**
   9. When you are prompted by Windows NT to reboot, click **No.**
   10. Close the Control Panel window.
   11. Click **Reboot** on the Personal Firewall Installer Progress window. Your computer will restart.

McAfee.com Services

If you are installing a McAfee.com product for the first time, the McAfee.com Services window will appear.

This window will prompt you to set a time for Services to periodically check for updates, alerts, and information.

Enter a time that you will be connected to the Internet, and click **OK.** You will not be allowed to continue until you set a time.

There will also be a small yellow padlock icon in the Windows status area near the clock (see Figure 2).

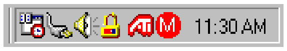


Figure 2

This icon opens the **McAfee.com Agent**, also referred to as **Agent**.

To use the Agent:

1. Right-click the Agent icon.
2. Select an application from the list of McAfee.com applications. A list of options for that application will appear (see Figure 3).
3. Select the option that you want and click it.

Note: This is where you open the Personal Firewall window.

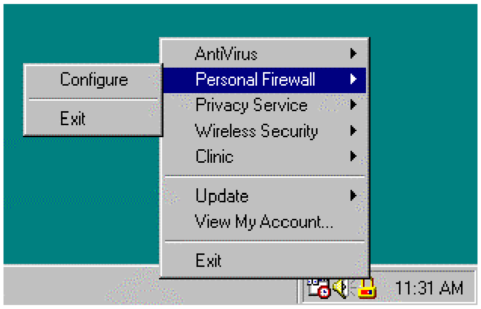


Figure 3

To make any changes in the Personal Firewall settings:

1. Right-click the Agent icon.
2. Select **Personal Firewall**.
3. Click **Configure**. This will open the Personal Firewall Status window.

You can exit Personal Firewall here as well (not recommended while you are connected to the Internet or a network) by clicking the exit option shown in Figure 3.

To start Personal Firewall again:

1. Right-click the Agent icon.
2. Select **Personal Firewall**.
3. Click **Run**.

If the application that you select is not installed, the option to install it is offered.

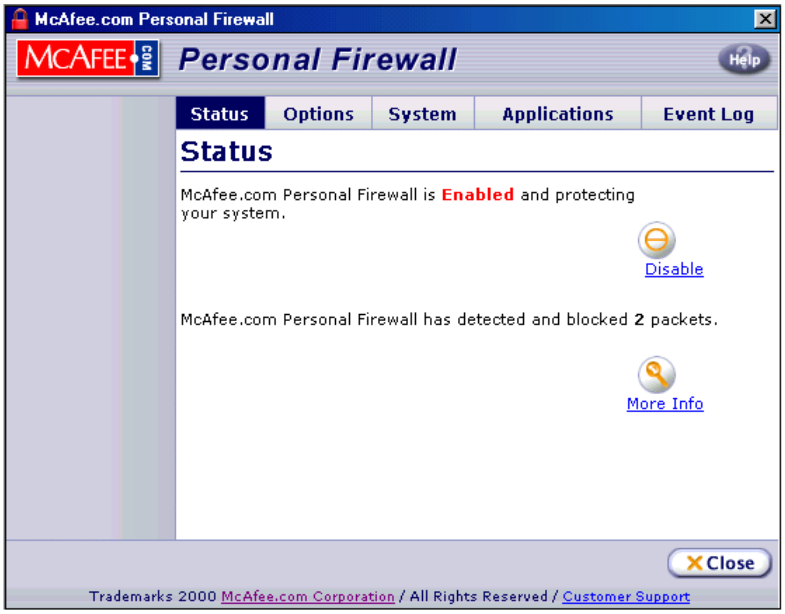
Note: If you do not have a subscription to the application that you want to install, you must buy a subscription to the application before you use it. If you already have a subscription to the application, click **Install** and follow the installation instructions for the application.

The Status Window

The Status window (see Figure 4) tells you whether Personal Firewall is enabled or disabled, and it tells you how many packets Personal Firewall has blocked.

This is the first Personal Firewall window you will see when you click **Configure** in the Agent.

Use the tabs toward the top of the window to navigate through the features in Personal Firewall.



Status

McAfee.com Personal Firewall is **Enabled** and protecting your system.

McAfee.com Personal Firewall has detected and blocked **2** packets.

Trademarks 2000 McAfee.com Corporation / All Rights Reserved / Customer Support

Figure 4

Enabling and Disabling Personal Firewall

This feature allows you to enable and disable Personal Firewall without exiting the application.

1. Click **Disable** on the Status window to disable Personal Firewall (see Figure 4). Note the **Enable** button replaced the **Disable** button.
2. Click **Enable** to enable Personal Firewall. The **Disable** button will replace the **Enable** button.

Note: Your system will not be protected if you disable Personal Firewall.

Blocked Packets

Personal Firewall monitors Internet and network traffic, which consists of small pieces of information called packets, and allows traffic that is intended for trusted applications such as your Internet browser. Personal Firewall blocks any network traffic not intended for trusted applications.

Personal Firewall tracks and displays the number of packets it blocks in the Status window.

Personal Firewall also logs the packets that it blocks to a log file on your computer's hard drive. You can view the logs in the Event Log in Personal Firewall.

Note: Seeing any number of blocked packets on the blocked packet counter does not necessarily mean that someone has tried to hack into your computer. Personal Firewall blocks packets that are not needed for your computer to operate properly.

The Options Window

Filter Level

This allows you to tell Personal Firewall how to treat all of the traffic coming into your computer.

To set the Filter Level:

1. Open Personal Firewall by right clicking the Agent icon, selecting **Personal Firewall** and then clicking **Configure**.
2. Click **Options**.
3. Click **Filter Level**.
4. Select one of the following settings:
   - The default level is **Filter Everything.** This will tell Personal Firewall to check all incoming traffic and block all unknown traffic. Personal Firewall then records the blocked traffic in your log file. You can view your log file in the Event Log.
   - If you choose **Block Everything,** all data will be blocked, making your computer seem like it is not on a network. This is useful when you are leaving your computer unattended and do not need it to send or receive any information. Personal Firewall will not log blocked traffic while using this setting.
   - If you choose **Allow Everything,** all data will be allowed. Personal Firewall will not stop any data and will not log traffic it does not recognize.
     Note: This is not recommended unless you are disconnected from your network or Internet connection.
5. Click **Save** to save your settings.

Incoming Fragments

Personal Firewall blocks fragmented packets by default. Hackers can use fragmented packets to crash computers. If you have an application that does not work unless fragmented packets are allowed, then you should allow them; otherwise, block them.

To block incoming fragments:

1. Open Personal Firewall by right clicking the Agent icon, selecting **Personal Firewall** and then clicking **Configure**.
2. When the Personal Firewall window opens, click **Options**.
3. Click **Incoming Fragments**.
4. Select the check box next to **Block Incoming Fragments**.
5. Click **Save** to save your settings.

Note: This setting does not apply to the IP protocols selected under the Operating System-IP Protocols window of Personal Firewall.

Unknown Traffic

When Personal Firewall is set to **Filter Everything** in the Filter Level window, it monitors what applications send and receive information, and it blocks unexpected traffic. When you choose to log unknown traffic, the log entries are saved in log files so you have a record of events if you experience a serious attack. These records may be helpful during an investigation.

To log unknown traffic:

1. Open Personal Firewall by right clicking the Agent icon, selecting **Personal Firewall** and then clicking **Configure**.
2. Select the check box next to **Log Unknown Traffic**.
3. Click **Save** to save your settings.

To view your log files, please see the section of this manual regarding the Event Log feature of Personal Firewall.

Protect Option

This feature protects the options on Personal Firewall from being changed without your knowledge. This is useful in cases when others have access to your system, or when you share your files with others over a network. To enable this feature:

1. Open Personal Firewall by right clicking the Agent icon, selecting **Personal Firewall** and then clicking **Configure**.
2. When the Personal Firewall window opens, click **Options**, and then select **Protect Option.**
3. Select **Use Password Protection.**
4. Enter a new password in the **New Password** box.
5. Confirm your password by reentering your password in the **Confirm Password** box.
6. Click **Save** to save your settings.

Note: It is important to keep your password secret, and it is equally important to remember your password because you will no longer be able to change the Personal Firewall settings.

System

In the System window, you can tell Personal Firewall what operating system traffic to allow for each network device (many computers have more than one). Personal Firewall detects the network device(s) in your computer and displays them in a list in the **Select Adapter** window.

To change settings on a network device, do the following:

1. Select a network device by clicking it. The network device will be highlighted when it is selected.
2. Click **Edit.** Several tabs representing different network protocols will appear on the left of the Personal Firewall window. Click the protocol you want to configure and follow the instructions in the window.

The following is a look at the various network protocol windows, along with a brief description of each protocol:

NetBIOS over TCP

NetBIOS is the protocol your computer uses to communicate over a network such as one in most offices.

Since you can allow or block NetBIOS for each network device on your computer, you can allow NetBIOS to work on your office network device while blocking it on a modem at your home.

1. Select **Allow network login and access to other systems' file and print shares** if you connect to a network to send e-mail and use the Internet, and/or if you use a network printer.
2. Select **Allow other systems to access my file and print shares** if you share your files over a network.
3. Click **Save** to save your settings.

Important: If you are not connected to a network, or if you are unsure, do not choose these options. This is important because if NetBIOS is allowed to connect outside a network, your computer will become vulnerable to attack by hackers. If you are in an office and are unsure whether you should select any of the NetBIOS options, consult your network administrator.

Note: If you answered **Yes, I am connected to the network** during the configuration, then **Allow network login and access to other systems' file and print shares** should already be allowed. If not, select it now.

Note: If you answered **Yes, allow others to access my files** during the configuration, then **Allow other systems to access my file and print shares** should already be allowed. If not, select it now.

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. For example, a hacker could disable a computer that performs critical network tasks by flooding (overloading) the computer with ICMP packets. Then the hacker can make other packets that redirect Internet or network traffic to his or her computer.

A hacker can get privileged information such as account numbers, credit card numbers, and other information by exploiting ICMP. Thankfully, ICMP is usually not necessary for the desktop/laptop computer user, and it can be blocked without causing problems. For this and similar reasons, Personal Firewall blocks ICMP by default.

Some Internet service providers (ISP) send ICMP packets to your computer to see if you are connected. (This is called pinging.) If your computer acknowledges the ping, then the ISP knows you are connected.

If your ISP uses this technique, ICMP should be allowed or limited. If your computer works properly with ICMP blocked, leave it that way. If not, try limiting it to 2 packets per second.

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 e-mail 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 e-mail, the Internet, nor can you print on a network printer.

Personal Firewall allows ARP by default. You should always allow ARP unless you want to block all communication between your computer and the network and unless you know your computer will operate properly with it blocked.

DHCP

DHCP stands for Dynamic Host Configuration Protocol. It is a protocol used on many networks to assign IP addresses to computers automatically (dynamic IP address). Every computer on a network needs an IP address so it can log in to the network, get e-mail, and connect to the Internet. Dynamic IP addresses are used mainly because it is easier to assign IP addresses to computers automatically, and because the number of users may exceed the number of available IP addresses. With dynamic IP addresses, only the users who are in the office and logged on to the network will have IP addresses; the rest will not, thus conserving available IP addresses.

A hacker can take advantage of DHCP by hacking into a network through a connected computer and disabling the DHCP server. Then the hacker can impersonate the disabled DHCP server and have access to virtually the entire network.

Personal Firewall allows DHCP by default. However, if you use a modem over regular phone lines to connect to the Internet instead of connecting to the office's network, or if your computer has a static IP address (a permanent IP address) assigned to it, you can block DHCP.

RIP

RIP stands for Routing Information Protocol. It is used to send information about how computers should route network traffic. Unfortunately, it can also be used to interfere with communications.

Most Windows computers don't use RIP, so Personal Firewall blocks it by default. If your network uses RIP, you should allow it by selecting **Allow RIP.** If you are in an office and you don’t know if you should allow RIP, contact your network administrator.

PPTP

PPTP stands for Point-to-Point Tunneling Protocol. It is a protocol used by Windows to encrypt data packets, such as those in a Virtual Private Network (VPN). A VPN allows a company to allow its remote employees (at home, in a hotel, a remote office, etc.) to connect over public telephone lines, with as much security as an actual network. A company without a VPN may have to lease telephone lines if they want to have remote users to their network.

Thanks to PPTP, companies can use VPNs over public lines to achieve the same result. If your computer connects to your office or some other location over a VPN, you should allow PPTP by selecting **Allow PPTP.** Most people don't use PPTP, so Personal Firewall blocks by default. To determine if your computer uses PPTP, contact your network administrator.

IP Protocols

If your computer uses a VPN to access a network through the Internet, you may have to allow one of the many IP protocols. You may also have to allow fragments for some IP protocols if you are unable to access the Internet when they are blocked. See your network administrator about allowing any of these protocols.

Others

If you have a DSL connection and/or use PPPoE (Point to Point Protocol over Ethernet) to connect to your Internet service provider (ISP), select **Allow Other Protocols**.

Note: If you selected the check box next to **Yes, I use DSL or a cable modem** in step 3 of the configuration, then **Allow Other Protocols** should already be selected. If not, you can select it now.

Your computer may use a protocol other than standard IP protocols while you are in an office. Two of the most common are NetBEUI and IPX. If you use these or other protocols not covered elsewhere in Personal Firewall, then select **Allow Other Protocols**. If you are not sure whether you should use this option, ask your network administrator.

If you are sure you do not need to allow other protocols, clear the check box to disable this option.

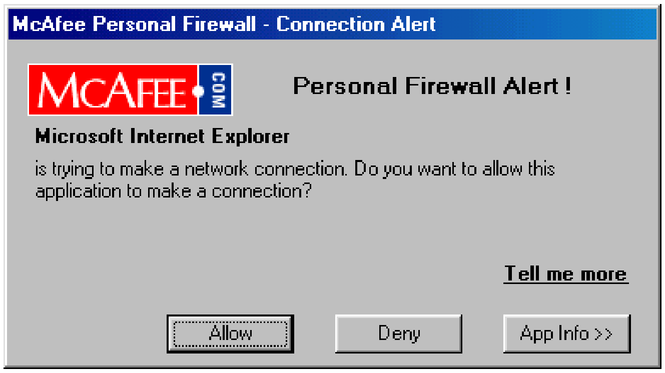
Allow/Deny Applications

While you use Personal Firewall, a window will occasionally appear telling you a certain application is trying to make a network connection (see Figure 5). It will ask you if you want to allow the connection. In most cases, you need to allow the application to connect.

Click **Allow** to allow the application to connect.

There are also cases where you may not recognize the application that is trying to connect.

Click **Deny** if you do not recognize the application.



McAfee Personal Firewall - Connection Alert

Personal Firewall Alert !

Microsoft Internet Explorer

is trying to make a network connection. Do you want to allow this application to make a connection?

Figure 5

If all your applications still work, then the denied application may be a Trojan, or it is an application that did not need to connect to the network to work properly. If this happens, it is a good idea to scan your computer with the latest virus protection from McAfee.com to remove any Trojan programs from your computer.

If you clicked **Deny** and one of your applications stopped working properly, then that application needed to connect to the network. To allow the application to connect:

1. Open Personal Firewall by right-clicking the Agent icon, selecting **Personal Firewall** and then clicking **Configure**.
2. When the Personal Firewall window opens, click **Applications**.
3. Find the application you just denied. A cleared check box next to the application name below the list denotes a denied application.
4. Select the check box next to the application.
5. Click **Save**.
6. Click **Close** if you are done making changes.

There are some circumstances when you will be asked to allow or deny an application that you already allowed. See **Application Alerts** to learn more.

Note: Personal Firewall gives you the option to tell it to trust all applications trying to connect to your computer. Please be aware that selecting **Trust all applications** allows any application to make a network connection to your computer, and Personal Firewall will not inform you when an application connects.

Application Alerts

When you allow an application, Personal Firewall creates a unique identity, or signature, for each application. When the application tries to connect to the network at a later time, Personal Firewall will automatically allow it if it matches the signature. If the application does not match the signature, Personal Firewall will prompt you to allow or deny the application.

Note: **GenSock.exe** and **Microsoft Windows** are used as examples.

Network Connection Attempt

GenSock.exe is trying to make a network connection. Do you want to allow this application to make a connection?

Click **Allow** if you are certain the application listed above should connect to the network.

Click **Deny** if you are unsure about the safety of this application.

Some computer applications use network connections to run correctly. Unfortunately, malicious applications can also use network connections to steal passwords or allow remote access to your computer.

To prevent malicious applications from connecting to the network, Personal Firewall prompts you each time a new application tries to connect. When you allow an application to connect, Personal Firewall creates a unique application identity, or signature.

If this application tries connecting to the network again and has the same signature, Personal Firewall will automatically allow a connection. If the application has changed, Personal Firewall will prompt you to allow or deny it.

Application has Changed

GenSock.exe is trying to make a network connection. This application has changed since you last allowed the application to connect. Do you want to allow this application to make a connection?

The unique identity signature Personal Firewall created for this application does not match the application's present identity. This often happens when you update or upgrade an application.

Click **Allow** if the application listed is this window is one you trust to connect to the network. When a component does not match its signature, it could be a sign that the component has been tampered with.

Click **Deny** if you are unsure about the safety of this application. Use the "advanced search" at http://vil.mcafee.com to learn more about malicious programs associated with the above application.

Application or its Location has Changed

GenSock.exe is trying to make a network connection. This application or its location has changed since you last allowed the application to connect. Do you want to allow this application to make a connection?

When you last allowed this application to connect to the network, Personal Firewall created a unique identity signature for the application based on its properties and location. Both the properties and the location of the present application are different from the one you previously allowed.

Often, malicious computer programs called Trojan horses, or Trojans, will pretend to be an allowed application by using the same name but reside in a different folder.
If you have not moved the location of this application, you should:

1. Click **Deny**.
2. Scan your computer for Trojans using an "on-demand" scanner such as McAfee.com Scan.

Use the "advanced search" at http://vil.mcafee.com to learn more about malicious programs associated with the above application.

Operating System Component is Different from the Expected Component

Microsoft Windows is trying to make a network connection. This operating system component is different from the expected component. Do you want to allow this component to make a connection?

Many applications use your computer's operating system (Windows 98, NT, 2000, etc.) to help make network connections. Personal Firewall previously created a unique identity signature for the component listed above; this signature is not the same as the one used by the component now. This often happens when you update or upgrade your operating system.

When a component does not match its signature, it could be a sign that the component has been tampered with.

Click **Allow** if you have recently updated or upgraded your operating system, or you are certain the component above should be allowed to connect to the network.

Click **Deny** if you are unsure about the safety of this component.
Use the "advanced search" at http://vil.mcafee.com to learn more about malicious programs associated with the above component.

Operating System Component Trying to Connect

Microsoft Windows is trying to make a network connection. It is an operating system component. Do you want to allow this component to make a connection?

Many applications use your computer's operating system (Windows 98, NT, 2000, etc.) to help make network connections. When the component above first connected to the network, Personal Firewall created a unique identity signature for it and stores the information in a small database.

This database has been tampered with. As a result, Personal Firewall has erased all the signatures and must recreate the database.

Click **Allow** if you are certain that the listed component is safe.

Click **Deny** if you are unsure about the safety of this component.

Use the "advanced search" at http://vil.mcafee.com to learn more about malicious programs associated with the above application.

Operating System Component or its Location has Changed

Microsoft Windows is trying to make a network connection. This operating system component or its location has changed since you last allowed it to connect. Do you want to allow this component to make a connection?

When the component above first connected to the network, Personal Firewall created a unique identity signature for it based on its properties and location. Both the properties and the location of the present component are different from this identity signature.

Malicious computer programs called Trojan horses, or Trojans, can pretend to be allowed components by using the same name as an allowed component but reside in a different folder. If you have not moved the location of this component, you should:

1. Click **Deny**.
2. Scan your computer for Trojans using an "on-demand" scanner such as McAfee.com Scan.

Use the "advanced search" at http://vil.mcafee.com to learn more about malicious programs associated with the above application.

The Location of this Operating System Component is Different from what Personal Firewall Expected

Microsoft Windows is trying to make a network connection. The location of this operating system component is different from what Personal Firewall expected. Do you want to allow this component to make a connection?

When an operating system component first tries to connect to the network, Personal Firewall checks the component's location. If this location is the same as Personal Firewall expects, Personal Firewall allows the connection. If the location is different, Personal Firewall prompts you to allow or deny the connection.

Malicious computer programs called Trojan horses, or Trojans, can pretend to be allowed components by using the same name as an allowed component but reside in a different folder. Personal Firewall expected this component in a different location.

Click **Allow** if you have moved this component or if you trust it.

If allowed, Personal Firewall will note the component's location and will not prompt you again unless the component is changed or moved.

1. Click **Deny** if you do not trust this component.
2. Scan your computer for Trojans using an "on-demand" scanner such as McAfee.com Scan.

Use the "advanced search" at http://vil.mcafee.com to learn more about malicious programs associated with the above application.

Event Log

Log files can be viewed in two ways. The simplest way is to use the Event Log. This is good for when you want to take a quick look at what Personal Firewall is doing. The other way is by going to the location on your computer's hard drive where the log files are stored. This is good for when you need to send the log files to another person, such as an IT professional, if you suspect a hacker tried to get into your computer.

Viewing the Event Log

1. Open Personal Firewall by right clicking the Agent icon, selecting **Personal Firewall** and then clicking **Configure**.
2. When the Personal Firewall window opens, click **Event Log**.
3. In the Event Log window, select the day of the week the log file was created from the **All Days** menu. If needed, select **All Days** to display the log files for up to the past seven days (present day included).

   Note: Personal Firewall only keeps the logs for any given day for a week before the log is overwritten. For example, a log recorded on a Monday can only be viewed until the following Sunday at 11:59 P.M. After midnight on Monday, the log file will be overwritten with a new log file.

4. Select the type of information you are looking for in the **All Entries** menu and click **Start**. The log entries you specified will be displayed.
5. Click the individual entry to view the log description of each entry. The description will be displayed toward the bottom of the window.

The following are the types of entries you can retrieve from the Event Log for a certain day or for all days:

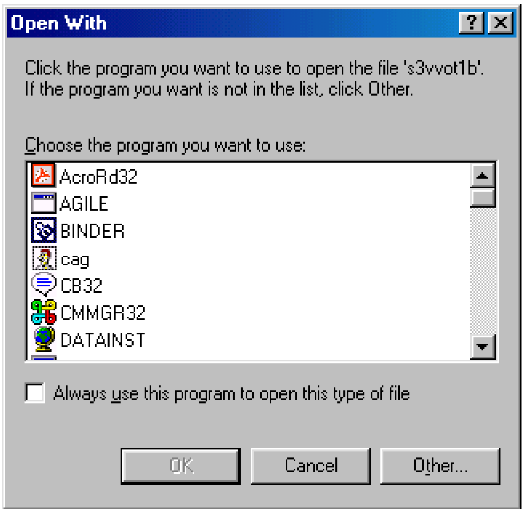
- **All Entries** – Displays all log file entries.
- **Information** – Displays log file entries for a wide range of activities such as configuration changes, setting information and blocked Internet or network traffic.
- **Warning** – Displays log file entries regarding errors between your computer's operating system, software and Personal Firewall.
- **Error** – Displays log file entries regarding errors with Personal Firewall. These files are useful for troubleshooting problems with Personal Firewall.
- **Unknown** – Displays log file entries regarding unknown Internet or network traffic Personal Firewall blocked.

6. Click **Close** when you are finished viewing the log files.

Viewing the Log Files on the Hard Drive

The preferred method of viewing the log files is with the Event Log. However, you may have to access your log files from their location on your computer's hard drive. If this need arises, perform the following steps:

1. Exit Personal Firewall by right-clicking the Agent icon, select **Personal Firewall** and then click **Exit.**
2. Double-click **My Computer** on the Windows desktop.
3. Double-click the drive letter where you loaded Personal Firewall. For most people, this is drive C.
4. Double-click **Program Files.**
5. Double-click **mcafee.com.**
6. Double-click **mpf,** and then double-click **logs.**
7. Double-click the log file for the day of the week you need to view. You may see a message similar to the one in Figure 6. Select either **NotePad** or **WordPad** from the list and click **OK.** The log file will open for you to view or to send to someone else.
8. When you are done viewing the log file, make sure you start Personal Firewall again.



Open With

Click the program you want to use to open the file 's3vvot1b'.
If the program you want is not in the list, click Other.

Choose the program you want to use:

☐ Always use this program to open this type of file

Figure 6

Uninstalling Personal Firewall

Windows 95, 98, 2000 and Me

1. Exit Personal Firewall by right-clicking the Agent icon in the system tray, selecting **Personal Firewall** and then clicking **Exit.**
2. Click **Start,** select **Programs**, select **McAfee.com Personal Firewall** and then click **Uninstall McAfee.com Personal Firewall.**
3. The message "Are you sure you want to uninstall McAfee.com Personal Firewall?" will appear. Click **Yes.**
4. Click **Reboot** on the Personal Firewall Uninstall window when you are prompted to do so.

Note: To finish uninstalling Personal Firewall, you must reboot your computer.

Windows NT 4.0

1. First, you must exit Personal Firewall by right clicking the Agent Icon in the system tray, selecting **Personal Firewall**, and clicking **Exit.**
2. Click the **Start** button and select **Programs**, select **McAfee.com Personal Firewall** and click **Uninstall Personal Firewall.**
3. The message, "Are you sure you want to uninstall McAfee.com Personal Firewall?" will appear. Click **Yes.**
4. A message will appear telling you to uninstall the Personal Firewall driver. Do so by following these steps:
    1. Open the Control Panel by clicking **Start**, selecting **Settings** and clicking **Control Panel.**
    2. Double-click **Network.**
    3. Click the **Services** tab.
    4. Select **McAfee.com Personal Firewall driver.**
    5. Click **Remove.**
    6. A warning message stating "This action will permanently remove the component from the system. If you wish to reinstall it, you will have to restart the system before doing so. Do you still wish to continue?" Click **Yes**. This will remove the driver.
    7. Click the **Close** button on the Network window.
    8. Another message will appear telling you "You must shut down and restart your computer before the new settings will take effect. Do you want to restart your computer now?" Click **No**.
5. Click **Reboot** on the Personal Firewall Uninstall window to restart your computer and finish the uninstallation.

Glossary

Application – Performs a specific task for the user or for another application. In this manual, program and application are interchangeable terms.

DSL (Digital Subscriber Line) – A type of high-speed Internet connection that is delivered to homes or small businesses over regular telephone lines.

Cable Modem – A modem that sends and receives data through a cable television network instead of telephone lines, as with a conventional modem or DSL.

Log file – A file that contains important information about an application(s) and what it has done.

Network; Local Area Network (LAN) – An environment in which two or more computers and other devices (printers, copiers, etc.) share a common communications line and are all connected to a server. This environment is commonly found in an office setting.

Operating System – Manages all aspects of your computer, attached hardware (monitor, mouse, keyboard, etc.) and applications. Ex. Windows 98, Windows NT, etc.

Packet – A unit of data that, combined with other packets, make up a file sent over the Internet. Files are broken down by the TCP protocol into packets, sent over the Internet and are reassembled by TCP at the recipient's computer.

Server – A server allows users to share files with other users and as a place to store files. The server also performs other functions, such as a place to put e-mail messages until a user logs in to retrieve them.

Trojan (Trojan horse) – A destructive program disguised as a game, utility, or application. When run, a Trojan does something harmful to the computer system while appearing to do something useful.

Trusted Applications – In Personal Firewall, applications known to the user and Personal Firewall to be safe that are allowed to make Internet connections on a user's computer. These applications are necessary to perform necessary tasks on your computer.