PRODUCT GUIDE

McAfee Internet Security

VERSION 5.0

McAfee SECURITY

Contents

Welcome to McAfee Internet Security 5.0

1

The Internet provides a vast wealth of information and entertainment at your fingertips. Yet, as soon as you connect, your computer is exposed to a multitude of privacy and security threats. Protect your privacy and secure your computer and your data with McAfee Internet Security. Incorporating McAfee's award-winning technologies, McAfee Internet Security provides one of the most comprehensive sets of privacy and security tools you can buy. McAfee Internet Security destroys viruses, outwits hackers, secures your personal information, privatizes your Web browsing, blocks ads and pop ups, manages your cookies and passwords, locks down your files, folders and drives, filters objectionable content, and puts you in control of the communications in and out of your PC. McAfee Internet Security provides powerful protection for today's Internet users.

Introduction

In the last few years the Internet has changed from a communications network that government entities and universities used almost exclusively, to an information treasure house that people of all ages and occupations can now access. With an Internet account, you can send electronic mail (e-mail) around the world in seconds, do research without leaving home, meet new friends in an online chat room, or shop without getting out of your bathrobe. However, with all these conveniences come a certain element of risk. When you use the Internet, information is transmitted from your computer to other computers on the Internet – information you may not want other people to have. And those computers can also send files to your computer that may contain viruses. While most of these files are harmless, some can invade your privacy or even damage the data on your computer’s hard drive.

McAfee Internet Security addresses any of these potential risks with its comprehensive features designed to protect your privacy and security when using the Internet.

With its new features, you can now also act as an Administrator and apply customized protection settings not only for yourself, but for other users of your computer and easily monitor potential risks they may encounter while browsing the Internet.

What's included with McAfee Internet Security?

- The Administrator: As the Administrator, you are able to set up protection settings for other users of your computer. You can add, edit and delete a user's profile—then setup individual privacy, security and Internet filtering options that McAfee Internet Security will apply whenever any of these users are browsing the Web through your computer.
- Activity Logs: Activity Logs allow you to view a list of all the interactions that you and other profiled users of your computer had with McAfee Internet Security, including the date and time of the activity. You can print, save or clear this list.
- Security Check: You can run an extensive check of your computer for any privacy or security problems via this feature. After McAfee Internet Security performs the check, it displays any problem found, provides additional information about the problem, and guides you through on how to solve the problem.
- VirusScan: McAfee Internet Security uses McAfee VirusScan to address virus-related problems you may encounter through the Internet. This feature allows you to set how to perform a virus scan operation on your computer; what to do if a virus is found; and how it should alert you once the virus is detected. You can also direct VirusScan to keep a record of actions performed on your computer.
- Firewall: McAfee Internet Security incorporates McAfee Firewall to protect your computer while it is connected to the Internet. McAfee Firewall is a highly-flexible, easy-to-use program. Whether you are connected to the Internet via DSL, cable modem or standard dial-up, Internet communication in to and out of your PC is secure.
- QuickClean Lite: Remove unnecessary files using QuickClean Lite. The QuickClean Lite wizard enables you to clean your computer of unnecessary files and free valuable hard disk space.
- Shredder: For privacy and security reasons, you may want to be positive that the information stored in files you delete is permanently erased from your computer. Shredder does this for you by "security wiping" deleted files so they cannot be restored or rebuilt using an "undelete" type of utility.

What's new in this release?

This release of McAfee Internet Security includes the following new features and functional enhancements.

- **Includes VirusScan Home Edition 7** - Includes the latest version of the award winning VirusScan anti-virus software to protect your system from viruses, Trojans, Internet worms, harmful scripts, and other malware. With automated updates and exclusive H.A.W.K. (Hostile Activity Watch Kernel) protections, VirusScan keeps your computing free of even the latest threats.
- **Includes McAfee Firewall 4** - Includes the latest version of McAfee Firewall. McAfee Firewall enables you to control the communications in and out of your PC and helps keep hackers at bay. With powerful Application Control, Intrusion Detection, and easy Home Networking and Custom Rule Creation Wizards, McAfee Firewall provides essential security for your Internet connection.
- **Spyware/Adware Protection** - Helps enhance your privacy by rooting out snooper programs that attempt to track your Web surfing habits. Now you can easily find and shut down these tracking programs that often piggyback on popular freeware utilities and games.
- **Extended Stealth Program Protection** - Helps keep your PC free of hidden key loggers that try to capture and steal your passwords and a whole host of even more insidious programs that may be watching and recording everything you do on your PC. Adds an essential layer of protection against this growing threat to your privacy and security.
- **Pop-Up Blocker** - Puts an end to those pesky and annoying pop-up ads so prevalent on the Internet. Now you'll be able to surf the Internet without these and other ads getting in your way and slowing you down.
- **Allow/Block Applications Per User** - Lets you to control which applications are available to different family members. Parents can readily use installed programs while blocking access to younger family members, protecting the family PC while restricting access to questionable material.
- **Filtering of Usenet Newsgroups** - Usenet is said to exemplify the best and worst of the Internet. Now you can take charge of which newsgroups and content various family members might be exposed to and filter out objectionable material while retaining access to the wealth of information Usenet provides.
- **MRU Cleaner** - Deletes the telltale trail left behind the files you've opened and viewed recently. Enhances your privacy by clearing MRU's (Most Recently Used) of Windows based utilities and many other popular programs.

- **Usability Enhancements** - McAfee Internet Security 5.0 includes user interface enhancements to make it easier than ever to protect your online security and privacy.

About this manual

This manual provides the basic information you need to install, set up and get started with McAfee Internet Security 5.0. More detailed information about how to perform tasks within McAfee Internet Security is provided via online Help. You can get Help while working with the different windows and dialog boxes.

You can also view the Readme.txt file which contains other general information, known issues, etc., about this product.

McAfee Internet Security and your online connection

You must have an Internet connection through a local network or a modem to use all McAfee Internet Security features. Some networks have an Internet connection that you can use by connecting to the network – either directly or through dial–up networking. Your computer must have a modem installed if you don't connect through a network.

You can establish an Internet connection through an Internet Service Provider (ISP) such as MSN, AOL, or Earthlink, etc. An ISP acts as a middleman between you and the Internet. Your computer connects (using your modem) to the ISP's equipment, which in turn connects your computer to the Internet.

In addition, you must also have a browser. A browser is software, such as Microsoft Internet Explorer or Netscape Navigator, that allows you to view text and graphics and download files from Web sites.

McAfee Internet Security features

This section briefly describes other features of McAfee Internet Security that protect you from the most common Internet threats.

Only the designated administrator or a user with administrative rights can have access to these features which allow them to customize protection settings for themselves and in the case of the Administrator, protection for other profiled users of the same computer.

Protection from privacy threats

- **Identity Protector** monitors your Internet connection and warns you before private information is sent to an nonsecure Internet site. It stops programs and other people that use your computer (like your kids) from sending your name and credit card numbers over the Internet without your approval.
- **Cookie Blocker** prevents Web sites from storing cookies on your hard drive. Third-party Web sites use cookies to track your Web browsing habits. You can choose your level of interaction with Cookie Blocker.
- **Web Trail Cleaner** cleans your Web browsing trails such as cached files; list of URLs (Uniform Resource Locator, also known as Web address) visited; and history files—when you close your browser. This feature prevents other users of your computer from tracking your online movements by viewing the files and URL addresses left over from your Internet browsing.
- **Referer Filter** prevents search information that you request at one Web site from being passed along to the next site you visit. Without Referer Filter, your browser may be allowing the transfer of your search request information from one Web site to another.

Protection from security threats

- **Gatekeeper** allows you to control the programs that have access to your Internet connection. Programs on your PC can be programmed to access to the Internet without your consent.
- **File Guardian** protects files that contain your sensitive data from being opened, renamed, copied, moved, or deleted. Programs, such as ActiveX and Java programs, can scan your PC for personal information or delete files without your permission.

  File Guardian also limits access to protected files either to programs you specify or through file encryption. It can limit the programs that can access your tax, online banking, or personal accounting data files.

- **Password Manager** stores your Web site login names and passwords for protected Web sites in one secure location. When you are visiting a site that requires this information, you can drag it from Browser Buddy to the form displayed in your browser. No more storing your login names and passwords in an nonsecure location, such as post-it notes on your monitor or in a text file on your Windows desktop.
- **Browser Buddy** is convenient tool with a dual purpose. First, Browser Buddy lets you view a summary of cookie activity. Just choose a Web site that you have visited from the drop-down list. Second, Browser Buddy gives you access to the passwords that you have stored in Password Manager. When you log on a password-controlled Web Site, you can drag and drop a user name and password from Browser Buddy to the appropriate box in the login form. To access Browser Buddy, right-click the McAfee Guardian icon in the Windows system tray and click Browser Buddy in the pop-up menu.

Protection from virus threats

Using McAfee VirusScan, the following features are available:

- Scan to start the default virus scan task immediately, or configure a virus scan task that suits your needs.
- Scheduler to launch the McAfee VirusScan Scheduler. This utility enables you to configure and run unattended virus scan operations.
- Virus info to display virus information via the McAfee Web site.

Safeguard your computer against intrusions and attacks

Protect yourself while online with the advanced security of McAfee Firewall. Easy-to-use, yet highly secure, McAfee Firewall safeguards your PC's connection to the Internet whether you connect via DSL, cable modem, or dial-up. McAfee Firewall gives you the powerful tools you need to control the communications into and out of your PC.

Installing McAfee Internet Security 2

Before you begin

McAfee distributes McAfee Internet Security 5.0 in two formats:

1. As an archived file that you can download from the McAfee web site.
2. On CD-ROM.

Although the method you use to transfer files from an archive obtained via download differs from the method you use to transfer files from a CD that is placed in your CD-ROM drive, the installation steps followed after that are the same for both distribution types. Review the system requirements shown below to verify that this software will run on your computer.

System requirements

To install this product, you require the following:

Desktop and notebook computers

- Windows 98, Windows Me, Windows 2000 Professional, Windows XP Home Edition, or Windows XP Professional.
- Internet Explorer 4.01, Service Pack 2 or higher required for Windows NT; IE 5.01 or later recommended.
- 71 megabytes (MB) of hard disk space.
- 32 MB of RAM.
- An Intel Pentium-class or compatible processor rated at 100 MHz or higher.
- CD-ROM drive.
- Internet access for product updating.

Additional requirements for wireless devices

McAfee Internet Security includes the latest version of McAfee VirusScan software. In order to fully protect your wireless device from viruses, trojans, and worms, etc., your wireless device requires the following:

Palm OS and Palm requirements

McAfee VirusScan for Palm Desktop with HotSync Manager 3.0 will install and run on any IBM PC or PC-compatible computer equipped with Palm Desktop 3.0 or later. The latest version of Palm Desktop and HotSync 3.0 is a free download from Palm's site (at www.palm.com). The device-resident portion is quite simple and should work on any device with the Palm OS.

Windows CE or Pocket PC System requirements

McAfee VirusScan for Windows CE or Pocket PC will install and run on any IBM PC or PC-compatible computer equipped with ActiveSync 3.0 or later. Any CE device with ActiveSync 3 will function properly.

Symbian EPOC System requirements

McAfee VirusScan for Symbian's EPOC will install and run on any IBM PC or PC-compatible computer equipped with PsiWin 2.3 (or equivalent for non-Psion EPOC devices. All EPOC devices should ship with PsiWin 2.3 / EPOC Connect 5. These include:

- Psion Revo
- Psion Series 5mx
- Psion Series 7
- Psion netBook
- Oregon Scientific Osaris
- Ericsson MC218
- Ericsson R380

If you have an older device but the current PsiWin / EPOC Connect software, McAfee VirusScan for Symbian's EPOC will function properly, including the Psion HC, the MC series, the Workabout series, all Psion Series 3 models, the Psion Sienna, the Psion Series 5, the Geofox One, and the Phillips Illium.

If you do not have PsiWin 2.3, Symbian offers a free product called EPOC Connect Lite which also works.

Installation steps

After inserting the McAfee Internet Security 5.0 installation CD into your computer's CD-ROM drive, an Autorun image should automatically display. To install McAfee Internet Security software immediately, click Install McAfee Internet Security, then skip to Step 5 to continue with Setup.

Use the steps below to install your software.

1. If your computer runs Windows 2000 Professional, or Windows XP, log on to your computer as a user with administrative rights. You must have administrative rights to install this software.
2. Insert the McAfee Internet Security 5.0 CD in to your computer's CD-ROM drive. If the Installation Wizard does not automatically display, go to Step 3. Otherwise, skip to Step 4.
3. Use the following procedure if the Autorun installation menu does not display, or, if you obtained your software via download at a McAfee web site.
   a. From the Windows Start menu, select Run.
   The Run dialog box displays.
   b. Type <X>:\SETUP.EXE in the text box provided, then click OK.
4. Here, <X> represents the drive letter for your CD-ROM drive or the path to the folder that contains your extracted McAfee Firewall files. To search for the correct files on your hard disk or CD-ROM, click Browse.
   a. Before proceeding with the installation, Setup first checks to see whether your computer has the Microsoft Windows Installer (MSI) utility running as part of your system software. If your computer runs Windows XP, the current version of MSI already exists on your system. If your computer runs an earlier Windows release, you may still have MSI in your computer if you previously installed other software that uses MSI. In either of these cases, Setup will display its first wizard panel immediately. Skip to Step 5 to continue.
   b. If Setup does not find MSI or an earlier version of MSI is installed in your computer, it installs files necessary to continue the installation, then prompts you to restart your computer. Click Restart System. When your computer restarts, Setup will continue from where it left off.
5. Refer to steps displayed on the Installation Wizard to complete your installation.

NOTE
If your computer does not have the required fonts to view the End User's License Agreement (EULA), then you may locate the appropriate EULA on your McAfee software installation CD. You must read and agree to the terms of the agreement to complete your installation.

Troubleshooting installation problems

A failed installation can cause software problems that are difficult to track down. The major causes of installation failure are:

- Attempting to install while other software is running.
- Temporary files that conflict with the installation.
- Hard drive errors.

Follow the procedure outlined below to minimize the affect that these common conditions may have on your installation.

Step 1: Close other software

Disable all software running in the background:

1. Hold down the Ctrl and Alt keys on your keyboard, and then press the Delete key once. The Close Program dialog box appears.
2. Click End Task for every item on the list except Explorer.
3. Repeat steps 2 and 3 until you've closed everything except Explorer.
4. When you see only Explorer in the Close Program dialog box, click Cancel.

Step 2: Remove temporary files

Delete the contents of the Windows Temp folder:

1. Double-click the My Computer icon on your desktop. The My Computer window opens. Double-click the C: drive. You are now viewing the contents of your hard drive.
2. Double-click the Windows folder.
3. In the Windows folder, double-click the Temp folder.
4. In the menu, click Edit, then click Select All. All of the items in your Temp folder are highlighted.
5. Press the Delete key on your keyboard to delete the files. If Windows asks about deleting files, click Yes.

6 In the Windows taskbar, click Start, then click Shut Down.

7 Click Restart the computer, then click Yes in the Shut Down Windows dialog box to restart your PC.

Step 3: Clean your hard drive

Run the Windows hard drive utilities, ScanDisk and Disk Defragmenter to identify and fix any errors on your hard drive:

1 Click Start on the Windows taskbar, point to Programs, then Accessories, then System Tools, and click ScanDisk.

2 In the ScanDisk window, select Standard and Automatically fix errors.

3 Click Advanced. In the Advanced Settings dialog box, make sure the following settings are selected:

- Only if errors found
- Replace log
- Delete
- Free

4 Ignore the other options, and click OK. Click Start. ScanDisk begins scanning your drive for errors. Depending on the size of your hard drive, ScanDisk may take several minutes to complete its job.

5 When ScanDisk is finished, close ScanDisk.

6 Click Start on the Windows taskbar, point to Programs, then Accessories, then System Tools, and click Disk Defragmenter.

7 Click OK to start Disk Defragmenter. Depending on the speed of your computer and the size of your drive, this may take several minutes to complete.

8 Close Disk Defragmenter when it has finished defragmenting your disk.

Removing or modifying your McAfee Internet Security installation

If your computer's operating system is...

- Windows 2000 Professional
- Windows XP Home Edition
- Windows XP Professional Edition

... you must log on to your computer using a profile with administrative rights.

Then do the following.

1. From the Windows Control Panel, start the Add/Remove applet.
2. Select McAfee Internet Security and click:
   - **Remove** to remove McAfee Internet Security from your computer.
   - **Change** to modify your McAfee Internet Security installation.
3. Refer to steps displayed on the McAfee Internet Security Installation Wizard to complete your changes.

   Restart your computer as directed by setup.

Important information about Windows XP migration

Upgrading your computer's operating system from any version of Windows to Windows XP causes all McAfee products installed before migration to become disabled after migration to Windows XP.

You will be made aware of this situation as you make your first attempt to start a McAfee product (after migration) - you will be instructed to reinstall the product.

As such, you will need to uninstall all McAfee products and reinstall using your installation CD or the software obtained from McAfee via download.

Getting Started with McAfee Internet Security 5.0

3

McAfee Internet Security is a simple program to use. In fact, this one chapter covers the main things you need to know about using McAfee Internet Security. You begin with answering a few questions via the Interview so that McAfee Internet Security can effectively use its feature to protect you from Internet threats.

Introduction

The McAfee Internet Security 5.0 Home page is your central entry point to access and use all of McAfee Internet Security's tasks, wizards, and components. This screen displays three regions that provide you with dynamic information about current status and navigation links to all tasks.

The Title bar and Tool bar

Title bar

The Home page displays most of your standard Windows elements; that which includes:

- The title bar displays the name of the program that is currently running.
- Close and minimize buttons. McAfee Internet Security 5.0's interface is of fixed length and width. You cannot resize the interface.

Tool bar

The tool bar displays four browser-like buttons that are common to all screens.

- **Back**. Click Back to return to the last screen viewed.
- **Home**. Click Home to go to the McAfee Internet Security Home page from any screen.
- **Next**. In conjunction with the Back button, use Next to go to any previously viewed screen during your current session.
- **Help**. Click Help to view its submenu. The Help submenu may include any of the following items.

Help submenu item	Select this item to...
Help on this page	View online Help for the screen you are currently viewing.
Contents and index	View online Help for McAfee Internet Security.
Help on the Web	Start your Internet browser and go directly to the McAfee Help Web site at McAfeeHelp.com.
McAfee at Home on the Web	Start your Internet browser and go directly to McAfee-at-home.com.
About McAfee Internet Security	Version information about McAfee Internet Security.

Status information

Depending upon your configuration, the McAfee Internet Security 5.0 Home page displays other helpful information such as:

- The name or user name of the person currently logged in represented by Welcome (name)...
- Running status:

- If **McAfee Internet Security is not running** displays, click ***Start McAfee Internet Security*** to start the program.
- If **McAfee Internet Security is running** displays, click ***Stop McAfee Internet Security*** to stop the program.

- Update status:
  - If **McAfee Internet Security is up-to-date** displays, you are using the most current version of McAfee Internet Security 5.0.
  - If **Check for an update** displays, click ***Download update*** to start McAfee Instant Updater and check for an update to McAfee Internet Security 5.0.
- Number of warnings logged.
  - If one or more warnings were logged and not reviewed, click View warnings to start the Activity log page.
  - For more information about Activity logs, please refer to online Help.

McAfee Firewall status

In order to view McAfee Firewall status information, you must first activate McAfee Firewall. Activation requires that you perform a few preliminary configuration steps; the Firewall Configuration Assistant guides you through this process.

If the **Network Traffic** monitor does not display on the McAfee Internet Security home page, click **Activate McAfee Firewall** to start the McAfee Firewall Configuration Assistant.

For more information about the Network Traffic monitor or the McAfee Firewall Configuration assistant, please refer to ***McAfee Firewall*** on page 67.

About Tasks

The Task pane displays links that allow you to start McAfee Internet Security's **Tasks**. Depending upon your configuration, the Task pane displays **McAfee**, links that allow you start the Home page for any other current McAfee product that you have installed in your computer.

Starting a task is as easy as clicking its link. The Task list allows you to start McAfee Internet Security's major components. Although the tasks you can perform will vary based upon your computer's operating system and its configuration, primary tasks include:

Change user settings

Select this task to perform the following:

- Add or remove a user.
- Change a user or the Administrator's settings.

The User Settings properties sheet

The User Settings property sheet allows the Administrator to configure their own personal settings or any other user's settings. Self-administrating users can only change their personal settings.

There are four tabs on the user settings property sheet Each tab allows you to configure settings - grouped by their classification.

- **Privacy settings**:

  Click the Privacy Settings tab to configure your Internet privacy level. For example, you can filter Cookies, Web bugs and block annoying ads and pop up windows encountered while browsing the Internet.

  You can also configure Web Trail cleaner to remove records stored on your computer that were created as you used the Internet. Records of this type include Temporary Internet Files and historical records such as URLs visited, created by your Internet browser.

  The Privacy settings sheet allows you to protect personal information about each user that you want to protect from prying eyes and programs while browsing the Internet.

- **Security Settings**:

  Click the Security Setting tab to monitor your Internet connection and safeguard your computer against suspicious and potential malicious activities. Additionally, you can configure McAfee Internet Security to alert you if you visit harmful Web sites; or if a program in your computer attempt to access the Internet without your knowledge.

- From this page of the Change User Settings property sheet, you can setup File Guardian to protect files, folders, programs, and drives from unauthorized access.

- **User Preferences**:

  The User Preferences tab on the Change User Settings property sheet enables all users to configure how McAfee Internet Security responds to particular events. Here you configure how McAfee Internet Security starts, how it should alert you, and manage user passwords.

- **Parental Controls**:

  This page of the Change User Settings property sheet displays for restricted user profiles - only. In other words, this page does not display if the user possesses a self-administrating profile or is the McAfee Internet Security Administrator.

  Here you will enable or disable parental controls, and set the content ratings for the selected user. Other tasks that you can perform from this section of the Change User Settings property sheet include:

  - Filter Web sites, chat, and instant messaging for content, that which includes the blocking of access to proxy sites.
  - Identify the time-of-day a restricted user profile is allowed to access the Internet.
  - Explicitly block or allow a restricted user profile the ability to use specific programs installed in the computer and limit their access to Internet Newsgroups.

Perform a Security Check

After completing the interview, you'll want to find out how your PC may be at risk. Security Check examines your PC for privacy and security problems and then guides you through fixing any problem it finds. If you are using the settings suggested by McAfee Internet Security in the interview, you only need to run Security Check right after installation and then every month or so. If you reduce the level of protection, you should run Security Check more frequently.

You can also change the Security Check settings to customize how you want this feature to work on your computer.

View Activity Log

McAfee Internet Security now provides a list of activities that an Administrator can view via the Activity Logs feature. This list is generated based on his preferred security and privacy settings for himself and for other profiled users he created. Anything from dates and time that a user logged on, to PC maintenance, and violation (e.g., a user attempting to pass a credit card number) can be viewed at the single click of a button.

The Administrator can print, save or clear this list which contain any of the following:

Activity log tab	Description
Violations	◆ Displays any activity of a profiled user that violates any of the preset protection settings that the Administrator has indicated (e.g., attempting to pass a credit card number). It also displays the day, date and time that the user logon and off on the computer.
All	◆ Displays list of actions that McAfee Internet Security performed including the specific feature used to complete the task.
Firewall	◆ Displays detailed logging information as it relates to McAfee Firewall.

For step-by-step instructions on working with any of the report logs, see McAfee Internet Security online Help.

Set Startup Options

This task allows you to start and stop McAfee Internet Security manually and to configure McAfee Internet Security to start as Windows starts.

Configuration Assistant

Select this task to start the McAfee Internet Security Configuration Assistant. The Configuration Assistant provides you with an easy means of customizing your McAfee Internet Security settings.

Other Tasks

McAfee Internet Security 5.0 is a fully integrated suite that protects and secures your computer and connection to the Internet. In addition to the wizards and features described earlier in this chapter, McAfee Internet Security also includes utilities such as QuickClean Lite, McAfee Shredder, Instant Updater.

Although you can start McAfee Internet Security's shared features from the the Windows Start Menu, you can also start these programs directly from the **Other Tasks** Task list item.

From the **Other Tasks** screen you can start:

- McAfee Instant Updater.
- QuickClean Lite

- Shredder
- Safe & Sound (Please note, the link to start this utility displays only if your computer's operating systems is Windows 98 or Windows Me.).
- Visual Trace (You must install McAfee Firewall to see this link).

About the McAfee list

The McAfee list displays links to start the Home page to any other supported McAfee product. With this release of McAfee Internet Security 5.0, click the **Firewall** and **VirusScan Home Edition** links to start the respective program.

How to use the McAfee Internet Security Configuration Assistant

Although McAfee Internet Security is set up to use security and privacy settings that are appropriate for most users, some features require your input.

Each interview screen either tells you about a McAfee Internet Security feature, asks you to enter information, or asks you how you want McAfee Internet Security to respond to certain situations.

On each interview screen you can click Back to return to a previous screen or click Next to move to the next screen. In the final interview screen, you click Finish to save the settings you selected and close the Interview.

What information does McAfee Internet Security ask me to enter?

The McAfee Internet Security interview asks you to enter the personal and financial information that you want to protect. All the information you enter into McAfee Internet Security is stored in an encrypted form on your hard disk – it is never sent to McAfee Software.

You may want to gather your personal information before you start the interview. During the interview, McAfee Internet Security allows you to enter:

- A password that you can use to protect your McAfee Internet Security information.
- Information about other users of your computer. If you are the Administrator, you can create user profiles and set protection settings that McAfee Internet Security uses whenever a user is using the Internet via your computer.
- Personal and financial information that you want to protect from being sent out over the Internet without your knowledge:
  - Name
  - Address
  - Telephone number
  - Social Security number
  - E-mail address
  - Other financial numbers such as bank account, brokerage account, credit card, phone card, and so on.
- Any Web site login names and passwords that you want to store in Password Manager.

- For optimal protection by Identity Protector, include all dashes (such as Social Security number, bank account numbers, brokerage accounts, and ATM cards). For example, if you enter 123-45-6789 as your social security number, McAfee Internet Security will recognize the number with or without the dashes. If you enter 123456789, McAfee Internet Security won't alert you if the number is sent out with dashes (123-45-6789). Credit cards do not need dashes because you type the numbers into separate boxes.

How the McAfee Internet Security Administrator Works

Since McAfee Internet Security now offers multi-user logon capabilities, this feature allows one user to act as the administrator of personal information, protection and security settings entered via the McAfee Internet Security features. This is particularly useful if for example, you would want to filter, block or monitor certain types of information that you do not want your children to access when browsing the Internet.

Creating the McAfee Internet Security Administrator account can only be done in the Interview feature of McAfee Internet Security. And only the designated Administrator can access and change information and protection settings of the computer.

After this setup is complete, the Administrator can add other users and set the levels of security and protection for each user profile.

TIP
When adding user profiles, the Administrator can designate a user as a Self-Administrator.

See the McAfee Internet Security online Help to view step-by-step instructions on how to set an Administrator account.

Self-Administrating users

The McAfee Internet Security Administrator may designate another user as a Self-Administrator. This feature may be used if for example, the user is an adult and is deemed responsible enough to customize their privacy and protection settings.

Self-administrating users cannot change the Privacy, Security, or User Preferences settings for any other McAfee Internet Security user.

See the McAfee Internet Security online Help to view step-by-step instructions on how to designate a user as a Self-Administrator.

The Administrator's password

As Windows starts, McAfee Internet Security prompts you to enter the password set during the Interview. Without the password, the owner of the Administrator profile cannot log into and start McAfee Internet Security.

Although the owner of the Administrator profile cannot log in, users with a self-administrating or restricted user profiles can continue to use McAfee Internet Security normally. However, if the McAfee Internet Security administrator cannot log in, he or she cannot add, delete, or modify the settings for any user profile, including their own. Additionally, McAfee Internet Security settings cannot be modified.

Therefore, it is very highly recommended that the owner of the Administrator profile create a password that they will not forget, or, write the password down on a piece of paper and store it in a secure location.

Forgotten passwords

Please do not lose or forget the Administrator's password.

As described above, you must use the Administrator's profile to effectively use and configure McAfee Internet Security. Due to the high security risk it poses to you, we cannot describe the solution to recovering a lost or forgotten Administrator profile password in this Product Guide, via online Help, or at our Internet web site.

If you need to obtain a solution to this problem, you may contact our Technical Support department for assistance. Please refer to ***Product Support and Customer Service*** on page 95 for further details.

Again, we must stress, please do not forget, or misplace the Admin profile password.

How User Setup Works

The Administrator can add, edit and delete profiles of other users who browse the Internet through the same computer. After profiling users, the Administrator can customize their individual protection settings, including Internet filtering options and monitor their browsing habits.

To customize protection settings for another user, click the Change user settings task displayed on the McAfee Internet Security Home page, the User Setup screen is displayed. You can add, edit or delete a user's profile from this screen. Click any of the buttons available and follow through the instructions displayed on screen. Refer to online Help to view more about how to add, edit or delete a user's profile.

Using McAfee VirusScan

McAfee Internet Security uses McAfee VirusScan to address virus-related problems you may encounter through the Internet. This feature allows you to set how to perform a virus scan operation on your computer; what to do if a virus is found; and how it should alert you once the virus is detected. You can also direct VirusScan to keep a record of actions performed on your computer. For more information, see ***McAfee VirusScan Home Edition on page 49*****.**

Viewing Activity Logs

McAfee Internet Security now provides a list of activities that an Administrator can view via the Activity Logs feature. This list is generated based on his preferred security and privacy settings for himself and for other profiled users he created. Anything from dates and time that a user logged on, to PC maintenance, and violation (e.g., a user attempting to pass a credit card number) can be viewed at the single click of a button.

The Administrator can print, save or clear this list which contain any of the following:

Log Type	Description
Violation	◆ Displays any activity of a profiled user that violates any of the preset protection settings that the Administrator has indicated (e.g., attempting to pass a credit card number).
Maintenance	◆ Displays list of actions that McAfee Internet Security performed including the specific feature used to complete the task.
Activity	◆ Displays identity of profiled user who browsed the Internet using the computer. It also displays the day, date and time that the user logon and off on the computer.

For step-by-step instructions on working with any of the report logs, see McAfee Internet Security online Help.

Keep your program up-to-date

As technologies advance, we continually provide updates to McAfee software products. Updates include new product content, updates to anti-virus signature files, etc. To ensure the highest level of protection, you should always obtain the latest version of your McAfee product. McAfee's Instant Updater component allows you to obtain and apply updates to your McAfee products while connected to the Internet. To learn more about Instant Updater, please see ***Updating McAfee Internet Security on page 93*.**

If you purchased McAfee Internet Security on CD, you should run Update even if you've just installed McAfee Internet Security. In the time between when the CD was created and when you installed it, updates to the product itself as well as new virus patterns are likely to be available.

TIP

McAfee Internet Security comprises of several major components. Updates must be individually obtained and downloaded for each component.

For example, if you are viewing the Firewall component from within the McAfee Internet Security main window, then if you select Check for a Firewall Update, Instant Updater checks for, downloads, and installs updates to McAfee Firewall only. This applies to all McAfee Internet Security components.

What Mcafee Internet Security does while your computer is running

While you use your PC, McAfee Internet Security is on the lookout for potential privacy and security problems and takes action when it finds a problem. McAfee Internet Security uses the settings stored in Protection Settings to determine what to monitor and how to react.

Responding to McAfee Internet Security Alert Messages

To protect your privacy and security, McAfee Internet Security works as you work. When McAfee Internet Security detects a potential problem, it either handles the problem automatically or warns you with an alert message based on your McAfee Internet Security settings.

Each alert message tells you what potential problem triggered the message and McAfee Internet Security's recommendation on how to respond. If you want more information about the problem, click the Question Mark button and then click anywhere inside the alert message.

If you find over time that you are being alerted to potential security risks too often, you can adjust the alert message settings in Protection Settings. Cookie Blocker and Gatekeeper require a period of adjustment before McAfee Internet Security has learned to address your concerns with the least amount of disruption.

Using the McAfee Guardian shortcut menu

Even when you aren't running the main McAfee Internet Security program, you still have quick access to several features using the McAfee Guardian shortcut menu. Right-click the Guardian icon  located in the Windows system tray to display this menu. You can then do any of the following:

- Start McAfee Internet Security.
- Display Browser Buddy, which lets you retrieve your Internet passwords and displays statistics on how many cookies have been allowed or blocked, and how often it has cleared search information.
- Display Windows help for McAfee Internet Security.
- Encrypt and decrypt files that File Guardian protects.

Using Browser Buddy to manage your web site passwords

You can depend on McAfee Internet Security to help you easily navigate through the intricacies of the Web. For example, when you connect to Web sites that require a name and password, you can use Browser Buddy to:

- Drag your user name or password from Password Manager and drop it on the login form for the Web site.
- Add new password information for a Web site.

Browser Buddy can also tell you how many cookies have been allowed or rejected by Cookie Blocker and how many times a search information you initiated from one Web site, was blocked by Referer filter and not passed to another Web site.

Browser Buddy always remains displayed on top of any programs open on your screen. If Browser Buddy is located in an awkward position, you can close it and reopen it as needed.

To add a new user name and password

1. In Browser Buddy, select Add New Entry from the Password Manager drop-down list.
   The Enter password to save dialog box displays.
2. In the Web site text box, enter the Web site address; in the User name text box, type the name by which you identify yourself to this Web site, this may correspond to User Name, Member ID, Member Name, Login ID, or Login Name, and so on.
3. In the Password text box, type the password that confirms your identity. In Password Manager, McAfee Internet Security displays one asterisk for each character in your password.
4. Click OK.

To retrieve your user name and password

1. In Browser Buddy, select the site name if it doesn't appear automatically in the Current Web Site list.
2. Drag your user name or password from the Password Manager box to appropriate field in your Web site's login form.

   The text appears in the field. (If the site that you are logging into displays your password text as a series of asterisks (*), McAfee Internet Security will display one asterisk for each character in your password.)
3. Continue logging in as usual to the Web site.

Using File Encryption

File encryption translates a file into a “secret” code that makes the file unreadable. You must decode or decrypt the file before you can use it. The file encryption in McAfee Internet Security is designed so that you can easily encrypt or decrypt all of the files that you designate for encryption in File Guardian.

Before you can encrypt a file, you must add it to the Guarded Files list in File Guardian. For step-by-step instructions on adding a file to the Guarded Files list, see McAfee Internet Security Help.

To encrypt or decrypt files

- Right-click the McAfee Guardian icon on the Windows taskbar, then click Encrypt File Guardian files or Decrypt File Guardian files.

Security Features

McAfee Internet Security's security features safeguard your Internet connection and protect the files on your PC from prying eyes and destructive programs.

What Gatekeeper Does

Gatekeeper lets you control what programs on your PC can have access to your Internet connection. Gatekeeper can also warn you about any of these potentially harmful actions:

- Your browser is directed to a harmful site—one that has been known to contain virus-infected files (e.g., Trojan horses, prank or destructive ActiveX controls, or other security concerns).
- A program silently uses your modem to connect to another computer.
- A program starts up another program.
- A program sends out over the Internet a number that follows a common credit card number pattern.

Responding to Gatekeeper Alert Messages

McAfee Internet Security can display five different Gatekeeper-related alert messages. If you are using the default settings suggested by the Interview, you will see the messages related to Internet access, harmful sites, programs starting another program, and programs sending out credit card-like numbers.

Internet Access Alert Message

Each time you start a program that attempts to use your Internet connection, McAfee Internet Security checks to see if that program is in the list of programs allowed to access the Internet. If the program is not in the list, McAfee Internet Security displays an alert message to tell you that the program is trying to connect to the Internet and asks you how to deal with the program.

Because McAfee Internet Security displays an alert the first time you start an Internet program, you may want to start each of the Internet-connected programs you use regularly in order to get those alerts out of the way at one time.

You can respond to the Internet access alert message in the following ways:

If you choose ...	Then McAfee Internet Security ...
This time only	• allows the program to access the Internet this time only and warns you the next time it tries to access the Internet.
Allow always	• allows the program to access the Internet at any time. In Protection Settings for Gatekeeper, the program is added to the list of programs allowed to automatically access the Internet. If you decide later that you do not want this program to use your Internet connection, select its name and click Remove.
Not this time	• prevents the program from accessing the Internet. This choice stays in effect until the next time you restart Windows or for Internet Explorer 4 users, until you close your browser. Use this option if you want McAfee Internet Security to warn you the next time the program tries to access the Internet.

Harmful Site Alert Message

Before you can connect to a harmful site, McAfee Internet Security displays an alert message, “Your browser is visiting Sitename, a Web site that may harm your PC or data.”

You must immediately close your browser to end your browser’s connection to this site. The faster you close your browser, the less time the site has to transfer harmful data to your PC.

If you want to view the Web site anyway, click Continue.

Program Starts Another Program Message

When another program starts to run another program, McAfee Internet Security checks to see if you’ve authorized this action. If you haven’t allowed the program to always open the other program, McAfee Internet Security displays an alert message.

You can respond to the alert message in the following ways:

If you choose ...	Then McAfee Internet Security ...
Allow always	• allows the program to start the other program.

If you choose ...	Then McAfee Internet Security ...
Not this time	◆ prevents the program from starting the other program just this time.
This time only	◆ allows the program to start the other program just this time.

Any Credit Card Number Goes Out Message

When a program sends a number resembling a credit card number over the Internet, an alert message is displayed.

You can respond to the alert message in the following ways:

If you choose ...	Then McAfee Internet Security ...
Not this time	◆ prevents the program from sending the number this time.
This time only	◆ allows the program to send the number just this time.

Why should I change my Gatekeeper settings?

The Gatekeeper settings suggested by the Interview will display the fewest number of alert messages. If you are using an older browser version or just want a higher level of security, you may want to change your settings under the following circumstances:

Use this option	If you ...
Going to harmful sites.	◆ want to be warned when the site that you are going to has been known to cause damage, e.g. contains virus-infected files, Trojan horses, prank or destructive ActiveX controls, or other security concerns. (To keep McAfee Internet Security's list of harmful sites current and effective, use Instant Update monthly.)
My modem dials silently.	◆ want to be warned when a program is using your modem to dial out.
Program tries to launch another program.	◆ want to be warned when a program starts up another program. Many newer programs will warn you before doing this, but older programs may not do so. For example, Internet Explorer 4 uses "helper programs" to display documents.

Use this option	If you ...
Any credit card number goes out.	◆ want to be warned before any number that resembles a credit card number is sent out over the Internet.
These programs are always allowed access to the Internet	◆ want to see a list of what programs you have allowed to automatically access the Internet. (A program is added to the list when you click Accept Always in the Internet access alert message.) If you change your mind, you can remove a program from the list. You will be warned the next time that program tries to access the Internet.

What File Guardian Does

File Guardian can protect files that contain your sensitive data from being opened, renamed, copied, moved, or deleted. For added protection, you can even encrypt files protected by File Guardian. McAfee Internet Security can also alert you if a program attempts one of the following potentially harmful activities:

- A program attempts to reformat your hard drive.
- An ActiveX control attempts to delete files on your hard drive.
- An ActiveX control attempts to scan files on your hard drive.
- A program attempts to access your system password files.

When McAfee Internet Security displays an alert message, you can decide if the program should be allowed to continue the operation or not.

Responding to File Guardian Alert Messages

McAfee Internet Security can display five different File Guardian-related alert messages. If you are using the default setting suggested by the Interview, you will only see: guarded file; ActiveX scan; ActiveX delete; and drive format messages.

Guarded File Alert Message

Using File Guardian, you can set which files to guard on your hard drive and what programs can be used to open the files. If an unauthorized application attempts to access a guarded file, McAfee Internet Security displays an alert message that tells you what application is trying to open which file.

You can then decide whether you want to give the program in question access to the file. If you did not run the unauthorized program yourself, you should immediately investigate the program to determine its source.

If you choose ...	Then McAfee Internet Security ...
Allow always	• permits the program to open the file and adds the program to the list of programs that are authorized to access the file without further warnings.
Not this time	• stops the program from opening the file and warns you the next time the program tries to open the file.

ActiveX Scan Alert Message

There are legitimate reasons for allowing an ActiveX control to read through, or scan, all of your files. For example, you can go to one site on the Web that uses an ActiveX control to look for viruses on your PC. However, if a site begins to scan your files without warning you, McAfee Internet Security gives you a chance to think about how much you trust the site.

When McAfee Internet Security detects an ActiveX control scanning the files on your PC, it displays an alert message that tells you what ActiveX controls are scanning your hard drive.

You can respond to the alert message in the following ways:

If you choose ...	Then McAfee Internet Security ...
Not this time	• Stops the ActiveX control from running this time. If you change your mind, reload the page in your browser and click This time only the next time McAfee Internet Security displays its ActiveX scan message.
This time only	• Permits the ActiveX control to scan your drive just this time.

ActiveX Delete Alert Message

There are legitimate reasons for allowing an ActiveX control to delete files. For example, if a control installs special software on your PC to let you interact with its Web site, the control may need to delete files that it created for temporary use. However, if a site doesn't warn you and begins to delete files, McAfee Internet Security gives you a chance to see what file is being deleted and think about how much you trust the site.

When McAfee Internet Security detects an ActiveX control deleting files on your PC, it displays an alert message that tells you the name of the control.

You can respond to the alert message in the following ways:

If you choose ...	Then McAfee Internet Security ...
Not this time	• Stops the ActiveX control from running this time. If you change your mind, reload the page in your browser and click Allow this time the next time McAfee Internet Security displays its ActiveX delete message.
This time only	• Permits the ActiveX control to delete files just this time.

Drive Format Alert Message

When a format command is started, McAfee Internet Security doesn't know whether you told your PC to format a Zip disk or whether a rogue ActiveX control has started to format your hard disk. You know that this activity is legitimate when you start the formatting command or if you know that a program you are using needs to format a hard disk (or a Zip or Jaz disk).

When McAfee Internet Security detects a format command, it displays an alert message that tells you which program started the format command.

If you don't know why your disk is being formatted, note the name of the program in the alert message and then turn off your computer using its power switch. If the program has the letters OCX as part of its name, it is an ActiveX control. Do not restart your browser until you have run a Security CheckUp and removed the suspicious ActiveX control from your PC.

Click Continue if you want the program to format your disk.

Why should I change my File Guardian settings?

You may want to change your settings under the following circumstances:

Use this option	If you ...
ActiveX scans my drive	• want to be warned when an ActiveX control looks through the files on your PC. This may happen legitimately if the control needs to find a file to use. If you are concerned, check with the site that sent you the control.
ActiveX deletes files from my drive	• want to be warned when an ActiveX control deletes a files. This may happen legitimately if the control is deleting older or temporary files that it uses. If you are concerned, check with the site that sent you the control.

Use this option	If you ...
My drive is being formatted	◆ want to be warned when any program tries to format any of your drives. An alert message appears whenever you format a floppy disk, other removable media, or hard disk. You may want to turn this option off temporarily if you are going to format a lot of disks and don't want to see any messages.
Password files are accessed	◆ want to be warned when any program accesses your Windows password files (i.e., any file with the.pwl extension located in the Windows directory). Windows functions that are password-protected use these password files.
Guarded files	◆ want to prevent any program from opening a file or files. For further protection, you can have McAfee Internet Security include the file when you encrypt files. You can protect individual files, files in a specific folder, files of the same type, files on the same drive.

TIP

For step-by-step instructions on adding, editing, or removing files in the Guarded Files list, allowing a program to access a guarded file, or encrypting or decrypting files, see McAfee Internet Security Help.

What Password Manager Does

Password Manager lets you store your various Web site login names and passwords in one secure location. When you are visiting a Web site that requires this information, you can drag it from the Browser Buddy to the form displayed in your browser.

In Protection Settings, you can:

- Add a record
- Edit a record
- Remove a record
- View a list of stored login names and passwords

Whether you wish to add, edit, or remove a password or record, the McAfee Internet Security Inductive User Interface guides you through the steps.

Privacy Features

McAfee Internet Security's Privacy features protect browsing and personal information that you don't want anybody to access as a result of your surfing through the Internet.

What Cookie Blocker Does

Cookies are small files that your Web browser stores on your PC at the request of a Web server. Each time you view a Web page from the Web server, your browser sends the cookie back to the server. These cookies can act like a tag, which lets the Web server track what pages you view and how often you return to them. Some Web sites, such as Microsoft Expedia, use cookies to store your password and preferences so that you can automatically log on to the site.

McAfee Internet Security's Cookie Blocker offers three options for controlling the use of cookies on your computer. McAfee Internet Security can:

- Reject all cookies
- Accept all cookies
- Display an alert message each time a cookie is sent to your browser. The alert displays the name of the entity trying to set the cookie, and provides you the option either to accept the cookie or not.

  When setting up Cookie Blocker in Protection Settings, you can select one option for direct sites and another for indirect sites. Direct sites are those that you deliberately access. For example: typing the URL address in the location bar of your Web browser; clicking a link in a Web page; or selecting from your list of bookmarks or favorite sites. Indirect sites are those that you access because the site you are connecting to directly displays content from another site as part of its own content. For example, if you went directly to Cool_site.com, it could display an ad from Ads-r-us.com (the indirect site) in a separate frame in the Cool_site page.

  If during the Interview, you accepted McAfee Internet Security's recommendation on how to respond to cookies, Cookie blocker will:

  - Automatically allow cookies to be accepted from direct sites.
  - Blocks cookies when indirect sites try to set a cookie.

Responding to a Cookie Blocker Alert Message

If during the Interview, you set McAfee Internet Security to prompt you for action then it will display the Cookie Blocker alert message the first time a site tries to set a cookie.

You can respond to the alert message in the following ways:

If you choose ...	Then McAfee Internet Security ...
Allow always	• accepts the cookie and adds the site to the Allowed list. The next time you go to that site, all cookies from that site are allowed automatically.
Never accept	• rejects the cookie and adds the site to the Rejected list. The next time you go to that site, all cookies from that site are refused automatically.(In some cases, the cookie may be written to your local hard disk, but your privacy is protected because the cookie is never sent back to the requesting page.)

Each time you visit a site that appears in either the Allowed or Rejected list, McAfee Internet Security adds the number of cookies accepted or rejected to the list. You can see the totals for a Web site in the Browser Buddy.

If you change your mind about a site, you can remove it from the Allowed or Rejected list in the Cookie Blocker settings. The next time that you visit that site it will be as if you are visiting it for the first time. If you want to remove cookies for a site from which you've previously accepted cookies, run a Security Check and remove the cookies for that site.

TIP

You can run Security Check so that it only looks for cookies. On the Perform an Internet Security Check of Your Computer window, select Change How My Computer is Checked. In this window, clear all options except Cookies. Click OK and select Check My computer Now. After you are finished with the CheckUp, don't forget to revert to your previous settings.

Why should I change my Cookie Blocker settings?

If you want a good level of privacy protection without having to see any Cookie Blocker alert messages, configure your settings to always accept cookies from sites that you visit directly; and to always block cookies from sites that you haven't visited directly.

If you ...	Then choose this option.
Want the least number of cookies set and highest assurance of privacy.	• Reject for both Direct Sites and Indirect Sites. If a site requires you to accept a cookie, you can change this setting temporarily to Prompt.
Always want to know when cookies are sent.	• Prompt for both Direct Sites and Indirect Sites. Be prepared to respond to a large number of alert messages. After you respond to the Cookie Blocker alert message, you won't see additional alert messages for that site.
Are not concerned at all about cookies.	• Either turn off Cookie Blocker or change the Indirect Sites setting to Accept. You should choose the second method if you want to keep a total of the cookies added to your PC, which you can view in the Browser Buddy.

What Identity Protector Does

It is easy to forget that when you send information over the Internet, it doesn't go directly from your computer to the computer that is storing the Web page information. Instead, the information can pass through many computers before it reaches its final destination.

Identity Protector can keep your software from sending any personal information over the Internet to an unsecure site. Although you don't have to worry about a site when it using a secure connection, there are many Web sites that use a secure connection only when dealing with credit card transactions.

If more than one person is using your computer, make sure that you create a McAfee Internet Security password. If the person using your computer doesn't enter the McAfee Internet Security password, it automatically replaces any protected personal information sent to an unsecure site with the text, "xxxx." For example, if your child tries to order an item online without entering your McAfee Internet Security password, it replaces your credit card number with xxxx xxxx xxxx."

Identity Protector offers three optional responses whenever an application tries to send out information over the Internet to an unsecure site:

- Let the information go out.

- Block the information from going out.
- Display an alert message when any application tries to send the information over the Internet to an unsecure site. This is the response that McAfee Internet Security sets up when you add information to protect in the McAfee Internet Security Interview.

Responding to an Identity Protector Alert Message

During the Interview, McAfee Internet Security asked you to enter your personal and financial information that you want to protect. McAfee Internet Security displays the Identity Protector alert message the first time an application tries to send out this information to an unsecure site.

You can respond to the alert message in the following ways:

If you choose ...	Then McAfee Internet Security ...
This time only	• Allows the information to go out just this time.
Not this time	• Prevents the information from going out this time.

Why should I change my Identity Protector settings?

You may want to change your settings under the following circumstances:

If you ...	Then use this option
Are the only person using your PC and you don't want to be alerted every time.	• Enter all of the information that you want to prevent from going out and select Allow Always. Create a McAfee Internet Security password. If the McAfee Internet Security password is not entered after you start Windows, an unauthorized user of your PC can't view or send out your personal information.
Have more than one person using your PC.	• Enter all of the information that you may want to prevent from going out and select Allow Always or Ask Before Blocking. For information that you always want to prevent from going out, select Block Always. Create a McAfee Internet Security password. If the McAfee Internet Security password is not entered after you start Windows, any information entered in Identity Protector will be blocked from being sent out.
You want to be warned any time this information is being sent out.	• Enter all of the information that you may want to prevent from going out and select Ask Before Blocking.

A Note About Passwords

When McAfee Internet Security asks for your password and you enter it, the password stays in effect until one of the following events takes place. For all Windows operating systems:

- You log out of McAfee Internet Security.
- You log out of your computer.
- You shut down your computer.

Fast User Switching is a Windows XP feature that makes it possible for you to quickly switch between users without having to log off the computer. Multiple users can share a computer and use it simultaneously, switching back and forth without closing the programs they are running.

If you are using Windows XP with Fast User Switching enabled, McAfee Internet Security detects a fast user switch and as such, requires each respective user to input their password in order to use password required tasks.

What Web Trail Cleaner Does

As you surf the Internet, your browser stores information that makes your browsing experience more satisfying. It uses the information as follows:

If your browser uses ...	To ...
Cached files	• Speed up the display of Web page elements such as graphics.
URLs visited	• Display a list of sites that you've visited using Web addresses.
History	• Display a list of sites that you've visited using Web site names.

Then ...

- The files left on your PC can be viewed by others and depending on your browser's settings, can take up many megabytes of disk space.
- If you accepted McAfee Internet Security's recommendation during the interview, McAfee Internet Security displays the Web Trail Cleaner alert message when you close your browser.

Responding to the Web Trail Cleaner Alert Message

You can respond to the alert message in the following ways.

If you choose ...	Then McAfee Internet Security ...
Clean	• Deletes all of the cached files, history and URL information associated with the selected Web site (Domain). Select a site for cleaning by selecting the check box next to the site name.
Don't clean	• Closes the Alert message and continues closing your browser.

By default, McAfee Internet Security selects the sites that are not bookmarked (that is, part of your list of favorite sites) because it is less likely that you'll return to these sites. If you don't return to a site, the cached files for the site are never used again—they just sit and take up disk space until they are ultimately deleted by your browser.

If you later want to delete the files that you've left behind, run the McAfee Internet Security's Security Check.

Why should I change my Web Trail Cleaner settings?

You may want to change your settings under the following circumstances:

If you ...	Then use this option
Want to see exactly what files are being deleted.	• Prompt to Clean Up after closing Web browser.
Want to remove all traces of your browsing.	• Automatically Clean Up after closing Web browser. (Clear the check box for "Keep bookmarked items.")
Want to remove files only for Web sites that you haven't bookmarked or added to your list of favorites.	• Automatically Clean Up after closing Web browser. Keep bookmarked items.

What Referer Filter Does

When you perform a search in your Web browser, the search information displays in the address box of your Web browser. When you go to another site, the browser retains the search information and the next site you visit can extract it without your knowledge. Referer filter blocks this information from being passed along to the next site.

If you have Referer Filter selected in the Security Settings of McAfee Internet Security, it automatically removes search information before you go to another Web site. McAfee Internet Security does not display an alert message for this feature, but you can see the number of times Referer Filter blocks this information in the Browser Buddy.

McAfee VirusScan Home Edition 4

Stop viruses and keep your PC safe with McAfee VirusScan! When you're surfing the Internet, there's more to worry about than just viruses. You need to be able to control the communications into and out of your PC to ensure that your computer is safe. VirusScan includes extra firewall protection to keep your computer safe when you're connected to the Internet. VirusScan destroys threats at all entry points to your PC including email and synchronization with your PDA. It constantly monitors and stops virus-like activity on your computer to prevent any new threats from spreading. If you've got an Internet connection, you need more than just anti-virus protection, you need VirusScan!

What's new in this release?

- **Hostile Activity Watch Kernel (HAWK)** constantly monitors your computer for virus-like activity providing even more protection from Internet-based threats. It looks for events that may indicate new mass-mailers are present, or attachments with double file extensions.

  HAWK has been enhanced to include email clients other than just Microsoft Outlook - it now supports Outlook Express, Eudora, and other email that uses SMTP (Simple Mail Transfer Protocol) - this includes many popular email clients however does not include Internet-based email (like Hotmail, for example).

- **Script Stopper™**: Many of the fastest spreading viruses, like I Love You, use scripts to infect your PC. VirusScan 7 stops new malicious threats from infecting your system with Script Stopper™. Using HAWK's constant monitoring to detect actions that are often included in script-based viruses, Script Stopper™ alerts you of the attempted activity and will stop the actions that are initiated on your computer without your knowledge. Script Stopper™ detects, alerts, and blocks malicious script actions to keep your computer safe from script-initiated threats.

- **Integrated with Windows Explorer**: VirusScan 7 includes a Windows Explorer plug-in that lets you quickly scan files and access other VirusScan features directly from Windows Explorer making it easier than ever to use award-winning VirusScan technology.

- **Microsoft Office Integration**: VirusScan 7 scans Microsoft Office 2000+ documents to provide extra protection to users of Microsoft Word, Excel, and PowerPoint (2000+) in the event that VShield background scanning must be disabled.
- **Usability enhancements**: McAfee VirusScan includes many user interface enhancements to make it easier than ever to keep your computer and electronic files virus free.

What comes with McAfee VirusScan?

McAfee VirusScan consists of several components that combine one or more related programs, each of which play a part in defending your computer against viruses and other malicious software. These components are:

- **The VirusScan Home page**. This is your central entry point in using all of tasks and components. The Home page provides relevant information such as your computer's current Automatic Protection Settings status and version information about your virus definitions. The Home page also informs you if an update to McAfee VirusScan is available for download and the total number of scan operations performed.

- **On-Demand Scanning (ODS)**. On-demand scanning enables you to scan at any time. For example, if you suspect you have come in contact with an infected file, but have not accessed the file, you may manually scan the suspect file, folder, drive, etc.

  To perform an on-demand scan, simply select the **Scan for viruses now** task from the McAfee VirusScan Home page.

- **The VShield Scanner**. This is an On-access Scanning (OAS) component that gives you continuous anti-virus protection from viruses that arrive on floppy disks, from your network, or from various sources on the Internet. The VShield scanner starts when you start your computer, and stays in memory until you shut down. A flexible set of property pages lets you tell the scanner which parts of your system to examine, what to look for, which parts to leave alone, and how to respond to any infected files it finds. In addition, the scanner can alert you when it finds a virus, and can summarize each of its actions.

- **Hostile Activity Watch Kernel**. HAWK monitors your computer for suspicious activity that may indicate a virus is present on your system. As opposed to VirusScan, which cleans the virus, HAWK prevents viruses, worms, and trojans from spreading further. HAWK monitors e-mail clients such as Outlook, Outlook Express, Eudora, and any other client that supports SMTP (Simple Mail Transfer Protocol), but does not support Internet-based e-mail such as MSN's Hotmail.

  HAWK incorporates McAfee's Script Stopper™ to detect, alert, and block malicious script actions to keep your computer safe from script-initiated threats.

- **Safe & Sound**. This component allows you to create backup sets in protected volume files, which is the safest and preferred type of backup. A protected volume file is a sectioned-off area of the drive, sometimes called a logical drive.

NOTE
Safe & Sound is a VirusScan utility that is only functional when McAfee VirusScan is installed in conjunction with a Windows 98, Windows 98 SE, or Windows Me operating system.

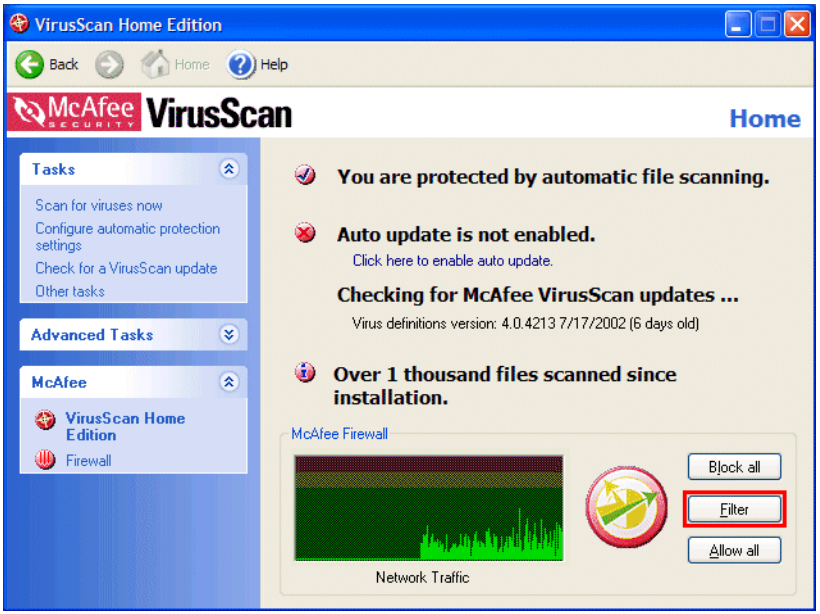
- **Quarantine**. This component allows you to move infected files to a quarantine folder. This moves infected files from areas where they can be accessed and enables you to clean or delete them at your convenience.
- **The E-mail Scan extension**. This component allows you to scan your Microsoft Exchange or Outlook mailbox, or public folders to which you have access, directly on the server. This invaluable "x-ray" peek into your mailbox means that VirusScan software can find potential infections before they make their way to your desktop, which can stop a Melissa-like virus in its tracks.
- **The Emergency Disk creation utility**. This essential utility helps you to create a floppy disk that you can use to boot your computer into a virus-free environment, then scan essential system areas to remove any viruses that could load at startup.
- **Bootable CD**. The VirusScan Installation CD includes a CD version of the emergency startup disk. If your computer is configured to start using its CD drive, then you can use the CD to boot your computer in to a virus-free environment then scan for viruses that load during startup.
- **McAfee Instant Updater**. Enables your computer to automatically communicate with McAfee while you are connected to the internet and inquire of the availability of product updates, updates to anti-virus signature files, and updates to the VirusScan scan engine. You will also use this feature to register your McAfee product.
- **Wireless device protection**. In addition to total anti-virus protection for your PC, VirusScan protects your wireless device and PC from harmful viruses transferred during the synchronization process.
- **Command-line Scanners**. This component consists of a set of full-featured scanners you can use to run targeted scan operations from the MS-DOS Prompt or Command Prompt windows, or from protected MS-DOS mode. The set includes:
  - **SCAN.EXE**, a scanner for 32-bit environments only. This is the primary command-line interface. When you run this file, it first checks its environment to see whether it can run by itself. If your computer is running in 16-bit or protected mode, it will transfer control to one of the other scanners.

- **SCANPM.EXE**, a scanner for 16-bit and 32-bit environments. This scanner provides you with a full set of scanning options for 16-bit and 32-bit protected-mode DOS environments. It also includes support for extended memory and flexible memory allocations. SCAN.EXE will transfer control to this scanner when its specialized capabilities can enable your scan operation to run more efficiently.
- **SCAN86.EXE**, a scanner for 16-bit environments only. This scanner includes a limited set of capabilities geared to 16-bit environments. SCAN.EXE will transfer control to this scanner if your computer is running in 16-bit mode, but without special memory configurations.
- **BOOTSCAN.EXE**, a smaller, specialized scanner for use primarily with the Emergency Disk utility. This scanner ordinarily runs from a floppy disk you create to provide you with a virus-free boot environment.

All of the command-line scanners allow you to initiate targeted scan operations from an MS-DOS Prompt or Command Prompt window, or from protected MS-DOS mode. Ordinarily, you'll use the VirusScan application's graphical user interface (GUI) to perform most scanning operations, but if you have trouble starting Windows or if the VirusScan GUI components will not run in your environment, you can use the command-line scanners as a backup.

Getting Started

The McAfee VirusScan Home page is your central entry point to access and use all of McAfee VirusScan's tasks, wizards, and components. This screen displays three regions that provide you with dynamic information about current status and navigation links to all tasks.



The Title bar and Tool bar

Title bar

The Home page displays most of your standard Windows elements; that which includes:

- The title bar displays the name of the program that is currently running.
- Close and minimize buttons. McAfee VirusScan's interface is of fixed length and width. You cannot resize the interface.

Tool bar

The tool bar displays four browser-like buttons that are common to all screens.

- **Back**. Click Back to return to the last screen viewed.

- **Home**. Click Home to go to the McAfee VirusScan Home page from any screen.
- **Next**. In conjunction with the Back button, use Next to go to any previously viewed screen during your current session.
- **Help**. Click Help to view its submenu. The Help submenu may include any of the following items.

Help submenu item	Select this item to...
Help on this page	View online Help for the screen you are currently viewing.
Contents and index	View online Help for McAfee VirusScan.
Virus Information Library	Start your Internet browser and go directly to the McAfee AVERT Virus Information Library Web site.
Help on the Web	Start your Internet browser and go directly to the McAfee Help Web site at McAfeeHelp.com.
McAfee at Home on the Web	Start your Internet browser and go directly to McAfee-at-home.com.
About McAfee VirusScan	Version information about McAfee VirusScan.

Status information

Depending upon your configuration, the McAfee VirusScan Home page displays other helpful information such as:

- **Status of automatic file scanning**. This message lets you know if you computer is or is not protected by automatic file scanning. If you are not protected, "**Click here to enable automatic file scanning**" displays. You can click this message to instantaneously enable automatic file scanning.
- **Update availability**. If an update for McAfee VirusScan is available, or if you have not registered this product with McAfee, a message displays describing as such. Additionally, virus definition files (DATs) version information displays here as well.

  If there is an update to McAfee VirusScan available, **Click here to update McAfee VirusScan** displays. You can click this message to start McAfee Instant Updater and update this product.
- **The total number of scanning operations performed.** The number represented by this status message indicates the total number of scan operations performed since you installed McAfee VirusScan.

The Task pane

The Task pane displays links that allow you to start McAfee VirusScan's **Tasks** and **Advanced Tasks**. Depending upon your configuration, the Task pane displays **McAfee**, links that allow you start the Home page for any other current McAfee product that you have installed in your computer.

About Tasks

Starting a task is as easy as clicking its link. The Task list allows you to start McAfee VirusScan's major components. Although the tasks you can perform will vary based upon your computer's operating system and its configuration, primary tasks include:

- **Scan for viruses now**: This task allows you to scan your entire computer for viruses. Here you can also choose to scan a specific drive, folder, or file. When the scan is complete, VirusScan scan Summary Report displays.
- **Configure automatic protection settings**: Select this task to configure VShield background scan settings.
- **Check for a VirusScan update**: This task starts McAfee Instant Updater and checks to see if there is an update to McAfee VirusScan available.
- **Other Tasks**: Depending upon your McAfee VirusScan configuration, this task provides you a quick and convenient method to start McAfee VirusScan's shared features.

About Advanced Tasks

Similar to the primary Task list, the Advanced task list may vary depending upon your version of Windows, its configuration, and other software that may be installed in your computer. McAfee VirusScan' s advanced tasks include:

- **Configure and scan my wireless device:** Select this task to configure and defend your wireless device against viruses.
- **Manage quarantined files**: Select this task to manage files infected with a virus. Here you can choose to add, remove, clean, and delete infected and quarantined files.
- **View and edit scheduled scans**: This advanced task allows you to schedule scan events. You can use the default settings for scan events or create a custom list of scan events.
- **View VirusScan's activity logs**: Activity logs contains records about VirusScan settings, scan results, and historical records of scans performed. Select this task to view these records.

- **Configure Instant Updater**: Instant Updater is the mechanism used to register your product and to communicate with McAfee to check for an update to virus definition files (DATs), the virus scanning engine, and for updates to the McAfee VirusScan product. Select this advanced task to check for updates to McAfee VirusScan.

About the McAfee list

The McAfee list displays links to start the Home page to any other supported McAfee product.

Other McAfee VirusScan features

The VShield Tray Icon

The VShield icon located in the Windows system tray allows you to perform several tasks.

- **Launch VirusScan**: Select this option to Start McAfee VirusScan, if it is not running.
- **View VirusScan Status**: Select this option to view the VirusScan background scanner (VShield) property sheet. Here you can view real-time status information about VirusScan's background scan modules.
- **Disable VirusScan**: Select this option to stop VirusScan's background scanner (VShield).
- **About VirusScan**: This option provides you with version information about McAfee VirusScan.

Windows Explorer plug-in

With functionality similar to that of the VShield system tray icon, you can display a VirusScan toolbar in Windows Explorer.

To display the VirusScan toolbar, right-click the Windows Explorer toolbar and select McAfee VirusScan. The VirusScan toolbar allows you to:

- Scan objects displayed in Windows Explorer. For example, you can select a file, group of files, folder, or a drive.

  To use this feature, select the object you want to scan in Windows Explorer. Click the VirusScan toolbar drop-down arrow and click **Scan for Viruses**.

- View current VirusScan Status information. To view real-time scan data about System scan, E-mail scan, and HAWK.

About VShield Scanner

The VShield scanner has unique capabilities that make it an integral part of the VirusScan comprehensive anti-virus software security package. These capabilities include:

- **On-access scanning**: This means that the scanner looks for viruses in files that you open, copy, save, or otherwise modify, and files that you read from or write to floppy disks and network drives. It therefore can detect and stop viruses as soon as they appear on your system, including those that arrive via e-mail. This means you can make the VShield scanner both your first line of anti-virus defense, and your backstop protection in between each scan operation that you perform. The VShield scanner detects viruses in memory and as they attempt to execute from within infected files.
- **Automatic operation**: The VShield scanner integrates with a range of browser software and e-mail client applications. VShield Scanner starts when you start your computer, and stays in memory until you shut it or your system down.

VShield automatic protection settings

The VShield scanner consists of related modules, each of which has a specialized function. You can configure settings for all of these modules in the VShield properties sheet.

System Scan

The System scanner looks for viruses on your hard disk as you work with your computer. It tracks files as your system or other computers read files from your hard disk or write files to it. It can also scan floppy disks and network drives mapped to your system.

The System scanner provides scanning protections against viruses embedded in or attached to e-mail messages as well as well as files that you download from the Internet. The System scanners functionality replaces that which was included in the Download and Internet scanners included with previous versions of McAfee VirusScan.

E-mail Scan

The E-mail scanner monitors e-mail messages and message attachments that you receive via interoffice e-mail systems, and via the Internet. It scans your Microsoft Exchange or Outlook mailbox systems.

Hostile Activity Watch Kernel

HAWK monitors your computer for suspicious activity that may indicate a virus is present on your system. As opposed to VirusScan, which cleans the virus, HAWK prevents viruses, worms, and trojans from spreading further.

Hostile Activity Watch Kernel (HAWK) is a VirusScan option that enables constant monitoring for suspicious activity that may indicate a virus is present on your system. Suspicious activity includes:

- An attempt to forward e-mail to a large portion of your address book.
- Attempts to forward multiple e-mail messages in rapid succession.

E-mail attachments containing program files (executable files with an .exe file extension) or scripts that can be used to mask the actual type document transmitted to you.

By monitoring for these typically malicious activities, HAWK notifies you and lets you take action before damage occurs. HAWK can prevent viruses, worms, and trojans from spreading further, while VirusScan cleans the virus to remove it from your computer.

About Script Stopper™

Script Stopper™ is a VirusScan protection mechanism associated with the HAWK. Script Stopper™ detects malicious activities script methods or routines, perform. For example, Script Stopper™ detects scripts that try to:

- Delete, open, or make files in your computer.
- Send e-mail messages without your knowledge or consent.
- Access your computer's registry.

Script Stopper™ allows you to create a list of trusted scripts. If you encounter a script that is acting in a hostile manner, an Alert message displays. At such time, you can block the script from running now, and at any time in the future.

If you recognize the script, you can allow it to run. If you allow a script to run, and indicate that you recognize the script, McAfee VirusScan adds the script to its records of trusted scripts. If there are scripts that you frequently use, or want to allow to run, you can add scripts to a trusted database directly from the Script Stopper™ property sheet in the HAWK scan module.

How to Start and Stop VShield Scanner

Using the VShield tray icon

The VShield icon located in the Windows system tray allows you to start and stop automatic file protection. To do this right-click the VShield icon and select:

- **Launch VirusScan** to Start McAfee VirusScan, and to enable automatic file protection.
- **Disable VirusScan** to disable automatic file protection. Please note, automatic file protection, by default, restarts without your intervention within 10 minutes of disablement.

> **TIP**
> To maintain the highest level of anti-virus protection, it is not recommended that you disable automatic file protection.

Using the Windows Control Panel applet

1. With the VShield Scanner running, from the Windows task bar select **Start > Settings > Control Panel**.
   The Windows Control Panel displays.
2. Double–click the **VirusScan** icon.
   The VirusScan Services dialog box displays.
3. Select the Service tab and click **Stop**.
   VShield Scanner stops.
4. By default, setup configures McAfee VirusScan to start as Windows starts. If you do not want McAfee VirusScan to start as Windows starts, clear the check box next to **Load on startup**.
5. Click **Apply** to save your settings.
6. Click **OK** to close the VirusScan Services dialog box.

> **TIP**
> You can start or re-start the VShield Scanner using the steps described above.

VShield Scanner, by default, is configured to automatically start each time your computer starts. To prevent VShield Scanner to run at startup, clear the Load on startup check box.

Using Quarantine

Many VirusScan components allow you to move infected files to a quarantine folder. This moves infected files from areas where they can be accessed and enables you to clean or delete them at your convenience.

How to managing quarantined files

This list describes the options available to you when managing quarantined files:

- **Add**. Select this option to browse for and quarantine a suspected file.
- **Clean**. Select this option to remove the virus code from infected file. If the virus cannot be removed, it will notify you in its message area.
- **Restore**. Select this option to restore a file to its original location. Please note, ***this option does not clean the file***. Make sure the file is not infected before selecting Restore.
- **Delete**. Select this option to delete the infected file. Make sure to note the file location so you have a record of the deleted files. You will need to restore deleted files from backup copies.

  WARNING
  Choose **Delete** only if a backup copy of the file is available. To learn more about how to restore Windows system files, please visit ***www.avertlabs.com***.

- **Submit quarantined files to AVERT via WebImmune**: Select this option to submit new viruses to McAfee's investigative labs.

  NOTE
  McAfee is committed to providing you with effective and up-to-date tools you can use to protect your system. To that end, we invite you to report any new viruses, Java classes, ActiveX controls, or dangerous web sites that VirusScan does not now detect.

  If you have found what you suspect to be a new or unidentified virus, send the infected file to McAfee Labs Anti-Virus Emergency Response Team for analysis, using WebImmune. For more information about WebImmune, please visit ***www.webimmune.net***.

TIP
You can also attempt to obtain an antidote from A.V.E.R.T. using WebImmune at ***www.webimmune.net***.

Network Associates reserves the right to use any information you supply as it deems appropriate without incurring any obligations whatsoever.

Safe & Sound

Safe & Sound is a unique backup utility that automatically creates backup files of your documents as you work on them. You can configure Safe & Sound to back up to a different drive, across a network connection, or to a protected area within your local (c:\) drive. If your files become corrupted due to a virus, or your system crashes, or if you lose your files, McAfee's Safe & Sound utility provides you the ability to recover files using the Safe & Sound Windows or DOS recover utility.

Please note, Safe & Sound is a VirusScan utility ***that is only functional*** when McAfee VirusScan is installed in conjunction with a **Windows 98**, **Windows 98 SE**, or **Windows Me** operating system.

How Safe & Sound creates automatic backups:

When you select to have Safe & Sound automatically create a backup set for you, it creates the first backup set while you are stepping through the Safe & Sound Wizard. Thereafter, while the Enable Automatic Backup option is selected, it continues to update your backup set at the time delay you've specified. If you chose to make Mirror backups, Safe & Sound updates your backup set at the same time that you re-save the original source files.

Defining your backup strategy

After you decide which backup type you want to use (either a protected volume file or a directory backup set), the most important questions you must answer when defining your own backup strategy are:

Where will you store the backup set?

In today's computer marketplace, you may discover that it is as cost effective to acquire a separate backup hard drive where you can keep a current mirror backup copy of one or more other drives that you use on your PC.

In addition, you may want the backup copy to be stored at a remote location, for increased protection. As long as Safe & Sound can access a logical drive mapped on your PC, it can store the backup set there. That is, the backup set can be stored on a shared network drive.

What files are important (which files must be backed up)?

Safe & Sound automatically selects files that are typically important to include in a backup set. However, you can select other files or types of files to include in your backup set.

How often should you or safe & sound make these backups?

The more recent your backup set, the happier you'll be if your PC does encounter a problem that compromises the data on your primary drives. However, you may want to keep the default Write-behind Delay of 20 minutes to give you time to recover a previous version of a file if you ever need to

Safe & Sound configuration

The Safe & Sound setup wizards guides you through your initial setup. Please access online Help for information about Safe & Sound configuration.

Emergency disk creation

As it installs itself, VirusScan software will examine your computer's memory and your hard disk's boot sectors to verify that it can safely copy its files to your hard disk without risking their infection. During that installation, Setup offers to create an Emergency Disk you can use to start your system in a virus-free environment. Should the VirusScan software itself become infected, or if you want to be sure your computer is clean before you install any other software, create and use an Emergency Disk to start your computer.

VirusScan software comes with an Emergency Disk wizard that makes disk creation simple and fast.

The Emergency Disk you create includes BOOTSCAN.EXE, a specialized, small-footprint command-line scanner that can scan your hard disk boot sectors and Master Boot Record (MBR). BOOTSCAN.EXE works with specialized set of virus definition (.DAT) files that focus on ferreting out boot-sector viruses. If you have already installed VirusScan software with default Setup options, you'll find these .DAT files in this location on your hard disk:

C:\Program Files\Common Files\Network Associates\VirusScan Engine\4.0.xx

The special .DAT files have these names:

- EMCLEAN.DAT
- EMNAMES.DAT
- EMSCAN.DAT

McAfee periodically updates these .DAT files to detect new boot-sector viruses. You can download updated Emergency .DAT files from this location:

http://www.mcafeeb2b.com/naicommon/avert/avert-research-center/tools.asp

McAfee recommends that you download new Emergency .DAT files directly to a newly formatted floppy disk in order to reduce the risk of infection.

Using VirusScan With a Wireless Device

Introduction

As the demand for wireless devices continue to grow, it carries with it, the threat of compromising your data against viruses especially whenever you exchange information between your PC and your wireless device.

Wireless devices that are currently available in the market today are primarily designed as a more convenient alternative in storing and retrieving information such as personal activities, people's addresses, telephone numbers, appointments, expenses, etc. Either at work or at home, you can easily keep track of records in all of these areas by simply using your wireless device. You can even set an alarm to alert you of important meetings, events or tasks to do during the day, week or month.

How VirusScan protects your wireless device

McAfee VirusScan is an application designed to protect your data by scanning the files on your wireless device every time a data exchange or update is performed with your computer. It protects your system from viruses that may have been placed on your wireless device during the use of features such as infrared transfers and wireless transactions. McAfee VirusScan supports most types of wireless devices using Palm OS, Pocket PC, Windows CE, and EPOC operating systems (please refer to the following table).

Table 4-1. Examples of wireless devices that McAfee VirusScan supports

Operating System	Wireless Device	Manufacturer
Palm OS	• Palm VII Series • Palm V Series • Palm III Series • Palm M Series	Palm, Inc.
Palm OS	• Visor • Visor Edge	HandSpring
Palm OS	• Clie	Sony
Pocket PC	• E-115	Casio
Pocket PC	• iPAQ • iPAQ H3600 Series • Aero • Aero 2100 Series	Compaq
Pocket PC	• PPT 2700 Series	Symbol Technologies

Table 4-1. Examples of wireless devices that McAfee VirusScan supports

Operating System	Wireless Device	Manufacturer
Pocket PC	• Jornada 540 • Jornada 680 • Jornada 720	Hewlett-Packard
Pocket PC	• E125 • EM500	Cassiopeia
Windows CE	• PenCentra 130	Fujitso
Windows CE	• HPW-600 ET	Hitachi
Windows CE	• WorkPad z50	IBM
EPOC	• Psion Series 5MX • Psion - Revo	Psion PLC
EPOC	• Mako	Diamond

TIP

For more information about protecting your wireless device, please refer to online Help for McAfee VirusScan.

McAfee Firewall 5

Introduction

Protect yourself while online with the advanced security of McAfee Firewall. Easy-to-use, yet highly configurable, McAfee Firewall secures your PCs connection to the Internet whether you connect via DSL, cable modem or dial-up. With intrusion detection, color coded security alerts, customizable audible alerts, detailed logging, and an application scan for Internet enabled applications, McAfee Firewall gives you the power you need to control the communications into and out of your PC, ensuring that your online experience is as safe as it is enjoyable.

McAfee Firewall:

- Controls file and print share access.
- Shows who is connecting to your computer if you allow sharing.
- Stops floods and other attack packets from being received by the Operating System.
- Blocks untrusted applications from communicating over the network.
- Provides detailed information about which sites you have contacted and the type of connection that was made.
- Can be set to block all traffic or traffic from a specific IP address immediately.

What's new in this release?

- **Firewall security check:** Examines your security settings for possible vulnerabilities.
- **Enhanced hacker tracing** with the addition of McAfee's Visual Trace technology.
- **Intrusion Detection System:** Detects common attack types and suspicious activity.
- **Home networking wizard:** Set up protection for personal computers sharing an Internet connection.
- **Wizard for creating custom rules:** Create custom configurations for specific programs.

- **Password protection:** Prevent others from tampering with your firewall settings using password protection.
- **Improved support for broadband connections.**
- **Usability enhancements:** McAfee Firewall 4.0 includes many user interface enhancements to make it easier than ever to secure your computer.

How McAfee Firewall works

McAfee Firewall is a simple-to-operate security tool that dynamically manages your computing security behind the scenes.

Setup

During the installation process, the Configuration Assistant prompts you with basic questions to set up McAfee Firewall to do specific tasks – according to your needs (e.g. allow sharing of files or not).

Operation

McAfee Firewall filters traffic at the devices that your system uses - network cards and modems. This means that it can reject inbound traffic before that traffic can reach vital functions in your computer and waste valuable system resources.

McAfee Firewall – the Gatekeeper

When McAfee Firewall is running, it monitors trusted and untrusted programs that communicate using the Internet. If a trusted application attempts to communicate, McAfee Firewall allows the program to function without restrictions. If an untrusted program attempts to communicate into or out of your computer, McAfee Firewall blocks the program's attempt to communicate via the Internet.

Configuration

Some network communications are needed to maintain network-based services. These are managed through user defined rules under the system settings of McAfee Firewall. The default system settings feature provides superior protection from hostile threats.

Frequently asked questions

The following are some frequently asked questions that you can briefly review:

How will McAfee Firewall help me?

McAfee Firewall protects your computer at the network level. It acts as a gatekeeper, checking every data packet going in or out of your PC. It allows only what you tell it to allow.

McAfee Firewall has been designed to be easy to use, while providing superior protection. Once you install and run it, it is configured to block known attacks and to ask you before allowing applications to communicate.

How is my PC at risk on the Internet?

When you connect to the Internet, you share a network with millions of people from around the world. While the Internet is a wonderful and amazing accomplishment, it brings with it all the problems of being accessible to complete strangers.

While communicating via the Internet, you should take safety precautions to protect your computing environment. If you use IRC (Internet Relay Chat) programs, be suspicious of files total strangers send you. Programs that give others remote access to your computer, such as Back Orifice (BO), are frequently disseminated in this manner. It is a good practice to scan files received using anti-virus programs such as McAfee VirusScan before you open or view files and their attachments.

When on the Internet, others can try to access your file shares. Therefore, you should check that they are only accessible to those you trust. Otherwise, untrusted parties can read and delete what is in your computer.

What other protection do I need?

McAfee Firewall provides network level protection. Other important types of protection are:

- Anti-virus programs for application-level protection.
- Logon screens and screen saver passwords to prevent unauthorized access.
- File encryption or encrypting file systems to keep information secret.
- Boot-time passwords to stop someone else from starting your PC.
- Physical access to the computer, e.g. stealing the hard drive.

A separate but also important issue is controlling access to information, misinformation and “filth” that is widely available on the Internet. You can use a number of content-filtering services or programs such as McAfee’s Internet Security that can filter the contents of data packets or restrict access to certain sites.

Are there any data packets that McAfee Firewall cannot stop?

Inbound Data: No. As long as McAfee Firewall supports a network device and is running, it is intercepting all incoming packets and will allow or block according to the way you have it configured. If you choose to block everything, it will.

Outbound Data: Yes and no. McAfee Firewall intercepts outbound data packets as they are passed to the network device driver. All popular applications communicate this way. A malicious program could communicate by other means, however.

What network devices does McAfee Firewall support?

McAfee Firewall supports Ethernet and Ethernet-like devices. This includes dial-up connections, most cable and ISDN modems and most Ethernet cards. It does not support Token Ring, FDDI, ATM, Frame Relay and other networks.

What protocols can McAfee Firewall filter?

McAfee Firewall can filter TCP / IP, UDP / IP, ICMP / IP and ARP. It intercepts all protocols, but others, such as IPX, must be either allowed or blocked - no filtering is done. The Internet uses the IP protocols. No others are sent. Also, IP networks are the most common.

How can I still be harassed, even with McAfee Firewall?

Many people use McAfee Firewall to block the “nukes” that cause their IRC connections to be broken. While McAfee Firewall blocks the nukes, there are other ways that attackers can still cause the connections to be broken:

- **Server-side nuking**. This is when the "nukes" are sent to the IRC server, not to your computer, telling the server that you can no longer be reached. To prevent this, the IRC server needs a firewall.
- **Flood blocking a TCP connection**. If a flood of packets is sent to you from a higher speed connection, McAfee Firewall can stop the packets, but the flood takes up all your bandwidth. Your system does not get a chance to send anything. Dial-up users are particularly vulnerable since they have the lowest speed connections.

> **TIP**
> To read additional frequently asked questions, refer to the Readme.txt file.

Getting Started with McAfee Firewall

After installing McAfee Firewall, you will need to configure your software for its first use. The Configuration Assistant guides you through this process.

TIP
Previous versions of McAfee Firewall did not allow you to run the Configuration Assistant more than once. However, McAfee Firewall 4.0 allows you to run the Configuration Assistant with an easily accessible link on the McAfee Firewall Home page.

The Configuration Assistant

Welcome Screen

The McAfee Firewall Configuration Assistant displays the first time you start McAfee Firewall. This wizard guides you through initial setup and activates McAfee Firewall on your computer. Select Back, Next, Cancel, and Finish to navigate the Configuration Assistant screens.

If you select Cancel on any Configuration Assistant screen, the activation and configuration process stops. **You must complete the Configuration Assistant on first use in order to activate and use McAfee Firewall.**

Network Control Settings

Network Control Settings identify how you want McAfee Firewall to respond when a program attempts to access the Internet; either into or out of your computer.

1 To set your Network Control settings, from the Welcome to McAfee Firewall screen, select one of the following.

Table 5-2. McAfee Firewall's Network Control Settings

Internet Traffic Setting	Description
Block all traffic	Configures McAfee Firewall to block all Internet traffic into and out of your computer. This is the most secure firewall setting; however, programs in your computer cannot access the Internet.

Table 5-2. McAfee Firewall's Network Control Settings

Internet Traffic Setting	Description
Filter all traffic	Gives you the opportunity to decide whether an application or program in your computer will be allowed to access the Internet. If an unrecognized program attempts to access your computer from the Internet, you will also be given an opportunity to allow or block its access your computer.
Allow all traffic	Configures McAfee Firewall to allow all Internet traffic into and out of your computer. All programs in your computer will be allowed to access the Internet; programs attempting to access your computer from the Internet will not be blocked. Allow all traffic disables all McAfee Firewall protection features and should only be used for diagnostic purposes.

2 Click Next.

Startup Options

This screen allows you to choose how you want McAfee Firewall to respond as you start your computer.

For your convenience, recommended Startup Load Options have been pre-selected for you.

1 Select **Load McAfee Firewall automatically at startup** if you want firewall protection as you start your computer. If you do not want McAfee Firewall to start as your computer starts, then clear this check box.

2 If you want to display a McAfee Firewall icon on your Windows desktop, then select **Place a McAfee Firewall icon on the desktop**. If you do not want an icon on your Windows desktop, then clear this check box.

3 Click Next.

Access to shares

If your computer is part of a workgroup, such as a home network, you can configure McAfee Firewall to allow access to your computer's network shares as well as allow your computer to access other computer's shares. A **share** is a resource such as a drive, directory, file, or printer available to a workgroup or home networked computers.

1. **Access to other shares**: check the **Allow my computer to access other computer's shares** if you want to allow your computer to have access to the shared drives, directories, folders, and printers, etc. of other computers in your workgroup or home network.
2. **Access to my shares**: check the **Allow other computers to access my shares** check box to allow other computers in your workgroup or home network to have access to your shared drives, directories, folders, and printers, etc.
3. Click Next.

Allowed applications

During the configuration process, McAfee Firewall scanned your computer's hard disk to identify programs that use the Internet. For example, programs of this type would include Internet browsers, Internet e-mail programs, and ftp (file transfer protocol) clients. On this screen, you will identify programs that you will allow to access the Internet through McAfee Firewall.

To allow specific programs to access the Internet, do the following:

1. From the list of applications displayed on this, check the check box corresponding to each program you will allow access to the Internet.

   Click **Search all drives** to search all of your computer's partitions, logical drives, and physical hard drives for programs that communicate using the Internet.

   If you do not allow any or all of the programs displayed on this screen to communicate, you will be notified when each attempts to do so and decide whether to allow access to the Internet at that time.
2. Click **Finish**.

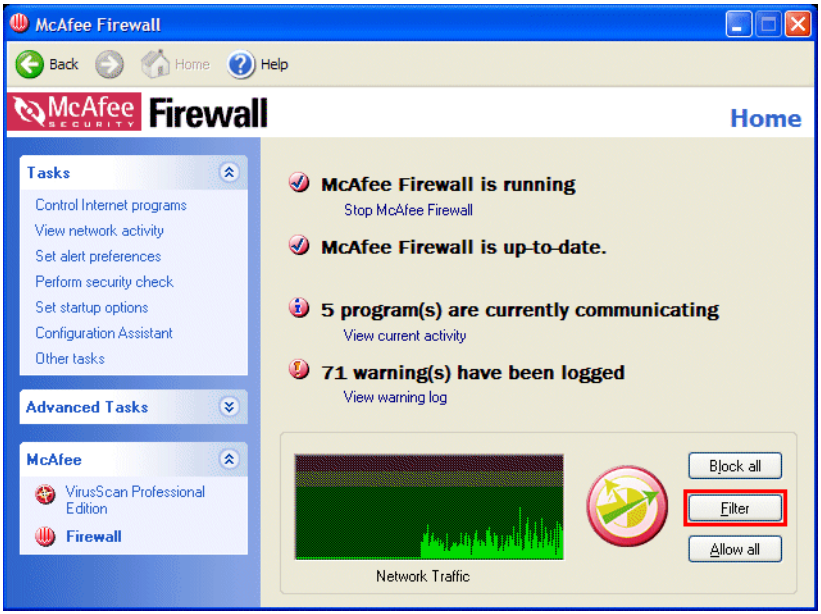
What's happens next?

After you complete the steps associated with setting up your initial configuration, the following events take place:

1. The firewall service starts.
2. The McAfee Firewall Home page displays.

You are now ready to start using McAfee Firewall!

The McAfee Firewall Home page



The McAfee Firewall main window is your central entry point to all of McAfee Firewall's Tasks, Advanced Tasks, and shared features. The McAfee Firewall interface displays three regions common to all of McAfee Firewall's screens.

The Title bar and Tool bar

Title bar

The Home page displays most of your standard Windows elements; that which includes:

- The title bar displays the name of the program that is currently running.
- Close and minimize buttons. McAfee Firewall's interface is of fixed length and width. You cannot resize the interface.

Tool bar

The tool bar displays four browser-like buttons that are common to all screens.

- **Back**. Click Back to return to the last screen viewed.
- **Home**. Click Home to go to the McAfee Firewall Home page from any screen.

- **Next**. In conjunction with the Back button, use Next to go to any previously viewed screen during your current session.
- **Help**. Click Help to view its submenu. The Help submenu may include any of the following items.

Help submenu item	Select this item to...
Help on this page	View online Help for the screen you are currently viewing.
Contents and index	View online Help for McAfee Firewall.
Help on the Web	Start your Internet browser and go directly to the McAfee Help Web site at McAfeeHelp.com.
McAfee at Home on the Web	Start your Internet browser and go directly to McAfee-at-home.com.
About McAfee Firewall	Version information about McAfee Firewall.

Status information

Depending upon your configuration, the McAfee Firewall Home page displays other helpful information such as:

- Firewall Status: **Running** or **Stopped**. Click the link below the status to start or stop McAfee Firewall.
- Home page notification. If there is an update to your version of McAfee Firewall available for download, select this task.
- The number of programs currently communicating. If you want to identify the program's communication, select this task to view your current activity.
- Firewall warning information. If there are any communication warnings, select this task to view the warning log.

Internet traffic settings

The Internet Traffic setting frame displays your current filtering setting. Here you determine if you want to **Block all**, **Allow all**, or **Filter** Internet Traffic. For more information about these settings, refer to Table 5-2 on page 71.

To change an Internet traffic setting, simply click the desired setting. Changes are real-time and effective immediately.

McAfee Firewall status

This region of the Home page displays the current running state of McAfee Firewall. It is either running or not running.

If the McAfee Firewall status message is...	Then...
McAfee Firewall is Running	◆ Click Stop McAfee Firewall to disable firewall protection.
McAfee Firewall is Stopped	◆ Click Start McAfee Firewall to enable firewall protection.

Network Traffic monitor

The Network Traffic monitor displays a graphic representation of real-time network activity. The monitor is color-coded to help you identify normal network traffic, port scans, and worst of all, attacks.

- **Green zone**: Activity displayed in this zone is normal network activity. It is not uncommon to see activity in this zone reaching the yellow area.
- **Yellow zone**: This is the caution zone. You can view the Activity Log to analyze data for this traffic. Activity in the yellow zone could represent a port scan.
- **Red zone**: Red represents the worst level of network activity and usually represents an attack. You can view the details of the attack by accessing McAfee Firewall Activity Log. If the attacker's IP address is available, you can attempt to trace the attacker using McAfee Firewall's Visual Trace component.

The Task pane

The Task pane displays links that allow you to start McAfee Firewall's **Tasks** and **Advanced Tasks**. Depending upon your configuration, the Task pane displays a **McAfee** list, links that allow you start the Home page for any other current McAfee product installed in your computer.

About Tasks

Starting a task is as easy as clicking its link. The Task list allows you to start McAfee Firewall's major components. Although the tasks you can perform will vary based upon your computer's operating system and its configuration, primary tasks include:

- **Control Internet programs**: This task allows you to explicitly block or allow specific programs to access the Internet.

- **View network activity**: Select this task to view real-time network activity and view your current activity log.
- **Set alert preferences**: Choose how you want McAfee Firewall to notify you when a potential security breach occurs.
- **Set up Home Networking:** Helps make setting up protections for your PCs sharing an Internet connection a breeze.
- **Perform a security check**: This task allows you to start the McAfee Firewall Security Check process.
- **Set startup options**: Choose how you want McAfee Firewall to start.
- **Configuration Assistant**: This task starts the Configuration Assistant.

About Advanced Tasks

Similar to the primary Task list, the Advanced task list may vary depending upon your version of Windows, its configuration, and other software that may be installed in your computer. McAfee Firewall's advanced tasks include:

- **Advanced options and logging**: Select this task to configure intrusion defense mechanisms, set up the automatic configuration of filtering rules, and identify the type of traffic you want to log.
- **Configure network adapters**: Choose this task to view your current network adapter and configure their communication settings.
- **Intrusion detection settings**: Select this task to configure how you want McAfee Firewall to respond upon its detection of an intrusion.
- **Block IP address**: If there is a specific IP address that you want to block from accessing your computer, or, if there is an IP address that is currently blocked that you want to allow, choose this task.
- **Set up password**: This task helps you to secure your McAfee Firewall settings with password security.
- **Other Tasks**: Select this task to navigate to a screen that allows you to start McAfee Firewall's shared features

About the McAfee list

The McAfee list displays links to start the Home page to any other supported McAfee product.

Other McAfee Firewall features

McAfee Firewall settings security check

Examines your firewall security settings, allowing you to rectify weaker settings before hackers get a chance to exploit them. The McAfee Firewall Settings Security Check flags and suggests changes to help you keep your system set to optimal security.

If Security Check detects an issue, click Fix and McAfee Firewall helps you analyze and correct potential problems.

Home networking wizard

Helps make setting up protections for your PCs sharing an Internet connection a breeze, providing helpful wizards to walk you through the process.

All networking media and hardware (such as cables and network adapters) must be installed on each computer in order for this wizard to locate your computers.

Password protection

Prevent others from tampering with your firewall settings by locking access to them with password security. Also helps keep your firewall protections secure by preventing the firewall from being shut down without your password.

About Visual Trace

Visual Trace is a multi-purpose Internet tool used for finding information and trouble-shooting connection problems.

At the simplest level Visual Trace shows you how packets (data) get from your computer to another computer on the Internet. You see all the nodes (equipment of various types on the Internet that is passing traffic) between your computer and the trace target.

There are many situations where you need this information. Visual Trace is a useful tool when troubleshooting connections or just verifying that everything is working OK. There is also a wealth of information presented by Visual Trace, including the domain owners, relative locations, and in many cases, the location of nodes.

Besides using Visual Trace to look for weak spots in a connection you can use it to:

- Discover whether you can't reach a site due to a failure at your Internet Service Provider (ISP) or further into the Internet
- Determine the point of a network failure that is preventing you from reaching a Web site.

- Determine the location of sites and their users, uncover the owners of a site, and help track down the origin of unwanted e-mail messages ('spam').
- Get detailed contact information on sites all over the world (where available).

How to start Visual Trace

You can start Visual Trace directly from the Windows start menu. You can also start Visual Trace from the McAfee Firewall Detail Activity screen, the Block IP dialog box, and if you are attacked, from the Windows system tray pop-up notification.

For more information about Visual Trace, please refer to online Help for Visual Trace.

McAfee Firewall Configurations

The configuration of McAfee Firewall is divided into two classifications – application (program) and system. Upon installation, a base set of rules for system services such as ICMP, DHCP and ARP are installed (these are considered default settings).

On the other hand, the programs classification is personalized. Whenever you run a new program that attempts to communicate over the Internet, McAfee Firewall will prompt and ask you whether you want to trust the program or not.

For example, using Internet Explorer, enter an Internet address or URL (i.e: http://www.mcafee-at-home.com) in the address bar of your browser and press ENTER. Internet Explorer will attempt to connect to that URL over the Internet. The first time you do this, McAfee Firewall prompts if you “trust” Internet Explorer. If you say “Yes,” McAfee Firewall notes Internet Explorer is allowed and whenever you use Internet Explorer in the future, McAfee Firewall will allow its traffic.

As you allow programs to use the Internet, McAfee Firewall “learns” the rules you are creating for the program and saves them for future use. If a Trojan horse program attempts to communicate out from your computer, McAfee Firewall will also prompt you whether you trust them or not, and the decision to block the Trojan horse program from communicating is easy and instantaneous.

Program configuration

During your first attempt to start McAfee Firewall, the Configuration Assistant asked you to identify programs that you want to allow to communicate. At such time, McAfee Firewall created a default set of communication rules for the programs (applications); designated as **allowed** to communicate.

Based upon the type of program, for example, Internet browsers, e-mail, ftp, IRC, and file sharing programs, McAfee Firewall identifies the type of program and creates a default set of communication rules for each program in your computer. That is, to either block, allow, or filter a program's communication attempts via the Internet.

Firewall Communication Alert Messages

A **McAfee Firewall Communication Alert** message displays if an unrecognized program attempts to communicate. There are several scenarios that could cause a program to be unrecognized.

- If you install a program that communicates via the Internet after installing McAfee Firewall, the program's first attempt to communicate will cause an alert message to display.
- Although the Configuration Assistant performs a thorough analysis of your computer's programs that use the Internet to communicate, it may not have been able to identify all of your computer's programs that use the Internet to communicate.

If an unrecognized program attempts to communicate, the resulting alert message generally asks you to select one of the following options:

- **No, deny at this time**: Blocks the program's current and all future attempts to communicate. The active program is added to the trusted list of programs with an allowed state of "blocked."
- **Yes, allow this time**: The active attempt to communicate is allowed. The program is not added to the trusted programs list.
- If you recognize the program and do not want to receive any future alerts for this program, check the **I recognize this program** check box.

> **TIP**
> If you allow or block a program the first time you are prompted, McAfee Firewall provides you with the flexibility to change this setting and block or allow it to communicate at any time in the future. As you exit McAfee Firewall, your settings are saved and will be the same the next time it is run.

Changing a program's allowed state

McAfee Firewall monitors Internet traffic to see which programs are communicating. Depending on your settings, it will allow, block, or filter a program's attempt to communicate.

If you choose to "Allow all" programs to communicate through your firewall, then all programs installed in your computer can communicate.

To view and configure the current list of trusted programs

1. From the Task list, select Control Internet programs.
2. Select the program whose filtering settings you wish to configure (or click Browse to add a program to the list).
3. Select one of the following options:
   - Filter this program's access to the Internet.
   - Allow this program to have full unfiltered access to the Internet.
   - Block this program from accessing the Internet.
4. To add a program to the list, click Add and browse to select the program you want to add. To remove a program from the list, select the program you want to remove and click Remove.
5. Click Apply.

How to customize filtering rules for a specific program

For all programs designated as "filter," McAfee Firewall provides power users with the flexibility to create a set of custom filtering rules for each filtered program.

> **TIP**
> The **Customize** button becomes accessible if and only if you select the **Filter this program's access to the Internet** option.

To create a custom filtering rule

1. From the Control Internet Programs screen, select the program for which you want to create a custom filtering rule.
2. Select the **Filter this program's access to the Internet** radio button.
3. Click **Customize**.

   If the program currently maintains a default set of rules created by McAfee Firewall, then the **Customize filtering rules** dialog displays. If the program *does not* maintain a default set of rules, then the **What do you want this filtering rule to do?** dialog displays.

4 Refer to the instruction's displayed on the Custom Filtering rules dialog boxes to complete your custom configuration.

Table 5-3. Customize Filtering Rules dialog buttons

Button	Description
Add	◆ Click **Add** to add a new rule and to display the **What do you want this rule to do?** dialog.
Remove	◆ Click **Remove** to remove a rule from the selected program. **CAUTION**: There is no "undo" feature.
Edit	◆ Click Edit to refine a filtering rule.
Restore	◆ Click **Restore** to restore the default rules for the selected program. **TIP**: If you inadvertently Remove a filtering rule, click this button to restore the default rules for the selected program.
OK	◆ Click **OK** to close the Customize Filtering Rules dialog and save your changes.
Cancel	◆ Click **Cancel** to close the Customize Filtering Rules dialog without saving your changes.

Primary functions

From the list of primary functions displayed on the Customize Filtering Rules dialog, you can choose one of the following:

Table 5-4. Primary Functions

You can choose to...	by...
Allow communication...	◆ protocol ◆ local port ◆ remote port
Block communication...	◆ IP address ◆ domain name ◆ direction

Refining conditions

After you select the primary function for the rule, you can further refine the rule by checking the check boxes for any or all of the communication characteristics:

With...	Using...
• direction	• protocols
• domain names	• remote ports
• IP addresses	• local ports

To customize the refinement condition, click [click here to select]. Depending upon the communication characteristics selected, various dialog and text boxes display. For example, if the custom rule states “Block this program from communicating and the IP address is,” then an Add / Edit rule text displays allowing you to enter an IP address. Similarly, if you want to block a program from communicating by protocol, an Edit Protocols dialog displays.

To save your changes, click OK.

System configuration

Your computer’s operating system performs many types of network communication without reporting directly to you. McAfee Firewall lets you explicitly allow or block different system functions. Settings may be different for each network device, since a computer, for example, can be connected to an internal network as well as having a dial-up connection to the Internet.

Use the steps below to control your System settings.

1. From the Advanced Task list, select Configure network adapters.
2. From the Configure Network Adapter Settings screen, select the adapter you want to configure and click Adapter Settings to view or change the properties of this adapter.
   Result: The Properties sheet for the selected network adapter displays.

You can then choose to allow or block NetBIOS over TCP, Identification, ICMP, ARP, DHCP, RIP, PPTP and other protocols (IP and non-IP).

Table 5-5. Default Settings for System Activity

System Activity Type	Description
NetBIOS over TCP: Blocked	This will block all file share activity over TCP as well as UDP broadcasts. Your system will not appear in anyone's “Network Neighborhood” and theirs will not appear in yours. If your system is configured to support NetBIOS over other protocols, such as IPX or NetBEUI, then file sharing may be allowed if “non-IP protocols” are allowed (see “Other Protocols” below).
Identification: Blocked	This service is often required when getting email and is required by most IRC servers.
ICMP: Blocked	This protocol is often abused as a method of breaking people's network connections (especially on IRC).
ARP: Allowed	ARP is a necessary Ethernet protocol and is not known to be a threat.
DHCP: Allowed if your system uses DHCP	The program looks in your system Registry to see if one of your network devices uses DHCP. If so, then DHCP is allowed for all devices. If not, then it is blocked for all devices. If you have more than one network device and one uses DHCP, you should check the DHCP setting for each device and allow only for the device that uses it (most often cable or ADSL modems and some internal networks, not for dial-up).
RIP: Blocked	Allow RIP if your administrator or ISP advises you to.
PPTP: Blocked	This should only be altered by the administrator.
Other Protocols: Blocked	If you are on an IPX network, you should allow “non-IP protocols”. If you use PPTP, you should allow “other IP protocols”. Ask your network administrator before making any change here.

McAfee Firewall's Intrusion Detection System

Unlike other intrusion detection tools, McAfee Firewall's powerful Intrusion Detection System (IDS) is simple to configure and activate. Instead of requiring users to learn and understand a complex set of attacks to build their own defense lines against intrusions, McAfee Firewall's development team created a tool that, when activated with the click of a button, detects common attack types and suspicious activity.

Unprotected computers can be victimized. For example, attackers can use a TCP port scan to find out what services you are running on your machine. Once this is accomplished, they can try to connect to those services and attack your computer. If the attacker discovers that you are running a TELNET, ftp, or Web server, the attacker can try each of your computer's ports sequentially, from 1 to 65535, until an open port is found that they can connect to.

McAfee Firewall's IDS feature looks for specific traffic patterns used by attackers. McAfee Firewall checks each packet that your machine receives to detect suspicious or known attack traffic. For example, if McAfee Firewall sees ICMP packets, it analyzes those packets for suspicious traffic patterns by comparing the ICMP traffic against known attack patterns. When McAfee Firewall matches packets with a known attack pattern, the software generates an event to warn you of a possible security breach.

When intrusion detection is on, traffic is checked by the intrusion detection system. When intrusion detection is active and McAfee Firewall detects an attack, you can block further communication from the suspected machine's IP address indefinitely or for a specific time period. When an attack is detected, McAfee Firewall alerts you with a Windows system tray notification.

NOTE
Because McAfee Firewall is analyzing packets and looking for patterns of packets that identify specific types of attacks, this feature may result in a very slight impact on your machine's performance.

How to Configure the Intrusion Detection System

Use the steps below to configure McAfee Firewall's intrusion detection system:

1. From the McAfee Firewall Home page, click Advanced Tasks.
2. From the Advanced Tasks list, select Intrusion detection settings.

Refer to the instructions displayed on the Configure Intrusion Detection Settings screen to complete this task.

Common attacks recognized by IDS

The following table lists attacks recognized by McAfee Firewall's IDS, a description of each attack, and the risk factor assigned to each attack.

Attack	Description	Risk Factor
1234	Also known as the Flushot attack, an attacker sends an oversize ping packet that networking software could not handle. Usually, computers hang or slows down. If a total lockup occurs, unsaved data may be lost.	Medium
Back Orifice	Back Orifice is a back door program for Windows 9x written by a group calling themselves the Cult of the Dead Cow. This back door allows remote access to the machine once installed, allowing the installer to run commands, get screen shots, modify the registry, and perform other operations. Client programs to access Back Orifice are available for Windows and UNIX.	High
Bonk	Designed to exploit an implementation error in the first Teardrop patch released by Microsoft, this attack is basically a Windows-specific variant of the original Teardrop attack.	High
Fraggle	This attack is a UDP variant of the Smurf attack. By sending a forged UDP packet to a particular port on a broadcast address, systems on the "amplifier" network will respond to the target machine with either a UDP response or an ICMP UNREACHABLE packet. This flood of incoming packets results in a denial of service attack against the target machine.	High
IP Spoofing	IP spoofing involves sending data with a falsified return IP address. There is nothing inherently dangerous about spoofing a source IP address, but this technique can be used in conjunction with others to carry out attacks TCP session hijacking, or to obscure the source of denial of service attacks (SYN flood, PING flood, etc.).	Medium
Jolt	A remote denial of service attack using specially crafted ICMP packet fragments. May cause slowdowns or crashes on target systems.	High
Jolt 2	A remote Denial of Service (DoS) attack similar to Jolt that uses specially crafted ICMP or UDP packet fragments. May cause slowdowns or crashes on target systems.	High
Land	This attack is performed by sending a TCP packet to a running service on the target host, with a source address of the same host. The TCP packet is a SYN packet, used to establish a new connection, and is sent from the same TCP source port as the destination port. When accepted by the target host, this packet causes a loop within the operating system, essentially locking up the system.	High
Nestea	This attack relies on an error in calculating sizes during packet fragment reassembly. In the reassembly routine of vulnerable systems, there was a failure to account for the length of the IP header field. By sending carefully crafted packets to a vulnerable system, it is possible to crash the target.	High

Attack	Description	Risk Factor
Newtear	A Denial of Service (DoS) attack that usually causes computers with a Windows NT-based operating system to crash. Although the attack is not usually harmful to the computer itself, data from running applications will most certainly be lost.	High
Oshare	A Denial of Service (DoS) attack caused by sending a unique packet structure to your computer. The results of these attacks can vary from a complete system crash, increased CPU load, or momentary delays, depending upon your computer's configuration. This will affect almost all versions of Windows 98 and NT-based systems with varying degrees based on the hardware involved.	High
Ping Flood	This attack involves sending very large numbers of ICMP ECHO (PING) requests to the host under attack. This attack is particularly effective when the attacker has a faster network connection than the victim.	High
Ping of Death	With this attack, a remote user can cause your system to reboot or panic by sending it an oversized PING packet. This is done by sending a fragmented packet larger than 65536 bytes in length, causing the remote system to incorrectly process the packet. The result is that the remote system will reboot or panic during processing.	High
Port Scanning	While not an attack in and of itself, a port scan often indicates that an attacker has begun looking at your system for potential weaknesses. A port scan consists of checking every TCP and/or UDP port to see what services (and hence, what vulnerabilities) might be present.	Low
Saihyousen	The Saihyousen attack may cause some firewalls to crash. It is caused by an attacker sending a stream of UDP packets.	High
Smurf	This attack is carried out by sending an ICMP ECHO REQUEST (PING) packet with a forged source address matching that of the target system. This packet is sent to "amplifier" networks — networks that allow sending packets to the broadcast address — so that every machine on the amplifier network will respond to what they think is a legitimate request from the target. As a result, the target system is flooded with ICMP ECHO REPLY messages, causing a denial of service attack.	High
SynDrop	Overlapping fragmented data sent by an attacker causes your computer to become unstable and or crash. Unsaved data could be lost.	High
Syn Flood	This attack can be used to completely disable your network services by flooding them with connection requests. This will fill the queue which maintains a list of unestablished incoming connections, forcing it to be unable to accept additional connections.	High
Teardrop	On vulnerable systems, it is possible to take advantage of a flaw in the way the TCP/IP stack handles fragmented packet reassembly to consume available memory resources. By sending a specially crafted IP datagram, this attack can cause many operating systems to hang or reboot.	High

Attack	Description	Risk Factor
UDP Flood	A remote denial of service attack designed to flood the target machine with more data than it can process, thereby preventing legitimate connections from being established. Machine is inaccessible via TCP/IP. Occurs when machine is put to sleep and then awakened. Make sure that “Load Only When Needed” is not checked in the TCP/IP control panel. Then TCP/IP is loaded all the time, allowing McAfee Firewall to function while the machine is asleep.	High
Winnuke	This attack is a Denial of Service (DoS) attack that completely disables networking on many Win95 and WinNT machines. Although Winnuke will not necessarily damage your computer, you may lose any unsaved data at the time of the attack. Restarting your computer should restore full operation.	High

McAfee Internet Security's Shared Features 6

QuickClean Lite

Clean your computer with QuickClean Lite

QuickClean Lite enables you to clean your computer of unnecessary files and free valuable hard disk space.

You can use the QuickClean Lite wizard to perform any of the following cleaning tasks:

- Clean your Recycle Bin.
- Remove files that accumulate as you browse the Internet. Files of this type are stored in folders called Temporary Internet or Cache folders.
- Remove Shortcuts without an associated program, application, hypertext link, etc.
- Delete lost file fragments.
- Delete Windows Registry information, shortcuts, and system file references for applications that no longer exist on your computer.
- Delete temporary files.
- Remove deleted and sent messages from a Microsoft supported e-mail client (i.e.: Outlook, Outlook Express).
- Delete Most Recently Used shortcuts.
- Use McAfee Shredder to securely shred the items you want to remove from your computer.

How QuickClean Lite works

First, you select the types of files you wish to remove from your computer. A wizard guides you through this process. Next, the QuickClean Lite wizard scans the contents of your hard disk and identifies all files meeting your pre-selected criteria.

The user proceeds with the cleaning task if they are satisfied with the results of the scan. Finally, QuickClean Lite provides a graphic representation of the amount of reclaimed space after deleting the files.

WARNING
Deleted files are not backed up. You cannot restore files deleted by QuickClean Lite.

How to start QuickClean Lite

There are two methods you can use to start the QuickClean Lite wizard.

1. From any VirusScan Professional screen click the "Other tasks" Task, and select Start QuickClean Lite.
2. From the Windows task bar click the Start button, point to Programs > McAfee > McAfee Shared Features and click QuickClean Lite.

If you need help...

For additional information about using QuickClean Lite refer to online Help. You can access online Help for QuickClean Lite by clicking Help on any QuickClean Lite window.

McAfee Shredder

Securely delete files using McAfee Shredder

When you save a file in Windows, it is stored in multiple pieces (in clusters made up of multiple sectors) on the disk. Windows also saves a road map, or index, that points to these clusters in two copies of the FAT (File Allocation Table). The FAT contains the directions to all the pieces of your files, so that applications can find them again later.

In addition to FAT file systems, McAfee Shredder supports New Technology Filing System (NTFS). NTFS is the file system used by Windows NT, Windows 2000 and Windows XP.

When you delete a file, all the information stored in that file is not actually erased from your disk. Instead, Windows simply frees the clusters where the file was stored, making those locations available in the FAT. Thereafter, applications can write new information to those clusters. This means that all or part of your files can be reconstructed even after you delete them. Undelete programs can reconstruct a deleted file very easily, especially immediately after you delete the file and before you save any new information that might be written over the deleted file's contents.

For privacy and security reasons, you may want to be positive that the information stored in files you delete is permanently erased from your computer. McAfee Shredder does this for you by "security wiping" deleted files so they cannot be restored or rebuilt using undelete utilities. Unlike other file security erase programs, McAfee Shredder erases even the filename and the compressed data on DriveSpace drives. Note that it is not possible to shred network files, or files compressed with compression other than DriveSpace in an absolutely secure manner.

TIP

You can select McAfee Shredder properties to specify the shredding level to perform. You can select: Quick to shred the information once; U.S. Government Multipass to make seven passes of repeatedly erasing the data; or Custom to indicate how many passes to make which allows up to 99 passes.

Shredder is easy to use!

You can shred files using drag and drop, which is a fast way if all the files are centrally located. If the files are in several places, you can shred them by starting McAfee Shredder and selecting the files to erase. A wizard guides you through the process.

McAfee Shredder allows you to shred files on your PC's Recycle Bin, Temporary Internet, as well as Web site history folder. You can also specify the number of shredding passes (1-99) and can now have the option to shred an entire drive.

TIP
If your computer is running on Windows Me, some files even if shred, may be retained on your PC since these are protected by the Windows Me System Restore.

Refer to the online Help file to display step-by-step instructions on how to shred selected files and non-file data.

WARNING
After you shred non-file data, you will not be able to undelete any deleted files that utilized this information.

Updating McAfee Internet Security 7

About Instant Updater

As technologies advance, we continually provide updates to McAfee software products. To ensure the highest level of protection, you should always obtain the latest version of your McAfee product.

Updating your software is simple using McAfee's Instant Updater. It is a seamless process and requires minimal interaction on your part.

Instant Updater is also the mechanism used to register your product with McAfee. In order to obtain product updates, you must register your product with McAfee.

Why Do You Need to Update?

- New features may be released for your McAfee product.
- Product fixes are periodically available.
- New product content is updated periodically.
- Updates to anti-virus signature files are frequently available.

How Does the Updating Process Work?

Instant Updater allows you to obtain and apply updates to your McAfee products while connected to the Internet. If an update exists, you will receive a notification. At that time, you can download and apply the updates to your products.

Instant Updater features

- **Auto Update is Instant Updater's default setting**.

  Instant Updater silently checks for, and as appropriate, applies product updates while you are connected to the Internet.

  Occasionally, Instant Updater may ask you to restart your computer to apply the updates. Auto Update checks for updates daily to ensure that your McAfee product, product content, and related elements such as the virus scan engine and DATs are current.

- **Auto Inquiry**: If Auto Inquiry is enabled, it allows you to receive notification of product updates while connected to the Internet. We do not recommend Auto Inquiry if you have slow internet connection
- **Manual Updating**: If you rarely connect to the Internet, you may prefer to use Manual Updating with your McAfee product. You can manually update while connected to the Internet. To do this, select the UPDATE function from within the individual product.

  Manual Updating provides you with explicit control of the updating process.

Home page query

Related to Instant Updater is **Home page query**. This feature allows to configure your McAfee product's home page to display a message when an update is available. After you install your McAfee software, Home-page query "on" is the default setting.

Configuration

For additional information regarding auto inquiry and auto update settings, please refer to online Help.

Product Support and Customer Service

A

Contacting Customer Service and Technical Support

For Product Support and Customer Service, please visit http://www.mcafeehelp.co.uk. Our support Web site offers 24-hour access to solutions to the most common support requests in our easy-to-use 3 step Answer Wizard. You may use our advanced options, which include a Keyword Search and our Help Tree, a tool designed for the more knowledgeable user in mind.

If you cannot find a solution to your problem, you may also access our FREE Chat Now! and E-mail Express! options. Chat and E-mail enables you to quickly reach our qualified support engineers and customer service agents, through the Internet, at no cost. Phone support information can also be obtained from our self-help web site at: http://www.mcafeehelp.co.uk.

About McAfee-at-home.com

McAfee is famous for its dedication to customer satisfaction. We continue this tradition by making our site on the World Wide Web a valuable resource for answers to your questions about McAfee Consumer Products. We encourage you to visit us at http://www.mcafee-at-home.com and make this your first stop for all of your product needs.

Emergency Support

If you installed a McAfee retail product into your computer and a computer-related emergency arises that prevents you from connecting to the Internet, you may call the telephone number displayed below to obtain a technical support callback.

Emergencies consist of the following:

- Your computer cannot connect to the Internet.
- Your computer was attacked by a virus and it cannot connect to the Internet.
- Your computer freezes after installing a McAfee product.

- You would like to speak with a customer service agent to purchase a McAfee product, rather than make a purchase at our eStore.

For a technical support callback, please be sure to leave your complete name and telephone number; and our expert technical support representatives and customer service agents will return your call as soon as possible.

When we call you, please have the following information readily available:

- The version number of you McAfee software. You can locate this information by selecting Help > About.
- The Windows operating system and version number
- Amount of memory (RAM)
- Model name of hard disk (internal / external)
- Extra card, boards, or hardware
- A complete description of the problem, for example, the EXACT error message as it appears on screen, what actions did you performed before you received the error message, is the error persistent, can you duplicate the problem.

Contact addresses:

Network Associates International B.V.
P.O. Box 58326
1040 HH Amsterdam
The Netherlands

Customer Service
McAfee Consumer Products
Apollo Contact Centre
Units 2-6, Boucher Business Centre
Apollo road, Belfast BT12 6 HP
UK

Emergency Telephone Numbers:

Country:	Telephone Number:
Austria	017 908 75 810
Belgium	02 27 50 703
Denmark	03 5258 321
Finland	09 229 06 000
France	01 70 20 0 008
Germany	06 966 404 330
Ireland/Eire	01 601 55 80
Italy	02 45 28 15 10
Luxembourg	040 666 15670
Netherlands	020 504 0586
Norway	02 3050420
Portugal	00 31 20 586 6430 (English spoken)
Spain	901-120 175 (*toll share)
Sweden	08 57 92 9004
Switzerland	022 310 1033
United Kingdom	020 794 901 07

Virus definition renewal

This product includes twelve (12) months of free virus protection updates obtained using Instant Updater. Renewal subscriptions are available at a cost of **$9.95 USD **** or **€ 10,95 EUR** ** per year at the ***www.McAfee-at-home.com*** **Buy** page.

Note

** Please note that pricing is subject to change and we suggest that you refer to ***www.McAfee-at-home.com*** for the latest price quote. Other payment methods may be available at an additional price.

Eleven months after registering this product, Instant Updater will prompt you to renew your virus protection subscription. You must renew your subscription in order to update your virus protection. Your product will continue to function if you do not renew your subscription.

Internet Security and Privacy B

This chapter provides some background information that will help you understand Internet security and privacy threats, and discusses strategies for using McAfee Internet Security to protect yourself and your computer.

Networks and the Internet

A computer network links individual computers together so they can share data and resources. To network, computers need some means of connection—either a modem or a Network Interface Card (NIC—some computers have NICs already built-in). The modem or NIC is responsible for sending and receiving data through the network. Networks are sometimes called local area networks (LAN) because they link the computers at a single locale, such as an office or building. In a small office, computers can be linked directly by connecting them together with cable. This very simple network is called a peer-to-peer network, wherein all of the computers are equal to one another. Windows has peer-to-peer networking capabilities built into the operating system. The increased traffic in larger networks requires the services of a special computer, called a server. Servers help larger networks operate by figuring out how to route messages to the appropriate recipient.

The Internet is a vast computer network, connecting computers together from around world and allowing them to work together and share information. When you connect to the Internet, your computer becomes a part of a worldwide network of computers.

TCP/IP Is the Subsystem

The Internet is based on a system called Transmission Control Protocol / Internet Protocol (TCP / IP). TCP allows computers to share data by first breaking it down into little segments called packets. In addition to data, each packet contains the address of the machine sending the packet, and the address of the intended recipient. The TCP part of the system is what is responsible for addressing the data and breaking into packets. IP, the second part of the system, is responsible for routing packets from the sending computer to the recipient computer. Special computers called routers read the address on each packet, and figure out how to route them to the appropriate destination.

Why packets?

Why go through all this trouble, breaking data down into packets? The answer lies in the origins of TCP/IP. Like the Internet itself, it is a product of the Cold War. The United States Department of Defense originally developed the Internet. It was designed to ensure secure communications, even with multiple communications network failures anticipated in the event of a nuclear war. TCP/IP solves the problem of network failure by assuming that a certain amount of noise always exists in the network— noise referring either to random data errors or more serious system crashes. If you have ever tried to speak in a noisy room, you know the necessity of repeating yourself—and that is exactly what TCP/IP is designed to do. Breaking the data down into packets allows the Internet to seek alternate routes if one route is inaccessible. If a packet cannot get through or arrives damaged, the receiving computer simply requests it again until it arrives successfully.

When you send an e-mail message, for example, it is broken into several packets. Depending on how noisy the network is, each packet may need to be routed over a separate route in order to find its way to its destination. Furthermore, network problems may cause some of the packets to be delayed so they arrive out of order. To compensate, TCP examines each packet as it arrives to verify that it's OK. Once all the packets are received, TCP puts them back in their original order. Of course, all of this happens quickly and automatically, so you will never see the process at work.

The Internet and the Web…what is the difference?

Before the Web, the Internet was mostly command-line driven and character-based— you had to type in the exact Internet address of the place you wanted to go at a command line. In 1989, Tim Berners-Lee of the European Particle Physics Laboratory proposed a new way to share information over the Internet. The essential feature in Berner-Lee's vision of the Web is that it links documents together. When you click a link on a Web page, you are automatically connected to another Web site. This linking function, combined with the increasing graphics abilities of home computers, transformed the Internet into a graphically rich place, complete with video, sound, and pictures. Through the linking of information together in a graphically appealing package, the Web made the Internet more attractive to the typical consumer.

The Internet is a network of linked computers that uses TCP/IP as its underlying messaging system. The World Wide Web (WWW, or just "Web" for short) is hosted by the Internet, and is an ever-expanding collection of documents employing a special coding scheme named Hypertext Markup Language (HTML).

HTML is a set of commands designed to be interpreted by Web browsers. An HTML document consists of content (prose, graphics, video, etc.) and a series of commands that tell a Web browser how to display the content.

About Privacy and Security on the Web

Before the advent of the Web, Internet security usually posed a problem only for system administrators trying to keep meddlesome hackers away from their systems. When the Web arrived, the popularity of the Internet skyrocketed. Almost overnight, people began doing all sorts of potentially sensitive activities over the Internet, including: banking and stock transactions; sending personal data to Web sites; performing Web searches; and ordering books and clothes. While the Web is responsible for making the Internet more accessible, it also opens new possibilities for data theft, invasions of privacy, and fraud.

Why does Internet privacy matter to me?

Step back and consider the range of sensitive transactions we make every day. As an example, consider a simple ATM transaction. We assume that following conditions prevail whenever we use our ATM cards:

- **Privacy**: Only you and the intended recipient can access the transaction information. The PIN you use to access your bank account provides a fairly high level of privacy—as long as you don't share your PIN with others, and don't leave your card lying around, your checking account balance is safe from prying eyes.
- **Integrity**: Nothing can intervene and change the information during the transaction. When we take twenty dollars out of our checking account, we have a reasonable expectation that the ATM will not add an extra zero.
- **Trust**: You can trust that the recipient is who they claim to be; the recipient can trust that you are who you claim to be.

Organizations like banks and insurance companies are legally obliged to abide by federal statutes that govern the sanctity of your transaction information. The problem with Internet is that it has not yet evolved into well-established institutional mechanisms that guarantee the sanctity of your information.

Privacy on the Web

Who is snooping?

Hackers are a breed of human being that thrive on gaining illegal access to computers in order to access, steal, and sometimes corrupt data. Many hackers are quite benign—breaking into a secure system is a challenge and a thrill. But some computer hackers think that if they don't care for someone or some organization, it is OK to break in to their computers and wreak havoc. Other hackers think that the online theft of money and resources is legitimate, as long as it goes to support more hacking.

Snooping and Sniffing

Since its inception, the Internet has been (and largely remains) an open network. Openness means that information on the Internet travels without any special security: Anyone who can monitor network traffic can intercept it. This sort of monitoring is called “sniffing,” and is easy to perform using “sniffers.” Sniffers are programs (or hardware devices) designed to monitor data traveling over a network. Originally, sniffers were designed to help network administrators track down networking problems. Unfortunately, the same tool can also be used to steal information. Sniffers are insidious and difficult to detect.

Sniffing often begins when a hacker breaches the security of a local Internet Security Provider (ISP). A hacker does not need physical access to the ISP’s premises—sometimes a telephone line is sufficient (although it is also possible to sniff with physical access to network cables). Once a hacker compromises an ISP’s system, the network traffic that travels through the ISP is no longer secure.

Web Servers and Firewalls

Secure transactions are only one part of the problem. When an ISP’s Web server receives information, the ISP must be able to keep the information safe. Hackers like to attack the security of Web servers because Web server security is still in its infancy. As a consequence, Web administrators assume that a Web server is open to attack, and try to keep them separated from other, mission-critical computers. Some Web applications must, however, interact with corporate databases, an open door to a clever hacker. One form of security technology called a “firewall” can close the door, however, cannot safeguard certain services.

What can I do to keep my stuff safe?

With sniffer in place, a hacker can intercept credit card numbers and other private information by capturing data transmissions, and then using pattern matching algorithms to filter out the valuable information. Intercepted credit card info can be sold to criminals, intent on committing fraud.

To avoid this problem, Web browsers incorporate encryption technology that cloaks information and makes it difficult to get at. Encryption is the basic technique that the Web uses to guarantee information security.

The current encryption standard is called “Secure Sockets Layer” (SSL), supported both by Microsoft and Netscape, and incorporated in their browsers. An icon in the browser changes to indicate that SSL is active. When you make a transaction with SSL active, you can be fairly comfortable that the transaction is safe.

When you visit an SSL-secured site, the latest versions of Netscape Communicator and Microsoft Internet Explorer use a visual cue to tell you that the site is secure. For more information, see How can I tell if a Web site is secure?

TIP

McAfee Internet Security's Security Check lets you know if your Web browser is up-to-date. The latest browser versions usually offer an enhanced degree of security.

How can I tell if a Web site is secure?

Today, many sites use SSL to set up secure commerce on the Web. In addition to Web server security, the most common Internet browsers provide feedback about the security level of the site to which you are currently connected. For example, Netscape Communicator displays a lock icon in the lower left corner of the browser window. If the lock icon is broken, the site is not secure. If the lock symbol is not broken, the site is secure. In addition, if the lock symbol has a gold background, the site is using strong, 128-bit encryption.

Recent versions of Microsoft Internet Explorer and America Online browsers also display security information. For more information about how your browser indicates the security level of sites, refer to your browsers online help, or the printed documentation.

If SSL is so great, what is the problem?

SSL is affected by a couple of problems. One problem is that not everyone has an SSL-enabled server or browser. Some Web administrators don't want to use SSL because they have to pay for it, and it can also slow down server transactions. A more onerous problem that affects SSL is the way it is implemented. It turns out that some developers made incorrect assumptions about SSL, which means some older browser versions are less secure. The good news is that Microsoft and Netscape now coordinate their security efforts, which means a more secure, universal standard for Web security.

What about authentication?

Authentication is a method of assuring that both parties to an Internet transaction are who they claim to be. For example, if you get account balance information from your bank, you want to be sure that you are contacting the bank, and not some unauthorized entity. In addition, the bank wants to be sure that they are providing the information to you, and not just to a person who happens to know your bank account number.

Authentication usually entails entering a user ID and a password. To circumvent intercepted passwords and IDs, authentication employs encryption to scramble this information before transmitting it.

Certificates are Microsoft technologies designed to guarantee a person's identity and Web site security. Personal certificates verify that you are who you claim to be. Web site certificates verify that a Web site is secure and what it claims to be (so Web sites can't falsify their identity). When you open a Web site that has a certificate, Internet Explorer checks if the certificate is correct. If the certificate is not OK, Internet Explorer warns you. Certificates are great, in theory. The problem is that they only establish a security standard—Web sites are free to choose to use certificates, or not.

How does encryption work?

The only way to keep a secret is if you do not tell anyone, and if you do not jot it down. If you need to share the secret, you can hide it within another message, and let the intended recipient know how to find it. Computer encryption hides messages by making the original data unintelligible. The intent is to garble the data so that it can not be read. In this case, the data it self is useless if access by an unintended recipient.

The simplest encryption systems use letter shifting, in which a message is encrypted by shifting every letter n letters later in the alphabet. For example, say A is changed to B, and B to C, etc. As long as the recipient knows how you shifted the letters, they can easily decrypt the message by reversing the process. Of course, a brute force approach to breaking this sort of encryption would simply try all possible 26-letter combinations until the final message was retrieved—not a very strong method of encryption.

Computer encryption uses a much more difficult technique of hiding the message. Rather than a simple letter-shifting scheme, the original message is transformed by a mathematical algorithm. The algorithm uses a secret "key" to scramble the message, and the key is necessary to unscramble it. The key is similar to a house key: The more teeth a key has, the more difficult it is to pick the lock. Similarly, "strong" encryption uses keys with many "teeth"—in this case, bits of data.

There are two commonly used levels of encryption. The international standard is 40-bit encryption, but some sites in the United States use a higher level of 128-bit encryption. The number of bits indicates the length of the key used to encrypt data. The longer the key, the stronger and more secure the encryption.

On the Web, your browser works with secure Web sites to establish and manage the encryption that secures information. If your browser security options include the Secure Sockets Layer (SSL), which ensures data transmission privacy, you should turn on this option to facilitate secure data transmission.

TIP

McAfee Internet Security's Security Check automatically checks your browser's security level, and lets you know if you need to change it.

Security on the Web

One of the most exciting Web developments is the evolution of downloadable, executable programs. Java and ActiveX are two tools that help developers create programs that can “live” inside Web pages, and use your Web browser to automatically run over the Internet. Java allows Web pages to host small programs called “applets.” When Java-enabled browsers access a Web page containing Java, they automatically download and run the applets they find on the page. This is an intriguing development, since it makes it possible to download and run programs over the Web. Complete, Web-driven programs written entirely in Java are on the horizon. ActiveX is a similar technology, developed by Microsoft.

Java contains an internal security system that addresses security risks. ActiveX uses a different model, based on certificate authentication. Certificates contain information about who developed the ActiveX code. The idea here is that if you know who developed the code, it is safe to run it. Both security schemes offer a level of safety, but no one can yet promise that executable content is entirely safe.

Nasty Applets

One possible security threat is a malign Java or ActiveX program that attacks your computer over the Web. A nasty applet might, for example, thwart Java security by circumventing its security model, and destroy data on your hard disk, or grab sensitive information from your hard drive. The latest browsers have done a good job of fixing these issues. As long as you are using the latest version of your browser, you are protected. To date, there have been no legitimate reports of hostile Java or ActiveX harming anyone. However, there is no guarantee that an attack will not happen in the future.

Can I prevent programs from accessing the Internet?

You can use McAfee Internet Security to specify the applications that are allowed to access the Internet from your computer. Obviously, your default Internet browser is one of these applications.

If the McAfee Internet Security Gatekeeper is running in the background while you work on the Internet, each time an application tries to access the Internet a dialog box appears to ask if you want to allow this access once only, always, or never.

Computer Viruses and the Web

A computer virus is a small computer program that automatically replicates itself and spreads from one computer to another. Viruses may infect programs, your hard drive, and even some document files that employ macros. Viruses do not infect data files, but they can create problems that prevent you from accessing your data. Viruses are not accidents—they are always created by computer programmers. PC viruses are similar to biological viruses in that they:

- Are spread from host to host—the "host," in this instance, is your PC.
- Are very good at reproducing themselves.
- Can wreak havoc on an infected host system.

Biological viruses have proven to be tenacious— modern medicine's success in fighting viral infection has, so far, been rather limited. Fortunately, PC viruses differ from biological viruses in that they are easier to combat, once they are identified.

Are viruses really that dangerous?

Bear in mind that your chances of contracting a PC virus are slim, and even more so, your chances of contracting a truly vicious virus. The scariest viruses are malicious programs that intentionally corrupt or delete the data on your PC. More benign viruses might simply display a message on your monitor or make a strange sound, and then disappear. But even the most benign virus occupies some disk space, and many remain in memory, which can cause your PC to crash or behave erratically.

Types of Viruses

There are three main types of viruses:

- **File or program viruses**: A program virus attaches itself to a specific program on your PC. Since many PC's share certain files in common (for example, the DOS program command.com, or the command "dir"), which make these files tempting targets for virus programmers. Program viruses are dormant until you run the associated program.
- **Boot viruses (or Master Boot Record viruses)**: The boot sector of a disk is a physical location on the disk that contains information about the disk and the files it contains. All disks and drives have a boot sector, even if they aren't "bootable." A boot virus infects the boot sector of floppy disks and hard drives, and are activated when you access or boot from an afflicted disk.

- **Macro viruses**: Macro viruses are contained in document files, such as Microsoft Word or Excel files. These files can contain macros that can automate your work—but macros can also be written to do damage to your PC. Macro viruses are activated when you open an infected document file.

- A final word should be said about **hoax "viruses,"** which are not viruses in the strictest sense of the term. A hoax virus replicates a hoax, spread by misinformed (if well intentioned) e-mail claiming that if you download a certain file, or if you receive an e-mail with a certain subject line, you will infect your PC with a virus. E-mail messages are always safe; they are simple text files, and cannot contain viruses. Attachments to e-mail messages (an attachment is a file that a message sender attaches to a message—it is downloaded to your PC when you retrieve the message) can contain viruses. (If E-mail file access is turned on in Virus Sentry, McAfee Internet Security automatically scans e-mail attachments before you open them.)

How can my PC become infected with a virus?

An important thing to keep in mind is that viruses are spread only when you run an infected application (or open an infected document file, in the case of macro viruses). A virus cannot travel over your telephone line and infect your PC on its own. You must first download or copy an infected application and then run the application in order to infect your PC with a virus.

The only way to entirely avoid virus infection is to do nothing—don't use the Internet; never download a file; never accept a diskette from someone else; never share Word or Excel files. Of course, this draconian "Robinson Crusoe" cure is unrealistic in today's computing environment, where sharing data is the norm and accessing the Internet is an everyday occurrence.

> **TIP**
> McAfee Internet Security offers comes with McAfee VirusScan which is easy to use. It automatically scans your PC for signs of virus infection, and investigates suspect files before they have a chance of infecting your PC.

Viruses are spread when infected diskettes are shared between PCs, and when you download and run infected files from online services, bulletin boards, or the Internet. Another potential (but remote) route for virus transmission is when you access Web pages that use Microsoft ActiveX technology or Sun's Java. Web pages that use ActiveX, for example, can automatically download programs to your PC, and these programs might be infected with a virus. Although there is no known case where ActiveX and Java have spread viruses, there is still a possibility— remote as it may be—for your PC to encounter a virus in this way.

A virus might be hidden in the next file you download, or on a diskette you borrow —even diskettes purchased at a store. Downloaded shareware is also a source of infection.

Although Java and ActiveX are not, strictly speaking, viruses (i.e., it can't spread and replicate), they can still harm your PC. McAfee Internet Security's default settings allow it to monitor all Java and ActiveX activity on your PC, and warn you before something potentially dangerous occurs.

Frequently Asked Questions About Internet Privacy

What information do Web sites collect about me?

Web sites collect information about you in two major ways.

- First, you can provide the information yourself when you register software or respond to Internet questionnaires.
- Second, when you ask to be allowed access to the electronic version of a newspaper, or use a "shopping cart" to buy products on the Web, a cookie, described in "What are cookies and how are they used?," on page 112, might be written to your computer where it stores information, such as your user ID and password for the newspaper or the articles you bought with their quantity and price.

What information do companies get when I register products online?

Companies get only the information that you enter in the registration form when you register electronically. They do not get any information about your computer system, your use of your computer, or other stored information unless you provide it as part of the registration.

This information is used for the company's marketing research and to send you information about new releases, other products, and so on. The information might be sold to other companies, just as mailing lists of magazine subscribers or mail order companies can be sold to others.

Some companies allow you to specify that you do not want to receive mailings or to have your name and address sold to other companies. If the company does not provide this option, you can enter false information to prevent mailings, either postal or electronic, from reaching you.

What are cookies and how are they used?

A cookie is a small file that contains data. The data in the cookie varies, depending on its purpose. Upon the request of a Web site, your Web browser stores cookies on your computer. Usually, cookies just contain information that enhances your Web experience. For example, when you use an Internet site to buy computer equipment, you may add items to a "shopping basket."

Information about the items you add to the shopping basket is stored in a cookie on your computer because the Internet browser cannot retain information that you entered in one Internet page when you switch to another Internet page. The cookie saves information about your purchases and allows the site to create a final order form for you.

Another example is the cookie that a Web store keeps on your computer, holding your user name and password so that you do not need to enter this information each time you connect to the site.

Some stores may use the cookie information to record each time you connect to the site, what pages you use, and whether you click any of advertiser banners. Reputable sites provide privacy information to tell you how the information that is gathered is used.

The above examples of cookies are clearly useful to you, at least in some way. However, other sites might download cookies just to collect information about your Internet use. These cookies are clearly not useful to you at all.

Your McAfee Internet Security To-do List

C

After you finish installing McAfee Internet Security, and you have completed the preliminary setup using the Configuration Assistant, you will want to create and customize all of your user profiles.

The purpose of this section is to guide you through the customization process. Although each user or family member may have their own personal settings, it is the McAfee Internet Security Administrator that controls the user's access and safely while travel the Internet.

Privacy & Security

There is a wealth of information on the World Wide Web, and apart from the monthly fee to your Internet Service Provider (ISP), it's practically free.

Global access to information, shopping, on-line banking and finance management, instant messaging, file sharing, streaming video, etc., brings about today's paradigms.

Tips

- Filter and remove Internet cookies.

  There are good cookies and then there are not so good cookies. A cookie is a small text file placed in your computer's Temporary Internet (cache) folder by a Web site and is used the next time you visit that same Web site.

  A good cookie might record your logon name so that you do not need to log in every time you visit the Web site. Perhaps you purchased accessories at this same Web site – a unique, encrypted transaction identifier was placed on a cookie. As you revisit the online store, and you click the "Check my last order" button, all relevant information displays, without a keystroke!

Conversely, cookies can record “what you did” on a particular Web site. For example, you visit one of the major search engine’s Web site and shop for an automobile. You revisit the same Web site a few days later and shop for an automobile again. The following week, you turn on your computer and go directly the same Web site. This time you’re looking for the local weather forecast. As the page loads into memory, there are ads for autos all over the screen. The cookie retained information about your past actions at their Web site. The Web page displayed information based upon what was stored in the cookies.

To maintain privacy on the Internet, filter cookies. This allows you to select only those cookies that are truly good cookies. Additionally, you should delete unwanted cookies as you complete an Internet session, to remove the footprints resulting from your travels in the digital highway.

- Block Web bugs.

  Web bugs are very small graphic files, usually 1 pixel by 1 pixel in size (hence the term "bug" or invisible) that send messages to third parties about your Internet browsing habits. Third parties use this information to create user profiles. Web bugs have been known to capture the date and time the Web bug was accessed, the browser version used and even the IP address of the computer that received the Web bug.

  To maintain your privacy against Web bugs, always block Web bugs.

- Protect your identity.

  It you want to make a purchase online, do not provide personal information (name, address, credit card numbers) unless the Web Site uses Secure Sockets Layer (SSL) encryption. You can recognize secured sites if the Web site's URL begins with https://.

  It is also makes for good practice to use software that monitors your Internet connection and warns you if there is an attempt to transmit personal information over the Internet. This type of software requires that you create a database of information about you and the other users of the computer; thus establishing a record of that which should not be transmitted via the Internet.

  Remove records of where browsed the Internet from your computer. As you browse the Internet, your browser stores files in a repository called Temporary Internet or "cache" files. Basically, as you revisit a Web site or click your browser's Back button, rather than download all of the graphics displayed on the Web page, your browser reloads the cached files. In a location on your hard disk labeled History, your browser records all of the URLs visited as well s the URLs that you typed into your browser's address bar. All of these records reveal information about where you’ve been on the Internet.

- Improve your Internet browsing experience by preventing ads and pop-up windows from displaying.
- Shield younger family members from distasteful or undesirable content.

  Users of the Internet, at all age levels can exposed to inappropriate Web site content. A simple typographical error in the text box of your favorite search engine could return graphic gore, rather than cartoons; or pornography, rather than recipes.

  Therefore, when possible, configure your software to enable parental controls and block access to inappropriate content. Here are a few tips.

  - Scan site content ratings and vocabulary.

    Identify the content that you want to allow the user to view; filter and scan for inappropriate vocabulary. If the user is multi-lingual, you may wish to consider scanning and blocking inappropriate vocabulary in more than one language.

  - Block access to specific Web sites, Proxy sites, and Newsgroups.

    If there is a specific Web site or proxy site that you do not want a user or family to have access to, configure the user's profile as such.

    Newsgroups may also be a source for undesirable content. When possible, identify the specific Newsgroup that you want to explicitly block or allow access to and update the user's profile.

- Block access to specific programs.

  If there are any programs that you do not want to allow a user or family member to use, block the user's ability to start the program.

- Limit the time a user may access the Internet.

  Designate a specific time of day that you will allow a user or family member the ability to connect to the Internet. Modify each user profile as necessary.

- And **clean up** when you are finished!

  Configure your software to remove all files associated with browsing the Internet. You can configure the program to remove cookies as you close your Internet browser.

Virus Detection and Prevention Tips

Although far from harmless, most viruses that infect your personal computer or laptop will not destroy data, play pranks, or render your computer unusable. Even the comparatively rare viruses that do carry a destructive payload usually produce their nasty effects in response to a trigger event. In most cases, unless you actually see evidence of a payload that has activated, you will have time to deal with the infection properly. The very presence of these small snippets of unwanted computer code can, however, interfere with your computer's normal operation, consume system resources and have other undesirable effects, so you should take them seriously and be sure to remove them when you encounter them.

A second idea to keep in mind is that odd computer behavior, unexplained system crashes, or other unpredictable events might have causes other than virus infections. If you believe you have a virus on your computer because of occurrences such as these, scanning for viruses might not produce the results you expect, but it will help eliminate one potential cause of your computer problems.

TIPs

- Do not open any files attached to an e-mail message from an unknown, suspicious, or untrustworthy source. Do not open any files attached to an e-mail message unless you know what it is, even though it appears the e-mail message came from someone you know. Some viruses replicate themselves and spread through email. Better be safe than sorry and confirm that they really sent it.
- Watch for attachments with double file extensions. File naming convention use a "file name" followed by a 3-letter file extension separated by a "dot." For example, Readme.txt - here 'txt' is the file extension. It you receive and e-mail message and there is an attachment that displays two file extensions (for example Readme.txt.exe) do not open the message. ·Do not open any files attached to an e-mail message if the subject line is questionable or unexpected. If necessary, save the file to removable storage disk and run your VirusScan software to scan for viruses.
- Delete chain e-mail and junk e-mail messages. Do not forward or reply to any to them. These types of e-mail messages are considered spam, which is unsolicited, intrusive mail that clogs up the network.
- Do not download any files from strangers. Exercise caution when downloading files from the Internet. Ensure that the source is a legitimate and reputable one. Verify that an anti-virus program checks the files on the download site. If you are uncertain, do not download the file at all or download the file to a floppy or removable device and run your VirusScan program.

- Update your anti-virus software regularly. These updates should be at the least the product's virus signature files (DATs). You may also need to update the scanning engine as well.
- Back up your files on a regular basis. If a virus destroys your files, at least you can replace them with your back-up copy. You should store your backup copy in a separate location from your work files, one that is preferably not on your computer.

Use a Firewall

The best defense against an intrusion or attack from the Internet is to install an invisible barrier known as a firewall. Firewalls protect your computer by filtering incoming and outgoing Internet traffic.

The advent of broadband Internet connections in the home, such as Cable and DSL, has manifested itself as the "always on" connection. To maintain its "always on" connection, your computer must maintain a fixed IP address - as opposed to a dialup connection, that which assigns an IP address every time you connect to the Internet. (An IP address is a network address that identifies your computer and enables it to exchange packets of data with other networks, servers, and computers connected to the Internet.) Firewalls can hide your computer's identity. For example, if a hacker tries to invade your computer by scanning for a susceptible open port, the data returned, if any that exposes your computer's identity is essentially useless - thus, thwarting the attack.

Other benefits to using a firewall include the ability to block access to your personal information such as financial or password files. Firewalls can block illegal distribution of software. There are programs known as spyware and stealth programs that track your Internet browsing habits and log your keyboard strokes. A firewall can block access to files, folders, or any shared network device.

Firewalls can prevent a hacker's attempt to use your computer to launch a Denial of Service (DoS) attack against a server, web site, or network. A DoS attack overwhelms the entity's resources, thus causing a shutdown. A DoS attack does not usually result in compromised information, rather the loss of services and revenue, as well as the cost to restore the lost services.

Tips

- Install a Firewall.
- Configure your Firewall to start as Windows starts; and allow it to remain "always on."
- Select the programs that you want to explicitly allow to communicate.
- Filter traffic at all times, except during an attack - then block.

- If you allow your computer to run 24 hours per day, then configure your Firewall to block communication while you are away from the desk.
- Check for an update your software frequently, and configure it to notify you if there is an update available.
- Review your activity logs periodically. If the logs display suspicious activity, or frequent violations, investigate the activity.

Tips to maintaining your computer and its software

- After you install your software, register it immediately. Updates, bug fixes, and patches could have been released after the installation CD was placed in the box.
- Configure the program to automatically notify you when product updates are available for download.
- Download and install updates upon their availability. Updates include patches, fixes, updates to DATs (virus definition files), content, and the virus scan engine itself.
- Configure your Internet security programs to start as Windows starts, especially if your computer maintains and "always on" Internet connection.
- Do not share, misplace, or forget the Administrator profile password. Lost passwords could render your software and computer ineffective; and you may not be able to access the files that you created and you stored in your computer.
- Schedule tasks. For example, if you want to scan your computer's 60-gigabyte hard disk for viruses, you may just want to consider scheduling the scan at a time when the computer is running, however, not in use.
- Scan you computer for viruses and run security and firewall checkups on a regular basis. Whether you are scanning for security, privacy, or firewall weaknesses, if you use your computer and the Internet daily, then you should run checkups routinely.

Index

L

M

N

O

P

Q

S

T

U

V

W

For more information on products, worldwide services, and support, contact your authorized McAfee sales representative or visit us at:

www.mcafeehelp.co.uk

Customer Service
McAfee Consumer Products
Apollo Contact Centre
Units 2-6, Boucher Business Centre
Apollo road, Belfast BT12 6 HP
UK

www.mcafee-at-home.com

NA-592-0010-UK-1