internetsecuritysuite

User Guide

Version 8.0

McAfee®

COPYRIGHT

TRADEMARK ATTRIBUTIONS

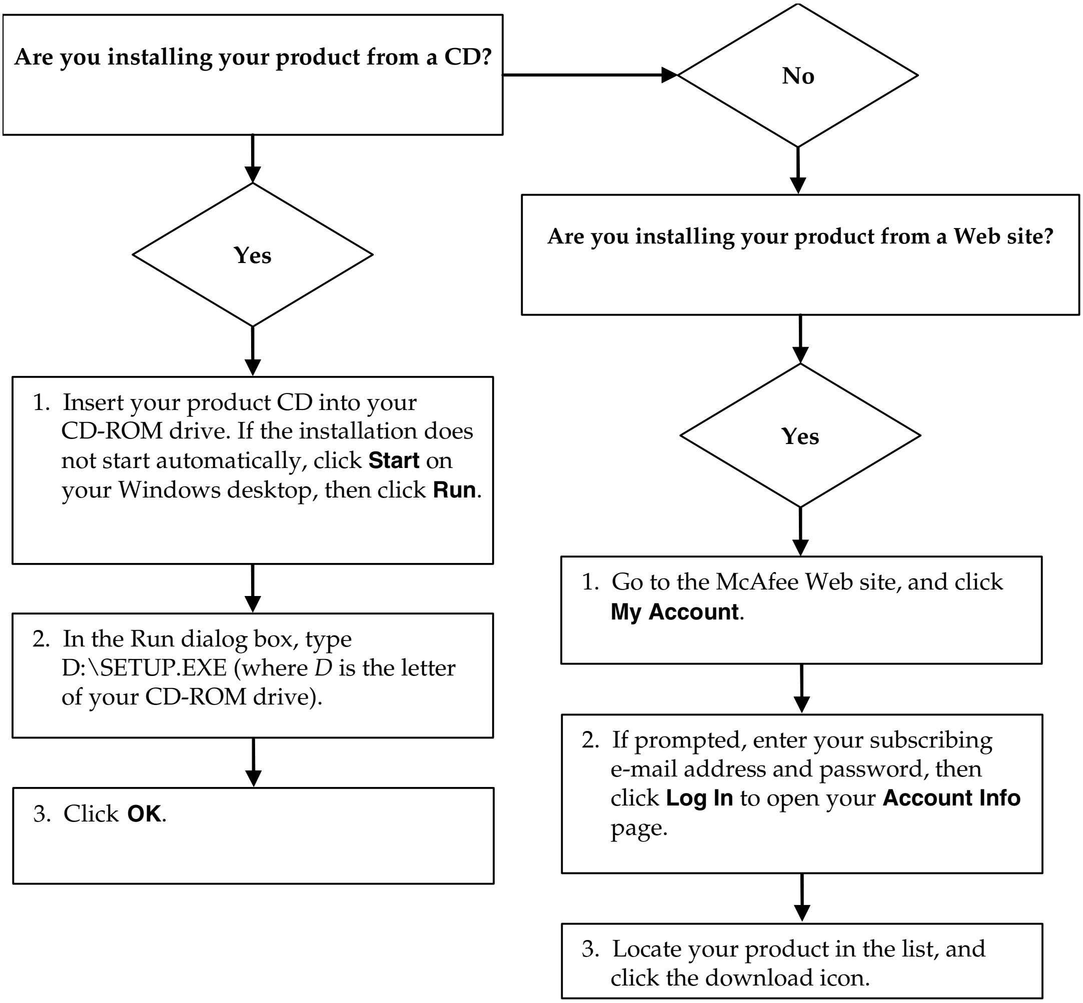
LICENSE INFORMATION

License Agreement

Attributions

Quick Start Card

If you are installing your product from a CD or a Web site, print this convenient reference page.



Are you installing your product from a CD?

Yes

1. Insert your product CD into your CD-ROM drive. If the installation does not start automatically, click **Start** on your Windows desktop, then click **Run**.
2. In the Run dialog box, type D:\SETUP.EXE (where *D* is the letter of your CD-ROM drive).
3. Click **OK**.

No

Are you installing your product from a Web site?

Yes

1. Go to the McAfee Web site, and click **My Account**.
2. If prompted, enter your subscribing e-mail address and password, then click **Log In** to open your **Account Info** page.
3. Locate your product in the list, and click the download icon.

McAfee reserves the right to change Upgrade & Support Plans and policies at any time without notice. McAfee and its product names are registered trademarks of McAfee, Inc. and/or its affiliates in the US and/or other countries.

For more information

To view the User Guides on the product CD, ensure that you have Acrobat Reader installed; if not, install it now from the McAfee product CD.

1. Insert your product CD into your CD-ROM drive.
2. Open Windows Explorer: Click **Start** on your Windows desktop, and click **Search**.
3. Locate the Manuals folder, and double-click the User Guide .PDF you want to open.

Registration benefits

McAfee recommends that you follow the easy steps within your product to transmit your registration directly to us. Registration ensures that you receive timely and knowledgeable technical assistance, plus the following benefits:

- FREE electronic support
- Virus definition (.DAT) file updates for one year after installation when you purchase VirusScan software

  Go to http://www.mcafee.com/ for pricing of an additional year of virus signatures.
- 60-day warranty that guarantees replacement of your software CD if it is defective or damaged
- SpamKiller filter updates for one year after installation when you purchase SpamKiller software

  Go to http://www.mcafee.com/ for pricing of an additional year of filter updates.
- McAfee Internet Security Suite updates for one year after installation when you purchase MIS software

  Go to http://www.mcafee.com/ for pricing of an additional year of content updates.

Technical Support

For technical support, please visit http://www.mcafeehelp.com/.

Our support site offers 24-hour access to the easy-to-use Answer Wizard for solutions to the most common support questions.

Knowledgeable users can also try our advanced options, which include a Keyword Search and our Help Tree. If a solution cannot be found, you can also access our FREE Chat Now! and E-mail Express! options. Chat and e-mail help you to quickly reach our qualified support engineers through the Internet, at no cost. Otherwise, you can get phone support information at http://www.mcafeehelp.com/.

Contents

Quick Start Card iii

1 Introduction 11

McAfee Internet Security software 12
System requirements 12
Using McAfee SecurityCenter 13
Removing Internet Security Suite programs 14

2 McAfee VirusScan 15

New features 15
Testing VirusScan 17
    Testing ActiveShield 17
    Testing Scan 17
Using ActiveShield 19
    Enabling or disabling ActiveShield 19
    Configuring ActiveShield options 20
    Understanding security alerts 29
Manually scanning your computer 32
    Manually scanning for viruses and other threats 32
    Automatically scanning for viruses and other threats 35
    Understanding threat detections 37
Managing quarantined files 38
Creating a Rescue Disk 40
    Write-protecting a Rescue Disk 41
    Using a Rescue Disk 41
    Updating a Rescue Disk 41
Automatically reporting viruses 41
    Reporting to the World Virus Map 42
    Viewing the World Virus Map 43
Updating VirusScan 44
    Automatically checking for updates 44

Manually checking for updates 44

3 McAfee Personal Firewall Plus 47

New features 47
Removing other firewalls 49
Setting the default firewall 49
Setting the security level 50
Testing McAfee Personal Firewall Plus 52
About the Summary page 52
About the Internet Applications page 57
Changing application rules 58
Allowing and blocking Internet applications 58
About the Inbound Events page 59
Understanding events 60
Showing events in the Inbound Events log 62
Responding to inbound events 64
Managing the Inbound Events log 68
About alerts 69
Red alerts 70
Green alerts 75
Blue alerts 77

4 McAfee Privacy Service 79

Features 79
The Administrator 79
Setup Assistant 80
Retrieving the Administrator Password 80
The Startup user 80
Opening McAfee Privacy Service 81
Opening and signing in to Privacy Service 81
Disabling Privacy Service 81
Updating McAfee Privacy Service 81
Adding Users 81
Setting the password 82
Setting the age group 82
Setting the cookie blocker 82
Setting the Internet time limits 82
Editing Users 83

Changing passwords 83
Changing a user’s information 84
Changing cookie blocker setting 84
Editing the Accept and Reject Cookie List 84
Changing the age group 85
Changing Internet time limits 85
Changing the startup user 86
Removing users 86
Options 86
Blocking web sites 86
Allowing Web sites 86
Blocking information 87
Adding information 87
Editing information 87
Removing personal information 87
Blocking Web bugs 88
Blocking advertisements 88
Allowing cookies from specific Web sites 89
Event Log 89
Date and time 89
User 89
Summary 89
Event Details 89
Saving the Current Log 90
Viewing Saved Logs 90
Utilities 90
Erasing files permanently using McAfee Shredder 90
Why Windows leaves file remnants 91
What McAfee Shredder erases 91
Permanently erasing files in Windows Explorer 91
Emptying the Windows Recycle Bin 91
Customizing Shredder settings 91
Backing up the Privacy Service database 92
Restoring the Backup Database 92
User Options 93
Changing your password 93
Changing your user name 93
Clearing your cache 94

Accepting cookies 94
If you need to remove a web site from this list: 94
Rejecting cookies 95
If you need to remove a web site from this list: 95
5 McAfee SpamKiller 97
Features 97
User options 97
Filtering 98
Understanding the top pane 98
Disabling SpamKiller 99
Understanding the Summary page 100
Microsoft Outlook and Outlook Express integration 100
Managing E-mail Accounts and Users 101
Adding e-mail accounts 101
Pointing your e-mail client to SpamKiller 102
Deleting e-mail accounts 102
Deleting an e-mail account from SpamKiller 102
Editing e-mail account properties 103
POP3 accounts 103
MSN/Hotmail accounts 105
MAPI accounts 106
Adding users 108
User passwords and protecting children from spam 109
Logging on to SpamKiller in a multi-user environment 110
Using the Friends List 111
Opening a Friends List 112
Importing address books 112
Importing an address book by automatic import 113
Importing an address book manually 113
Editing address book information 114
Deleting an address book from the automatic import list 114
Adding friends 115
Adding friends from the Blocked E-mail or Accepted E-mail page 115
Adding friends from the Friends page 116
Adding friends from Microsoft Outlook 116
Editing friends 116
Deleting friends 117

Working With Blocked and Accepted Messages 118
Blocked E-mail page 118
Accepted E-mail page 120
Tasks for Blocked E-mail and Accepted E-mail 121
Rescuing messages 122
From the Blocked E-Mail page 122
From the SpamKiller folder in Microsoft Outlook or Outlook Express 122
Blocking messages 122
From the Accepted E-mail page 122
From Microsoft Outlook 123
Where are the blocked messages 123
Deleting a message manually 123
Modifying how spam messages are processed 123
Tagging 123
Blocking 123
Modifying how SpamKiller processes spam messages 124
Using the AntiPhishing filter 124
Adding friends to a Friends List 125
Adding filters 125
Regular expressions 127
Reporting spam to McAfee 130
Sending complaints manually 130
Sending error messages 130
Sending an error message manually 131

Index 133

Introduction 1

The Internet provides a wealth of information and entertainment at your fingertips. However, 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 data with McAfee Internet Security Suite. Incorporating McAfee's award-winning technologies, Internet Security Suite is one of the most comprehensive sets of privacy and security tools available. McAfee Internet Security Suite 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 your computer’s incoming and outgoing Internet connections.

McAfee Internet Security Suite is a proven security solution that provides powerful protection for today's Internet users.

McAfee Internet Security Suite comprises the following products:

- *McAfee VirusScan* on page 15
- *McAfee Personal Firewall Plus* on page 47
- *McAfee Privacy Service* on page 79
- *McAfee SpamKiller* on page 97

McAfee Internet Security software

- **McAfee SecurityCenter —** Assesses, informs, and warns you about your computer’s security vulnerability. Each security index quickly evaluates your exposure to security and Internet-based threats, and then provides recommendations to quickly and securely protect your computer.
- **McAfee VirusScan —** Scans, detects, fixes, and removes Internet viruses. You can customize virus scans and determine the response and action when a virus is detected. You can also configure VirusScan to log virus-related actions performed on your computer.
- **McAfee Personal Firewall Plus —** Protects your computer while it is connected to the Internet, and secures your computer’s outgoing and incoming Internet connections.
- **McAfee Privacy Service —** Combines personal information protection, online advertisement blocking, and content filtering. It secures your personal information while providing greater control over your family's Internet experience. McAfee's Privacy Service ensures that you do not expose confidential information to online threats and protects you and your family from inappropriate online content.
- **McAfee SpamKiller —** The rise of fraudulent, inappropriate and offensive e-mail to adults, children and businesses makes spam protection an essential component of your computer’s security strategy.

System requirements

- Microsoft® Windows 98, Me, 2000, or XP
- Personal computer with Pentium-compatible processor
  - Windows 98, 2000: 133 MHz or higher
  - Windows Me: 150 MHz or higher
  - Windows XP (Home and Pro): 300 MHz or higher
- RAM
  - Windows 98, Me, 2000: 64 MB
  - Windows XP (Home and Pro): 128 MB
- 100 MB hard disk space
- Microsoft® Internet Explorer 5.5 or later

NOTE: To upgrade to the latest version of Internet Explorer, visit

the Microsoft Web site at http://www.microsoft.com/**.**

Using McAfee SecurityCenter

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

- Get free security analysis for your computer.
- Launch, manage, and configure all your McAfee subscriptions from one icon.
- See continuously updated virus alerts and the latest product information.
- Get quick links to frequently asked questions and account details at the McAfee web site.

> **NOTE**
> For more information about SecurityCenter features, click **Help** in the **SecurityCenter** dialog box.

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

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

To open McAfee SecurityCenter:

1. Right-click the McAfee icon M in the Windows system tray.
2. Click **Open SecurityCenter**.

To access your McAfee product:

1. Right-click the McAfee icon M in the Windows system tray.
2. Point to the appropriate McAfee product and select the feature you want to use.

Removing Internet Security Suite programs

In some situations, you might want to remove Internet Security Suite or some of its programs.

> **NOTE**
> Users must have Administrator rights to uninstall Internet Security Suite.

1. Save all your work and close any open applications.
2. Open **Control Panel**.
   - On your Windows taskbar, select **Start**, point to **Settings**, and then click **Control Panel** (Windows 98, ME, and 2000).
   - On your Windows taskbar, select **Start**, and then click **Control Panel** (Windows XP).
3. Click **Add/Remove Programs**.
4. Select the McAfee Uninstall Wizard, then one or more programs, and then click **Uninstall**. To remove all the Internet Security products, click **Select All**, then **Uninstall**.
5. To proceed with the removal, click **Yes**.
6. If prompted, restart your computer.

McAfee VirusScan 2

Welcome to McAfee VirusScan.

McAfee VirusScan is an antivirus subscription service offering comprehensive, reliable, and up-to-date virus protection. Powered by award-winning McAfee scanning technology, VirusScan protects against viruses, worms, Trojan horses, malicious scripts, and hybrid attacks.

With it, you get the following features:

ActiveShield — Scan files when they are accessed by either you or your computer.

Scan — Search for viruses and Potentially Unwanted Programs in hard drives, floppy disks, and individual files and folders.

Quarantine — Encrypt and temporarily isolate infected and suspicious files in the quarantine folder until an appropriate action can be taken.

Hostile activity detection — Monitor your computer for virus-like activity caused by worm-like activity and malicious scripts.

New features

This version of VirusScan provides the following new features:

- **Spyware and adware detection and removal**
  VirusScan identifies and removes spyware, adware, and other programs that jeopardize your privacy and slow down your computer performance.
- **Daily automatic updates**
  Daily automatic VirusScan updates protect against the latest identified and unidentified computer threats.
- **Fast background scanning**
  Fast unobtrusive scans identify and destroy viruses, Trojans, worms, spyware, adware, dialers, and other malicious programs without interrupting your work.
- **Real-time security alerting**
  Security alerts notify you about emergency virus outbreaks and security threats, and provide response options to remove, neutralize, or learn more about the threat.

- **Detection and cleaning at multiple entry points**
  VirusScan monitors and cleans at your computer's key entry points: e-mail, instant message attachments, and Internet downloads.

- **E-mail monitoring for worm-like activity**
  WormStopper™ monitors suspicious mass-mailing behaviors and stops viruses and worms from spreading through e-mail to other computers.

- **Script monitoring for worm-like activity**
  ScriptStopper™ monitors suspicious script executions and stops viruses and worms from spreading through e-mail to other computers.

- **Free instant messaging and e-mail technical support**
  Live technical support provides prompt, easy assistance using instant messaging and e-mail.

Testing VirusScan

Before initial use of VirusScan, it's a good idea to test your installation. Use the following steps to separately test the ActiveShield and Scan features.

Testing ActiveShield

NOTE
To test ActiveShield from the VirusScan tab in SecurityCenter, click **Test VirusScan** to view an online Support FAQ containing these steps.

To test ActiveShield:

1 Go to http://www.eicar.com/ in your web browser.

2 Click the **The AntiVirus testfile eicar.com** link.

3 Scroll to the bottom of the page. Under **Download**, you will see four links.

4 Click **eicar.com**.

If ActiveShield is working properly, it detects the eicar.com file immediately after you click the link. You can try to delete or quarantine infected files to see how ActiveShield handles viruses. See *Understanding security alerts* on page 29 for details.

Testing Scan

Before you can test Scan, you must disable ActiveShield to prevent it from detecting the infected files before Scan does, then download the test files.

To download the test files:

1 Disable ActiveShield: Right-click the McAfee icon, point to **VirusScan**, then click **Disable**.

2 Download the EICAR test files from the EICAR web site:

  a Go to http://www.eicar.com/.

  b Click the **The AntiVirus testfile eicar.com** link.

c Scroll to the bottom of the page. Under **Download**, you will see these links:

eicar.com contains a line of text that VirusScan will detect as a virus.

eicar.com.txt (optional) is the same file, but with a different file name, for those users who have difficulty downloading the first link. Simply rename the file "eicar.com" after you download it.

eicar_com.zip is a copy of the test virus inside a .ZIP compressed file (a WinZip™ file archive).

eicarcom2.zip is a copy of the test virus inside a .ZIP compressed file, which itself is inside a .ZIP compressed file.

d Click each link to download its file. For each one, a **File Download** dialog box appears.

e Click **Save**, click the **Create New Folder** button, then rename the folder **VSO Scan Folder**.

f Double-click **VSO Scan Folder**, then click **Save** again in each **Save As** dialog box.

3 When you are finished downloading the files, close Internet Explorer.

4 Enable ActiveShield: Right-click the McAfee icon, point to **VirusScan**, then click **Enable**.

To test Scan:

1 Right-click the McAfee icon, point to **VirusScan**, then click **Scan for Viruses**.

2 Using the directory tree in the left pane of the dialog box, go to the **VSO Scan Folder** where you saved the files:

a Click the **+** sign next to the C drive icon.

b Click the **VSO Scan Folder** to highlight it (do not click the **+** sign next to it).

This tells Scan to check only that folder for viruses. You can also put the files in random locations on your hard drive for a more convincing demonstration of Scan's abilities.

3 In the **Scan Options** area of the **Scan for Viruses** dialog box, ensure that all options are selected.

4 Click **Scan** on the lower right of the dialog box.

VirusScan scans the **VSO Scan Folder**. The EICAR test files that you saved to that folder appear in the **List of Detected Files**. If so, Scan is working properly.

You can try to delete or quarantine infected files to see how Scan handles viruses. See *Understanding threat detections* on page 37 for details.

Using ActiveShield

When ActiveShield is started (loaded into computer memory) and enabled, it constantly protects your computer. ActiveShield scans files when they are accessed by either you or your computer. When ActiveShield detects an infected file, it automatically tries to clean the virus. If ActiveShield cannot clean the virus, you can quarantine or delete the file.

Enabling or disabling ActiveShield

ActiveShield is started (loaded into computer memory) and enabled (denoted by the red M icon in your Windows system tray) by default as soon as you restart your computer after the installation process.

If ActiveShield is stopped (not loaded) or is disabled (denoted by the black M icon), you can manually run it, as well as configure it to start automatically when Windows starts.

Enabling ActiveShield

To enable ActiveShield for this Windows session only:

Right-click the McAfee icon, point to **VirusScan**, then click **Enable**. The McAfee icon changes to red M.

If ActiveShield is still configured to start when Windows starts, a message tells you that you are now protected from viruses. Otherwise, a dialog box appears that lets you configure ActiveShield to start when Windows starts (Figure 2-1 on page 20).

Disabling ActiveShield

To disable ActiveShield for this Windows session only:

1 Right-click the McAfee icon, point to **VirusScan**, then click **Disable**.

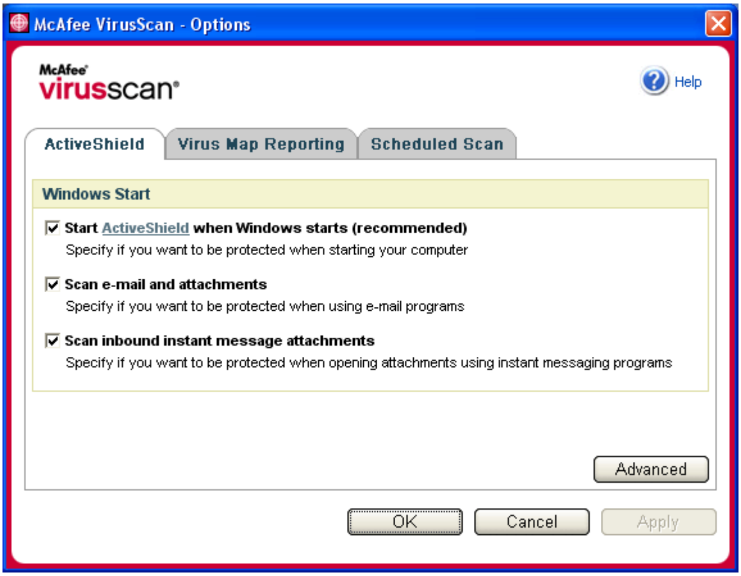
2 Click **Yes** to confirm.

The McAfee icon changes to black M.

If ActiveShield is still configured to start when Windows starts, your computer will be protected from viruses again when you restart your computer.

Configuring ActiveShield options

You can modify ActiveShield starting and scanning options in the **ActiveShield** tab of the **VirusScan Options** dialog box (Figure 2-1), which is accessible via the McAfee icon M in your Windows system tray.



Windows Start

☑ **Start ActiveShield when Windows starts (recommended)**
Specify if you want to be protected when starting your computer

☑ **Scan e-mail and attachments**
Specify if you want to be protected when using e-mail programs

☑ **Scan inbound instant message attachments**
Specify if you want to be protected when opening attachments using instant messaging programs

Figure 2-1. ActiveShield Options

Starting ActiveShield

ActiveShield is started (loaded into computer memory) and enabled (denoted by red M) by default as soon as you restart your computer after the installation process.

If ActiveShield is stopped (denoted by black M), you can configure it to start automatically when Windows starts (recommended).

NOTE
During updates to VirusScan, the **Update Wizard** might exit ActiveShield temporarily to install new files. When the **Update Wizard** prompts you to click **Finish**, ActiveShield starts again.

To start ActiveShield automatically when Windows starts:

1. Right-click the McAfee icon, point to **VirusScan**, then click **Options**.

   The **VirusScan Options** dialog box opens (Figure 2-1 on page 20).

2. Select the **Start ActiveShield when Windows starts (recommended)** checkbox, then click **Apply** to save your changes.

3. Click **OK** to confirm, then click **OK**.

Stopping ActiveShield

WARNING
If you stop ActiveShield, your computer is not protected from viruses. If you must stop ActiveShield, other than for updating VirusScan, ensure that you are not connected to the Internet.

To stop ActiveShield from starting when Windows starts:

1. Right-click the McAfee icon, point to **VirusScan**, then click **Options**.

   The **VirusScan Options** dialog box opens (Figure 2-1 on page 20).

2. Deselect the **Start ActiveShield when Windows starts (recommended)** checkbox, then click **Apply** to save your changes.

3. Click **OK** to confirm, then click **OK**.

Scanning e-mail and attachments

By default, e-mail scanning and automatic cleaning are enabled via the **Scan e-mail and attachments** option (Figure 2-1 on page 20).

When this option is enabled, ActiveShield automatically scans and attempts to clean inbound (POP3) and outbound (SMTP) infected e-mail messages and attachments for most popular e-mail clients, including the following:

- Microsoft Outlook Express 4.0 or later
- Microsoft Outlook 97 or later
- Netscape Messenger 4.0 or later
- Netscape Mail 6.0 or later
- Eudora Light 3.0 or later
- Eudora Pro 4.0 or later

- Eudora 5.0 or later
- Pegasus 4.0 or later

  NOTE
  E-mail scanning is not supported for these e-mail clients: Web-based, IMAP, AOL, POP3 SSL, and Lotus Notes. However, ActiveShield scans e-mail attachments when they are opened.

  If you disable the **Scan e-mail and attachments** option, the E-mail Scan options and the WormStopper options (Figure 2-2 on page 23) are automatically disabled. If you disable outbound e-mail scanning, the WormStopper options are automatically disabled.

  If you change your e-mail scanning options, you must restart your e-mail program to complete the changes.

Inbound e-mail

If an inbound e-mail message or attachment is infected, ActiveShield performs the following steps:

- Tries to clean the infected e-mail
- Tries to quarantine or delete an uncleanable e-mail
- Includes an alert file in the inbound e-mail that contains information about the actions performed to remove the infection

Outbound e-mail

If an outbound e-mail message or attachment is infected, ActiveShield performs the following steps:

- Tries to clean the infected e-mail
- Tries to quarantine or delete an uncleanable e-mail

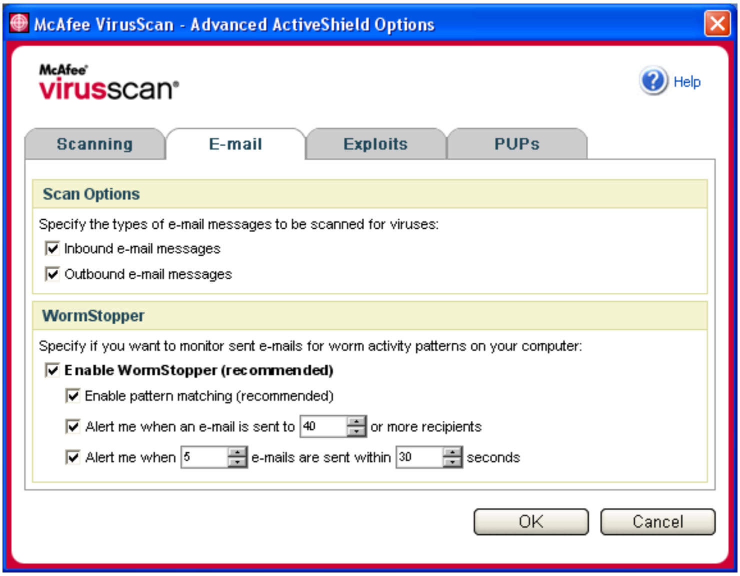
  NOTE
  For details about outbound e-mail scanning errors, see the online help.

Disabling e-mail scanning

By default, ActiveShield scans both inbound and outbound e-mail. However, for enhanced control, you can set ActiveShield to scan only inbound or outbound e-mail.

To disable scanning of inbound or outbound e-mail:

1. Right-click the McAfee icon, point to **VirusScan**, and then click **Options**.
2. Click **Advanced**, then click the **E-mail Scan** tab (Figure 2-2).
3. Deselect **Inbound e-mail messages** or **Outbound e-mail messages**, then click **OK**.



Scan Options

Specify the types of e-mail messages to be scanned for viruses:

☑ Inbound e-mail messages

☑ Outbound e-mail messages

WormStopper

Specify if you want to monitor sent e-mails for worm activity patterns on your computer:

☑ **Enable WormStopper (recommended)**

☑ Enable pattern matching (recommended)

☑ Alert me when an e-mail is sent to 40 or more recipients

☑ Alert me when 5 e-mails are sent within 30 seconds

Figure 2-2. Advanced ActiveShield Options - E-mail tab

Scanning for worms

VirusScan monitors your computer for suspicious activity that might indicate a threat is present on your computer. While VirusScan cleans viruses, WormStopper^{TM} prevents viruses and worms from spreading further.

A computer “worm” is a self-replicating virus that resides in active memory and might send copies of itself through e-mail. Without WormStopper, you might notice worms only when their uncontrolled replication consumes system resources, slowing performance or halting tasks.

The WormStopper protection mechanism detects, alerts, and blocks malicious activity. Suspicious activity might include the following actions on your computer:

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

If you set ActiveShield to use the default **Enable WormStopper (recommended)** option in the **Advanced Options** dialog box, WormStopper monitors e-mail activity for suspicious patterns and alerts you when a specified number of e-mails or recipients has been exceeded within a specified interval.

To set ActiveShield to scan sent e-mail messages for worm-like activity:

1. Right-click the McAfee icon, point to **VirusScan**, then click **Options**.
2. Click **Advanced**, then click the **E-mail** tab.

3. Click **Enable WormStopper (recommended)** (Figure 2-3).

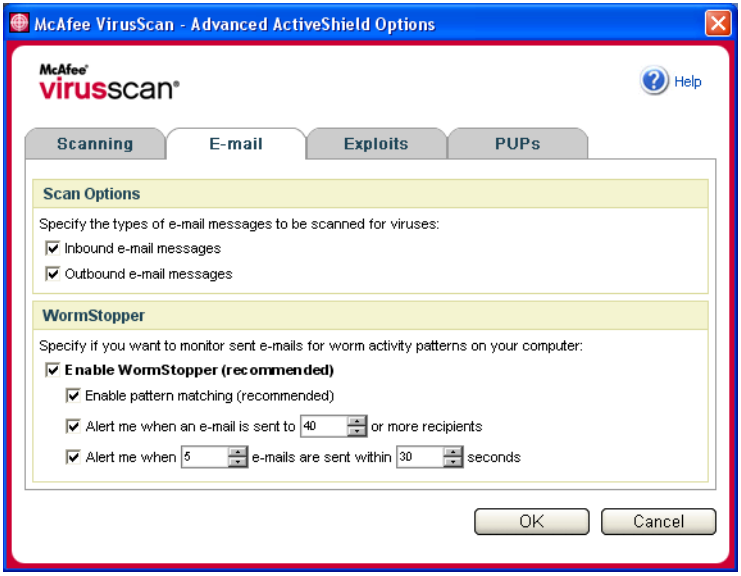
   By default, the following detailed options are enabled:

   - Pattern matching to detect suspicious activity
   - Alerting when e-mail is sent to 40 or more recipients
   - Alerting when 5 or more e-mails are sent within 30 seconds

   NOTE
   If you modify the number of recipients or seconds for monitoring sent e-mails, it might result in invalid detections. McAfee recommends that you click **No** to retain the default setting. Otherwise, click **Yes** to change the default setting to your setting.

   This option can be automatically enabled after the first time a potential worm is detected (see *Managing potential worms* on page 30 for details):

   - Automatic blocking of suspicious outbound e-mails



Scan Options

Specify the types of e-mail messages to be scanned for viruses:

☑ Inbound e-mail messages

☑ Outbound e-mail messages

WormStopper

Specify if you want to monitor sent e-mails for worm activity patterns on your computer:

☑ **Enable WormStopper (recommended)**

☑ Enable pattern matching (recommended)

☑ Alert me when an e-mail is sent to 40 or more recipients

☑ Alert me when 5 e-mails are sent within 30 seconds

Figure 2-3. Advanced ActiveShield Options - E-mail tab

Scanning inbound instant message attachments

By default, scanning of instant message attachments is enabled via the **Scan inbound instant message attachments** option (Figure 2-1 on page 20).

When this option is enabled, VirusScan automatically scans and attempts to clean inbound infected instant message attachments for most popular instant messaging programs, including the following:

- MSN Messenger 6.0 or later
- Yahoo Messenger 4.1 or later
- AOL Instant Messenger 2.1 or later

  NOTE
  For your protection, you cannot disable auto-cleaning of instant message attachments.

If an inbound instant message attachment is infected, VirusScan performs the following steps:

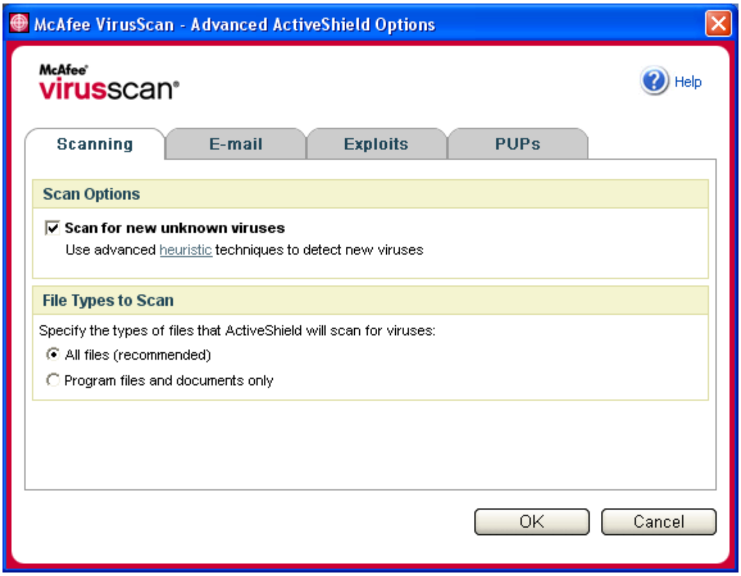
- Tries to clean the infected message
- Prompts you to quarantine or delete an uncleanable message

Scanning all files

If you set ActiveShield to use the default **All files (recommended)** option, it scans every file type that your computer uses, as your computer attempts to use it. Use this option to get the most thorough scan possible.

To set ActiveShield to scan all file types:

1. Right-click the McAfee icon, point to **VirusScan**, and then click **Options**.
2. Click **Advanced**, then click the **Scanning** tab (Figure 2-4 on page 26).
3. Click **All files (recommended)**, then click **OK**.



McAfee VirusScan - Advanced ActiveShield Options

Scan Options

☑ Scan for new unknown viruses

Use advanced heuristic techniques to detect new viruses

File Types to Scan

Specify the types of files that ActiveShield will scan for viruses:

● All files (recommended)

○ Program files and documents only

Figure 2-4. Advanced ActiveShield Options - Scanning tab

Scanning program files and documents only

If you set ActiveShield to use the **Program files and documents only** option, it scans program files and documents, but not any other files used by your computer. The latest virus signature file (DAT file) determines which file types that ActiveShield will scan.To set ActiveShield to scan program files and documents only:

1 Right-click the McAfee icon, point to **VirusScan**, and then click **Options**.

2 Click **Advanced**, then click the **Scanning** tab (Figure 2-4).

3 Click **Program files and documents only**, then click **OK**.

Scanning for new unknown viruses

If you set ActiveShield to use the default **Scan for new unknown viruses (recommended)** option, it uses advanced heuristic techniques that try to match files to the signatures of known viruses, while also looking for telltale signs of unidentified viruses in the files.

To set ActiveShield to scan for new unknown viruses:

1 Right-click the McAfee icon, point to **VirusScan**, and then click **Options**.

2 Click **Advanced**, then click the **Scanning** tab (Figure 2-4).

3 Click **Scan for new unknown viruses (recommended)**, then click **OK**.

Scanning for scripts

VirusScan monitors your computer for suspicious activity that might indicate a threat is present on your computer. While VirusScan cleans viruses, ScriptStopperTM prevents Trojan horses from running scripts that spread viruses further.

A “Trojan horse” is a malicious program that pretends to be a benign application. Trojans are not viruses because they do not replicate, but they can be just as destructive.

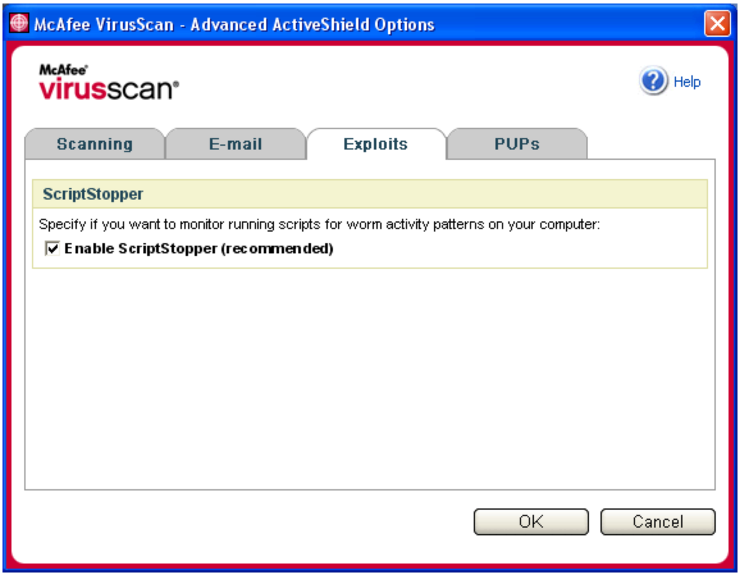
The ScriptStopper protection mechanism detects, alerts, and blocks malicious activity. Suspicious activity might include the following action on your computer:

- A script execution that results in the creation, copying, or deletion of files, or the opening of your Windows registry

If you set ActiveShield to use the default **Enable ScriptStopper (recommended)** option in the **Advanced Options** dialog box, ScriptStopper monitors script execution for suspicious patterns and alerts you when a specified number of e-mails or recipients has been exceeded within a specified interval.

To set ActiveShield to scan running scripts for worm-like activity:

1. Right-click the McAfee icon, point to **VirusScan**, then click **Options**.
2. Click **Advanced**, then click the **Exploits** tab (Figure 2-5).
3. Click **Enable ScriptStopper (recommended)**, then click **OK**.



ScriptStopper

Specify if you want to monitor running scripts for worm activity patterns on your computer:

☑ Enable ScriptStopper (recommended)

Figure 2-5. Advanced ActiveShield Options - Exploits tab

Scanning for Potentially Unwanted Programs (PUPs)

NOTE
If McAfee AntiSpyware is installed on your computer, it manages all Potentially Unwanted Program activity. Open McAfee AntiSpyware to configure your options.

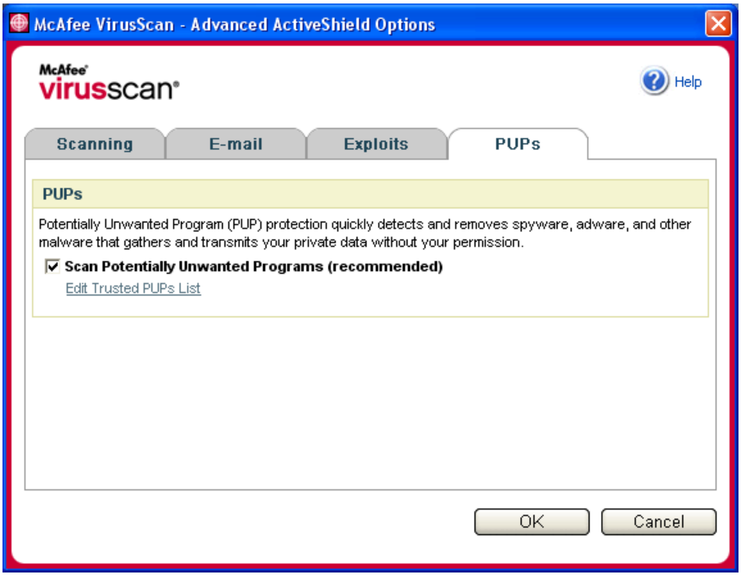
If you set ActiveShield to use the default **Scan Potentially Unwanted Programs (recommended)** option in the **Advanced Options** dialog box, Potentially Unwanted Program (PUP) protection quickly detects, blocks, and removes spyware, adware, and other malware that gathers and transmits your private data without your permission.

To set ActiveShield to scan for PUPs:

1 Right-click the McAfee icon, point to **VirusScan**, and then click **Options**.

2 Click **Advanced**, then click the **PUPs** tab (Figure 2-6).

3 Click **Scan Potentially Unwanted Programs (recommended)**, then click **OK**.



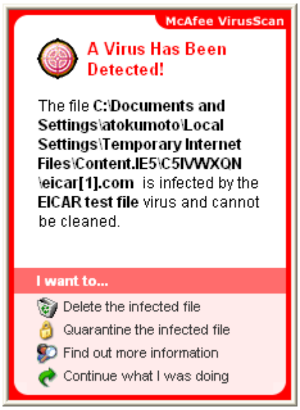
Potentially Unwanted Program (PUP) protection quickly detects and removes spyware, adware, and other malware that gathers and transmits your private data without your permission.

☑ Scan Potentially Unwanted Programs (recommended)

Figure 2-6. Advanced ActiveShield Options - PUPs tab

Understanding security alerts

If ActiveShield finds a virus, a virus alert similar to Figure 2-7 appears. For most viruses, Trojan horses, and worms, ActiveShield automatically tries to clean the file and alerts you. For Potentially Unwanted Programs (PUPs), ActiveShield detects the file, automatically blocks it, and alerts you.


McAfee VirusScan
I want to...
Delete the infected file
Quarantine the infected file
Find out more information
Continue what I was doing

A Virus Has Been Detected!

The file **C:\Documents and Settings\atokumoto\Local Settings\Temporary Internet Files\Content.IE5\C5IVWXQN \eicar[1].com** is infected by the **EICAR test file** virus and cannot be cleaned.

Figure 2-7. Virus alert

You can then choose how to manage infected files, infected e-mail, suspicious scripts, potential worms, or PUPs, including whether to submit infected files to the McAfee AVERT labs for research.

For added protection, whenever ActiveShield detects a suspicious file, you are prompted to scan your entire computer immediately. Unless you choose to hide the scan prompt, it will periodically remind you until you perform the scan.

Managing infected files

1. If ActiveShield can clean the file, you can learn more or ignore the alert:

   - Click **Find out more information** to view the name, location, and virus name associated with the infected file.

   - Click **Continue what I was doing** to ignore the alert and close it.

2. If ActiveShield cannot clean the file, click **Quarantine the infected file** to encrypt and temporarily isolate infected and suspicious files in the quarantine directory until an appropriate action can be taken.

   A confirmation message appears and prompts you to check your computer for viruses. Click **Scan** to complete the quarantine process.

3. If ActiveShield cannot quarantine the file, click **Delete the infected file** to try to remove the file.

Managing infected e-mail

By default, e-mail scanning automatically tries to clean infected e-mail. An alert file included in the inbound message notifies you whether the e-mail was cleaned, quarantined, or deleted.

Managing suspicious scripts

If ActiveShield detects a suspicious script, you can find out more and then stop the script if you did not intend to initiate it:

- Click **Find out more information** to view the name, location, and description of the activity associated with the suspicious script.
- Click **Stop this script** to prevent the suspicious script from running.

If you are sure that you trust the script, you can allow the script to run:

- Click **Allow this script this time** to let all scripts contained within a single file run once.
- Click **Continue what I was doing** to ignore the alert and let the script run.

Managing potential worms

If ActiveShield detects a potential worm, you can find out more and then stop the e-mail activity if you did not intend to initiate it:

- Click **Find out more information** to view the recipient list, subject line, message body, and description of the suspicious activity associated with the infected e-mail message.
- Click **Stop this e-mail** to prevent the suspicious e-mail from being sent and delete it from your message queue.

If you are sure that you trust the e-mail activity, click **Continue what I was doing** to ignore the alert and let the e-mail be sent.

Managing PUPs

If ActiveShield detects and blocks a Potentially Unwanted Program (PUP), you can find out more and then remove the program if you did not intend to install it:

- Click **Find out more information** to view the name, location, and recommended action associated with the PUP.
- Click **Remove this PUP** to remove the program if you did not intend to install it.

  A confirmation message appears.

  - If (a) you do not recognize the PUP or (b) you did not install the PUP as part of a bundle or accept a license agreement in connection with such programs, click **OK** to remove the program using the McAfee removal method.

  - Otherwise, click **Cancel** to exit the automatic removal process. If you change your mind later, you can manually remove the program using the vendor's uninstaller.
- Click **Continue what I was doing** to ignore the alert and block the program this time.

If you (a) recognize the PUP or (b) you might have installed the PUP as part of a bundle or accepted a license agreement in connection with such programs, you can allow it to run:

- Click **Trust this PUP** to whitelist this program and always let it run in the future.

  See "*Managing trusted PUPs*" for details.

Managing trusted PUPs

The programs that you add to the Trusted PUPs list will not be detected by McAfee VirusScan.

If a PUP is detected and added to the Trusted PUPs list, you can later remove it from the list if necessary.

If your Trusted PUPs list is full, you must remove some items before you can trust another PUP.

To remove a program from your Trusted PUPs list:

1. Right-click the McAfee icon, point to **VirusScan**, and then click **Options**.
2. Click **Advanced**, then click the **PUPs** tab.
3. Click **Edit Trusted PUPs List**, select the checkbox in front of the file name, and click **Remove.** When you are finished removing items, click **OK**.

Manually scanning your computer

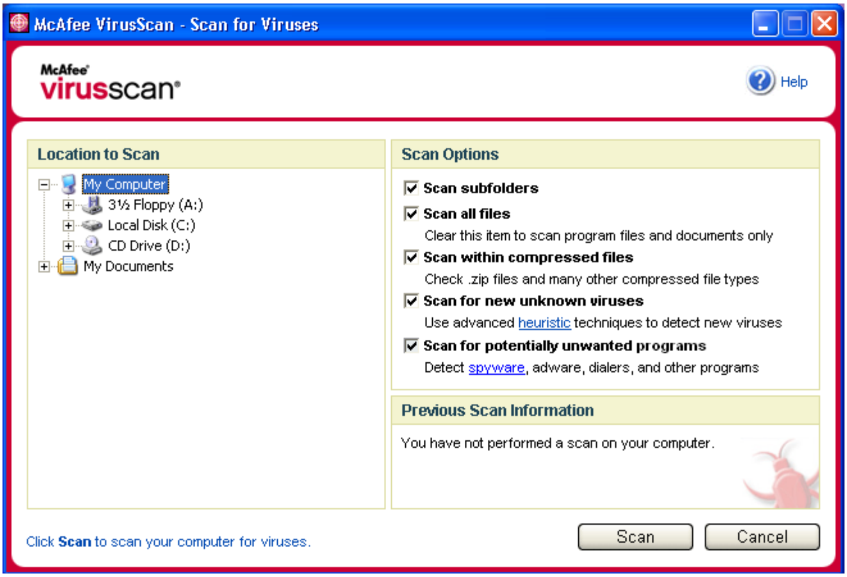
The Scan feature lets you selectively search for viruses and Potentially Unwanted Programs on hard drives, floppy disks, and individual files and folders. When Scan finds an infected file, it automatically tries to clean the file, unless it is a Potentially Unwanted Program. If Scan cannot clean the file, you can quarantine or delete the file.

Manually scanning for viruses and other threats

To scan your computer:

1 Right-click the McAfee icon, point to **VirusScan**, then click **Scan for Viruses**.

The **Scan for Viruses** dialog box opens (Figure 2-8).



☑ Scan subfolders

☑ Scan all files
Clear this item to scan program files and documents only

☑ Scan within compressed files
Check .zip files and many other compressed file types

☑ Scan for new unknown viruses
Use advanced heuristic techniques to detect new viruses

☑ Scan for potentially unwanted programs
Detect spyware, adware, dialers, and other programs

You have not performed a scan on your computer.

Click **Scan** to scan your computer for viruses.

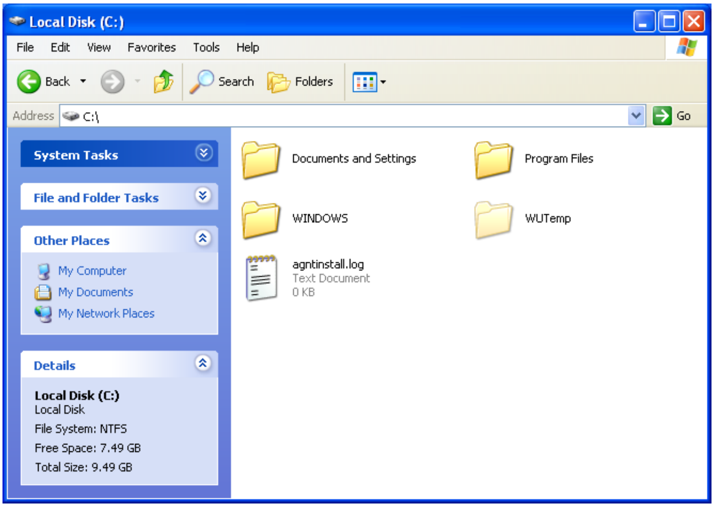
Figure 2-8. Scan for Viruses dialog box

2 Click the drive, folder, or file that you want to scan.

3 Select your **Scan Options**. By default, all of the **Scan Options** are pre-selected to provide the most thorough scan possible (Figure 2-8):

- **Scan subfolders** — Use this option to scan files contained in your subfolders. Deselect this checkbox to allow checking of only the files visible when you open a folder or drive.

Example: The files in Figure 2-9 are the only files scanned if you deselect the **Scan subfolders** checkbox. The folders and their contents are not scanned. To scan those folders and their contents, you must leave the checkbox selected.



Local Disk (C:)
Local Disk
File System: NTFS
Free Space: 7.49 GB
Total Size: 9.49 GB

Figure 2-9. Local disk contents

- **Scan all files** — Use this option to allow the thorough scanning of all file types. Deselect this checkbox to shorten the scanning time and allow checking of program files and documents only.
- **Scan within compressed files** — Use this option to reveal hidden infected files within .ZIP and other compressed files. Deselect this checkbox to prevent checking of any files or compressed files within the compressed file.

  Sometimes virus authors plant viruses in a .ZIP file, then insert that .ZIP file into another .ZIP file in an effort to bypass antivirus scanners. Scan can detect these viruses as long as you leave this option selected.
- **Scan for new unknown viruses** — Use this option to find the newest viruses that might not have existing “cures.” This option uses advanced heuristic techniques that try to match files to the signatures of known viruses, while also looking for telltale signs of unidentified viruses in the files.

  This scanning method also looks for file traits that can generally rule out that the file contains a virus. This minimizes the chances that Scan gives a false indication. Nevertheless, if a heuristic scan detects a virus, you should treat it with the same caution that you would treat a file that you know contains a virus.

  This option provides the most thorough scan, but is generally slower than a normal scan.

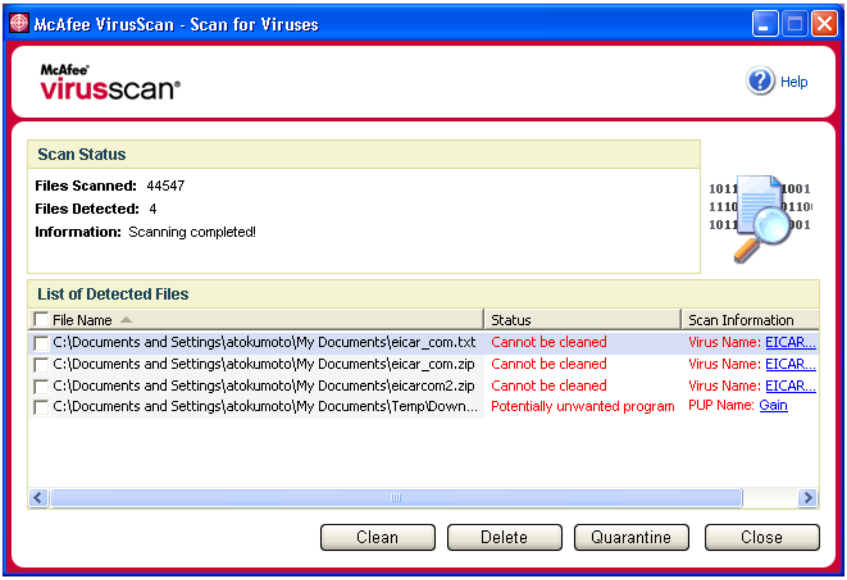
- **Scan for Potentially Unwanted Programs** — Use this option to detect spyware, adware, dialers, and other programs that you did not intend to install on your computer.

  NOTE
  Leave all options selected for the most thorough scan possible. This effectively scans every file in the drive or folder that you select, so allow plenty of time for the scan to complete. The larger the hard drive and the more files you have, the longer the scan takes.

4 Click **Scan** to start scanning files.

When the scan is finished, a scan summary shows the number of files scanned, the number of files detected, the number of Potentially Unwanted Programs, and the number of detected files that were automatically cleaned.

5 Click **OK** to close the summary, and view the list of any detected files in the **Scan for Viruses** dialog box (Figure 2-10).



Scan Status

Files Scanned: 44547
Files Detected: 4
Information: Scanning completed!

List of Detected Files

File Name	Status	Scan Information
C:\Documents and Settings\atokumoto\My Documents\eicar_com.txt	Cannot be cleaned	Virus Name: EICAR...
C:\Documents and Settings\atokumoto\My Documents\eicar_com.zip	Cannot be cleaned	Virus Name: EICAR...
C:\Documents and Settings\atokumoto\My Documents\eicarcom2.zip	Cannot be cleaned	Virus Name: EICAR...
C:\Documents and Settings\atokumoto\My Documents\Temp\Down...	Potentially unwanted program	PUP Name: Gain

Figure 2-10. Scan results

NOTE
Scan counts a compressed file (.ZIP, .CAB, etc.) as one file within the **Files Scanned** number. Also, the number of files scanned can vary if you have deleted your temporary Internet files since your last scan.

6 If Scan finds no viruses or Potentially Unwanted Programs, click **Back** to select another drive or folder to scan, or click **Close** to close the dialog box. Otherwise, see *Understanding threat detections* on page 37.

Scanning via Windows Explorer

VirusScan provides a shortcut menu to scan selected files, folders, or drives for viruses and Potentially Unwanted Programs from within Windows Explorer.

To scan files in Windows Explorer:

1 Open Windows Explorer.

2 Right-click the drive, folder, or file that you want to scan, and then click **Scan for Viruses**.

The **Scan for Viruses** dialog box opens and starts scanning files. By default, all of the default **Scan Options** are pre-selected to provide the most thorough scan possible (Figure 2-8 on page 32).

Scanning via Microsoft Outlook

VirusScan provides a toolbar icon to scan for viruses and Potentially Unwanted Programs in selected message stores and their subfolders, mailbox folders, or e-mail messages containing attachments from within Microsoft Outlook 97 or later.

To scan e-mail in Microsoft Outlook:

1 Open Microsoft Outlook.

2 Click the message store, folder, or e-mail message containing an attachment that you want to scan, and then click the e-mail scanning toolbar icon.

The e-mail scanner opens and starts scanning files. By default, all of the default **Scan Options** are pre-selected to provide the most thorough scan possible (Figure 2-8 on page 32).

Automatically scanning for viruses and other threats

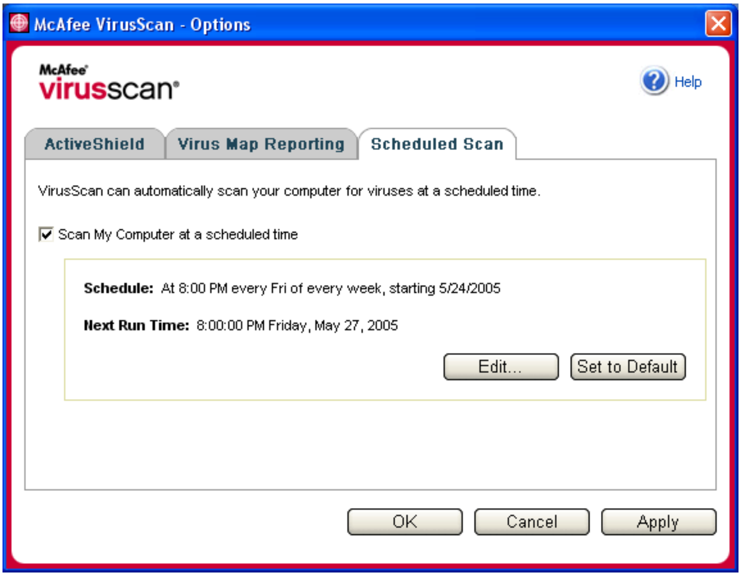
Although VirusScan scans files when they are accessed by either you or your computer, you can schedule automatic scanning in Windows Scheduler to thoroughly check your computer for viruses and Potentially Unwanted Programs at specified intervals.

To schedule a scan:

1 Right-click the McAfee icon, point to **VirusScan**, then click **Options**.

The **VirusScan Options** dialog box opens.

2 Click the **Scheduled Scan** tab (Figure 2-11 on page 36).



McAfee VirusScan - Options

VirusScan can automatically scan your computer for viruses at a scheduled time.

☑ Scan My Computer at a scheduled time

Schedule: At 8:00 PM every Fri of every week, starting 5/24/2005

Next Run Time: 8:00:00 PM Friday, May 27, 2005

Figure 2-11. Scheduled Scan Options

3 Select the **Scan My Computer at a scheduled time** checkbox to enable automatic scanning.

4 Specify a schedule for automatic scanning:

- To accept the default schedule (8PM every Friday), click **OK**.
- To edit the schedule:

  a. Click **Edit**.

  b. Select how often to scan your computer in the **Schedule Task** list, and then select additional options in the dynamic area below it:

  Daily - Specify the number of days between scans.

  Weekly (the default) - Specify the number of weeks between scans as well as the names of the day(s) of the week.

  Monthly - Specify which day of the month to scan. Click **Select Months** to specify which months to scan, and click **OK**.

  Once - Specify which date to scan.

NOTE
These options in Windows Scheduler are not supported: **At system startup**, **When idle**, and **Show multiple schedules**. The last supported schedule remains enabled until you select from among the valid options.

c. Select the time of day to scan your computer in the **Start time** box.

d. To select advanced options, click **Advanced**.

The **Advanced Schedule Options** dialog box opens.

i. Specify a start date, end date, duration, end time, and whether to stop the task at the specified time if the scan is still running.

ii. Click **OK** to save your changes and close the dialog box. Otherwise, click **Cancel**.

5 Click **OK** to save your changes and close the dialog box. Otherwise, click **Cancel**.

6 To revert to the default schedule, click **Set to Default**. Otherwise, click **OK**.

Understanding threat detections

For most viruses, Trojans, and worms, Scan automatically tries to clean the file. You can then choose how to manage detected files, including whether to submit them to the McAfee AVERT labs for research. If Scan detects a Potentially Unwanted Program, you can manually try to clean, quarantine, or delete it (AVERT submission is unavailable).

To manage a virus or Potentially Unwanted Program:

1 If a file appears in the **List of Detected Files**, click the checkbox in front of the file to select it.

NOTE
If more than one file appears in the list, you can select the checkbox in front of the **File Name** list to perform the same action on all of the files. You can also click the file name in the **Scan Information** list to view details from the Virus Information Library.

2 If the file is a Potentially Unwanted Program, you can click **Clean** to try to clean it.

3 If Scan cannot clean the file, you can click **Quarantine** to encrypt and temporarily isolate infected and suspicious files in the quarantine directory until an appropriate action can be taken. (See *Managing quarantined files* on page 38 for details.)

4 If Scan cannot clean or quarantine the file, you can do either of the following:

- Click **Delete** to remove the file.
- Click **Cancel** to close the dialog box without taking any further action.

If Scan cannot clean or delete the detected file, consult the Virus Information Library at http://us.mcafee.com/virusInfo/default.asp for instructions on manually deleting the file.

If a detected file prevents you from using your Internet connection or from using your computer at all, try using a Rescue Disk to start your computer. The Rescue Disk, in many cases, can start a computer if a detected file disables it. See *Creating a Rescue Disk* on page 40 for details.

For more help, consult McAfee Customer Support at http://www.mcafeehelp.com/.

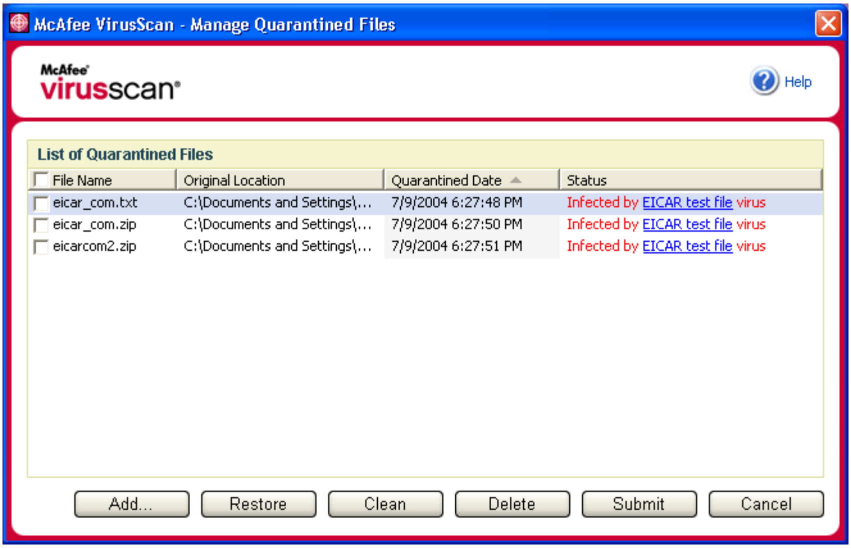
Managing quarantined files

The Quarantine feature encrypts and temporarily isolates infected and suspicious files in the quarantine directory until an appropriate action can be taken. Once cleaned, a quarantined file can then be restored to its original location.

To manage a quarantined file:

1 Right-click the McAfee icon, point to **VirusScan**, then click **Manage Quarantined Files**.

A list of quarantined files appears (Figure 2-12).



List of Quarantined Files

□ File Name	Original Location	Quarantined Date	Status
□ eicar_com.txt	C:\Documents and Settings\...	7/9/2004 6:27:48 PM	Infected by EICAR test file virus
□ eicar_com.zip	C:\Documents and Settings\...	7/9/2004 6:27:50 PM	Infected by EICAR test file virus
□ eicarcom2.zip	C:\Documents and Settings\...	7/9/2004 6:27:51 PM	Infected by EICAR test file virus

Figure 2-12. Manage Quarantined Files dialog box

2 Select the checkbox next to the file(s) you want to clean.

> **NOTE**
> If more than one file appears in the list, you can select the checkbox in front of the **File Name** list to perform the same action on all of the files. You can also click the virus name in the **Status** list to view details from the Virus Information Library.
>
> Or, click **Add**, select a suspicious file to add to the quarantine list, click **Open**, then select it in the quarantine list.

3 Click **Clean**.

4 If the file is cleaned, click **Restore** to move it back to its original location.

5 If VirusScan cannot clean the virus, click **Delete** to remove the file.

6 If VirusScan cannot clean or delete the file, and if it is not a Potentially Unwanted Program, you can submit the file to the McAfee AntiVirus Emergency Response Team (AVERT^{TM}) for research:

   a Update your virus signature files if they are more than two weeks old.

   b Verify your subscription.

   c Select the file and click **Submit** to submit the file to AVERT.

   VirusScan sends the quarantined file as an attachment with an e-mail message containing your e-mail address, country, software version, OS, and the file's original name and location. The maximum submission size is one unique 1.5-MB file per day.

7 Click **Cancel** to close the dialog box without taking any further action.

Creating a Rescue Disk

Rescue Disk is a utility that creates a bootable floppy disk that you can use to start your computer and scan it for viruses if a virus keeps you from starting it normally.

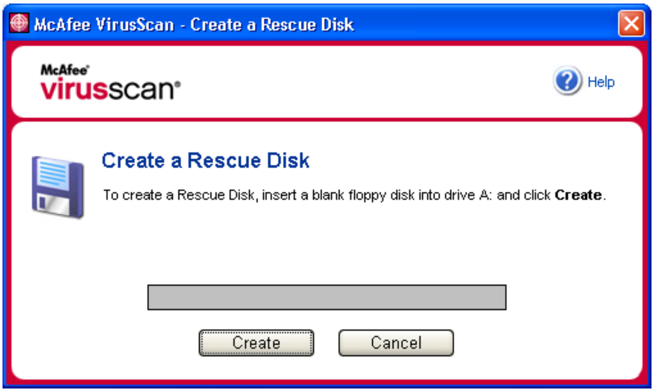
> **NOTE**
> You must be connected to the Internet to download the Rescue Disk image. Also, Rescue Disk is available for computers with FAT (FAT 16 and FAT 32) hard drive partitions only. It is unnecessary for NTFS partitions.

To create a Rescue Disk:

1 On a non-infected computer, insert a non-infected floppy disk in drive A. You might want to use Scan to ensure that both the computer and the floppy disk are virus-free. (See *Manually scanning for viruses and other threats* on page 32 for details.)

2 Right-click the McAfee icon, point to **VirusScan**, then click **Create Rescue Disk**.

The **Create a Rescue Disk** dialog box opens (Figure 2-13).



Create a Rescue Disk

To create a Rescue Disk, insert a blank floppy disk into drive A: and click **Create**.

Figure 2-13. Create a Rescue Disk dialog box

3 Click **Create** to create the Rescue Disk.

If this is your first time creating a Rescue Disk, a message tells you that Rescue Disk needs to download the image file for the Rescue Disk. Click **OK** to download the component now, or click **Cancel** to download it later.

A warning message tells you that the contents of the floppy disk will be lost.

4 Click **Yes** to continue creating the Rescue Disk.

The creation status appears in the **Create Rescue Disk** dialog box.

5. When the message “Rescue disk created” appears, click **OK**, then close the **Create Rescue Disk** dialog box.

6. Remove the Rescue Disk from the drive, write-protect it, and store it in a safe location.

Write-protecting a Rescue Disk

To write-protect a Rescue Disk:

1. Turn the floppy disk label-side down (the metal circle should be visible).

2. Locate the write-protect tab. Slide the tab so the hole is visible.

Using a Rescue Disk

To use a Rescue Disk:

1. Turn off the infected computer.

2. Insert the Rescue Disk into the drive.

3. Turn the computer on.

   A gray window with several options appears.

4. Choose the option that best suits your needs by pressing the Function keys (for example, F2, F3).

   NOTE
   Rescue Disk starts automatically in 60 seconds if you do not press any of the keys.

Updating a Rescue Disk

It is a good idea to update your Rescue Disk regularly. To update your Rescue Disk, follow the same instructions for creating a new Rescue Disk.

Automatically reporting viruses

You can anonymously send virus tracking information for inclusion in our World Virus Map. Automatically opt-in for this free, secure feature either during VirusScan installation (in the **Virus Map Reporting** dialog box), or at any time in the **Virus Map Reporting** tab of the **VirusScan Options** dialog box.

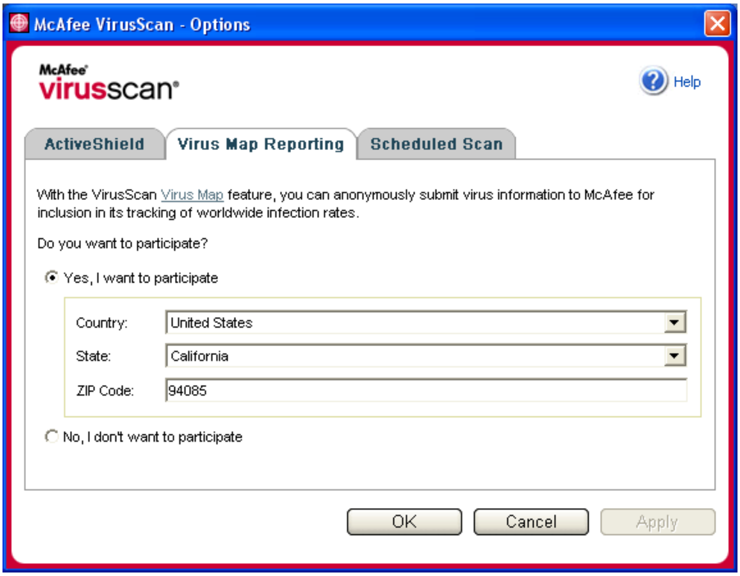
Reporting to the World Virus Map

To automatically report virus information to the World Virus Map:

1. Right-click the McAfee icon, point to **VirusScan**, then click **Options**.

   The **VirusScan Options** dialog box opens.

2. Click the **Virus Map Reporting** tab (Figure 2-14).



McAfee VirusScan - Options

With the VirusScan Virus Map feature, you can anonymously submit virus information to McAfee for inclusion in its tracking of worldwide infection rates.

Do you want to participate?

● Yes, I want to participate

Country: United States

State: California

ZIP Code: 94085

○ No, I don't want to participate

Figure 2-14. Virus Map Reporting Options

3. Accept the default **Yes, I want to participate** to anonymously send your virus information to McAfee for inclusion in its World Virus Map of worldwide infection rates. Otherwise, select **No, I don't want to participate** to avoid sending your information.

4. If you are in the United States, select the state and enter the zip code where your computer is located. Otherwise, VirusScan automatically tries to select the country where your computer is located.

5. Click **OK**.

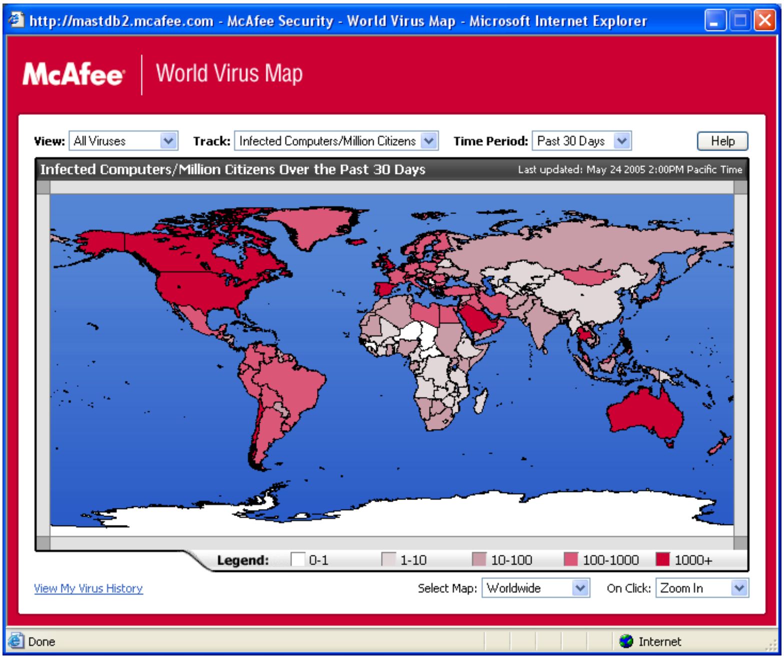
Viewing the World Virus Map

Whether or not you participate in the World Virus Map, you can view the latest worldwide infection rates via the McAfee icon in your Windows system tray.

To view the World Virus Map:

- Right-click the McAfee icon, point to **VirusScan**, then click **World Virus Map**.

  The **World Virus Map** web page appears (Figure 2-15).


http://mastdb2.mcafee.com - McAfee Security - World Virus Map - Microsoft Internet Explorer
McAfee
World Virus Map
Help
View My Virus History
Done
Internet

View: All Viruses Track: Infected Computers/Million Citizens Time Period: Past 30 Days

Infected Computers/Million Citizens Over the Past 30 Days Last updated: May 24 2005 2:00PM Pacific Time

Legend: □ 0-1 □ 1-10 ■ 10-100 ■ 100-1000 ■ 1000+

Select Map: Worldwide On Click: Zoom In

Figure 2-15. World Virus Map

By default, the World Virus Map shows the number of infected computers worldwide over the past 30 days, and also when the reporting data was last updated. You can change the map view to show the number of infected files, or change the time period to show only the results over the past 7 days or the past 24 hours.

The **Virus Tracking** section lists cumulative totals for the number of scanned files, infected files, and infected computers that have been reported since the date shown.

Updating VirusScan

When you are connected to the Internet, VirusScan automatically checks for updates every four hours, then automatically downloads and installs weekly virus definition updates without interrupting your work.

Virus definition files are approximately 100 KB and thus have minimal impact on system performance during download.

If a product update or virus outbreak occurs, an alert appears. Once alerted, you can then choose to update VirusScan to remove the threat of a virus outbreak.

Automatically checking for updates

McAfee SecurityCenter is automatically configured to check for updates for all of your McAfee services every four hours when you are connected to the Internet, then notify you with alerts and sounds. By default, SecurityCenter automatically downloads and installs any available updates.

NOTE
In some cases, you will be prompted to restart your computer to complete the update. Be sure to save all of your work and close all applications before restarting.

Manually checking for updates

In addition to automatically checking for updates every four hours when you are connected to the Internet, you can also manually check for updates at any time.

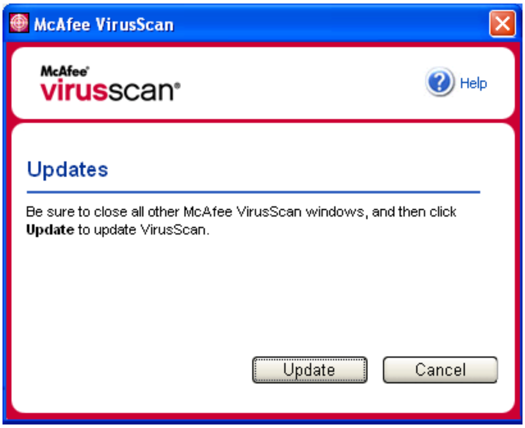
To manually check for VirusScan updates:

1. Ensure your computer is connected to the Internet.
2. Right-click the McAfee icon, then click **Updates**.

   The **SecurityCenter Updates** dialog box opens.
3. Click **Check Now**.

   If an update exists, the **VirusScan Updates** dialog box opens (Figure 2-16 on page 45). Click **Update** to continue.

   If no updates are available, a dialog box tells you that VirusScan is up-to-date. Click **OK** to close the dialog box.



Updates

Be sure to close all other McAfee VirusScan windows, and then click **Update** to update VirusScan.

Figure 2-16. Updates dialog box

4 Log on to the web site if prompted. The **Update Wizard** installs the update automatically.

5 Click **Finish** when the update is finished installing.

NOTE
In some cases, you will be prompted to restart your computer to complete the update. Be sure to save all of your work and close all applications before restarting.

McAfee Personal Firewall Plus 3

Welcome to McAfee Personal Firewall Plus.

McAfee Personal Firewall Plus software offers advanced protection for your computer and your personal data. Personal Firewall establishes a barrier between your computer and the Internet, silently monitoring Internet traffic for suspicious activities.

With it, you get the following features:

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

New features

- **Improved Gaming Support**
  McAfee Personal Firewall Plus protects your computer from intrusion attempts and suspicious activities during full-screen gameplay, but can hide alerts if it detects intrusion attempts or suspicious activities. Red alerts appear after you exit the game.
- **Improved Access Handling**
  McAfee Personal Firewall Plus lets users dynamically grant applications temporary access to the Internet. Access is restricted to the time the application launches until the time it closes. When Personal Firewall detects an unknown program, attempting to communicate with the Internet, a Red Alert provides the option to grant the application temporary access to the Internet.

- **Enhanced Security Control**
  Running the Lockdown feature in McAfee Personal Firewall Plus allows you to instantly block all incoming and outgoing Internet traffic between a computer and the Internet. Users can enable and disable Lockdown from three locations in Personal Firewall.

- **Improved Recovery Options**
  You can run Reset Options to automatically restore the default settings to Personal Firewall. If Personal Firewall exhibits undesirable behavior that you cannot correct, you can choose to undo your current settings and revert to the product's default settings.

- **Internet Connectivity Protection**
  To prevent a user from inadvertently disabling his or her Internet connection, the option to ban an Internet address is excluded on a Blue Alert when Personal Firewall detects an Internet connection originates from a DHCP or DNS server. If the incoming traffic does not originate from a DHCP or DNS server, the option appears.

- **Enhanced HackerWatch.org Integration**
  Reporting potential hackers is easier than ever. McAfee Personal Firewall Plus improves the functionality of HackerWatch.org, which includes event submission of potentially malicious events to the database.

- **Extended Intelligent Application Handling**
  When an application seeks Internet access, Personal Firewall first checks whether it recognizes the application as trusted or malicious. If the application is recognized as trusted, Personal Firewall automatically allows it access to the Internet so you do not have to.

- **Advanced Trojan Detection**
  McAfee Personal Firewall Plus combines application connection management with an enhanced database to detect and block more potentially malicious applications, such as Trojans, from accessing the Internet and potentially relaying your personal data.

- **Improved Visual Tracing**
  Visual Trace includes easy-to-read graphical maps showing the originating source of hostile attacks and traffic worldwide, including detailed contact/owner information from originating IP addresses.

- **Improved Usability**
  McAfee Personal Firewall Plus includes a Setup Assistant and a User Tutorial to guide users in the setup and use of their firewall. Although the product is designed to use without any intervention, McAfee provides users with a wealth of resources to understand and appreciate what the firewall provides for them.

- **Enhanced Intrusion Detection**
  Personal Firewall's Intrusion Detection System (IDS) detects common attack patterns and other suspicious activity. Intrusion detection monitors every data packet for suspicious data transfers or transfer methods and logs this in the event log.

- **Enhanced Traffic Analysis**
  McAfee Personal Firewall Plus offers users a view of both incoming and outgoing data from their computers, as well as displaying application connections including applications that are actively "listening" for open connections. This allows users to see and act upon applications that might be open for intrusion.

Removing other firewalls

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

> **NOTE**
> If you use Windows XP, you do not need to disable the built-in firewall before installing McAfee Personal Firewall Plus. However, we recommend that you do disable the built-in firewall. If you do not, you will not receive events in the Inbound Events log in McAfee Personal Firewall Plus.

Setting the default firewall

McAfee Personal Firewall can manage permissions and traffic for Internet applications on your computer, even if Windows Firewall is detected as running on your computer.

When installed, McAfee Personal Firewall automatically disables Windows Firewall and sets itself as your default firewall. You then experience only McAfee Personal Firewall functionality and messaging. If you subsequently enable Windows Firewall via Windows Security Center or Windows Control Panel, letting both firewalls run on your computer might result in partial loss of logging in McAfee Firewall as well as duplicate status and alert messaging.

NOTE

If both firewalls are enabled, McAfee Personal Firewall does not show all the blocked IP addresses in its Inbound Events tab. Windows Firewall intercepts most of these events and blocks those events, preventing McAfee Personal Firewall from detecting or logging those events. However, McAfee Personal Firewall might block additional traffic based upon other security factors, and that traffic will be logged.

Logging is disabled in Windows Firewall by default, but if you choose to enable both firewalls, you can enable Windows Firewall logging. The default Windows Firewall log is C:\Windows\pfirewall.log

To ensure that your computer is protected by at least one firewall, Windows Firewall is automatically re-enabled when McAfee Personal Firewall is uninstalled.

If you disable McAfee Personal Firewall or set its security setting to **Open** without manually enabling Windows Firewall, all firewall protection will be removed except for previously blocked applications.

Setting the security level

You can configure security options to indicate how Personal Firewall responds when it detects unwanted traffic. By default, the **Standard** security level is enabled. In **Standard** security level, when an application requests Internet access and you grant it access, you are granting the application Full Access. Full Access allows the application the ability to both send data and receive unsolicited data on non-system ports.

To configure security settings:

1. Right-click the McAfee icon M in the Windows system tray, point to **Personal Firewall**, then select **Options**.
2. Click the **Security Settings** icon.
3. Set the security level by moving the slider to the desired level.

   The security level ranges from Lockdown to Open:

   - **Lockdown —** All Internet connections on your computer are closed. You can use this setting to block ports you configured to be open in the System Services page.

- **Tight Security —** When an application requests a specific type of access to the Internet (for example, Outbound Only Access), you can allow or disallow the application an Internet connection. If the application later requests Full Access, you can then grant Full Access or restrict it to Outbound Only access.

- **Standard Security (recommended) —** When an application requests and then is granted Internet access, the application receives full Internet access to handle incoming and outgoing traffic.

- **Trusting Security —** All applications are automatically trusted when they first attempt to access the Internet. However, you can configure Personal Firewall to use alerts to notify you about new applications on your computer. Use this setting if you find that some games or streaming media do not work.

- **Open —** Your firewall is disabled. This setting allows all traffic through Personal Firewall, without filtering.

  NOTE
  Previously blocked applications continue to be blocked when the firewall is set to the **Open** or **Lockdown** security setting. To prevent this, you can either change the application's permissions to **Allow Full Access** or delete the **Blocked** permission rule from the **Internet Applications** list.

4 Select additional security settings:

  NOTE
  If your computer runs Windows XP and multiple XP users have been added, these options are available only if you are logged on to your computer as an administrator.

- **Record Intrusion Detection (IDS) Events in Inbound Events Log —** If you select this option, events detected by IDS will appear in the Inbound Events log. The Intrusion Detection System detects common attack types and other suspicious activity. Intrusion detection monitors every inbound and outbound data packet for suspicious data transfers or transfer methods. It compares these to a “signature” database and automatically drops the packets coming from the offending computer.

  IDS looks for specific traffic patterns used by attackers. IDS checks each packet that your machine receives to detect suspicious or known-attack traffic. For example, if Personal Firewall sees ICMP packets, it analyzes those packets for suspicious traffic patterns by comparing the ICMP traffic against known attack patterns.

- **Accept ICMP ping requests** — ICMP traffic is used mainly for performing traces and pings. Pinging is frequently used to perform a quick test before attempting to initiate communications. If you are using or have used a peer-to-peer file-sharing program, you might find yourself being pinged a lot. If you select this option, Personal Firewall allows all ping requests without logging the pings in the Inbound Events log. If you do not select this option, Personal Firewall blocks all ping requests and logs the pings in the Inbound Events log.
- **Allow restricted users to change Personal Firewall settings** — If you run Windows XP or Windows 2000 Professional with multiple users, select this option to allow restricted XP users to modify Personal Firewall settings.

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

Testing McAfee Personal Firewall Plus

You can test your Personal Firewall installation for possible vulnerabilities to intrusion and suspicious activity.

To test your Personal Firewall installation from the McAfee system tray icon:

- Right-click the McAfee icon M in the Windows system tray, and select **Test Firewall**.

Personal Firewall launches Internet Explorer and points to http://www.hackerwatch.org/, a Web site maintained by McAfee. Please follow the directions on the Hackerwatch.org Probe page to test Personal Firewall.

About the Summary page

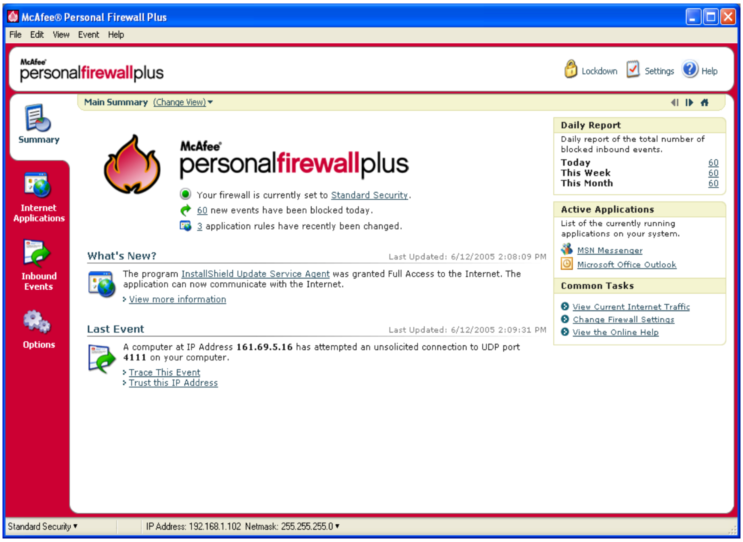
The Personal Firewall Summary includes four summary pages:

- Main Summary
- Application Summary
- Event Summary
- HackerWatch Summary

The Summary pages contain a variety of reports on recent inbound events, application status, and world-wide intrusion activity reported by HackerWatch.org. You will also find links to common tasks performed in Personal Firewall.

To open the Main Summary page in Personal Firewall:

- Right-click the McAfee icon in the Windows system tray, point to **Personal Firewall**, then select **View Summary** (Figure 3-1).


McAfee® Personal Firewall Plus
File Edit View Event Help
McAfee personalfirewallplus
Lockdown
Settings
Help
Main Summary (Change View)
Summary
Internet Applications
Inbound Events
Options
McAfee personalfirewallplus
Daily Report
Active Applications
MSN Messenger
Microsoft Office Outlook
Common Tasks
View Current Internet Traffic
Change Firewall Settings
View the Online Help
Standard Security
IP Address: 192.168.1.102 Netmask: 255.255.255.0

Your firewall is currently set to Standard Security.

60 new events have been blocked today.

3 application rules have recently been changed.

What's New? Last Updated: 6/12/2005 2:08:09 PM

The program InstallShield Update Service Agent was granted Full Access to the Internet. The application can now communicate with the Internet.

View more information

Last Event Last Updated: 6/12/2005 2:09:31 PM

A computer at IP Address **161.69.5.16** has attempted an unsolicited connection to UDP port **4111** on your computer.

Trace This Event

Trust this IP Address

Daily report of the total number of blocked inbound events.

Today	60
This Week	60
This Month	60

List of the currently running applications on your system.

Figure 3-1. Main Summary page

Click the following to navigate to different Summary pages:

Item	Description
Change View	Click **Change View** to open a list of Summary pages. From the list, select a Summary page to view.
Right arrow	Click the right arrow icon to view the next Summary page.
Left arrow	Click the left arrow icon to view the previous Summary page.
Home	Click the home icon to return to the **Main Summary** page.

The Main Summary page provides the following information:

Item	Description
Security Setting	The security setting status tells you the level of security at which the firewall is set. Click the link to change the security level.
Blocked Events	The blocked events status displays the number of events that have been blocked today. Click the link to view event details from the Inbound Event page.

Item	Description
Application Rule Changes	The application rule status displays the number of application rules that have been changed recently. Click the link to view the list of allowed and blocked applications and to modify application permissions.
What's New?	**What's New?** shows the latest application that was granted full access to the Internet.
Last Event	**Last Event** shows the latest inbound events. You can click a link to trace the event or to trust the IP address. Trusting an IP address allows all traffic from the IP address to reach your computer.
Daily Report	**Daily Report** displays the number of inbound events that Personal Firewall blocked today, this week, and this month. Click the link to view event details from the Inbound Event page.
Active Applications	**Active Applications** displays the applications that are currently running on your computer and accessing the Internet. Click an application to view which IP addresses the application is connecting to.
Common Tasks	Click a link in **Common Tasks** to go to Personal Firewall pages where you can view firewall activity and perform tasks.

To view the Application Summary page:

1 Right-click the McAfee icon M in the Windows system tray, point to **Personal Firewall**, then select **View Summary.**

2 Click **Change View**, then select **Application Summary**.

The Application Summary page provides the following information:

Item	Description
Traffic Monitor	The **Traffic Monitor** shows inbound and outbound Internet connections over the last fifteen minutes. Click the graph to view traffic monitoring details.
Active Applications	**Active Applications** shows the bandwidth use of your computer's most active applications during the last twenty-four hours. **Application**—The application accessing the Internet. **%**—The percentage of bandwidth used by the application. **Permission**—The type of Internet access that the application is allowed. **Rule Created**—When the application rule was created.
What's New?	**What's New?** shows the latest application that was granted full access to the Internet.

Item	Description
Active Applications	**Active Applications** displays the applications that are currently running on your computer and accessing the Internet. Click an application to view which IP addresses the application is connecting to.
Common Tasks	Click a link in **Common Tasks** to go to Personal Firewall pages where you can view application status and perform application-related tasks.

To view the Event Summary page:

1. Right-click the McAfee icon in the Windows system tray, point to **Personal Firewall**, then select **View Summary.**
2. Click **Change View**, then select **Event Summary**.

The Event Summary page provides the following information:

Item	Description
Port Comparison	**Port Comparison** shows a pie chart of the most frequently attempted ports on your computer during the past 30 days. You can click a port name to view details from the Inbound Events page. You can also move your mouse pointer over the port number to see a description of the port.
Top Offenders	**Top Offenders** shows the most frequently blocked IP addresses, when the last inbound event occurred for each address, and the total number of inbound events in the past thirty days for each address. Click an event to view event details from the Inbound Events page.
Daily Report	**Daily Report** displays the number of inbound events that Personal Firewall blocked today, this week, and this month. Click a number to view the event details from the Inbound Events log.
Last Event	**Last Event** shows the latest inbound events. You can click a link to trace the event or to trust the IP address. Trusting an IP address allows all traffic from the IP address to reach your computer.
Common Tasks	Click a link in **Common Tasks** to go to Personal Firewall pages where you can view details of events and perform event-related tasks.

To view the HackerWatch Summary page:

1. Right-click the McAfee icon in the Windows system tray, point to **Personal Firewall**, then select **View Summary.**
2. Click **Change View**, then select **HackerWatch Summary.**

The HackerWatch Summary page provides the following information.

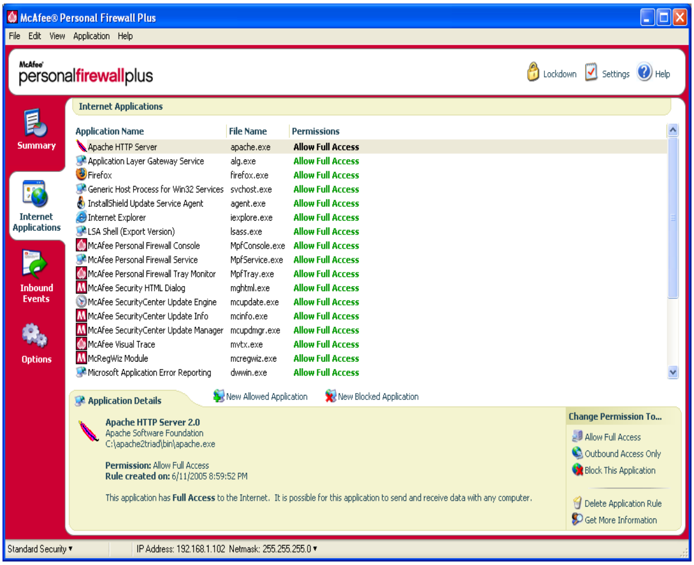
Item	Description
World Activity	**World Activity** shows a world map identifying recently blocked activity monitored by HackerWatch.org. Click the map to open the Global Threat Analysis Map in HackerWatch.org.
Event Tracking	**Event Tracking** shows the number of inbound events submitted to HackerWatch.org.
Global Port Activity	**Global Port Activity** shows the top ports, in the past 5 days, that appear to be threats. Click a port to view the port number and port description.
Common Tasks	Click a link in **Common Tasks** to go to HackerWatch.org pages where you can get more information on world-wide hacker activity.

About the Internet Applications page

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

To launch the Internet Applications page:

- Right-click the McAfee icon in the Windows system tray, point to **Personal Firewall**, then select **Applications** (Figure 3-2).



Internet Applications

Application Name	File Name	Permissions
Apache HTTP Server	apache.exe	Allow Full Access
Application Layer Gateway Service	alg.exe	Allow Full Access
Firefox	firefox.exe	Allow Full Access
Generic Host Process for Win32 Services	svchost.exe	Allow Full Access
InstallShield Update Service Agent	agent.exe	Allow Full Access
Internet Explorer	iexplore.exe	Allow Full Access
LSA Shell (Export Version)	lsass.exe	Allow Full Access
McAfee Personal Firewall Console	MpfConsole.exe	Allow Full Access
McAfee Personal Firewall Service	MpfService.exe	Allow Full Access
McAfee Personal Firewall Tray Monitor	MpfTray.exe	Allow Full Access
McAfee Security HTML Dialog	mghtml.exe	Allow Full Access
McAfee SecurityCenter Update Engine	mcupdate.exe	Allow Full Access
McAfee SecurityCenter Update Info	mcinfo.exe	Allow Full Access
McAfee SecurityCenter Update Manager	mcupdmgr.exe	Allow Full Access
McAfee Visual Trace	mvtx.exe	Allow Full Access
McRegWiz Module	mcregwiz.exe	Allow Full Access
Microsoft Application Error Reporting	dwwin.exe	Allow Full Access

Application Details

Apache HTTP Server 2.0
Apache Software Foundation
C:\apache2triad\bin\apache.exe

Permission: Allow Full Access
Rule created on: 6/11/2005 8:59:52 PM

This application has **Full Access** to the Internet. It is possible for this application to send and receive data with any computer.

IP Address: 192.168.1.102 Netmask: 255.255.255.0 ▾

Figure 3-2. Internet Applications page

The Internet Applications page provides the following information:

- Application names
- File names
- Current permission levels
- Application details: application name and version, company name, path name, permission, timestamps, and explanations of permission types.

Changing application rules

Personal Firewall lets you change access rules for applications.

To change an application rule:

1. Right-click the McAfee icon, point to **Personal Firewall**, then select **Internet Applications**.
2. In the **Internet Applications** list, right-click the application rule for an application, and select a different level:
   - **Allow Full Access —** Allow the application to establish outbound and inbound Internet connections.
   - **Outbound Access Only —** Allow the application to establish an outbound Internet connection only.
   - **Block This Application —** Disallow the application Internet access.

     NOTE
     Previously blocked applications continue to be blocked when the firewall is set to the **Open** or **Lockdown**. To prevent this from, you can either change the application's access rule to **Full Access** or delete the **Blocked** permission rule from the **Internet Applications** list.

To delete an application rule:

1. Right-click the McAfee icon in the Windows system tray, point to **Personal Firewall**, then select **Internet Applications**.
2. In the **Internet Applications** list, right-click the application rule, then select **Delete Application Rule**.

The next time the application requests Internet access, you can set its permission level to re-add it to the list.

Allowing and blocking Internet applications

To change the list of allowed and blocked Internet applications:

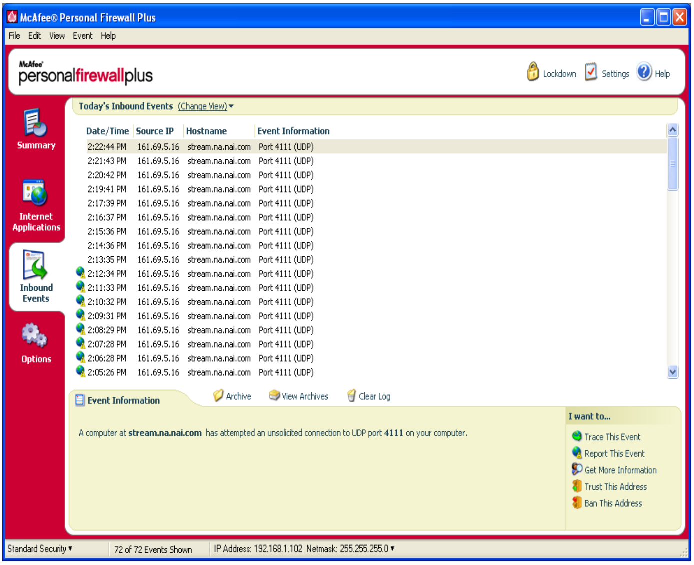
1. Right-click the McAfee icon in the Windows system tray, point to **Personal Firewall**, then select **Internet Applications**.
2. On the Internet Applications page, click one of the following options:
   - **New Allowed Application** — Allow an application full Internet access.
   - **New Blocked Application** — Disallow an application Internet access.
   - **Delete Application Rule** — Remove an application rule.

About the Inbound Events page

Use the Inbound Events page to view the Inbound Events log, generated when Personal Firewall blocks unsolicited Internet connections.

To launch the Inbound Events page:

- Right-click the McAfee icon M in the Windows system tray, point to **Personal Firewall**, then select **Inbound Events** (Figure 3-3).



Today's Inbound Events (Change View)

Date/Time	Source IP	Hostname	Event Information
2:22:44 PM	161.69.5.16	stream.na.nai.com	Port 4111 (UDP)
2:21:43 PM	161.69.5.16	stream.na.nai.com	Port 4111 (UDP)
2:20:42 PM	161.69.5.16	stream.na.nai.com	Port 4111 (UDP)
2:19:41 PM	161.69.5.16	stream.na.nai.com	Port 4111 (UDP)
2:17:39 PM	161.69.5.16	stream.na.nai.com	Port 4111 (UDP)
2:16:37 PM	161.69.5.16	stream.na.nai.com	Port 4111 (UDP)
2:15:36 PM	161.69.5.16	stream.na.nai.com	Port 4111 (UDP)
2:14:36 PM	161.69.5.16	stream.na.nai.com	Port 4111 (UDP)
2:13:35 PM	161.69.5.16	stream.na.nai.com	Port 4111 (UDP)
2:12:34 PM	161.69.5.16	stream.na.nai.com	Port 4111 (UDP)
2:11:33 PM	161.69.5.16	stream.na.nai.com	Port 4111 (UDP)
2:10:32 PM	161.69.5.16	stream.na.nai.com	Port 4111 (UDP)
2:09:31 PM	161.69.5.16	stream.na.nai.com	Port 4111 (UDP)
2:08:29 PM	161.69.5.16	stream.na.nai.com	Port 4111 (UDP)
2:07:28 PM	161.69.5.16	stream.na.nai.com	Port 4111 (UDP)
2:06:28 PM	161.69.5.16	stream.na.nai.com	Port 4111 (UDP)
2:05:26 PM	161.69.5.16	stream.na.nai.com	Port 4111 (UDP)

Event Information

A computer at **stream.na.nai.com** has attempted an unsolicited connection to UDP port **4111** on your computer.

Standard Security ▾ | 72 of 72 Events Shown | IP Address: 192.168.1.102 Netmask: 255.255.255.0 ▾

Figure 3-3. Inbound Events page

The Inbound Events page provides the following information:

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

Understanding events

About IP addresses

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

IP address types

Several IP addresses are unusual for various reasons:

Non-routable IP addresses — These are also referred to as "Private IP Space." These IP addresses cannot be used on the Internet. Private IP blocks are 10.x.x.x, 172.16.x.x - 172.31.x.x, and 192.168.x.x.

Loop-back IP addresses — Loop-back addresses are used for testing purposes. Traffic sent to this block of IP addresses comes right back to the device generating the packet. It never leaves the device, and is primarily used for hardware and software testing. The Loop-Back IP block is 127.x.x.x.

Null IP address — This is an invalid address. When detected, Personal Firewall indicates that the traffic used a blank IP address. Frequently, this indicates that the sender is deliberately obscuring the origin of the traffic. The sender will not be able to receive any replies to their traffic unless the packet is received by an application that understands the contents of the packet that will include instructions specific to that application. Any address that starts with 0 (0.x.x.x) is a null address. For example, 0.0.0.0 is a null IP address.

Events from 0.0.0.0

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

The other situation occurs when the source IP is spoofed, or faked. Spoofed packets can be a sign that someone is scanning your computer for Trojans. Personal Firewall blocks this kind of activity, so your computer is safe.

Events from 127.0.0.1

Events will sometimes list their source IP as 127.0.0.1. This is called a loopback address or localhost.

Many legitimate programs use the loopback address for communication between components. For example, you can configure many personal E-mail or Web servers through a Web interface. To access the interface, you type “http://localhost/” in your Web browser.

Personal Firewall allows traffic from these programs, so if you see events from 127.0.0.1, it is likely that the source IP address is spoofed, or faked. Spoofed packets are usually indicate that another computer is scanning yours for Trojans. Personal Firewall blocks such intrusion attempts, so your computer is safe.

Some programs, notably Netscape 6.2 and higher, require you to add 127.0.0.1 to the Trusted IP Addresses list. These programs' components communicate between each other in such a manner that Personal Firewall cannot determine if the traffic is local or not.

In the example of Netscape 6.2, if you do not trust 127.0.0.1, then you will not be able to use your buddy list. Therefore, if you see traffic from 127.0.0.1 and all of the applications on your computer work normally, then it is safe to block this traffic. However, if a program (like Netscape) experiences problems, add 127.0.0.1 to the Trusted IP Addresses list in Personal Firewall.

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

Events from computers on your LAN

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

In most corporate LAN settings, you should select **Make all computers on your LAN Trusted** in the Trusted IP Addresses options.

In some situations, your "local" network can be as dangerous than the Internet, especially if your computer runs on a high-bandwidth DSL or cable modem based network. In this case, do not to select **Make all computers on your LAN Trusted**. Instead, add the IP addresses of your local computers to the Trusted IP Addresses list.

Events from private IP addresses

IP addresses of the format 192.168.xxx.xxx, 10.xxx.xxx.xxx, and 172.16.0.0 - 172.31.255.255 are referred to as non-routable or private IP addresses. These IP addresses should never leave your network, and can be trusted most of the time.

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

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

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

Showing events in the Inbound Events log

The Inbound Events log displays events in a number of ways. The default view limits the view to events which occur on the current day. You can also view events that occurred during the past week, or view the complete log.

Personal Firewall also lets you display inbound events from specific days, from specific Internet addresses (IP addresses), or events that contain the same event information.

For information about an event, click the event, and view the information in the **Event Information** pane.

Showing today's events

Use this option to review the day’s events.

To show today’s events:

1. Right-click the McAfee icon in the Windows system tray, point to **Personal Firewall**, then select **Inbound Events**.
2. On the Inbound Events log, right-click an entry, then click **Show Today's Events**.

Showing this week's events

Use this option to review weekly events.

To show this week’s events:

1. Right-click the McAfee icon in the Windows system tray, point to **Personal Firewall**, then select **Inbound Events**.
2. On the Inbound Events log, right-click an entry, then click **Show This Week's Events**.

Showing the complete Inbound Events log

Use this option to review all events.

To show all of the events in the Inbound Events log:

1. Right-click the McAfee icon, point to **Personal Firewall**, and click **Inbound Events**.
2. On the Inbound Events log, right-click an entry, then click **Show Complete Log**.

   The Inbound Events log displays all events from the Inbound Events log.

Showing events from a specific day

Use this option to review events from a specific day.

To show a day's events:

1. Right-click the McAfee icon in the Windows system tray, point to **Personal Firewall**, then select **Inbound Events**.
2. On the Inbound Events log, right-click an entry, then click **Show Only Events From this Day**.

Showing events from a specific Internet address

Use this option to review other events which originate from a particular Internet address.

To show events of an Internet address:

1. Right-click the McAfee icon in the Windows system tray, point to **Personal Firewall**, and click **Inbound Events**.
2. On the Inbound Events log, right-click an entry, then click **Show Only Events From Selected Internet Address**.

Showing events that share identical event information

Use this option to review other events in the Inbound Events log that have the same information in the Event Information column as the event you selected. You can find out how many times this event happened, and if it is from the same source. The Event Information column provides a description of the event and, if known, the common program or service that uses that port.

To show events that share identical event information:

1. Right-click the McAfee icon in the Windows system tray, point to **Personal Firewall**, and click **Inbound Events**.
2. On the Inbound Events log, right-click an entry, then click **Show Only Events with the same Event Information**.

Responding to inbound events

In addition to reviewing details about events in the Inbound Events log, you can perform a Visual Trace of the IP addresses for an event in the Inbound Events log, or get event details at the anti-hacker online community HackerWatch.org web site.

Tracing the selected event

You can try to perform a Visual Trace of the IP addresses for an event in the Inbound Events log.

To trace a selected event:

1. Right-click the McAfee icon in the Windows system tray, point to **Personal Firewall**, and select **Inbound Events**.
2. On the Inbound Events log, right-click the event you want to trace, then click **Trace Selected Event**. You can also double-click an event to trace an event.

By default, Personal Firewall begins a Visual Trace using the integrated Personal Firewall Visual Trace program.

Getting advice from HackerWatch.org

To get advice from HackerWatch.org:

1. Right-click the McAfee icon, point to **Personal Firewall**, and select **Inbound Events**.
2. Select the event's entry on the Inbound Events page, then click **Get More Information** on the **I want to** pane.

Your default Web browser launches and opens the HackerWatch.org to retrieve information about the event type, and advice about whether to report the event.

Reporting an event

To report an event that you think was an attack on your computer:

1. Right-click the McAfee icon in the Windows system tray, point to **Personal Firewall**, and select **Inbound Events**.
2. Click the event you want to report, then click **Report This Event** in the **I want to** pane.

Personal Firewall reports the event to the HackerWatch.org using your unique ID.

Signing up for HackerWatch.org

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

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

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

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

Trusting an address

You can use the Inbound Events page to add an IP address to the Trusted IP Addresses list to allow a permanent connection.

If you see an event in the Inbound Events page that contains an IP address that you need to allow, you can have Personal Firewall allow connections from it at all times.

To add an IP address to the Trusted IP Addresses list:

1. Right-click the McAfee icon in the Windows system tray, point to **Personal Firewall**, and select **Inbound Events**.
2. Right-click the event whose IP address you want trusted, and click **Trust the Source IP Address**.

Verify that the IP address displayed in the Trust This Address dialog is correct, and click **OK**. The IP address is added to the Trusted IP Addresses list.

To verify that the IP address was added:

1. Right-click the McAfee icon in the Windows system tray, point to **Personal Firewall**, and select **Options**.
2. Click the **Trusted & Banned IPs** icon, then the **Trusted IP Addresses** tab.

The IP address appears checked in the Trusted IP Addresses list.

Banning an address

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

Add an IP address to your banned list only if you have one or more ports that are deliberately open and if you have reason to believe that you must block that

If you see an event in the Inbound Events page that contains an IP address that you want to ban, you can configure Personal Firewall to prevent connections from it at all times.

You can use the Inbound Events page, which lists the IP addresses of all inbound Internet traffic, to ban an IP address that you suspect is the source of suspicious or undesirable Internet activity.

To add an IP address to the Banned IP Addresses list:

1. Right-click the McAfee icon in the Windows system tray, point to **Personal Firewall**, then select **Inbound Events**.
2. The Inbound Events page lists the IP addresses of all inbound Internet traffic. Select an IP address, and then do one of the following:
   - Right-click the IP address, and then select **Ban the Source IP Address**.
   - From the **I want to** menu, click **Ban This Addres**s.
3. In the Add Banned IP Address Rule dialog, use one or more of the following settings to configure the Banned IP Address rule:
   - **A Single IP Address**: The IP address to ban. The default entry is the IP address that you selected from the Inbound Event page.
   - **An IP Address Range**: The IP addresses between the address you specify in From IP Address and the IP address you specify in To IP Address.

- **Make this rule expire on**: Date and time in which the Banned IP Address rule expires. Select the appropriate drop down menus to select the date and the time.
- **Description**: Optionally describe the new rule.
- Click **OK**.

4 In the dialog box, click **Yes** to confirm your setting. Click **No** to return to the Add Banned IP Address Rule dialog.

If Personal Firewall detects an event from a banned Internet connection, it will alert you according to the method you specified on the Alert Settings page.

To verify that the IP address was added:

1 Click the **Options** tab.

2 Click the **Trusted & Banned IPs** icon, then click the **Banned IP Addresses** tab.

The IP address appears checked in the Banned IP Addresses list.

Managing the Inbound Events log

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

Archiving the Inbound Events log

You can archive the current Inbound Events log to save all of the logged inbound events, including their date and times, source IPs, hostnames, ports, and event information. You should archive your Inbound Events log periodically to prevent the Inbound Events log from growing too large.

To archive the Inbound Events log:

1. Right-click the McAfee icon in the Windows system tray, point to **Personal Firewall**, then select **Inbound Events**.
2. On the Inbound Events page, click **Archive**.
3. On the Archive Log dialog, click **Yes** to proceed with the operation.
4. Click **Save** to save the archive in the default location, or browse to a location where you want to save the archive.

Note: By default, Personal Firewall automatically archives the Inbound Events log. Check or clear **Automatically archive logged events** in the Event Log Settings page to enable or disable the option.

Viewing an archived Inbound Events log

You can view any Inbound Events log that you previously archived. The saved archive includes date and times, source IPs, hostnames, ports, and event information for the events.

To view an archived Inbound Events log:

1. Right-click the McAfee icon in the Windows system tray, point to **Personal Firewall**, then select **Inbound Events**.
2. On the Inbound Events page, click **View Archives**.
3. Select or browse for the archive file name and click **Open**.

Clearing the Inbound Events log

You can clear all information from the Inbound Events log.

WARNING: Once you clear the Inbound Events log, you cannot recover it. If you think you will need the Events Log in the future, you should archive it instead.

To clear the Inbound Events log:

1 Right-click the McAfee icon, point to **Personal Firewall**, then select **Inbound Events**.

2 On the Inbound Events page, click **Clear Log**.

3 Click **Yes** in the dialog to clear the log.

Copying an event to the Clipboard

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

To copy events to the clipboard:

1 Right-click the McAfee icon, point to **Personal Firewall**, then select **Inbound Events**.

2 Right-click the event in the Inbound Events log.

3 Click **Copy Selected Event to Clipboard**.

4 Launch Notepad.

- Type `notepad` on the command line or click the Windows **Start** button, point to **Programs**, then **Accessories**. Select **Notepad**.

5 Click **Edit**, and then click Paste. The event text appears in Notepad. Repeat this step until you have all of the necessary events.

6 Save the Notepad file in a safe place.

Deleting the selected event

You can delete events from the Inbound Events log.

To delete events from the Inbound Events log:

1 Right-click the McAfee icon in the Windows system tray, point to **Personal Firewall**, then select **Inbound Events**.

2 Click the event's entry on the Inbound Events page that you want to delete.

3 On the Edit menu, click **Delete Selected Event**. The event is deleted from the Inbound Events log.

About alerts

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

NOTE
Recommendations on alerts help you decide how to handle an alert. For recommendations to appear on alerts, click the **Options** tab, click the **Alert Settings** icon, then select either **Use Smart Recommendations** (the default) or **Display Smart Recommendations only** from the **Smart Recommendations** list.

Red alerts

Red alerts contain important information that requires your immediate attention:

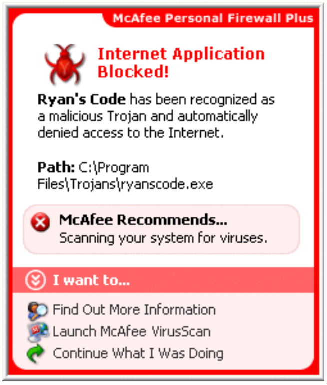
- **Internet Application Blocked** — This alert appears if Personal Firewall blocks an application from accessing the Internet. For example, if a Trojan program alert appears, McAfee automatically denies this program access to the Internet and recommends that you scan your computer for viruses.
- **Application Wants to Access the Internet —** This alert appears when Personal Firewall detects Internet or network traffic for new applications.
- **Application Has Been Modified —**This alert appears when Personal Firewall detects that an application, previously allowed to access the Internet, has changed. If you have not recently upgraded the application, be careful about granting the modified application access to the Internet.
- **Application Requests Server Access —** This alert appears when Personal Firewall detects that an application you have previously allowed to access the Internet has requested Internet access as a server.

NOTE
The Windows XP SP2 default Automatic Updates setting downloads and installs updates for the Windows OS and other Microsoft programs running on your computer without messaging you. When an application has been modified from one of Windows silent updates, McAfee Personal Firewall alerts appear the next time the Microsoft application is run.

IMPORTANT
You must grant access to applications that require Internet access for online product updates (such as McAfee services) to keep them up-to-date.

Internet Application Blocked alert

If a Trojan program alert appears (Figure 3-4), Personal Firewall automatically denies this program access to the Internet and recommends that you scan your computer for viruses. If McAfee VirusScan is not installed, you can launch McAfee SecurityCenter.


McAfee Personal Firewall Plus

Internet Application Blocked!

Ryan's Code has been recognized as a malicious Trojan and automatically denied access to the Internet.

Path: C:\Program Files\Trojans\ryanscode.exe

McAfee Recommends...
Scanning your system for viruses.

I want to...
Find Out More Information
Launch McAfee VirusScan
Continue What I Was Doing

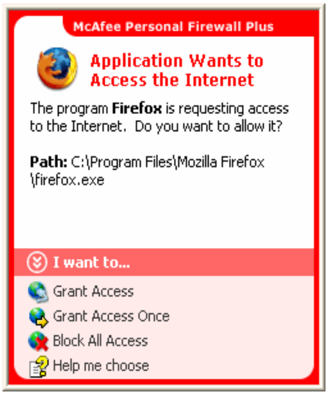
Figure 3-4. Internet Application Blocked alert

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

- Click **Find Out More Information** to get details about the event through the Inbound Events log (see *About the Inbound Events page* on page 59 for details).
- Click **Launch McAfee VirusScan** to scan your computer for viruses.
- Click **Continue What I Was Doing** if you do not want to take action beyond what Personal Firewall has already done.
- Click **Grant Outbound Access** to allow an outbound connection (**Tight** security).

Application Wants to Access the Internet alert

If you selected **Standard** or **Tight** security in the Security Settings options, Personal Firewall displays an alert (Figure 3-5) when it detects Internet or network connections for new or modified applications.



McAfee Personal Firewall Plus

Application Wants to Access the Internet

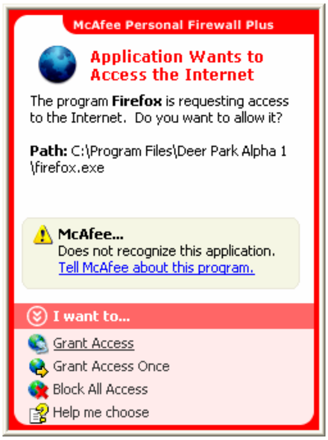
The program **Firefox** is requesting access to the Internet. Do you want to allow it?

Path: C:\Program Files\Mozilla Firefox \firefox.exe

Figure 3-5. Application Wants to Access the Internet alert

If an alert appears recommending caution in allowing the application Internet access, you can click **Click here to learn more** to get more information about the application. This option appears on the alert only if Personal Firewall is configured to use Smart Recommendations.

McAfee might not recognize the application trying to gain Internet access (Figure 3-6).



McAfee Personal Firewall Plus

Application Wants to Access the Internet

The program **Firefox** is requesting access to the Internet. Do you want to allow it?

Path: C:\Program Files\Deer Park Alpha 1 \firefox.exe

McAfee...
Does not recognize this application.
Tell McAfee about this program.

Figure 3-6. Unrecognized Application alert

Therefore, McAfee cannot give you a recommendation on how to handle the application. You can report the application to McAfee by clicking **Tell McAfee about this program**. A web page appears and asks you for information related to the application. Please fill out as much information as you know.

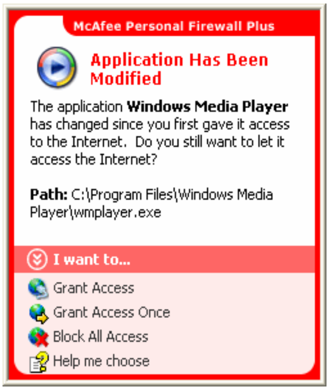
The information you submit is used in conjunction with other research tools by our HackerWatch operators to determine whether an application warrants being listed in our known applications database, and if so, how it should be treated by Personal Firewall.

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

- Click **Grant Access** to allow the application an outbound and inbound Internet connection.
- Click **Grant Access Once** to grant the application a temporary Internet connection. Access is limited to the time the application launches to the time it closes.
- Click **Block All Access** to prohibit an Internet connection.
- Click **Grant Outbound Access** to allow an outbound connection (**Tight** security).
- Click **Help me choose** to view online Help about application access permissions.

Application Has Been Modified alert

If you selected **Trusting**, **Standard**, or **Tight** security in the Security Settings options, Personal Firewall displays an alert (Figure 3-7) when Personal Firewall detects that an application you have previously allowed to access the Internet has changed. If you have not recently upgraded the application in question, be careful about granting the modified application access to the Internet.



The application **Windows Media Player** has changed since you first gave it access to the Internet. Do you still want to let it access the Internet?

Path: C:\Program Files\Windows Media Player\wmplayer.exe

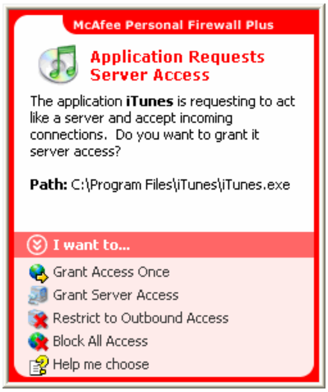
Figure 3-7. Application Has Been Modified alert

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

- Click **Grant Access** to allow the application an outbound and inbound Internet connection.
- Click **Grant Access Once** to grant the application a temporary Internet connection. Access is limited to the time the application launches to the time it closes.
- Click **Block All Access** to prohibit an Internet connection.
- Click **Grant Outbound Access** to allow an outbound connection (**Tight** security).
- Click **Help me choose** to view online Help about application access permissions.

Application Requests Server Access alert

If you selected **Tight** security in the Security Settings options, Personal Firewall displays an alert (Figure 3-8) when it detects that an application you have previously allowed to access the Internet has requested Internet access as a server.



McAfee Personal Firewall Plus

Application Requests Server Access

The application **iTunes** is requesting to act like a server and accept incoming connections. Do you want to grant it server access?

Path: C:\Program Files\iTunes\iTunes.exe

Figure 3-8. Application Requests Server Access alert

For example, an alert appears when MSN Messenger requests server access to send a file during a chat.

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

- Click **Grant Access Once** to allow the application temporary Internet access. Access is limited to the time the application launches to the time it closes.
- Click **Grant Server Access** to allow the application an outbound and inbound Internet connection.
- Click **Restrict to Outbound Access** to prohibit an incoming Internet connection.

- Click **Block All Access** to prohibit an Internet connection.
- Click **Help me choose** to view online Help about application access permissions.Green alerts

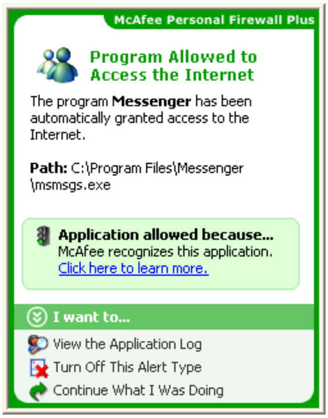
Green alerts

Green alerts notify you of events in Personal Firewall, such as applications that have been automatically granted Internet access.

Program Allowed to Access the Internet — This alert appears when Personal Firewall automatically grants Internet access for all new applications, then notifies you (**Trusting** Security). An example of a modified application is one with modified rules to automatically allow the application Internet access.

Application Allowed to Access the Internet alert

If you selected **Trusting** security in the Security Settings options, Personal Firewall automatically grants Internet access for all new applications, then notifies you with an alert (Figure 3-9).



McAfee Personal Firewall Plus

Program Allowed to Access the Internet

The program **Messenger** has been automatically granted access to the Internet.

Path: C:\Program Files\Messenger \msmsgs.exe

Application allowed because...
McAfee recognizes this application.
Click here to learn more.

Figure 3-9. Program Allowed to Access the Internet

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

- Click **View the Application Log** to get details about the event through the Internet Applications Log (see *About the Internet Applications page* on page 57 for details).
- Click **Turn Off This Alert Type** to prevent these types of alerts from appearing.
- Click **Continue What I Was Doing** if you do not want to take action beyond what Personal Firewall has already done.
- Click **Block All Access** to prohibit an Internet connection.

Application Has Been Modified alert

If you selected **Trusting** security in the Security Settings options, Personal Firewall automatically grants Internet access for all modified applications. View a brief description of the event, then choose from these options:

- Click **View the Application Log** to get details about the event through the Internet Applications Log (see *About the Internet Applications page* on page 57 for details).
- Click **Turn Off This Alert Type** to prevent these types of alerts from appearing.
- Click **Continue What I Was Doing** if you do not want to take action beyond what Personal Firewall has already done.
- Click **Block All Access** to prohibit an Internet connection.

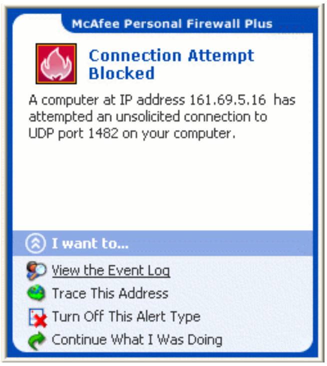
Blue alerts

Blue alerts contain information, but require no response from you.

- **Connection Attempt Blocked —** This alert appears when Personal Firewall blocks unwanted Internet or network traffic. (Trusting, Standard, or Tight Security)

Connection Attempt Blocked alert

If you selected **Trusting**, **Standard**, or **Tight** security, Personal Firewall displays an alert (Figure 3-10) when it blocks unwanted Internet or network traffic.


McAfee Personal Firewall Plus
Connection Attempt Blocked
I want to...
View the Event Log
Trace This Address
Turn Off This Alert Type
Continue What I Was Doing

A computer at IP address 161.69.5.16 has attempted an unsolicited connection to UDP port 1482 on your computer.

Figure 3-10. Connection Attempt Blocked alert

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

- Click **View the Event Log** to get details about the event through the Personal Firewall Inbound Events log (see *About the Inbound Events page* on page 59 for details).
- Click **Trace This Address** to perform a Visual Trace of the IP addresses for this event.
- Click **Ban This Address** to block this address from accessing your computer. The address is added to the Banned IP Addresses list.
- Click **Trust This Address** to allow this IP address to access your computer.
- Click **Continue What I Was Doing** if you do not want to take action beyond what Personal Firewall has already done

McAfee Privacy Service 4

Welcome to McAfee Privacy Service.

McAfee Privacy Service software offers advanced protection for you, your family, your personal data, and your computer.

Features

This release of McAfee Privacy Service includes the following features:

- Internet time usage rules - Use a time grid to specify days and times when users can access the Internet.
- Custom keyword filtering - Filter Web site access based on keywords the Administrator specifies for certain age levels.
- Privacy Service backup and restore - Save and restore Privacy Service settings at any time.
- Web bug blocker—Block Web bugs (objects obtained at potentially harmful web sites) so that they are not loaded within browsed Web pages.
- Pop-up blocker—Prevent pop-up windows from displaying as you browse the Internet.
- Shredder—McAfee Shredder protects your privacy by quickly and safely erasing unwanted files.

The Administrator

The Administrator specifies which users can access the Internet, when they can use it, and what they can do on the Internet.

NOTE
The Administrator is considered an adult and as such can access all web sites but is prompted to allow or prevent the transmission of added personal identifiable information (PII).

Setup Assistant

The Setup Assistant allows you to create the Administrator (if you have not done so previously), manage global settings, enter personal information, and add users.

> **NOTE**
> Remember your Administrator password and security answer so that you can log on to Privacy Service. If you cannot log on, you cannot use Privacy Service and the Internet. Keep your password secret so only you can change Privacy Service settings.
>
> Some Web sites require that cookies are enabled to work properly.
>
> Privacy Service always accepts cookies from McAfee.com.

Retrieving the Administrator Password

If you forget the Administrator password, you can access the password using the security information you entered when you created the Administrator profile.

1. Right-click the McAfee icon M in the Windows system tray, point to **McAfee Privacy Service**, then select **Sign In**.
2. Select **Administrator** from the **User Name** pull-down menu.
3. Click **Forgot your password?**
4. Enter the answer to the security question that appears, and then click **Get Password**. A message appears containing your password. If you forget the answer to the security question, you must uninstall McAfee Privacy Service from Safe Mode (Windows 2000 and Windows XP only).

The Startup user

The Startup user is automatically signed in to Privacy Service when the computer is started.

For example, if a user is on the computer or Internet more than the others, you can make that user the Startup user. When the Startup user uses the computer, the user is not required to sign in to Privacy Service.

If you have young children, you can also set the Startup user to the youngest. This way, when an older user uses the computer, they can log off from the young user's account and then log in again using their own user name and password. This protects younger users from seeing inappropriate web sites.

Opening McAfee Privacy Service

When you install McAfee Privacy Service, the McAfee icon appears in the Windows system tray, which is located near the system clock. From the McAfee icon, you can access McAfee Privacy Service, McAfee SecurityCenter, and other McAfee products installed on your computer.

Opening and signing in to Privacy Service

To open Privacy Service:

1. Right-click the McAfee icon, point to **McAfee Privacy Service**, and then select **Sign In**.
2. Select your user name from the **User name** pull-down menu.
3. Enter your Password in the **Password** field.
4. Click **Sign In**.

Disabling Privacy Service

You must be logged in to Privacy Service as the Administrator to disable it.

To disable Privacy Service:

Right-click the McAfee icon , point to **McAfee Privacy Service,** and then select **Sign Out**.

NOTE
If **Sign In** is in the place of **Sign Out**, then you are already signed out.

Updating McAfee Privacy Service

McAfee SecurityCenter regularly checks for updates to Privacy Service while your computer is running and connected to the Internet. If an update is available, McAfee SecurityCenter prompts you to update Privacy Service.

To manually check for updates, click the Updates icon located in the top pane.

Adding Users

To add users, you must sign in to Privacy Service as the Administrator.

1. Right-click the McAfee icon in the Windows system tray.
2. Point to **McAfee Privacy Service**, then select **Manage Users**. The **Select A User** dialog box appears.

3 Click **Add** and enter the new user's name in the **User name** field.

Setting the password

1 Enter a password in the **Password** field. The password can be up to 50 characters and can contain uppercase and lowercase letters and numbers.

2 Enter the password again in the **Confirm Password** field.

3 Select **Make this user the Startup user** if you want this user to be the Startup user.

4 Click **Next**.

When assigning passwords, consider the age of the person. For example, if you assign a password to a young child, make the password simple. If you assign a password to an older teenager or an adult, make the password more complex.

Setting the age group

Select the appropriate age-based setting, and then click **Next**.

Setting the cookie blocker

Select the appropriate option, and then click **Next**.

- **Reject all cookies**—Renders cookies unreadable to the web sites that sent them. Some web sites require you to enable cookies to work properly.

- **Prompt user to accept cookies**—Enables you to decide if you want to accept or reject cookies on a case-by-case basis. Privacy Service notifies you when a web site you are about to view wants to send a cookie to your computer. After you make your choice, you are not asked about that cookie again.

- **Accept all cookies**—Allows web sites to read the cookies they send to your computer.

NOTE
Some web sites, to work properly, require that cookies are enabled.

Privacy Service accepts cookies from McAfee at all times.

Setting the Internet time limits

To grant unrestricted Internet use:

1 Select **Can use Internet anytime**.

2 Click **Create**. The new user appears in the Select A User list.

To grant limited Internet use:

1. Select **Restrict Internet usage**, and then click **Edit**.
2. On the Internet Time Limits page, drag across the time grid to select the time and day the user can access the Internet.
   You can specify time limits in thirty-minute intervals. Green portions of the grid are the periods a user can access the Internet. Red portions show when a user cannot access the Internet. If a user tries to use the Internet when they are not allowed to, Privacy Service displays a message telling the user that they are not allowed to use the Internet at this time. To modify the periods a user can access the Internet, drag across the green portions of the grid.
3. Click **Done**.
4. Click **Create**. The new user appears in the Select A User page. If a user tries to use the Internet when they are not allowed to, Privacy Service displays a message telling the user that they are not allowed to use the Internet at this time.

To prohibit Internet use:

- Select **Restrict Internet Usage**, and then click **Create**. When the user uses the computer, they are prompted to sign in to Privacy Service. They can use the computer, but not the Internet.

Editing Users

To edit users, you must sign in to Privacy Service as the Administrator.

Changing passwords

1. Select the user whose information you are changing and click **Edit**.
2. Select **Password**, and enter the user's new password in the **New password** field. The password can be up to 50 characters and can contain uppercase and lowercase letters and numbers.
3. Enter the same password in the **Confirm password** field, and then click **Apply**.
4. Click **OK** in the confirmation dialog box.

   NOTE
   An Administrator can change a user’s password without knowing the user’s current password.

Changing a user’s information

1. Select the user whose information you are changing and click **Edit**.
2. Select **User Info**.
3. Enter the new user name in the **New user name** field.
4. Click **Apply**, and then click **OK** in the confirmation dialog box.
5. To restrict a user to viewing the web sites in the Allowed Web Sites list, select **Restrict this user to Web sites in the "Allowed Web Sites" list**.

Changing cookie blocker setting

1. Select the user whose information you are changing and click **Edit**.
2. Select **Cookies**, and then select the appropriate option.
   - **Reject all cookies**—Renders cookies unreadable to the web sites that sent them. Some web sites require you to enable cookies to work properly.
   - **Prompt user to accept cookies**—Enables you to decide if you want to accept or reject cookies on a case-by-case basis. Privacy Service notifies you when a web site you are about to view wants to send a cookie to your computer. After you make your choice, you are not asked about that cookie again.
   - **Accept all cookies**—Allows web sites to read the cookies they send to your computer.
3. Click **Apply**, and then click **OK** in the confirmation dialog box.

Editing the Accept and Reject Cookie List

1. Select **Prompt user to accept cookies** and click **Edit** to specify which web sites are allowed to read cookies.
2. Specify the list you are modifying by selecting **Web sites that can set cookies** or **Web sites that cannot set cookies**.
3. In the **http://** field, enter the address of the web site that you are accepting or rejecting cookies from.
4. Click **Add**. The web site appears in the Web site list.
5. Click **Done** when you are finished making changes.

NOTE
Some web sites, to work properly, require that cookies are enabled.

Privacy Service accepts cookies from McAfee at all times.

Changing the age group

1 Select the user whose information you are changing and click **Edit**.

2 Select **Age Group**.

3 Select a new Age Group for the user, and then click **Apply**.

4 Click **OK** in the confirmation dialog box.

Changing Internet time limits

1 Select the user whose information you are changing and click **Edit**.

2 Select **Time Limits** and do the following:

To allow the user Internet access all the time:

1 Select **Can use Internet anytime** and click **Apply**.

2 Click **OK** in the confirmation dialog box.

To restrict Internet access for the user:

1 Select **Restrict Internet usage** and click **Edit**.

2 On the Internet Time Limits page, select a green or red square, and then drag across the grid to change existing times and days a user can access the Internet. You can specify time limits in thirty-minute intervals. Green portions of the grid are the periods a user can access the Internet. Red portions show when a user cannot access the Internet. If a user tries to use the Internet when they are not allowed to, Privacy Service displays a message telling the user that they are not allowed to use the Internet at this time.

3 Click **Apply**.

4 On the Time Limits page, click **OK**.

5 In the McAfee Privacy Service McAfee Privacy Service confirmation dialog, click **OK**.

Changing the startup user

1. Select the user that you want to designate as the Startup user, and then click **Edit**.
2. Select **User Info**.
3. Select **Make this user the Startup user**.
4. Click **Apply** and then click **OK** in the confirmation dialog box.

   NOTE
   If a startup user already exists, you do not have to deselect them as a startup user.

Removing users

1. Select the user you want to remove, and then click **Remove**.
2. Click **Yes** in the confirmation dialog box.
3. Close the Privacy Service window when you are finished making changes.

Options

To configure Privacy Service options, you must sign in to Privacy Service as the Administrator.

Blocking web sites

1. Click **Options**, and then select **Block List**.
2. In the **http://** field, enter the URL of the web site that you want to block, and then click **Add**. The web site appears in the **Blocked Web Sites** list.

   NOTE
   Users (including Administrators) that belong to the Adult group level can access all web sites, even if the web sites are in the Blocked Web Sites list. To test blocked web sites, Administrators must log in as non-adult users.

Allowing Web sites

The Administrator can allow all users to view specific web sites. This overrides Privacy Service's default settings and web sites added to the Blocked list.

1. Click **Options**, and then select **Allow List**.

2 In the **http://** field, enter the URL of the web site that you want to allow, and then click **Add**. The web site appears in the **Allowed Web Sites** list.

Blocking information

The Administrator can prevent other users from sending specific personal information over the Internet (the Administrator can still send this information).

When Privacy Service detect personal identifiable information (PII) in something about to be sent out, the following occurs:

- If you are an Administrator, you are prompted, and can decide whether to send the information or not.
- If the logged in user is not the Administrator, the blocked information is replaced with *MFEMFEMFE*. For example, if you send the e-mail *Lance Armstrong wins tour*, and Armstrong is set as personal information that is to be blocked, then the e-mail that is actually sent is *Lance MFEMFEMFE wins tour*.

Adding information

1 Click **Options**, and then select **Block Info**.

2 Click **Add**. The **Select Type** pull-down menu appears.

3 Select the type of information that you want to block.

4 Enter the information in the appropriate fields, and then click **OK**. The information you entered appears in the list.

Editing information

1 Click **Options**, and then select **Block Info**.

2 Select the information that you want to edit, and click **Edit**.

3 Make the appropriate changes, and then click **OK**. If the information does not need to be changed, click **Cancel**.

Removing personal information

1 Click **Options**, and then select **Block Info**.

2 Select the information that you want to remove, and click **Remove**.

3 Click **Yes** in the confirmation dialog box.

Blocking Web bugs

Web bugs are small graphic files that can send messages to third parties, including tracking your Internet browsing habits or transmitting personal information to an external database. Third parties can then use this information to create user profiles.

To prevent web bugs from being loaded within browsed web pages, select **Block Web Bugs on this computer**.

Blocking advertisements

Advertisements are typically graphics served from a third party domain into a web page or pop-up window. Privacy Service does not block ads that are served from the same domain as the host web page.

Pop-ups are secondary browser windows presenting unwanted advertisements, which automatically display when as you visit a web site. Privacy Service only blocks those pop-ups that are automatically loaded when a web page loads. Pop-ups initiated by clicking a link are not blocked by Privacy Service. To display a blocked pop-up, hold down the CTRL key and refresh the web page.

Configure Privacy Service to block advertisements and pop-ups when you are using the Internet.

1. Click **Options**, and then select **Block Ads**.
2. Select the appropriate option.
    - **Block ads on this computer**—Blocks advertisements while you are using the Internet.
    - **Block Pop-Ups on this computer**—Blocks pop-ups while you are using the Internet.
3. Click **Apply**, and then click **OK** in the confirmation dialog box.

To disable pop-up blocking, right-click the web page, point to **McAfee Pop-Up Blocker**, and deselect **Enable Pop-up Blocker**.

Allowing cookies from specific Web sites

If you block cookies or require to be prompted before they are accepted, and find that certain web sites do not function properly, then configure Privacy Service to allow the site to read its cookies.

1 Click **Options**, and then select **Cookies**.

2 In the **http://** field, enter the address of the web site that needs to read its cookies, and then click **Add**. The address appears in the **Accept Cookie Web Sites** list.

Event Log

To view the event log, you must sign in to Privacy Service as the Administrator. Then, select **Event Log** and click any log entry to view its details. To save or view a saved log, select the Saved Logs tab.

Date and time

By default, the Event Log displays information in chronological order, with the most recent events at the top. If the Event Log entries are not in chronological order, click the Date and Time heading.

The date is displayed in a month/day/year format, and the time is displayed in the A.M./P.M. format.

User

The user is the person who was logged in and using the Internet at the time Privacy Service recorded the event.

Summary

Summaries display a short, concise description of what Privacy Service is doing to protect users and what users are doing on the Internet.

Event Details

The Event Details field displays entry details.

Saving the Current Log

The Current Log page displays information about recent administrative and user actions. You can save this information to view at a future date.

To save a current event log

1. Sign In to Privacy Service as the Administrator.
2. Select **Event Log**.
3. On the Current Log page, click **Save Log**.
4. In the **File name** field, type the name for the log file.
5. Click **Save**.

Viewing Saved Logs

The Current Log page displays information about recent administrative and user actions. You can save this information to view at a future date.

To view a saved log

1. Sign In to Privacy Service as the Administrator.
2. Select **Event Log**.
3. On Current Log page, click **Open Log**.
4. In the **Select a saved log to view** dialog, select the backup database file, and click **Open**.

Utilities

To access the utilities, you must sign in to Privacy Service as the Administrator, and then click **Utilities**.

To remove files, folders, or the entire contents of disks, click **McAfee Shredder**. To save your Privacy Service database settings, click **Backup**. To restore your settings, click **Restore**.

Erasing files permanently using McAfee Shredder

McAfee Shredder protects your privacy by quickly and safely erasing unwanted files.

Deleted files can be recovered from your computer even after you empty your Recycle Bin. When you delete a file, Windows merely marks that space on your disk drive as no longer being in use, but the file is still there.

Why Windows leaves file remnants

To permanently delete a file, you must repeatedly overwrite the existing file with new data. If Microsoft Windows securely deleted files, every file operation would be very slow. Shredding a document does not always prevent that document from being recovered because some programs make temporary hidden copies of open documents. If you only shred documents that you see in Explorer, you could still have temporary copies of those documents. We recommend that you periodically shred the free space on your disk drive to insure that these temporary copies are permanently deleted.

> **NOTE**
> With computer forensics tools, tax records, job resumes, or other documents that you had deleted, could be obtained.

What McAfee Shredder erases

With McAfee Shredder, you can securely and permanently erase:

- One or more files or folders
- An entire disk
- The trails that your web surfing leaves behind

Permanently erasing files in Windows Explorer

To shred a file via Windows Explorer:

1. Open Windows Explorer, then select the file or files that you want to shred.
2. Right-click your selection, point to **Send To**, and then select **McAfee Shredder**.

Emptying the Windows Recycle Bin

If files are in your Recycle Bin, McAfee Shredder offers a more secure method of emptying your Recycle Bin.

To shred the contents of the Recycle Bin:

1. On your Windows desktop, right-click the Recycle Bin.
2. Select **Shred Recycle Bin**, then follow the on-screen instructions.

Customizing Shredder settings

You can:

- Specify the number of shredding passes.

- Show a warning message when you shred files.
- Check your hard disk for errors before shredding.
- Add McAfee Shredder to your Send To menu
- Place a Shredder icon on your Windows desktop.

To customize Shredder settings, open McAfee Shredder, click **Properties**, and then follow the on-screen instructions.

Backing up the Privacy Service database

You can restore the Privacy Service database two ways. If your database becomes corrupted or is deleted, Privacy Service prompts you to restore the Privacy Service database. Alternatively, you can restore your database settings while running Privacy Service.

1. Click **Utilities**, and then select **Backup**.
2. Click **Browse** to select a location for the database file, and then click **OK**.
3. Enter a password in the **Password** field.
4. Enter the password again in the **Confirm password** field, and then click **Backup**.
5. Click **OK** in the confirmation dialog box.
6. Close the Privacy Service window when you are finished.

NOTE
Keep this password secret, and do not forget it. You cannot restore Privacy Service settings without this password.

Restoring the Backup Database

1. Privacy Service provides two ways to restore your original settings:
   - Load your backup database file after Privacy Service prompts you to restore your settings because the database is corrupt or deleted.
   - Load your backup database file while running Privacy Service.

To restore your Privacy Service Settings when prompted:

1. Click **Browse** to locate the file.
2. Type your password in the **Password** field.

3. Click **Restore**.
   If you did not back up the Privacy Service database, or you forgot your Backup password, or restoring the database does not work, please remove and reinstall Privacy Service.

To restore your Privacy Settings while running Privacy Service:

1. Click the **Utilities** tab.
2. Click **Restore**.
3. Click **Browse**, and type the path and name for the backup file.
4. Click **Open**.
5. Type your password in the **Password** field.
6. Click **Restore**, and then click **OK** in the McAfee Privacy Service confirmation dialog.

User Options

These instructions do not apply to the Administrator.

You can change your password and user name. We recommend that you change your password after the Administrator gives it to you. We also recommend that you change your password once a month, or if you think someone knows your password. This helps prevent others from using the Internet with your user name.

Changing your password

1. Right-click the McAfee icon, point to **McAfee Privacy Service**, and then select **Options**.
2. Click **Password** and enter your old password in the **Old password** field.
3. Enter your new password in the **New password** field.
4. Type your new password again in the **Confirm password** field, and then click **Apply**.
5. Click **OK** in the confirmation dialog box. You now have a new password.

Changing your user name

1. Right-click the McAfee icon, point to **McAfee Privacy Service**, and then select **Options**.
2. Click **User Info**.

3 Type your new user name in the **New user name** field and then click **Apply**.

4 Click **OK** in the confirmation dialog box. You now have a new user name.

Clearing your cache

We recommend that you clear your cache so that a child does not access web pages you recently visited. To clear your cache, do the following.

1 Open Internet Explorer.

2 From the **Tools** menu, click **Internet Options**. The Internet Options dialog box appears.

3 In the **Temporary Internet Files** section, click **Delete Files**. The Delete Files dialog box appears.

4 Select **Delete all offline content**, and then click **OK**.

5 Click **OK** to close the Internet Options dialog box.

Accepting cookies

This option is available only if the Administrator allows you to accept or reject cookies as they are intercepted.

If you access web sites that require cookies, you can allow those sites permission to read cookies.

1 Right-click the McAfee icon, point to **McAfee Privacy Service**, and then select **Options**.

2 Click **Accepted Cookies**.

3 Enter the URL of the web site in the **http://** field, and then click **Add**. The web site appears in the **Web Site** list.

If you need to remove a web site from this list:

1 Select the web site's URL in the **Web site** list.

2 Click **Remove**, and then click **Yes** in the confirmation dialog box.

Rejecting cookies

This option is available only if the Administrator allows you to accept or reject cookies as they are intercepted.

If you access web sites that do not require cookies, you can reject the cookies without being prompted.

1. Right-click the McAfee icon, point to **McAfee Privacy Service**, and then select **Options**.
2. Click **Rejected Cookies**.
3. Enter the URL of the web site in the **http://** field, and then click **Add**. The web site appears in the **Web site** list.

If you need to remove a web site from this list:

1. Select the web site's URL in the **Web Site** list.
2. Click **Remove**, and then click **Yes** in the confirmation dialog box.

McAfee SpamKiller 5

Welcome to McAfee SpamKiller.

McAfee SpamKiller software helps stop spam from entering your e-mail inbox. With it, you get the following features:

Features

This version of SpamKiller offers the following features:

- Filtering - advanced filtering options provide new filtering techniques, including support for meta-character filtering and junk text identification.
- Phishing - AntiPhishing browser plug-in via an Internet Explorer toolbar easily identifies and blocks potential phishing Web sites.
- Microsoft Outlook and Outlook Express integration - toolbar provides a folder within your mail client to block spam directly.
- Installation - streamlined setup and configuration. Automatic account detection assures smooth setup, configuration, and integration with existing e-mail accounts.
- Updates - auto-updates run silently in the background, always vigilant to minimize your exposure to emerging spam threats.
- Interface - intuitive user interface for keeping your computer free of spam.
- Support - free live instant messaging and e-mail technical support for easy, prompt, and live customer service.

Spam message processing - by default, spam messages are tagged as [SPAM] and placed in the SpamKiller folder in Outlook and Outlook Express, or your Inbox. Tagged messages also appear on the Accepted E-mail page.

User options

- Block spam using filters, and quarantine spam outside of your Inbox
- View blocked and accepted messages
- Monitor and filter multiple e-mail accounts
- Import friends’ addresses into the Friends List

- Fight back against spammers (report spam, complain about spam, create custom filters)
- Protect children from viewing spam messages
- One-click block and one-click rescue
- Double-byte character set support
- Multi-user support (for Windows 2000 and Windows XP)

Filtering

- Update filters automatically
- Create custom filters to block e-mail that contain mostly images, invisible text, or invalid formatting
- Multi-tiered core filtering engine
- Dictionary attack filter
- Multi-level adaptive filtering
- Security filters

Understanding the top pane

The following icons appear in the top pane of each SpamKiller page:

- Click **Switch User** to log on as a different user.

  Note: Switch user is available only if your computer runs Windows 2000 or Windows XP, multiple users have been added to SpamKiller, and you are logged on to SpamKiller as an administrator.

- Click **Support** to open the online Support page for McAfee, which provides hot topics on SpamKiller and other McAfee products, answers to frequently asked questions, and more. You must be connected to the Internet to access the Support page.
- Click **Help** to open the online Help, which provides detailed instructions on setting up and using SpamKiller.

When you install SpamKiller, the McAfee icon appears on your system tray located near your system clock. From the McAfee icon, you can access SpamKiller, McAfee SecurityCenter, and other McAfee products installed on your computer.

Disabling SpamKiller

You can disable SpamKiller and prevent e-mail from being filtered.

To disable filtering:

Right-click the McAfee icon , point to **SpamKiller**, and then click **Disable**. Or click the **Summary** tab, and then click **Click here to disable**.

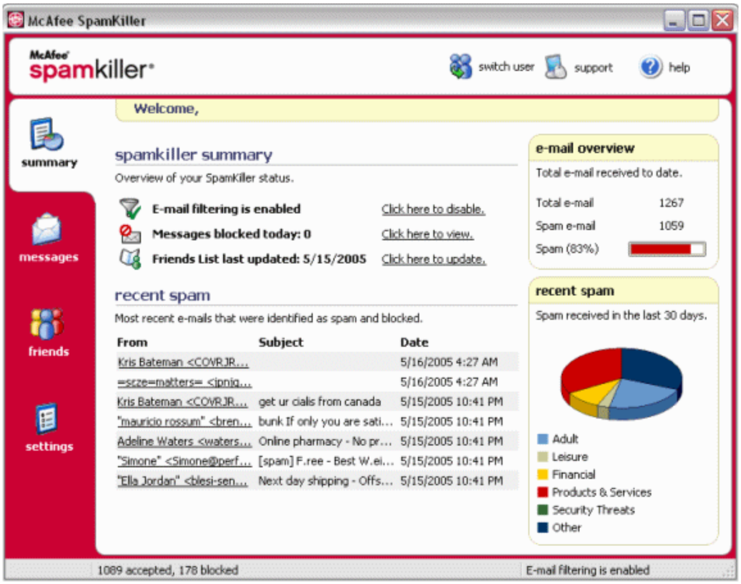
To enable filtering:

Right-click the McAfee icon, point to **SpamKiller**, and then click **Enable**. Or click the **Summary** tab, and then click **Click here to enable**.

Understanding the Summary page

Click the **Summary** tab to open the Summary page (Figure 5-11).

- **Overview of your SpamKiller status** - indicates if filtering is enabled, when a Friends List was last updated, and the number of spam messages you received today. From here you can disable or enable SpamKiller filtering, update Friends Lists, and open the Blocked E-mail page.
- **Most recent e-mails that were identified as spam and blocked** - the latest spam messages that SpamKiller blocked (messages removed from your Inbox).
- **E-mail Overview** - the total number of e-mail, spam (blocked messages), and percentage of total spam you have received.
- **Recent Spam** - a breakdown of the type of spam you received in the past 30 days.



Welcome,

spamkiller summary

Overview of your SpamKiller status.

E-mail filtering is enabled — Click here to disable.

Messages blocked today: 0 — Click here to view.

Friends List last updated: 5/15/2005 — Click here to update.

e-mail overview

Total e-mail received to date.

Total e-mail	1267
Spam e-mail	1059
Spam (83%)	

recent spam

Most recent e-mails that were identified as spam and blocked.

From	Subject	Date
Kris Bateman <COVRJR...		5/16/2005 4:27 AM
=scze=matters= <jpnig...		5/16/2005 4:27 AM
Kris Bateman <COVRJR...	get ur cialis from canada	5/15/2005 10:41 PM
"mauricio rossum" <bren...	bunk If only you are sati...	5/15/2005 10:41 PM
Adeline Waters <waters...	Online pharmacy - No pr...	5/15/2005 10:41 PM
"Simone" <Simone@perf...	[spam] F.ree - Best W.ei...	5/15/2005 10:41 PM
"Ella Jordan" <blesi-sen...	Next day shipping - Offs...	5/15/2005 10:41 PM

recent spam

Spam received in the last 30 days.

1089 accepted, 178 blocked

E-mail filtering is enabled

Figure 5-11. Summary page

Microsoft Outlook and Outlook Express integration

You can access core SpamKiller features from Outlook Express 6.0, Outlook 98, Outlook 2000, and Outlook XP, by selecting the SpamKiller menu or the SpamKiller toolbar.

The SpamKiller toolbar appears to the right of the standard toolbars in Outlook and Outlook Express. If the toolbar is not visible, expand the e-mail application window or click the arrows to see more toolbars.

When the SpamKiller toolbar first appears in your e-mail application, you can only use the toolbar commands on new messages. Existing spam e-mail must be manually deleted.

Managing E-mail Accounts and Users

This section describes how to manage accounts and users.

Adding e-mail accounts

You can add the following e-mail accounts:

- Standard e-mail account (POP3) - most home users have this type of account
- MSN/Hotmail account - MSN/Hotmail Web-based accounts

NOTE
If your computer runs Windows 2000 or Windows XP, and you plan to add multiple users to SpamKiller, you must add users before you can add e-mail accounts to their user profiles. For more information, see *Adding users* on page 108. If you add multiple users to SpamKiller, the account is added to the profile of the user who is currently logged on to SpamKiller.

To add an e-mail account:

1 Click the **Settings** tab to open the Settings page (Figure 5-12), and then click **E-mail Accounts**. The **E-mail Accounts** dialog box appears and displays all e-mail accounts added to SpamKiller.

> **NOTE**
> If multiple users were added to SpamKiller, the list displays the e-mail accounts of the user who is currently logged on to SpamKiller.

2 Click **Add**. The E-mail Accounts wizard appears.

Follow the instructions on the dialog boxes that appear.

If you add an MSN/Hotmail account, SpamKiller searches for an MSN/Hotmail address book to import into your Personal Friends List.

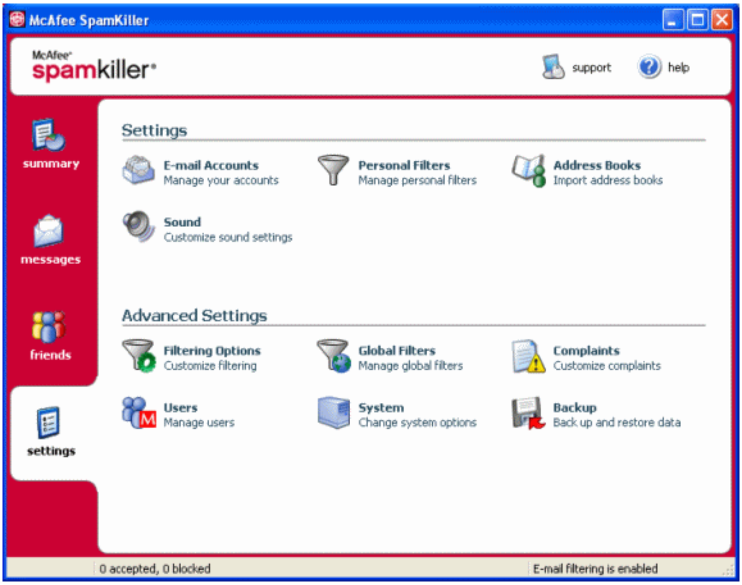


Figure 5-12. Settings page

Pointing your e-mail client to SpamKiller

If you add an account that SpamKiller does not detect (the account does not appear in the **Select Account** dialog box), or you want to read your MSN/Hotmail e-mail as a POP3 account in SpamKiller, point your e-mail client to SpamKiller by changing the incoming e-mail server.

For example, if your incoming e-mail server is “mail.mcafee.com”, change it to “localhost”.

Deleting e-mail accounts

Delete an e-mail account from SpamKiller if you no longer want SpamKiller to filter it.

Deleting an e-mail account from SpamKiller

1 Click the **Settings** tab, and then select **E-mail Accounts**. The **E-mail Accounts** dialog box appears and displays all e-mail accounts added to SpamKiller.

NOTE
If multiple users were added to SpamKiller, the list displays the e-mail accounts of the user who is currently logged on to SpamKiller.

2 Select an account, and then click **Delete**.

Editing e-mail account properties

You can edit information about an e-mail account you added to SpamKiller. For example, change the e-mail address, the account description, server information, how often SpamKiller checks the account for spam, and how your computer connects to the Internet.

POP3 accounts

Editing POP3 accounts

1 Click the **Settings** tab, and then click **E-mail Accounts**. The **E-mail Accounts** dialog box appears and displays all e-mail accounts added to SpamKiller.

NOTE
If multiple users were added to SpamKiller, the list displays the e-mail accounts of the user who is currently logged on to SpamKiller.

2 Select a POP3 account, and then click **Edit**.

3 Click the **General** tab to edit the account description and e-mail address.

- **Description** - description of the account. You can type any information in this box.
- **E-mail address** - e-mail address of the account.

4 Click the **Servers** tab to edit server information.

- **Incoming e-mail** - name of the server that receives incoming mail.
- **User name** - user name you use to access the account. Also known as Account Name.
- **Password** - password you use to access the account.
- **Outgoing e-mail** - name of the server that sends outgoing mail. Click **More** to edit authentication requirements for the outgoing server.

5 Click the **Checking** tab to edit how often SpamKiller checks the account for spam:

a Select **Check every** or **Check daily at**, and then type or select a time in the corresponding box. If you enter the number zero, SpamKiller only checks the account when it connects.

b Select additional times for SpamKiller to filter the account:

Check on startup - if you have a direct connection, and you want SpamKiller to check the account every time your computer starts.

Check when a connection is dialed - if you have a dial-up connection, and you want SpamKiller to check the account every time you connect to the Internet.

6 Click the **Connection** tab to specify how SpamKiller dials an Internet connection so that it can check your Inbox for new messages to filter.

- **Never dial a connection** - SpamKiller does not automatically dial a connection for you. You must first manually start your dial-up connection.
- **Dial when needed** - an Internet connection is not available, SpamKiller automatically attempts to connect using your default dial-up Internet connection.
- **Always dial** - SpamKiller automatically attempts to connect using the dial-up connection you specify.
- **Stay connected after filtering is done** - your computer stays connected to the Internet after filtering is finished.

7 Click the **Advanced** tab to edit advanced options.

- **Leave spam messages on the server** - if you want a copy of blocked messages to remain on your e-mail server. You can view mail from your e-mail client and the SpamKiller Blocked E-mail page. If the checkbox is not selected, you can only view blocked messages from the Blocked E-mail page.
- **POP3 port** - (POP3 port number) POP3 server handles incoming messages.
- **SMTP port** - (SMTP port number) SMTP server handles outgoing messages.
- **Server timeout** - length of time SpamKiller waits to receive e-mail before timing out and stopping.

  Increase the server time-out value if you have problems receiving mail. Your e-mail connection might be slow; therefore, increasing the server time-out value allows SpamKiller to wait longer before timing out.

8 Click **OK**.

MSN/Hotmail accounts

Editing MSN/Hotmail accounts

1 Click the **Settings** tab, and then click **E-mail Accounts**.

The **E-mail Accounts** dialog box appears and displays all e-mail accounts added to SpamKiller.

> **NOTE**
> If multiple users were added to SpamKiller, the list displays the e-mail accounts of the user who is currently logged on to SpamKiller.

2 Select an MSN/Hotmail account, and then click **Edit**.

3 Click the **General** tab to edit the account description and e-mail address.

- **Description** - description of the account. You can type any information in this box.
- **E-mail address** - e-mail address of the account.

4 Click the **Servers** tab to edit server information.

- **Incoming e-mail** - name of the server that receives incoming mail.
- **Password** - password you use to access the account.
- **Outgoing e-mail** - name of the server that sends outgoing mail.
- **Use an SMTP server for outgoing e-mail** - if you plan to send error messages and do not want to include the MSN signature line in the error message. The MSN signature line makes it easy for spammers to recognize that the error message is fake.

  Click **More** to change authentication requirements for the outgoing server.

5 Click the **Checking** tab to specify how often SpamKiller checks the account for spam:

a Select **Check every** or **Check daily at**, and then type or select a time in the corresponding box. If you enter the number zero, SpamKiller only checks the account when it connects.

b Select additional times for SpamKiller to filter the account:

Check on startup — Select this option if you have a direct connection, and you want SpamKiller to check the account every time SpamKiller starts.

Check when a connection is dialed — Select this option if you have a dial-up connection, and you want SpamKiller to check the account every time you connect to the Internet.

6 Click the **Connection** tab to specify how SpamKiller dials an Internet connection so that it can check your Inbox for new messages to filter.

- **Never dial a connection** - SpamKiller does not automatically dial a connection for you. You must first manually start your dial-up connection.
- **Dial when needed** - when an Internet connection is not available, SpamKiller automatically attempts to connect using your default dial-up Internet connection.
- **Always dial** - SpamKiller automatically attempts to connect using the dial-up connection you specify.
- **Stay connected after filtering is done** - your computer stays connected to the Internet after filtering is finished.

7 Click **OK**.

Configuring a Hotmail account to block spam in Outlook or Outlook Express

SpamKiller can filter Hotmail accounts directly. See the online help for details. However, you cannot block messages or add friends using the SpamKiller toolbar in Outlook or Outlook Express until you configure your Hotmail account.

1. Configure your Hotmail account in MSK.
2. If you have an existing Hotmail account in Outlook or Outlook Express, you must remove it first.
3. Add your Hotmail account to Outlook or Outlook Express. Ensure that you select **POP3** for the account type and incoming mail server type.
4. Name the incoming server as **`localhost`**.
5. Type the name of the available outgoing SMTP server (required).
6. Complete the account configuration process. You can now block new Hotmail spam e-mail or add a friend.

MAPI accounts

The following conditions are required for SpamKiller to successfully integrate with MAPI in Outlook:

- Only for Outlook 98, Outlook was initially installed with Corporate/Workgroup support.
- Only for Outlook 98, the first e-mail account is a MAPI account.
- The computer is logged on to the domain.

Editing MAPI accounts

1. Click the **Settings** tab, and then click **E-mail Accounts**. The **E-mail Accounts** dialog box appears and displays all e-mail accounts added to SpamKiller.

   NOTE
   If multiple users were added to SpamKiller, the list displays the e-mail accounts of the user who is currently logged on to SpamKiller.

2. Select a MAPI account, and then click **Edit**.

3. Click the **General** tab to edit the account description and e-mail address.

   - **Description** - description of the account. You can type any information in this box.

   - **E-mail address** - e-mail address of the account.

4. Click the **Profile** tab to edit profile information.

   - **Profile** - MAPI profile for the account.

   - **Password** - password that corresponds with the MAPI profile if you have set one up (not necessarily the e-mail account password).

5. Click the **Connection** tab to specify how SpamKiller dials an Internet connection so that it can check your Inbox for new messages to filter:

   - **Never dial a connection** - SpamKiller does not automatically dial a connection for you. You must first manually start your dial-up connection.

   - **Dial when needed** - when an Internet connection is not available, SpamKiller automatically attempts to connect using your default dial-up Internet connection.

   - **Always dial** - SpamKiller automatically attempts to connect using the dial-up connection you specify.

   - **Stay connected after filtering is done** - your computer stays connected to the Internet after filtering is finished.

6. Click **OK**.

Adding users

SpamKiller can set up multiple users, corresponding to the users set up on your Windows 2000 or Windows XP operating system.

When SpamKiller is installed on your computer, an administrator user profile is automatically created for the Windows user who was logged on. If you add e-mail accounts to SpamKiller during installation, the e-mail accounts are added to that administrator's user profile.

Before you add more e-mail accounts to SpamKiller, determine if you need to add more SpamKiller users. Adding users is beneficial if multiple people use your computer and have their own e-mail accounts. Each user's e-mail account is added to their user profile, allowing users to manage their e-mail accounts, personal settings, personal filters, and Personal Friends List.

User types define the tasks a user can perform in SpamKiller. The following table is a summary of permissions for each user type. Administrators can perform all tasks while limited users can only perform tasks according to their personal profiles. For example, administrators can view the whole content of blocked messages, while limited users can only view the subject line.

Tasks	Administrator	Limited User
Manage personal e-mail accounts, Personal Filters, Personal Friends List, and personal sound settings	X	X
Manage personal Blocked E-mail and Accepted E-mail pages	X	X
View message text of blocked messages	X	
View message text of accepted messages	X	X
Manage Global Filters and the Global Friends List	X	
Report spam to McAfee	X	X
Send complaints and error messages	X	X
Manage complaints and error messages (create, edit, and delete message templates)	X	
Manage users (create, edit, and remove users)	X	
Backup and restore SpamKiller	X	
View the Summary page of spam received	X	X

When a user logs on to your computer after being added, they are prompted to add an e-mail account to their user profile.

To add and manage users, the following is required:

- You must be logged on to SpamKiller as an administrator.

- You must have Windows 2000 or Windows XP on your computer.
- The users you are adding or managing must have Windows user accounts.

User passwords and protecting children from spam

Creating a user password enhances the privacy level. A user's personal settings, Friends List, and Accepted E-mail list cannot be accessed by another user without the log on password. Creating passwords is also beneficial in preventing children from accessing SpamKiller and viewing the content of spam messages.

Creating a password for an existing SpamKiller user

1. Click the **Settings** tab, and then click **Users**.
2. Select a user, and then click **Edit**.
3. Type a password in the **Password** box. When the user accesses SpamKiller, they must use the password to log on.

   IMPORTANT
   If you forget your password, you cannot retrieve it. Only a SpamKiller administrator user can create a new password for you.

Adding a user to SpamKiller

1. Click the **Settings** tab, and then click **Users**.
2. Click **Add**.

   A list of Windows users appears. To add a user who does not appear on the list, create a Windows user account for that person. Then, the new user must log on to your computer at least once. Afterwards, add the user to SpamKiller.

   NOTE
   Windows users with administrator rights have SpamKiller administrator rights.

3. Select a user to add, and then click **OK**. The user is added to SpamKiller, and the user name appears in the list of SpamKiller users.
4. Click **Close** when you are finished adding users.

To create a password for a user, see *Creating a password for an existing SpamKiller user* on page 109.

The next time the user logs on to your computer, they are prompted to add an e-mail account to their SpamKiller user profile. You can add e-mail accounts to the user profile if you are logged on to SpamKiller as the user and have the necessary e-mail account information. For details, see *Adding e-mail accounts* on page 101.

Editing SpamKiller user profile

1. Click the **Settings** tab, and then click **Users**. A list of SpamKiller users appears.
2. Select a user, and then click **Edit**.
3. Type a new name and password.

Deleting a SpamKiller user profile

WARNING
When you remove a user profile, you also remove the user's e-mail accounts from SpamKiller.

1. Click the **Settings** tab, and then click **Users**. A list of SpamKiller users appears.
2. Select a user from the list, and then click **Delete**.

Logging on to SpamKiller in a multi-user environment

When users log on to your computer and open SpamKiller, they are automatically logged on to SpamKiller under their user profiles. If SpamKiller passwords are assigned to users, they must type their passwords in the **Log On** dialog box that appears.

Switching between users

You must be logged on to SpamKiller as an administrator.

1. Click **Switch User** located at the top of the page. The **Switch User** dialog box appears.
2. Select a user, and then click **OK**. If the user has a password, the **Log On** dialog box appears. Type the user password in the **Password** box, and then click **OK**.

Using the Friends List

We recommend that you add your friends' names and e-mail addresses to a Friends List. SpamKiller does not block messages from those on the list; therefore, adding friends helps ensure that legitimate messages get through.

SpamKiller enables you to add names, e-mail addresses, domains, and mailing lists to the Friends Lists. You can add addresses one at a time, or all at once by importing an address book from your e-mail program.

SpamKiller maintains two types of lists:

- **Global Friends List** - affects all the e-mail accounts for the users in SpamKiller. If multiple users were added, you must be logged on to SpamKiller as an administrator in order to manage this list.
- **Personal Friends List** - affects all the e-mail accounts associated with a specific user. If multiple users were added, you must be logged on to SpamKiller as the user in order to manage this list.

You can add friends to a Friends List to ensure their e-mail is not blocked. The Friends page displays names and addresses that you added to the Friends List. The Friends page also shows the date you added a friend and the total number of messages received from that friend.

Click the **E-mail Addresses** tab to view e-mail addresses on the Friends List. Click the **Domains** tab to view domain addresses on the list. Click the **Mailing Lists** tab to view mailing lists in the Friends List.

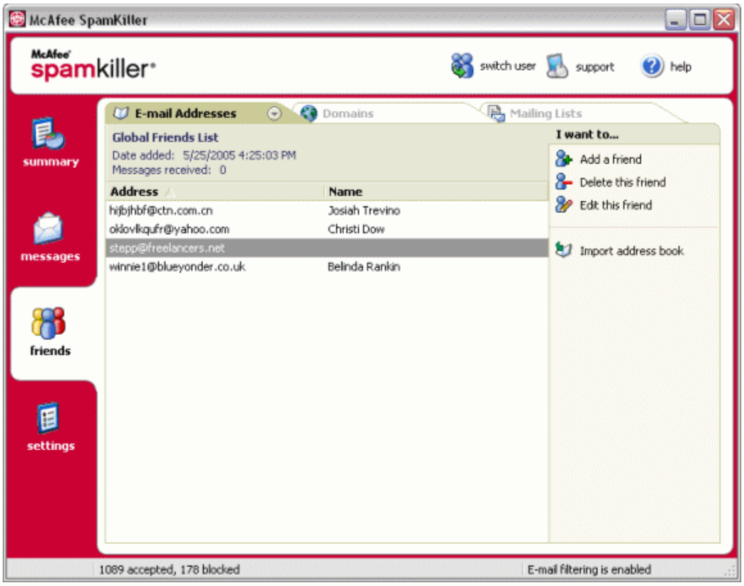
To switch between the Global Friends List and your Personal Friends List, click the down arrow ⌄ located on the **E-mail Address**, **Domains**, or **Mailing Lists** tab, and then select **Personal Friends List**.

Opening a Friends List

1 To open a Friends List, click the **Friends** tab. The Friends page appears (Figure 5-13).

2 Click the **E-mail Address**, **Domains**, or **Mailing List** tab. The Global Friends List appears. To view your Personal Friends List, click the down arrow ⊙ on one of the tabs, and then select **Personal Friends List**.

NOTE
If your computer runs Windows 2000 or Windows XP, and multiple users were added to SpamKiller, limited users can only view their Personal Friends List.



Global Friends List
Date added: 5/25/2005 4:25:03 PM
Messages received: 0

Address	Name
hijbjhbf@ctn.com.cn	Josiah Trevino
oklovlkqufr@yahoo.com	Christi Dow
stepp@freelancers.net	
winnie1@blueyonder.co.uk	Belinda Rankin

1089 accepted, 178 blocked
E-mail filtering is enabled

Figure 5-13. Friends page

Importing address books

Import address books into a Friends List manually or by automatic import. Automatic import enables SpamKiller to check your address books regularly for new addresses and automatically import them into a Friends List.

You can import address books from the following e-mail programs:

- Microsoft Outlook (version 98 and later)
- Microsoft Outlook Express (all versions)

- Netscape Communicator (version 6 and earlier versions if exported as an LDIF file)
- Qualcomm Eudora (version 5 and later)
- IncrediMail Xe
- MSN/Hotmail
- Any program that can export its address book as a plain text file

Importing an address book by automatic import

You can update your Personal Friends List regularly by creating a schedule for importing addresses from address books.

1. Click the **Settings** tab, and then click **Address Books**. The **Import Address Books** dialog box appears, which shows a list of address books that SpamKiller checks regularly and imports new addresses from.
2. Click **Add**. The **Import Schedule** dialog box appears.
3. Select the **Type** of address book to import and the address book **Source**.
4. From the **Schedule** box, select how often SpamKiller must check the address book for new addresses.
5. Click **OK**. After an update, new addresses appear in your Personal Friends List.

Importing an address book manually

You can manually import address books into your Personal Friends List or the Global Friends List.

> **NOTE**
> If your computer runs Windows 2000 or Windows XP, and multiple users were added to SpamKiller, you must be logged on as an administrator to add friends to the Global Friends List.

1. Click the **Friends** tab, and then click **Import Address Book**.

   The **Import Address Book** dialog box appears, showing a list of address book types that you can import.

2. Select a type of address book to import, or click **Browse** to import addresses stored in a file.

   To import the address book into your Personal Friends List only, ensure that the **Add to Personal Friends List** checkbox is selected. To import the address book into the Global Friends List only, ensure that the checkbox is not selected.

3 Click **Next**. A confirmation page lists the number of addresses that SpamKiller added.

4 Click **Finish**. The addresses appear in the Global Friends List or your Personal Friends List.

Editing address book information

Edit information for an address book that was imported automatically.

1 Click the **Settings** tab, and then click **Address Books**.

2 Select an address book, and then click **Edit**.

3 Edit address book information, and then click **OK**.

Deleting an address book from the automatic import list

Remove an address book entry when you no longer want SpamKiller to automatically import addresses from that book.

1 Click the **Settings** tab, and then click **Address Books**.

2 Select an address book, and then click **Delete**. A confirmation dialog box appears.

3 Click **Yes** to remove the address book from the list.

Adding friends

To ensure that you receive all e-mail from friends, add your friends' names and addresses to a Friends List. You can add friends from the Friends page, the Blocked E-mail page, the Accepted E-mail page, and from Microsoft Outlook or Outlook Express.

> **NOTE**
> If your computer runs Windows 2000 or Windows XP, and multiple users were added to SpamKiller, you must be logged on as an administrator to add friends to the Global Friends List.

Adding friends from the Blocked E-mail or Accepted E-mail page

1. Click the **Messages** tab, and then click the **Blocked E-mail** or **Accepted E-mail** tab.

   Or

   From the SpamKiller menu in Microsoft Outlook or Outlook Express, select **View Blocked Messages** to open the Blocked E-mail page for that account.

   The Blocked E-mail or Accepted E-mail page appears.

2. Select a message from a sender that you want to add to a Friends List, and then click **Add a Friend**.

3. In the **Address** box, type the address to add to the Friends List. The **Address** box might already contain the address from the selected message.

4. Type the name of the friend in the **Name** box.

5. Select the address type you want to add from the **Friend type** box:

   - **Single e-mail address** - the sender's e-mail address is added to the Domains section in the Friends List.

   - **Everyone at a domain** - the domain name is added to **Domains** section in the Friends List. SpamKiller accepts all e-mail coming from the domain.

   - **Mailing list** - the address is added to the **Mailing List** section in the Friends List.

   To add the address to your Personal Friends List only, ensure that the **Add to Personal Friends List** checkbox is selected. To add the address to the Global Friends List only, ensure that the checkbox is not selected.

6. Click **OK**. All messages from that friend are marked as being messages from a friend and appear in the Accepted E-Mail page.

Adding friends from the Friends page

1. Click the **Friends** tab, and then click **Add a Friend**. The **Friend Properties** dialog box appears.

2. In the **Address** box, type the address to add to the Friends List.

3. Type the name of your friend in the **Name** box.

4. Select the address type you want to add from the **Friend type** box:

   - **Single e-mail address** - the sender's e-mail address is added to the Domains section in the Friends List.

   - **Everyone at a domain** - the domain name is added to **Domains** section in the Friends List. SpamKiller accepts all e-mail coming from the domain.

   - **Mailing list** - the address is added to the **Mailing List** section in the Friends List.

   To add the address to your Personal Friends List only, ensure that the **Add to Personal Friends List** checkbox is selected. To add the address to the Global Friends List only, ensure that the checkbox is not selected.

5. Click **OK**. All messages from that friend are marked as being messages from a friend and appear in the Accepted E-Mail page.

Adding friends from Microsoft Outlook

1. Open your e-mail account in Microsoft Outlook or Outlook Express.

2. Select a message from a sender that you want to add to a Friends List.

3. Click 👤 in the Microsoft Outlook toolbar. All messages from that friend are marked as being messages from a friend and appear in the Accepted E-Mail page.

Editing friends

1. Click the **Friends** tab, and then click the **E-mail Addresses**, **Domains**, or **Mailing Lists** tab.

   The Global Friends List appears. To view your Personal Friends List, click the down arrow ⌄ on one of the tabs, and then select **Personal Friends List**.

   > **NOTE**
   > If your computer runs Windows 2000 or Windows XP, and multiple users were added to SpamKiller, only administrators can access the Global Friends List.

2. Select an address from the list, and then click **Edit**.

3 Edit the appropriate information, and then click **OK**.

Deleting friends

Remove addresses you no longer want in a Friends List.

1 Click the **Friends** tab, and then click the **E-mail Addresses**, **Domains**, or **Mailing Lists** tab.

The Global Friends List appears. To view your Personal Friends List, click the down arrow ⌄ on one of the tabs, and then select **Personal Friends List**.

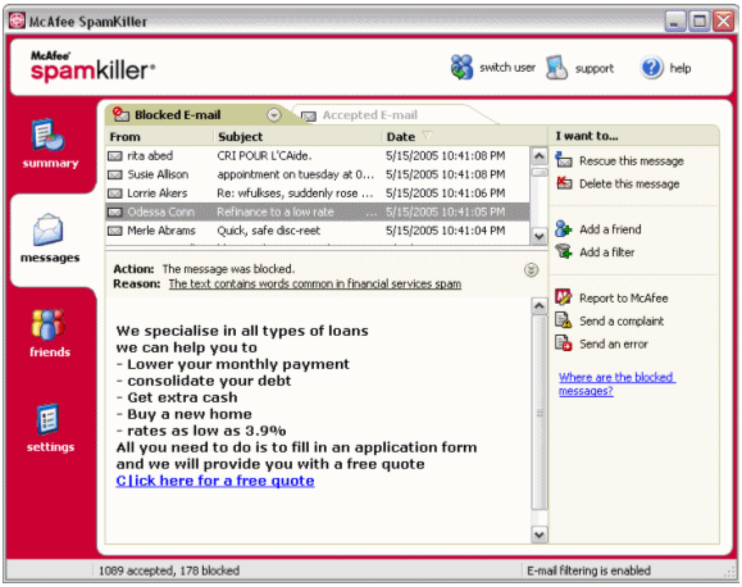
> **NOTE**
> If your computer runs Windows 2000 or Windows XP, and multiple users were added to SpamKiller, only administrators can access the Global Friends List.

2 Select an address from the list, and then click **Delete a friend**. A confirmation dialog box appears.

3 Click **Yes** to delete the friend.

Working With Blocked and Accepted Messages

Click the **Messages** tab to open the Messages page (Figure 5-14) and access your blocked and accepted messages. The Blocked E-mail and Accepted E-mail pages have similar features.



From	Subject	Date
rita abed	CRI POUR L'CAide.	5/15/2005 10:41:08 PM
Susie Allison	appointment on tuesday at 0...	5/15/2005 10:41:08 PM
Lorrie Akers	Re: wfulkses, suddenly rose ...	5/15/2005 10:41:06 PM
Odessa Conn	Refinance to a low rate ...	5/15/2005 10:41:05 PM
Merle Abrams	Quick, safe disc-reet	5/15/2005 10:41:04 PM

Action: The message was blocked.
Reason: The text contains words common in financial services spam

We specialise in all types of loans
we can help you to
- Lower your monthly payment
- consolidate your debt
- Get extra cash
- Buy a new home
- rates as low as 3.9%
All you need to do is to fill in an application form
and we will provide you with a free quote
Click here for a free quote

1089 accepted, 178 blocked
E-mail filtering is enabled

Figure 5-14. Messages page

Blocked E-mail page

Click the **Blocked E-mail** tab in the Messages page to view blocked messages.

NOTE
You can also access blocked messages in Microsoft Outlook by selecting the SpamKiller menu, and then clicking **View Blocked Messages**.

Blocked messages are messages that SpamKiller identified as spam, removed from your Inbox, and placed in the Blocked E-mail page.

The Blocked E-mail page displays all spam messages that were removed from your e-mail accounts. To view blocked e-mail for a specific account, click the down arrow ⊙ located on the **Blocked E-mail** tab, and then select the account to view.

The top message pane lists spam messages and are sorted by date. The most recent message appears first. The bottom preview pane contains the message text for the selected message.

> **NOTE**
> If your computer runs Windows 2000 or Windows XP, multiple users have been added to SpamKiller, and you are logged on to SpamKiller as a limited user, the message contents do not appear in the bottom preview pane.

The middle pane shows message details. Click the down arrows to expand the message details pane and view the message text and headers in native format, including any HTML formatting tags. The message details pane shows the following.

- **Action** - how SpamKiller processed the spam message. Action is associated with the action of the filter that blocked the message.
- **Reason** - why SpamKiller blocked the message. You can click the reason to open the filter editor and view the filter. The filter editor displays what the filter looks for in a message, and the action that SpamKiller takes against messages found by the filter.
- **From** - the sender of the message.
- **Date** - the date the message was sent to you.
- **To** - to whom the message was sent.
- **Subject** - the topic that appears in the message subject line.

The left column contains icons next to messages if manual complaints or error messages have been sent.

- Complaint sent - a complaint was sent about the message.
- Error message sent - an error message was sent to the reply address in the spam message.
- Complaint and error messages sent - both a complaint and error message were sent.

For more information on where blocked messages are, see *Where are the blocked messages* on page 123.

Accepted E-mail page

Click the **Accepted E-mail** tab in the Messages page to view accepted messages.

The Accepted E-mail page displays all Inbox messages in all of your e-mail accounts. However, for MAPI accounts, the Accepted E-mail page does not contain internal e-mail. To view accepted e-mail for a specific account, click the down arrow ⌄ on the **Accepted E-mail** tab, and then select an account to view.

> **NOTE**
> SpamKiller is designed to accept legitimate e-mail. However, if legitimate e-mail appears in the Blocked E-mail list, you can move the messages back to your Inbox (and the Accepted E-mail list) by selecting the messages, and then clicking **Rescue this message**.

Like the Blocked E-mail page, the top message pane lists messages that are sorted by date. The bottom preview pane contains the message text of the selected message.

The middle pane explains if a message was sent by someone on a Friends List, or if the message fits the criteria of a filter, but the filter action was set to either **Accept** or **Mark as Possible Spam**. Click the down arrows ⌄ to expand the message details pane, view the message text and headers in native format, including any HTML formatting tags.

The message details pane shows the following.

- **Action** - how SpamKiller processed the message.
- **Reason** - if a message was flagged, explains why SpamKiller flagged the message.
- **From** - the sender of the message.
- **Date** - the date the message was sent to you.
- **To** - to whom the message was sent.
- **Subject** - the topic that appears in the message subject line.

One of the following icons appears next to a message.

- E-mail from a friend ✉ - SpamKiller detected that the sender of the message is on a Friends List. This message is one you want to keep.
- Possible spam ✉ - the message matches a filter with an action set to Mark as possible spam.
- Complaint sent ✉ - a complaint was sent about the message.
- Error message sent ✉ - an error message was sent to the reply address on the spam message.

- Complaint and error messages sent - both a complaint and error message were sent.

Tasks for Blocked E-mail and Accepted E-mail

The right panel on the Blocked E-mail and Accepted E-mail pages lists tasks you can perform.

- **Block this message** - remove a message from your Inbox and put it in the SpamKiller Blocked E-mail page. (This option appears on the Accepted E-mail page only.)
- **Rescue this message** - put a message back in your Inbox (this option appears on the Blocked E-mail page only) and open the **Rescue Options** dialog box. You can automatically add the sender to your Friends list and rescue all messages from the sender.
- **Delete this message** - remove a selected message.
- **Add a friend** - add the sender's name, e-mail address, domain, or a mailing list to a Friends List.
- **Add a filter** - create a filter.
- **Report to McAfee** - inform McAfee of specific spam messages you receive.
- **Send a complaint** - send a complaint about spam to the administrator of the sender's domain or to another e-mail address you type.
- **Send an error** - send an error message to the reply address of a spam message.

Rescuing messages

If the Blocked E-mail page or the SpamKiller folder in Microsoft Outlook and Outlook Express contains legitimate mail, you can put those messages back in your Inbox.

From the Blocked E-Mail page

1 Click the **Messages** tab, and then click the **Blocked E-mail** tab.

Or

From the SpamKiller menu in Microsoft Outlook or Outlook Express, select **View Blocked Messages** to open the Blocked E-mail page for that account.

2 Select a message and click **Rescue this message** ✉. The **Rescue Options** dialog box appears.

- **Add Friend** - add the sender to your Friends list.
- **Rescue all from same sender** - rescue all blocked messages from the sender of the selected message.

3 Click **OK**. The message is put back in your Inbox and the Accepted E-mail page.

From the SpamKiller folder in Microsoft Outlook or Outlook Express

Select the message(s) and click **Rescue Selection** from the SpamKiller menu or toolbar. Your selection is put back in the Inbox and the message tag ([SPAM] by default) is removed.

Blocking messages

Block spam messages that are currently in your Inbox. When you block a message, SpamKiller automatically creates a filter to remove that message from your Inbox. You can block Inbox messages from the Accepted E-mail page, or from Microsoft Outlook or Outlook Express.

From the Accepted E-mail page

1 Click the **Messages** tab, and then click the **Accepted E-mail** tab. The Accepted E-mail page appears and displays messages that are currently in your Inbox.

2 Select a message, and then click **Block this message**. The message is removed from your Inbox and the Accepted E-mail page, and copy of the message appears in the Blocked E-mail page.

From Microsoft Outlook

In Microsoft Outlook, messages from members of an Exchange server are considered safe and are not filtered by SpamKiller. Only messages from external sources are filtered.

1 Open your Microsoft Outlook or Outlook Express Inbox.

2 Select a message, and then click ✉. A copy of the message is put in the Blocked E-mail page.

Where are the blocked messages

By default, spam messages are tagged as [SPAM] and placed in the SpamKiller folder in Outlook and Outlook Express, or your Inbox. Tagged messages also appear on the Accepted E-mail page.

Deleting a message manually

1 Click the **Messages** tab, and then click the **Blocked E-mail** tab.

Or

From the SpamKiller menu in Microsoft Outlook or Outlook Express, select **View Blocked Messages** to open the Blocked E-mail page for that account.

2 Select a message to delete.

3 Click **Delete this message**. A confirmation dialog box appears.

4 Click **Yes** to delete the message.

Modifying how spam messages are processed

When spam is found, the message is tagged or blocked. Spam messages are removed from your server every time SpamKiller connects to it.

Tagging

The e-mail subject line is tagged with [SPAM] and the message goes in your Inbox or SpamKiller folder, if you have Microsoft Outlook or Outlook Express.

Blocking

The message is removed and placed in the SpamKiller Blocked E-mail page. If legitimate mail is blocked, you can rescue the message (see Rescuing messages).

SpamKiller automatically removes blocked messages from the Blocked E-mail page after 15 days. You can change how often blocked messages are removed.

SpamKiller does not automatically remove messages from the Accepted E-mail page since this page reflects the messages currently in your Inbox.

Modifying how SpamKiller processes spam messages

1. Click the **Settings** tab, and then click the **Filtering Options** icon.
2. Click the **Processing** tab.
    - **Put spam in Blocked E-mail box** - spam messages are removed from your Inbox and put in the SpamKiller Blocked E-mail page.
    - **Tag spam and keep in Inbox** - this is the default setting. Spam messages remain in your Inbox, but the subject line of the message includes [SPAM].

      Keep blocked e-mail for ____ days - blocked messages remain in the Blocked E-mail page for the duration you specify.

      Keep accepted e-mail for ____ days - accepted messages remain in the Accepted E-mail page for the duration you specify.
3. Click **OK**.

Using the AntiPhishing filter

Unsolicited e-mail is categorized as spam (e-mails soliciting you to purchase), or phishing (e-mails soliciting you to provide personal information to a known or potential scam Web site).

The McAfee AntiPhishing filter helps protect you from Web sites that are blacklisted (confirmed phishing or related scam Web sites), or graylisted (contain some dangerous content or links to blacklisted Web sites).

If you browse to a known or potential scam Web site, you are redirected to the McAfee AntiPhishing Filter page.

To change AntiPhishing settings, follow these steps.

1. Open Internet Explorer.
2. In the **Tools** menu, select **McAfee AntiPhishing Filter**.

- **Enable Web site filtering** - enabled by default. To disable AntiPhishing filtering, clear this checkbox.
- **Allow access to blacklisted Web sites** - places a link on the redirection page for blacklisted sites. Clicking this link takes you to the Web site.

- **Allow access to graylisted Web sites** - places a link on the redirection page for graylisted sites. Clicking this link takes you to the Web site.

3 When you are finished, click **OK**.

Adding friends to a Friends List

See *Adding friends from the Blocked E-mail or Accepted E-mail page* on page 115.

Adding filters

For more information on filters, see *Working With Filters* in the online Help.

1 To create a Global Filter, click the **Settings** tab, select **Global Filters**, and click **Add**.

Or

To create a Personal Filter, click the **Settings** tab, select **Personal Filters**, and click **Add**.

Or

Click the **Messages** tab, click the **Blocked E-mail** or **Accepted E-mail** tab, and click **Add a Filter**.

2 Click **Add** to begin creating a filter condition. The **Filter Condition** dialog box appears.

3 Create a filter condition by following these steps.

A filter condition is a statement that tells SpamKiller what to look for in a message. In the example “The message text contains mortgage,” the filter searches for messages containing the word “mortgage.” For more information, see *Filter Conditions* in the Online Help.

a Select a condition type from the first box.

b Select or type values in the subsequent boxes.

c If the following options appear, select them to further define the filter condition.

Also look in formatting codes - this option appears only if the filter condition is defined to search the message text. If you select this checkbox, SpamKiller searches both the message text and the message formatting codes for the text you indicated.

Match variations - allows SpamKiller to detect common deliberate misspellings used by spammers. For example, the word “common” might be misspelled as “c0mm0n” to evade filters.

Regular Expressions (RegEx) - allows you to specify character patterns used in filter conditions. To test a character pattern, click **Test RegEx**.

Case-sensitive - this option only appears for conditions in which you typed a condition value. If you select this checkbox, SpamKiller distinguishes between upper-case and lower-case letters in the value you typed.

d Click **OK**.

4 Create another filter condition as follows, or go to Step 5 to select a filter action.

a Click **Add**, and then create the filter condition. Click **OK** when you are finished creating the filter condition.

Both filter conditions appear in the Filter Conditions list and are joined by **and**. The **and** indicates that SpamKiller looks for messages that match *both* filter conditions. If you want SpamKiller to look for messages that match either one of the conditions, change **and** to **or** by clicking **and**, and then selecting **or** from the box that appears.

b Click **Add** to create another condition, or go to Step 5 to select a filter action.

If you created a total of three or more filter conditions, you can group filter conditions to create clauses. For examples of grouping, see *Grouping Filters* in the online Help.

To group filter conditions, select a filter condition, and click **Group**. To ungroup filter conditions, select a grouped condition, and click **Ungroup**.

5 Select a filter action from the **Action** box. The filter action tells SpamKiller how to process messages found by that filter. For more information, see *Filter Actions* in the online Help.

6 Click **Advanced** to select advanced filter options (selecting advanced options is not required). For more information, see *Advanced Filter Options* in the online Help.

7 Click **OK** when you are finished creating the filter.

NOTE
To edit a condition, select it and click **Edit**. To delete a condition, select it and click **Delete**.

Regular expressions

Regular expressions are only available for the following filter conditions: **The subject**, **The message text**, **At least one of the following phrases**.

These special characters and sequences can be used as regular expressions when defining filter conditions. For example:

- The regular expression **[0-9]*\.[0-9]+** matches floating point numbers given non engineering notation. The regular expression matches: “12.12”, “.1212”, and “12.0”, but not “12” and “12”.
- The regular expression **\D*[0-9]+\D*** matches all words with numbers: “SpamKi11er” and V1AGRA” but not “SpamKiller” and “VIAGRA”.

\

Marks the next character as either a special character or a literal. For example, “n““ matches the character “n“. “\n“ matches a new line character. The sequence “\\“ matches “\“ and “\(“ matches “(“.

^

Matches the beginning of input.

$

Matches the end of input.

*

Matches the preceding character zero or more times. For example, “zo*“ matches either “z“ or “zoo“.

+

Matches the preceding character one or more times. For example, “zo+“ matches “zoo“ but not “z“.

?

Matches the preceding character zero or one time. For example, “a?ve?“ matches the “ve“ in “never“.

.

Matches any single character except a new line character.

(pattern)

Matches pattern and remembers the match. The matched substring can be retrieved from the resulting Matches collection, using Item [0]...[n]. To match parentheses characters ( ), use “\(“ or “\)“.

x|y

Matches either x or y. For example, “z | wood“ matches “z“ or “wood“. “(z | w)oo“ matches “zoo“ or “wood“.

{n}

The n is a non negative integer. Matches exactly n times. For example, “o{2}“ does not match the “o“ in “Bob,“ but matches the first two o's in “foooood“.

{n,}

The n is a non negative integer. Matches at least n times. For example, “o{2,}“ does not match the “o“ in “Bob“ and matches all the o's in “foooood.“ “o{1,}“ is equivalent to “o+“. “o{0,}“ is equivalent to “o*“.

{n,m}

The m and n are non negative integers. Matches at least n and at most m times. For example, “o{1,3}“ matches the first three o's in “fooooood.“ “o{0,1}“ is equivalent to “o?“.

[xyz]

A character set. Matches any one of the enclosed characters. For example, “[abc]“ matches the “a“ in “plain“.

[^xyz]

A negative character set. Matches any character not enclosed. For example, “[^abc]“ matches the “p“ in “plain“.

[a-z]

A range of characters. Matches any character in the specified range. For example, “[a-z]“ matches any lowercase alphabetic character in the range “a“ through “z“.

[^m-z]

A negative range characters. Matches any character not in the specified range. For example, “[m-z]“ matches any character not in the range “m“ through “z“.

\b

Matches a word boundary, that is, the position between a word and a space. For example, “er\b“ matches the “er“ in “never“ but not the “er“ in “verb“.

\B

Matches a non-word boundary. “ea*r\B“ matches the “ear“ in “never early“.

\d

Matches a digit character. Equivalent to [0-9].

\D

Matches a non-digit character. Equivalent to [^0-9].

\f

Matches a form-feed character.

\n

Matches a new line character.

\r

Matches a carriage return character.

\s

Matches any white space including space, tab, form-feed, etc. Equivalent to “[\f\n\r\t\v]“.

\S

Matches any nonwhite space character. Equivalent to “[^ \f\n\r\t\v]“.

\t

Matches a tab character.

\v

Matches a vertical tab character.

\w

Matches any word character including underscore. Equivalent to “[A-Za-z0-9_]“.

\W

Matches any non-word character. Equivalent to “[^A-Za-z0-9_]“.

\num

Matches num, where num is a positive integer. A reference back to remembered matches. For example, “(.)\1“ matches two consecutive identical characters.

\n

Matches n, where n is an octal escape value. Octal escape values must be 1, 2, or 3 digits long. For example, “\11“ and “\011“ both match a tab character. “\0011“ is the equivalent of “\001“ & “1“. Octal escape values must not exceed 256. If they do, only the first two digits comprise the expression. Allows ASCII codes to be used in regular expressions.

\xn

Matches n, where n is a hexadecimal escape value. Hexadecimal escape values must be exactly two digits long. For example, “\x41“ matches “A“. “\x041“ is equivalent to “\x04“ & “1“. Allows ASCII codes to be used in regular expressions.”

Reporting spam to McAfee

You can report spam to McAfee, where they analyze it to create filter updates.

1. Click the **Messages** tab, and then click the **Blocked E-mail** or **Accepted Mail** tab. The Blocked E-mail or Accepted E-mail page appears.
2. Select a message, and then click **Report to McAfee**. A confirmation dialog box appears.
3. Click **Yes**. The message is automatically sent to McAfee.

Sending complaints manually

Send a complaint to prevent a sender from sending you more spam. For more information on sending complaints, see *Sending Complaints and Error Messages* in the online Help.

1. Click the **Messages** tab, and then click the **Blocked E-mail** or **Accepted E-mail** tab. A list of messages appears.
2. Select a message to complain about, and then click **Send a complaint**. The **Send Complaint** dialog box appears.
3. Select whom you want to send the complaint to.

   WARNING
   In most cases you should not select **Sender**. Sending a complaint to the sender of the spam validates your e-mail address, which can increase the number of spam you receive from that sender.

4. Click **Next**, and then follow the instructions on the dialog boxes that appear.

Sending error messages

For more information on sending error messages, see *Sending Complaints and Error Messages* in the online Help.

Send an error message to prevent a sender from sending you more spam.

Sending an error message manually

1 Click the **Messages** tab, and then click the **Blocked E-mail** or **Accepted E-mail** tab. A list of messages appears.

2 To send an error message about a specific spam message, select the message, and then click **Send error**. An error message is sent to the reply address in the spam message.

Index

A

Accepted E-mail
- adding to a Friends List, 125
- icons in the accepted messages list, 120
- sending error messages, 130
- tasks, 121
- working with accepted messages, 118

Accepted E-mail page, 120

ActiveShield
- cleaning a virus, 29
- default scan setting, 21, 23 to 28
- disabling, 20
- enabling, 19
- scan options, 20
- scanning all file types, 25
- scanning all files, 25
- scanning e-mail and attachments, 21
- scanning for new unknown viruses, 26
- scanning for Potentially Unwanted Programs (PUPs), 28
- scanning for scripts, 27
- scanning for worms, 23
- scanning inbound instant message attachments, 25
- scanning program files and documents only, 26
- starting, 21
- stopping, 21
- testing, 17

adding an e-mail address to a Friends List, 115

adding e-mail accounts, 101

adding filters, 125

adding users, 81
- content blocking, 82
- cookie blocking, 82
- Internet time limits, 82

administrator, 79, 108 to 109
- retrieving password, 80

alerts
- Application Has Been Modified, 70
- Application Requests Internet Access, 70
- Application Requests Server Access, 70
- Connection Attempt Blocked, 77
- for infected e-mail, 30
- for infected files, 29
- for potential worms, 30
- for PUPs, 31
- for suspicious scripts, 30
- for viruses, 29
- Internet Application Blocked, 70
- New Application Allowed, 75

AntiPhishing filter, using, 124

AVERT, submitting suspicious files to, 39

B

Blocked E-mail
- adding to a Friends List, 125
- icons in the blocked messages list, 119
- modifying how spam messages are processed, 123
- rescuing messages, 122
- sending error messages, 130
- tasks, 121
- where are the blocked messages, 123
- working with blocked messages, 118

Blocked E-mail page, 118

blocking messages, 122

C

configuring
- VirusScan
  - ActiveShield, 19
  - Scan, 32

creating a Rescue Disk, 40

D

default firewall, setting the, 49

E

editing users, 83
  age group, 85
  cookie blocking, 84
  Internet time limits, 85
  password, 83
  removing users, 86
  startup user, 86
  user information, 84
editing whitelists, 31
e-mail accounts, 101
  adding, 101
  deleting, 102
  editing, 103
  editing MAPI accounts, 106
  editing MSN/Hotmail accounts, 105
  editing POP3 accounts, 103
  pointing your e-mail client to SpamKiller, 102
e-mail and attachments
  auto-cleaning
    enabling, 21
  scanning
    disabling, 22
    enabling, 21
    errors, 22
Event Log
  about, 59
  managing, 68
  viewing, 68
event log, 89
events
  about, 59
  archiving the Event Log, 68
  clearing the Event Log, 68
  copying, 69
  deleting, 69
  exporting, 69
  from 0.0.0.0, 60
  from 127.0.0.1, 60
  from computers on your LAN, 61
  from private IP addresses, 61
  HackerWatch.org advice, 64
  loopback, 60
  more information, 64
  reporting, 65
  responding to, 64
  showing
    all, 62
    from one address, 63
    one day's, 63
    this week's, 62
    today's, 62
    with same event info, 64
  tracing
    understanding, 59
    viewing archived Event Logs, 68

F

features, 79, 97
filtering
  disabling, 99
  enabling, 99
filters, adding, 125
Friends List, 111
  adding an e-mail address, 115
  adding friends from the Blocked E-mail or Accepted E-mail page, 115
  importing an address book, 112
Friends page, 112

H

HackerWatch.org
  advice, 64
  reporting an event to, 65
  signing up, 65
Help icon, 98

I

importing an address book into a Friends List, 112
inbound instant message attachments
  auto-cleaning, 25
  scanning, 25
Internet applications

about, 57
allowing and blocking, 58
changing application rules, 58

IP addresses
about, 60
banning, 66
trusting, 65

L

list of detected files (Scan), 34, 37

logging on to SpamKiller in a multi-user environment, 110

M

McAfee Privacy Service, 81
disabling, 81
opening, 81
signing in, 81
updating, 81

McAfee SecurityCenter, 13

Messages page, 118

Microsoft Outlook, 35

N

new features, 15, 47

O

options, 86
allowing cookies, 89
allowing web sites, 86
backup, 92
blocking advertisements, 88
blocking information, 87
blocking web sites, 86
web bugs, 88

P

passwords, 109

Personal Firewall
testing, 52

pointing your e-mail client to SpamKiller, 102

Potentially Unwanted Programs (PUPs), 28
alerts, 31
cleaning, 37
deleting, 38
detecting, 37
quarantining, 37
removing, 31
trusting, 31

protecting children, 109

Q

Quarantine
adding suspicious files, 38
cleaning files, 38 to 39
deleting files, 38
deleting suspicious files, 39
managing suspicious files, 38
restoring cleaned files, 38 to 39
submitting suspicious files, 39

Quick Start Card, iii

R

regular expressions, 127

reporting an event, 65

reporting spam to McAfee, 130

Rescue Disk
creating, 40
updating, 41
using, 38, 41
write-protecting, 41

rescuing messages, 122

S

Scan
automatic scanning, 35
cleaning a virus or Potentially Unwanted Program, 37
deleting a virus or Potentially Unwanted Program, 38
manual scanning, 32
manual scanning via Microsoft Outlook toolbar, 35
manual scanning via Windows Explorer, 35
quarantining a virus or Potentially Unwanted Program, 37
Scan all files option, 33

Scan for new unknown viruses option, 33
Scan for Potentially Unwanted Programs option, 34
Scan subfolders option, 32
Scan within compressed files option, 33
testing, 17 to 18
Scan all files option (Scan), 33
Scan for new unknown viruses option (Scan), 33
Scan for Potentially Unwanted Programs option (Scan), 34
scan options
ActiveShield, 20, 25 to 26
Scan, 32
Scan subfolders option (Scan), 32
Scan within compressed files option (Scan), 33
scanning
all files, 25, 33
compressed files, 33
for new unknown viruses, 33
for Potentially Unwanted Programs (PUPs), 28
for scripts, 27
for worms, 23
program files and documents only, 26
scheduling automatic scans, 35
subfolders, 32
via Microsoft Outlook toolbar, 35
via Windows Explorer, 35
scheduling scans, 35
scripts
alerts, 30
allowing, 30
stopping, 30
ScriptStopper, 27
Settings page, 101
setup assistant, 80
showing events in the Event Log, 62
Shredder, 90
SpamKiller
Accepted E-mail page, 120
Blocked E-mail page, 118
disabling filtering, 99
enabling filtering, 99
Startup user, 80, 82
submitting suspicious files to AVERT, 39
Summary Page, 52
Summary page, 100
Support icon, 98
Switch User icon, 98
switching users, 110

T

tasks for blocked and accepted messages, 121
technical support, 38
testing Personal Firewall, 52
testing VirusScan, 17
tracing an event, 64
Trojans
alerts, 29
detecting, 37
Trusted PUPs List, 31

U

uninstalling
other firewalls, 49
Update Wizard, 21
updating
a Rescue Disk, 41
VirusScan
automatically, 44
manually, 44
user options, 93
accepting cookies, 94
changing your password, 93
changing your user name, 93
clearing your cache, 94
rejecting cookies, 95
users, 101
adding users, 108
creating passwords, 109
deleting user profiles, 110
editing user profiles, 110
logging on to SpamKiller, 110
switching users, 110
user types, 108
using a Rescue Disk, 41
utilities, 90

V

viruses
- alerts, 29
- allowing suspicious scripts, 30
- cleaning, 29, 37
- deleting, 29, 37
- deleting infected files, 29
- detecting, 37
- detecting with ActiveShield, 29
- quarantining, 29, 37
- quarantining infected files, 29
- removing PUPs, 31
- reporting automatically, 41, 43
- stopping potential worms, 30
- stopping suspicious scripts, 30

VirusScan
- reporting viruses automatically, 41, 43
- scanning via Microsoft Outlook toolbar, 35
- scanning via Windows Explorer, 35
- scheduling scans, 35
- testing, 17
- updating automatically, 44
- updating manually, 44

W

whitelisted programs, 31

whitelisting
- PUPs, 31

Windows Automatic Updates, 70

Windows Explorer, 35

Windows Firewall, 49

World Virus Map
- reporting, 41
- viewing, 43

worms
- alerts, 29 to 30
- detecting, 29, 37
- stopping, 30

WormStopper, 23

write-protecting a Rescue Disk, 41