

McAfee®

wireless home network security suite

User Guide

McAfee®

COPYRIGHT

Copyright © 2005 McAfee, Inc. All Rights Reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the written permission of McAfee, Inc., or its suppliers or affiliate companies.

TRADEMARK ATTRIBUTIONS

ACTIVE FIREWALL, ACTIVE SECURITY, ACTIVESECURITY (AND IN KATAKANA), ACTIVESHIELD, ANTIVIRUS ANYWARE AND DESIGN, CLEAN-UP, DESIGN (STYLIZED E), DESIGN (STYLIZED N), ENTERCEPT, ENTERPRISE SECURECAST, ENTERPRISE SECURECAST (AND IN KATAKANA), EPOLICY ORCHESTRATOR, FIRST AID, FORCEFIELD, GMT, GROUPSHIELD, GROUPSHIELD (AND IN KATAKANA), GUARD DOG, HOMEGUARD, HUNTER, INTRUSHIELD, INTRUSION PREVENTION THROUGH INNOVATION, M AND DESIGN, MCAFFEE, MCAFFEE (AND IN KATAKANA), MCAFFEE AND DESIGN, MCAFFEE.COM, MCAFFEE VIRUSSCAN, NA NETWORK ASSOCIATES, NET TOOLS, NET TOOLS (AND IN KATAKANA), NETCRYPTO, NETOCTOPUS, NETSCAN, NETSHIELD, NETWORK ASSOCIATES, NETWORK ASSOCIATES COLLISEUM, NETXRAY, NOTESGUARD, NUTS & BOLTS, OIL CHANGE, PC MEDIC, PCNOTARY, PRIMESUPPORT, QUICKCLEAN, RINGFENCE, ROUTER PM, SECURECAST, SECURESELECT, SPAMKILLER, STALKER, THREATSCAN, TIS, TMEG, TOTAL VIRUS DEFENSE, TRUSTED MAIL, UNINSTALLER, VIREX, VIRUS FORUM, VIRUSSCAN, VIRUSSCAN, VIRUSSCAN (AND IN KATAKANA), WEBSCAN, WEBSHIELD, WEBSHIELD (AND IN KATAKANA), WEBSTALKER, WEBWALL, WHAT'S THE STATE OF YOUR IDS?, WHO'S WATCHING YOUR NETWORK, YOUR E-BUSINESS DEFENDER, YOUR NETWORK. OUR BUSINESS. are registered trademarks or trademarks of McAfee, Inc. and/or its affiliates in the US and/or other countries. Red in connection with security is distinctive of McAfee brand products. All other registered and unregistered trademarks herein are the sole property of their respective owners.

LICENSE INFORMATION

License Agreement

NOTICE TO ALL USERS: CAREFULLY READ THE APPROPRIATE LEGAL AGREEMENT CORRESPONDING TO THE LICENSE YOU PURCHASED, WHICH SETS FORTH THE GENERAL TERMS AND CONDITIONS FOR THE USE OF THE LICENSED SOFTWARE. IF YOU DO NOT KNOW WHICH TYPE OF LICENSE YOU HAVE ACQUIRED, PLEASE CONSULT THE SALES AND OTHER RELATED LICENSE GRANT OR PURCHASE ORDER DOCUMENTS THAT ACCOMPANIES YOUR SOFTWARE PACKAGING OR THAT YOU HAVE RECEIVED SEPARATELY AS PART OF THE PURCHASE (AS A BOOKLET, A FILE ON THE PRODUCT CD, OR A FILE AVAILABLE ON THE WEB SITE FROM WHICH YOU DOWNLOADED THE SOFTWARE PACKAGE). IF YOU DO NOT AGREE TO ALL OF THE TERMS SET FORTH IN THE AGREEMENT, DO NOT INSTALL THE SOFTWARE. IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO MCAFFEE OR THE PLACE OF PURCHASE FOR A FULL REFUND.

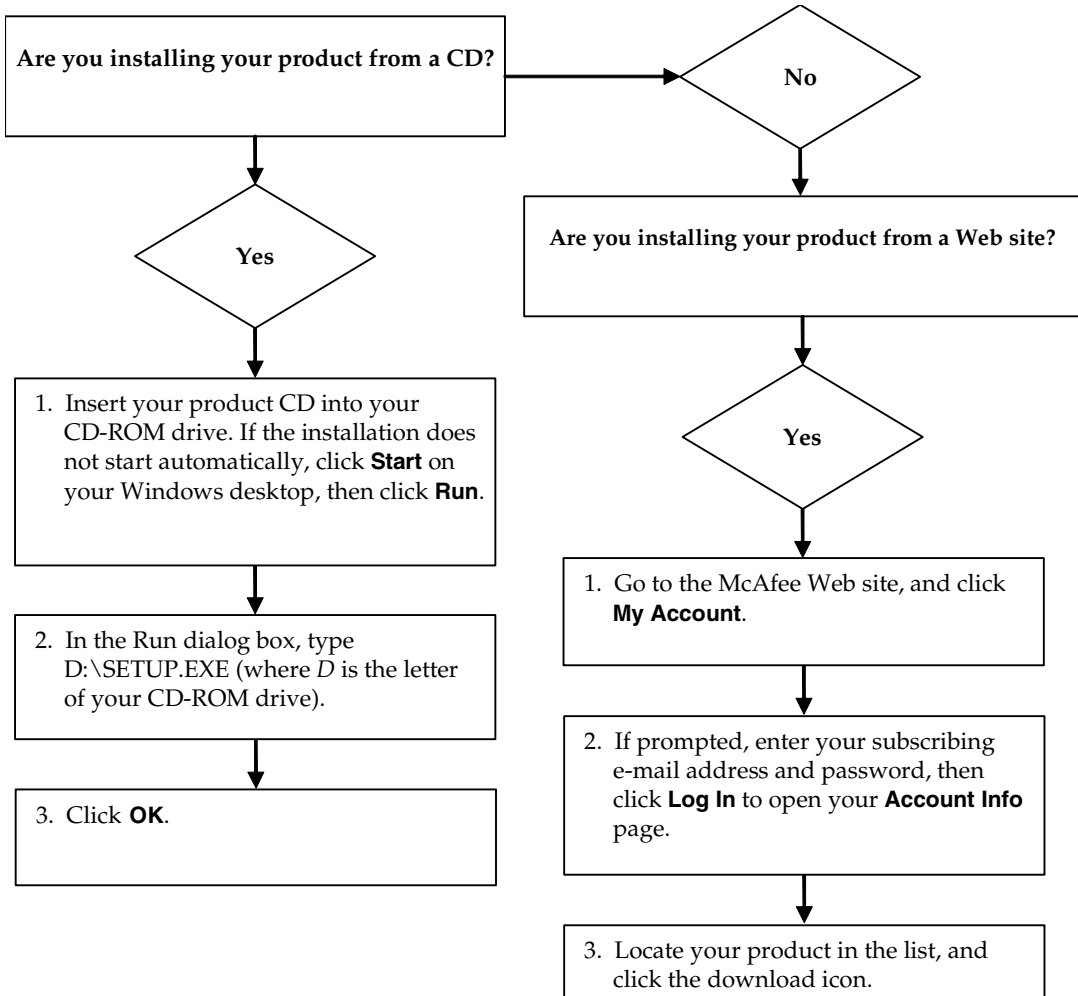
Attributions

This product includes or may include:

- Software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>).
- Cryptographic software written by Eric A. Young and software written by Tim J. Hudson.
- Some software programs that are licensed (or sublicensed) to the user under the GNU General Public License (GPL) or other similar Free Software licenses which, among other rights, permit the user to copy, modify and redistribute certain programs, or portions thereof, and have access to the source code. The GPL requires that for any software covered under the GPL which is distributed to someone in an executable binary format, that the source code also be made available to those users. For any such software covered under the GPL, the source code is made available on this CD. If any Free Software licenses require that McAfee provide rights to use, copy or modify a software program that are broader than the rights granted in this agreement, then such rights shall take precedence over the rights and restrictions herein.
- Software originally written by Henry Spencer, Copyright 1992, 1993, 1994, 1997 Henry Spencer.
- Software originally written by Robert Nordier, Copyright © 1996-7 Robert Nordier.
- Software written by Douglas W. Sauder.
- Software developed by the Apache Software Foundation (<http://www.apache.org/>). A copy of the license agreement for this software can be found at www.apache.org/licenses/LICENSE-2.0.txt.
- International Components for Unicode ("ICU") Copyright © 1995-2002 International Business Machines Corporation and others.
- Software developed by CrystalClear Software, Inc., Copyright © 2000 CrystalClear Software, Inc.
- FEAD[®] Optimizer[®] technology, Copyright Netopsystems AG, Berlin, Germany.
- Outside In[®] Viewer Technology © 1992-2001 Stellant Chicago, Inc. and/or Outside In[®] HTML Export, © 2001 Stellant Chicago, Inc.
- Software copyrighted by Thai Open Source Software Center Ltd. and Clark Cooper, © 1998, 1999, 2000.
- Software copyrighted by Expat maintainers.
- Software copyrighted by The Regents of the University of California, © 1989.
- Software copyrighted by Gunnar Ritter.
- Software copyrighted by Sun Microsystems[®], Inc. © 2003.
- Software copyrighted by Gisle Aas, © 1995-2003.
- Software copyrighted by Michael A. Chase, © 1999-2000.
- Software copyrighted by Neil Winton, © 1995-1996.
- Software copyrighted by RSA Data Security, Inc., © 1990-1992.
- Software copyrighted by Sean M. Burke, © 1999, 2000.
- Software copyrighted by Martijn Koster, © 1995.
- Software copyrighted by Brad Appleton, © 1996-1999.
- Software copyrighted by Michael G. Schwern, © 2001.
- Software copyrighted by Graham Barr, © 1998.
- Software copyrighted by Larry Wall and Clark Cooper, © 1998-2000.
- Software copyrighted by Frodo Looijaard, © 1997.
- Software copyrighted by the Python Software Foundation, Copyright © 2001, 2002, 2003. A copy of the license agreement for this software can be found at www.python.org.
- Software copyrighted by Beman Dawes, © 1994-1999, 2002.
- Software written by Andrew Lumsdaïne, Lie-Quan Lee, Jeremy G. Siek © 1997-2000 University of Notre Dame.
- Software copyrighted by Simone Bordet & Marco Craverio, © 2002.
- Software copyrighted by Stephen Purcell, © 2001.
- Software developed by the Indiana University Extreme! Lab (<http://www.extreme.indiana.edu/>).
- Software copyrighted by International Business Machines Corporation and others, © 1995-2003.
- Software developed by the University of California, Berkeley and its contributors.
- Software developed by Ralf S. Engelschall <rse@engelschall.com> for use in the mod_ssl project (<http://www.modssl.org/>).
- Software copyrighted by Kevlin Henney, © 2000-2002.
- Software copyrighted by Peter Dimov and Multi Media Ltd. © 2001, 2002.
- Software copyrighted by David Abrahams, © 2001, 2002. See <http://www.boost.org/libs/bind/bind.html> for documentation.
- Software copyrighted by Steve Cleary, Beman Dawes, Howard Hinnant & John Maddock, © 2000.
- Software copyrighted by Boost.org, © 1999-2002.
- Software copyrighted by Nicolai M. Josuttis, © 1999.
- Software copyrighted by Jeremy Siek, © 1999-2001.
- Software copyrighted by Daryle Walker, © 2001.
- Software copyrighted by Chuck Allison and Jeremy Siek, © 2001, 2002.
- Software copyrighted by Samuel Krempf, © 2001. See <http://www.boost.org> for updates, documentation, and revision history.
- Software copyrighted by Doug Gregor (gregod@cs.rpi.edu), © 2001, 2002.
- Software copyrighted by Cadenza New Zealand Ltd., © 2000.
- Software copyrighted by Jens Maurer, © 2000, 2001.
- Software copyrighted by Jaakko Järvi (jaakko.jarvi@cs.utu.fi), © 1999, 2000.
- Software copyrighted by Ronald Garcia, © 2002.
- Software copyrighted by David Abrahams, Jeremy Siek, and Daryle Walker, © 1999-2001.
- Software copyrighted by Stephen Cleary (shammah@voyager.net), © 2000.
- Software copyrighted by Housemarque Oy <<http://www.housemarque.com>>, © 2001.
- Software copyrighted by Paul Moore, © 1999.
- Software copyrighted by Dr. John Maddock, © 1998-2002.
- Software copyrighted by Greg Colvin and Beman Dawes, © 1998, 1999.
- Software copyrighted by Peter Dimov, © 2001, 2002.
- Software copyrighted by Jeremy Siek and John R. Bandela, © 2001.
- Software copyrighted by Joerg Walter and Mathias Koch, © 2000-2002.

Quick Start Card

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



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.
© 2005 McAfee, Inc. All Rights Reserved.

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 Getting Started	9
System requirements	9
Using McAfee SecurityCenter	11
2 McAfee Wireless Home Network Security	13
Using McAfee Wireless Home Network Security	13
Protecting your network	13
Understanding Wireless Home Network Security	14
Wireless Home Network Security makes it simple	14
Features	15
Installing Wireless Home Network Security	16
Installing from a CD	16
Installing from the Web site	16
Installing from the installation file	16
Using the configuration wizard	17
Using the Summary Page	18
Viewing your connection	18
Viewing your protected wireless network	19
Managing Wireless Networks	20
Connecting to a network	20
Disconnecting from a network	21
Using advanced options	21
Configuring Options	22
Viewing events	22
Configuring advanced settings	23
Configuring security settings	23
Configuring alert settings	23
Configuring other settings	23
Revoking access to the network	24
Repairing security settings	24
Protecting other computers	25

Rotating keys	25
Protecting wireless networks	26
Unprotecting wireless networks	26
Updating Wireless Home Network Security	26
Automatically checking for updates	26
Manually checking for updates	26
Understanding Alerts	28
Access revoked	28
Computer connected	28
Computer disconnected	28
Computer secured	28
Key rotation failed	28
Key rotation resumed	29
Key rotation suspended	29
Network configuration changed	29
Network renamed	29
Network repaired	29
Network settings changed	29
Password changed	29
Security key rotated	30
Security key rotation frequency changed	30
Wireless router/AP protected	30
Wireless router/AP unprotected	30
Troubleshooting	30
Installation	30
Which computers to install this software on	30
Wireless adapter not detected	31
Multiple wireless adapters	31
Unable to download on wireless computers because the network is already secure	31
Protecting or configuring your network	32
Unsupported router or access point	32
Updating router or access point firmware	32
Duplicate administrator error	32
Network appears unsecured	32
Unable to repair	33
Connecting computers to your network	33
Waiting for authorization	33
Granting access to an unknown computer	33

Connecting to a network or the Internet 34

 Bad connection to the Internet 34

 Connection briefly stops 34

 Devices (not your computer) losing connection 34

 Prompted to enter the WEP or WPA key 34

 Unable to connect 34

 Updating your wireless adapter 35

 Weak signal level 36

 Windows cannot configure your wireless connection 36

 Windows showing no connection 36

Other issues 37

 Network name is different when using other programs 37

 Problems configuring wireless routers or access points 37

 Replacing computers 38

 Software not working after upgrading operating systems 38

Glossary 39

3 McAfee VirusScan 49

New features 49

Testing VirusScan 51

 Testing ActiveShield 51

 Testing Scan 51

Using McAfee VirusScan 53

Using ActiveShield 53

 Enabling or disabling ActiveShield 53

 Configuring ActiveShield options 54

 Understanding security alerts 63

Manually scanning your computer 66

 Manually scanning for viruses and other threats 66

 Automatically scanning for viruses and other threats 69

 Understanding threat detections 71

Managing quarantined files 72

Creating a Rescue Disk 74

 Write-protecting a Rescue Disk 75

 Using a Rescue Disk 75

 Updating a Rescue Disk 75

Automatically reporting viruses 75

 Reporting to the World Virus Map 76

Viewing the World Virus Map	77
Updating VirusScan	78
Automatically checking for updates	78
Manually checking for updates	78
4 McAfee Personal Firewall Plus	81
New features	81
Uninstalling other firewalls	83
Setting the default firewall	83
Setting the security level	84
Testing McAfee Personal Firewall Plus	86
Using McAfee Personal Firewall Plus	86
About the Summary page	86
About the Internet Applications page	91
Changing application rules	92
Allowing and blocking Internet applications	92
About the Inbound Events page	93
Understanding events	94
Showing events in the Inbound Events log	96
Responding to inbound events	98
Managing the Inbound Events log	102
About alerts	103
Red alerts	104
Green alerts	109
Blue alerts	111
Index	113

The Internet provides a wealth of information and entertainment at your fingertips. However, as soon as you connect, your computer, data, and wireless network is exposed to a multitude of privacy and security threats. Protect your wireless network and secure your computer and data with McAfee Wireless Home Network Security Suite. Incorporating the award-winning technologies of McAfee Wireless Home Network Security, McAfee VirusScan, and McAfee Personal Firewall Plus, Wireless Home Network Security Suite provides one of the most comprehensive sets of privacy and security tools you can buy.

For more information about each McAfee product, see the following chapters:

- *McAfee Wireless Home Network Security on page 13*
- *McAfee VirusScan on page 49*
- *McAfee Personal Firewall Plus on page 81*

System requirements

- Microsoft® Windows 98SE, Windows Me, Windows 2000, or Windows XP
- Personal computer with Pentium-compatible processor
 - Windows 98 or 2000: 133 MHz or higher
 - Windows Me: 150 MHz or higher
 - Windows XP (Home and Pro): 300 MHz or higher
- RAM
 - Windows 98SE, Me, or 2000: 64 MB
 - Windows XP (Home and Pro): 128 MB
- 100MB 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/>.

Wireless network

- Standard wireless network adapter
- Standard wireless router or access point, including most Linksys®, NETGEAR®, D-Link®, and Belkin® models

Supported e-mail programs

- POP3 (Outlook Express, Outlook, Eudora, Netscape)

Supported instant messaging programs

- AOL Instant Messenger 2.1 or later
- Yahoo Messenger 4.1 or later
- Microsoft Windows Messenger 3.6 or later
- MSN Messenger 6.0 or later


Using McAfee SecurityCenter

The McAfee SecurityCenter is your one-stop security shop. Seamless integration with the McAfee SecurityCenter provides a consolidated view of your computer's security status, plus the latest security and virus alerts. You can run SecurityCenter from the McAfee icon in your Windows system tray or from your Windows desktop.


NOTE

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


While the SecurityCenter is running and all of the McAfee features installed on your computer are enabled, a red **M** icon  appears in the Windows system tray (Windows XP notification area).

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

To open the McAfee SecurityCenter:

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

To access a your McAfee product:

- 1 Right-click the McAfee icon .
- 2 Point to the appropriate McAfee product, and then click the feature you want to use.

McAfee Wireless Home Network Security

2

Welcome to McAfee Wireless Home Network Security, which offers advanced protection for your wireless network, your personal data, and your computer.

This product is designed for computers with wireless connections. When you install this product on computers that connect to your network using a cable, you do not have full functionality from those wired computers.

McAfee Wireless Home Network Security enhances the privacy of your computing experience by encrypting your personal and private data as it is sent over your protected wireless network, and blocks hackers from accessing your information.

Using McAfee Wireless Home Network Security

Before you protect your network, note the following.

- Cable connections - computers that are connected to the router with a cable do not need to be protected, because signals transmitted over a cable cannot be intercepted.
- Wireless connections - computers that have wireless connections should be protected, because their data can be intercepted. A wireless computer must be used to protect a network because only a wireless computer can grant access to another wireless computer.

Protecting your network

You do not need to protect your network if you are connected with a cable.

- 1 On your wireless computer, install your wireless adapter and ensure that it is enabled. The wireless adapter can be a card that is inserted on the side of your computer or USB port. Many newer computers come with a built-in wireless adapter, so you do not have to install it.
- 2 Install your wireless router or access point (access points are used to extend the wireless range) and ensure it is turned on and enabled. For a more complete definition of a router and an access point, see [Glossary on page 39](#).
- 3 Install McAfee Wireless Home Network Security on every wireless computer in your network. You do not need to install this software on computers that are connected with a cable. See [Installing Wireless Home Network Security on page 16](#).

- 4 From one of the wireless computers, protect your network. See [Protecting wireless networks](#) on page 26.
- 5 Join the network from other wireless computers. See [Protecting other computers](#) on page 25.

Understanding Wireless Home Network Security

Like many people, you use a wireless network at home because it is convenient and easy. Wireless lets you access the Internet from any room in your house or even your backyard, without the costs and hassles of attaching cables. Wireless networking makes it easy to allow friends and family to access the network.

However, this convenience comes with security vulnerability. Wireless networks use radio waves to transmit data, and these radio waves travel beyond the walls of your house. With specialized antennas, wireless intruders can access your wireless network or intercept your data from miles away.

To protect your wireless network and data, you need to restrict access to your wireless network and encrypt your data. Your wireless router or access point comes with built-in security standards, but the difficulty is properly enabling and managing your security settings. Over sixty percent of wireless networks do not properly use a high level of security like encryption.

Wireless Home Network Security makes it simple

McAfee Wireless Home Network Security activates the security on your wireless network and protects what is sent over it with a simple, one click process that automatically generates a strong encryption key. Most keys that are easy for people to remember can be quickly cracked by hackers. By having the computer remember the key for you, Wireless Home Network Security can use keys that are almost impossible to crack.

Running seamlessly behind the scenes, this software also creates and distributes a new encryption key every few minutes, thwarting even the most determined hackers. Legitimate computers, like those of your friends and family who want access to your wireless network, receive the strong encryption key and all key distributions.

This process offers strong security, while still being simple for an owner of a wireless network at home to implement. With one click, you can block hackers from stealing your data as it is sent over the air. Hackers cannot insert Trojans or other malware into your network. They cannot use your wireless network as a platform to launch spam or virus attacks. Even casual freeloaders cannot use your wireless network, so you will not be erroneously blamed for illegal movie or song downloads.

Other solutions do not offer the simplicity or the strength of security offered by Wireless Home Network Security. Filtering MAC Addresses or Disabling Broadcast SSID only offers cosmetic protection. Even simple hackers can circumvent these mechanisms by downloading freely available tools from the Internet. Other utilities like VPNs do not protect the wireless network itself, so you are still vulnerable to a myriad of attacks.

McAfee Wireless Home Network Security is the first product that truly locks down your home wireless network.

Features

This version of Wireless Home Network Security offers the following features:

- Always on protection - automatically detects and protects any vulnerable wireless network that you connect to.
- Intuitive interface - protect your network without having to make difficult decisions or knowing complex technical terms.
- Strong automatic encryption - only let your friends and family have access to your network and protect your data as it travels back and forth.
- Software only solution - Wireless Home Network Security works with your standard wireless router or access point and security software. You do not need to buy additional hardware.
- Automatic key rotation - even the most determined hackers cannot capture your information because the key is continuously rotating.
- Addition of network users - you can easily grant your friends and family access to your network.
- Intuitive connection tool - the wireless connection tool is intuitive and informative, with details about signal strength and security state.
- Event logging and alerts - easy to understand reports and alerts offer advanced users more information on your wireless network.
- Suspend mode - temporarily suspend key rotation so that particular applications can run without interruption.
- Compatibility with other equipment - Wireless Home Network Security automatically updates itself with the latest wireless router or access point modules from the most popular brands including: Linksys®, NETGEAR®, D-Link®, Belkin®, and others.

Installing Wireless Home Network Security

This section explains how to install Wireless Home Network Security and get started on protecting your network.

When installing Wireless Home Network Security, note the following.

- Install this software on all your wireless computers.
- You do not have to install this software on computers that are connected with a cable.

Installing from a CD

- 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**.
- 4 Go to [Using the configuration wizard on page 17](#).

Installing from the Web site

When you install Wireless Home Network Security from the Web site, you must save the installation file. This file is used to install Wireless Home Network Security on other computers.

- 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 **Save Target As...** The installation file is saved on your computer.

Installing from the installation file

If you downloaded the installation package (as opposed to having a CD), you must install the software on all the wireless computers. After the network is protected, wireless computers cannot connect to the network without entering the key. Do one of the following.

- Before protecting the network, download the installation package to every wireless computer.

- Copy the installation file to a USB memory key or a writable CD and install the software on the other wireless computers.
- If the network is already protected, plug a cable in the router to download the file. You can also click **View Network Key** to see the current key, and connect to the wireless network using this key.

After you install Wireless Home Network Security on all the wireless computers, follow the on-screen instructions. When you click **Finish**, the Configuration wizard appears. Go to [Using the configuration wizard on page 17](#).

Using the configuration wizard


The configuration wizard allows you to:

- Protect your network from one of the wireless computers. For more information, see [Protecting wireless networks on page 26](#).

If Wireless Home Network Security cannot determine the correct router or access point to protect, you are prompted to **Retry** or **Cancel**. Try moving closer to the router or access point you are protecting, and then click **Retry**.
- Join a protected network (this step is not necessary if there is only one wireless computer). For more information, see [Managing Wireless Networks on page 20](#).
- Connect to a network. For more information, see [Connecting to a network on page 20](#).

You are notified if your wireless adapter is not detected or your wireless router or access point is not turned on.

Using the Summary Page

To view the status of your connection, right-click the McAfee icon (), point to **Wireless Network Security**, and select **Summary**. The Summary page appears (Figure 2-1).

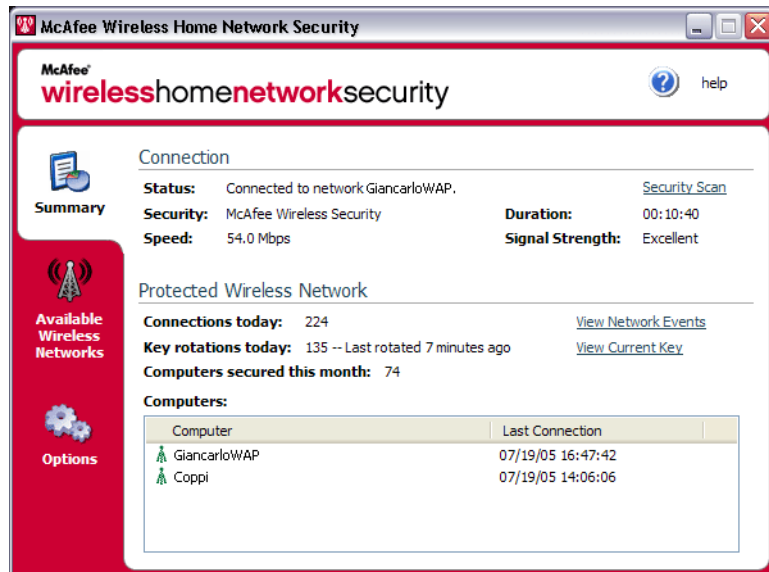


Figure 2-1. Summary page

Viewing your connection


The Connection pane shows the status of your connection. If you want to run a scan of your wireless connection, click **Security Scan**.

- Status - whether you are connected or disconnected. If you are connected, the name of the network appears.
- Security - the security mode of the network.
- Speed - connection speed from your wireless NIC (Network Interface Card).
- Duration - how long you have been connected to this network.
- Signal Strength - strength of your wireless connection.


Viewing your protected wireless network

The Protected Wireless Network pane provides information on your network.

- Connections today - how many times users connected to this network today.
- Key rotations today - how many times the key has rotated today, including the time elapsed since the key was last rotated.
- Key rotation suspended- key rotation on your network is suspended. To resume key rotation and ensure that your network is fully protected from hackers, click **Resume Key Rotation**.
- Computers secured this month - how many computers have been secured this month.
- Computers - if you are connected to a protected network, all the computers on the network and when each computer was last connected.

 - the computer is connected.

 - the computer can reconnect without joining the network.

 - the computer is not connected. The computer must rejoin the network because the key has been updated.

Click **View Network Events** to view network events. See [Viewing events on page 22](#).


Click **View Current Key** to view the key.

If you are connecting wireless devices that Wireless Home Network Security does not support (for example, connecting a wireless handheld computer to your network), follow these steps.

- 1 In the Summary screen, click **View Current Key**.
- 2 Write down the key.
- 3 Click **Suspend Key Rotation**. Suspending key rotation prevents devices that have been manually connected to the network from being disconnected.
- 4 Enter the key on the device.

When you are done using these devices, click **Resume Key Rotation**. McAfee recommends that you resume key rotation to ensure that your network is fully protected from hackers.

Managing Wireless Networks

To select wireless networks to connect to or join, right-click the McAfee icon (), point to **Wireless Network Security**, and select **Available Wireless Networks**. The Available Wireless Networks page appears ([Figure 2-2](#)).

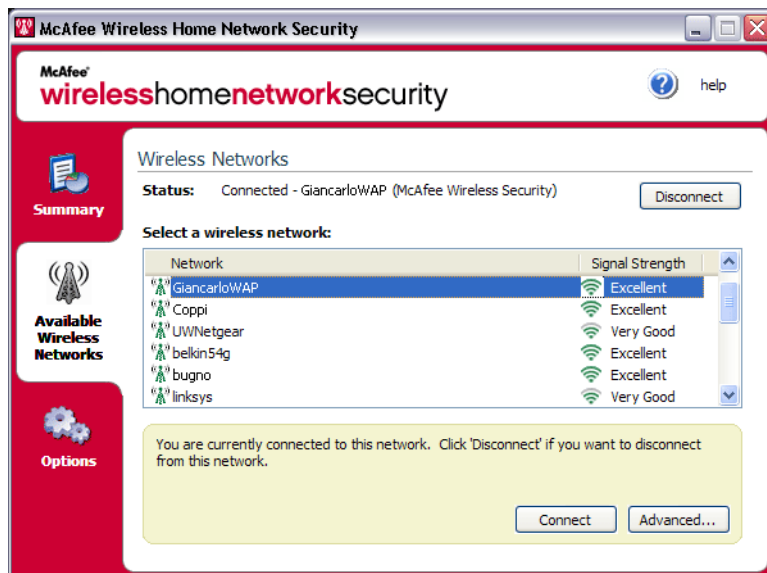




Figure 2-2. Available Wireless Networks page

When you are connected to a protected wireless network, the information that is sent and received is encrypted. Hackers cannot intercept the data that is transmitted over the protected network and cannot connect to your network.

 - the network is protected.

 - the network is protected using WEP or WPA-PSK security.

 - the network is not protected but you can still connect to it (not recommended).

Connecting to a network

To connect to a network, select the network you want to connect to, and click **Connect**. If you manually configured a pre-shared key for your router or access point, you must also enter the key.

If the network is protected, you must join it before you can connect to it. In order for you to join the network, a user that is already connected to the network must give you permission.

When you join a network, you can reconnect to it without having to join it again. You can also grant permission to other users to join that network.

Disconnecting from a network

To disconnect from the network you are connected to, click **Disconnect**.

Using advanced options

If you want to use advanced connection options, click **Advanced**. The Wireless Network Advanced Settings dialog box appears. From this dialog box, you can do the following.

- Change the order of the networks you automatically connect to - the network at the top of the list is the one that you last connected to, and is the one that Wireless Home Network Security tries to connect to first. To move a network, select it and click **Move Up** or **Move Down**. For example, if you moved from a location and the network you last connected to is far away and does not have a strong signal, you can move the network that has a stronger signal to the top of your list.
- Remove preferred networks - remove networks from this list. For example, if you connected to your neighbor's network by mistake, it is now included in this list. To remove it, select it and click **Remove**.
- Modify network properties - if you are having trouble connecting to a network that is not protected, you can modify its properties. Note that this option only applies to networks that are not protected. To modify properties, select a network and click **Properties**.
- Add networks that do not broadcast SSID - for example, if you are trying to connect to your friend's wireless network, but it does not appear in the list, click **Add** and enter the appropriate information. Note that the network that you add cannot be protected by Wireless Home Network Security.

Configuring Options

To configure options, right-click the McAfee icon (), point to **Wireless Network Security**, and select **Options**. The Options page appears ([Figure 2-3](#)).



Figure 2-3. Options page

Viewing events

Actions performed by Wireless Home Network Security are stored in event logs. To view these logs, click **View Network Events**. The information displays in chronological order by default.

In the Events for network box, you can select the type of events that display (all events are still logged), and you can view events for any network that you belong to (if you belong to more than one network).

When an event occurs, an alert appears with a brief description. For more information on alerts, see [Understanding Alerts on page 28](#).

Configuring advanced settings

This section is for advanced users. Click **Advanced Settings** to configure security, alert, and other settings.

When you change a setting, click **OK** for the changes to take effect. Note that after you click **OK**, all the computers that are connected temporarily lose connectivity for a few minutes.

Configuring security settings

Use the Security Settings tab to change your security settings.

- Protected Wireless Network Name - name of the current protected network. When you change the name of a network, it appears in the Available Wireless Networks list and you must reconnect to the network. See [Managing Wireless Networks on page 20](#).
- Security Mode - current security mode. To change the default security (WEP), select WPA-PSK TKIP for stronger encryption. Make sure that the routers, access points, and wireless adapters that connect to your network support this mode, or else they will not be able to connect. For more information on updating your adapter, see [Updating your wireless adapter on page 35](#).
- Enable automatic key rotation - to suspend key rotation, clear this option. To change the frequency of the key rotation, move the slider. For more information on key rotation, see [Viewing your protected wireless network on page 19](#).
- Change User Name or Password - for security reasons, you can change the default user name or password for the wireless router or access point by selecting it and clicking **Change User Name or Password**. The default user name or password is the one you used when you logged on and configured your router or access point.

Configuring alert settings

Use the Alert Settings tab to change your alert settings.

Select the type of events you want to be alerted to, and click **OK**. If you do not want to be alerted to certain types of events, clear the appropriate box.

Configuring other settings

Use the Other Settings tab to change other settings.

- Display keys in plain text - for networks not protected by Wireless Home Network Security. Keys for unprotected networks that appear in the Available Wireless Networks list can be shown in plain text instead of asterisks. If you display keys in plain text, your keys are discarded for security reasons.

- Discard All Saved Keys - for networks not protected by Wireless Home Network Security. Delete all the keys that have been saved. Note that if you delete these keys, you must re-enter a key when connecting to WEP and WPA-PSK networks.
- Leave Network - for networks protected by Wireless Home Network Security. You can give up your access rights to a protected wireless network. For example, if you want to leave a network and do not expect to connect to it again, select it from the list and click **Leave Network**.
- Display notification message when connected to a wireless network - when a connection is made, a notification message appears.

Revoking access to the network

To prevent computers that have joined the network, but are not currently connected to it, from accessing your network:

- 1 Click **Revoke Access**. The Revoke Access dialog box appears.
- 2 Click **Revoke**.

The key rotation for the network is reset, and the computers currently connected receive the new key and remain connected. Computers not currently connected do not receive the updated key and must rejoin the network before they can connect.

When you revoke access to a computer, that computer must rejoin the network before it can connect to the protected network again. To do this, the computer must have Wireless Home Network Security installed (see [Installing Wireless Home Network Security on page 16](#)), and then connect to the protected network and join it (see [Connecting to a network on page 20](#)).

Repairing security settings

Repair security settings only if you are having problems with your wireless network. For more information, see [Unable to connect on page 34](#).

To fix your router or access point settings on the current network, follow these steps.


- 1 Click **Repair Security Settings**. The Repair dialog box appears.
- 2 Click **Repair**.
- 3 Click **Close** when you are done.

An error message appears if a connection cannot be made with the network routers or access points. Connect to your network using a cable, then try repairing again. If the password for the router or access point was changed, you are prompted for the new password.

Protecting other computers

To obtain more information on protecting other computers and giving them access to your protected network, click **Protect Another Computer**.

To protect another computer:

- 1 Install McAfee Wireless Home Network Security on the computer you want to protect.
- 2 From the computer you are protecting, right-click the McAfee icon () , point to **Wireless Network Security**, and select **Available Wireless Networks**. The Available Wireless Networks page appears.
- 3 Select a protected network to join, and click **Connect**. Note that a user that is already connected to the network must give you permission to join the network.

When you join a network, you can reconnect to it without having to join it again. You can also grant permission to other users to join that network.

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

If you are connecting wireless devices that Wireless Home Network Security does not support (for example, connecting a wireless handheld computer to your network), follow these steps.

- 1 In the Summary screen, click **View Current Key**.
- 2 Write down the key.
- 3 Click **Suspend Key Rotation**. Suspending key rotation prevents devices that have been manually connected to the network from being disconnected.
- 4 Enter the key on the device.

When you are done using these devices, click **Resume Key Rotation**. McAfee recommends that you resume key rotation to ensure that your network is fully protected from hackers.

Rotating keys

To rotate the security key for your network, click **Manually Rotate Security Key**.

Protecting wireless networks

To protect a router or access point, follow these steps.

- 1 Click **Protect Wireless Router/AP**. The Protect Wireless Network dialog box appears. If the router or access point does not appear in the list, click **Refresh**.
- 2 Select the router or access point you are protecting, and click **Protect**.

Unprotecting wireless networks

You must be connected to the wireless router or access point you are unprotecting.

To unprotect a router or access point, follow these steps.

- 1 Click **Unprotect Wireless Router/AP**. The Unprotect Wireless Network dialog box appears. If the router or access point does not appear in the list, click **Refresh**.
- 2 Select the router or access point you are unprotecting, and click **Unprotect**.

Updating Wireless Home Network Security

When you are connected to the Internet, Wireless Home Network Security checks for software updates every four hours, then automatically downloads and installs weekly updates without interrupting your work. These updates have a minimal impact on system performance during download.

If a product update occurs, an alert appears. When alerted, you can choose to update Wireless Home Network Security.

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 are prompted to restart your computer to complete the update. Save all your work and close all applications before restarting.

Manually checking for updates

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

To manually check for Wireless Home Network Security updates:

- 1 Ensure your computer is connected to the Internet.
- 2 Right-click the McAfee icon, then click **Updates**. The **SecurityCenter Updates** dialog box appears.
- 3 Click **Check Now**.

If an update exists, the **Wireless Home Network Security Updates** dialog box appears. Click **Update** to continue.

If no updates are available, a dialog box tells you that Wireless Home Network Security is up-to-date. Click **OK** to close the 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 are prompted to restart your computer to complete the update. Save all your work and close all applications before restarting.

Understanding Alerts

Alerts appear when an event occurs, and notify you of changes to the network.

Access revoked

A user has updated the network key. For more information, see [Revoking access to the network on page 24](#).

Computer connected

A user has connected to the network. For more information, see [Connecting to a network on page 20](#).

Computer disconnected

A user has disconnected from the network. For more information, see [Disconnecting from a network on page 21](#).

Computer secured

A user that has access to the protected network has granted someone else access. For example: 'Lance' has given access to 'Mercks' and they can now use the wireless network 'CoppiWAP'.

Key rotation failed

The key rotation failed because:

- The logon information for your router or access point has been changed. If you know the logon information, see [Repairing security settings on page 24](#).
- The firmware version of your router or access point has been changed to a version that is not supported. For more information, see [Unable to connect on page 34](#).
- Your router or access point is not available. Ensure that the router or access point is turned on, and that it is connected to your network.
- Duplicate administrator error. For more information, see [Duplicate administrator error on page 32](#).

If you are having problems connecting to this network, see [Repairing security settings on page 24](#).

Key rotation resumed

A user has resumed the key rotation. Key rotation prevents hackers from accessing your network.

Key rotation suspended

A user has suspended the key rotation. McAfee recommends that you resume key rotation to ensure that your network is fully protected from hackers.

Network configuration changed

A user has changed the security mode for the network. For more information, see [Configuring security settings on page 23](#).

Network renamed

A user has renamed the network and you must connect to it again. For more information, see [Connecting to a network on page 20](#).

Network repaired

A user has attempted to repair the network because they have problems connecting.

Network settings changed

A user is about to change network security settings. Your connection may be briefly interrupted while this occurs. The setting that is being changed can be one or more of the following:

- Name of the network
- Security mode
- Key rotation frequency
- Status of automated key rotation

Password changed

A user has changed the user name or password on a router or access point on the network. For more information, see [Configuring security settings on page 23](#).

Security key rotated

The security key for the network has been rotated. McAfee Wireless Home Network Security automatically rotates your network encryption key, making it more difficult for hackers to intercept your data or connect to your network.

Security key rotation frequency changed

The security key rotation frequency for the network has been changed. McAfee Wireless Home Network Security automatically rotates your network encryption key, making it more difficult for hackers to intercept your data or connect to your network.

Wireless router/AP protected

A wireless router or access point has been protected on your network. For more information, see [Protecting wireless networks on page 26](#).

Wireless router/AP unprotected

A wireless router or access point has been removed from the network. For more information, see [Unprotecting wireless networks on page 26](#).

Troubleshooting

This chapter describes troubleshooting procedures for McAfee Wireless Home Network Security and third-party equipment.

Installation

This section explains how to resolve installation problems.

Which computers to install this software on

Install McAfee Wireless Home Network Security on every wireless computer in your network (unlike other McAfee applications, you can install this software on multiple computers).

You can (but are not required to) install on computers that do not have wireless adapters, but the software is not active on these computers because they do not need wireless protection. You must protect your router or access point (see [Protecting wireless networks on page 26](#)) from one of your wireless computers to secure your network.

Wireless adapter not detected

If your wireless adapter is not detected when it is installed and enabled, restart your computer. If the adapter is still not detected after restarting your computer, follow these steps.

- 1 Open the Wireless Network Connection Properties dialog box.
- 2 Clear the **MWL Filter** box and then select it.
- 3 Click **OK**.

If this does not work, your wireless adapter might not be supported. Update your adapter or buy a new one. To view a list of supported adapters, go to <http://www.mcafee.com/router>. To update your adapter, see *Updating your wireless adapter* on page 35.

Multiple wireless adapters

If an error states that you have multiple wireless adapters installed, you must disable or unplug one of them. Wireless Home Network Security only works with one wireless adapter.

Unable to download on wireless computers because the network is already secure

If you have a CD, install McAfee Wireless Home Network Security from the CD on all your wireless computers.

If you installed the software on one wireless computer and protected your network before installing the software on all the other wireless computers, you have these options.

- Unprotect your network (see *Unprotecting wireless networks* on page 26). Then, download the software and install it on all the wireless computers. Protect your network again (see *Protecting wireless networks* on page 26).
- View the network key (see *Viewing your protected wireless network* on page 19). Then, enter the key on your wireless computer to connect to the network. Download and install the software, and join the network from the wireless computer (see *Protecting other computers* on page 25).
- Download the executable on the computer that is already connected to the network and save it on a USB storage key or burn it to a CD so you can install it on the other computers.

Protecting or configuring your network

This section explains how to troubleshoot problems when protecting or configuring your network.

Unsupported router or access point

If an error states that your wireless router or access point may not be supported, McAfee Wireless Home Network Security was unable to configure your device because it did not recognize it or find it.

Verify that you have the latest version of Wireless Home Network Security by requesting an update (McAfee constantly adds support for new routers and access points). If your router or access point appears in the list at <http://www.mcafee.com/router> and you still receive this error, you are experiencing communication errors between your computer and the router or access point. See [Unable to connect on page 34](#) before protecting your network again.

Updating router or access point firmware

If an error states that the firmware revision of your wireless router or access point is not supported, your device is supported, but the firmware revision of the device is not. Verify that you have the latest version of Wireless Home Network Security by requesting an update (McAfee constantly adds support for new firmware revisions).

If you have the latest version of Wireless Home Network Security, refer to the manufacturer Web site or support organization for your router or access point and install a firmware version that is listed on <http://www.mcafee.com/router>.

Duplicate administrator error

After you configure your router or access point, you must log off the administration interface. In some cases, if you do not log off, the router or access point acts as if another computer is still configuring it and an error message appears.

If you cannot log off, unplug the power from the router or access point and then plug it in again.

Network appears unsecured

If your network is showing as unsecured, it is not protected. You must protect the network (see [Protecting wireless networks on page 26](#)) to secure it. Note that McAfee Wireless Home Network Security only works with compatible routers and access points (see <http://www.mcafee.com/router>).

Unable to repair

If the repair fails, try the following. Note that each procedure is independent.

- Connect to your network using a cable, then try repairing again.
- Unplug the power from the router or access point, plug it in again, then try connecting.
- Reset the wireless router or access point to its default setting and repair it.
- Using the advanced options, leave the network from all the computers and reset the wireless router or access point to its default settings, then protect it.

Connecting computers to your network

This section explains how to troubleshoot problems when connecting computers to your network.

Waiting for authorization

If you try to join a protected network and your computer remains in waiting for authorization mode, verify the following.

- A wireless computer that already has access to the network is turned on and connected to the network.
- Someone is present to grant access on that computer when it appears.
- The computers are within wireless range of each other.

If **Grant** does not appear on the computer that already has access to the network, try granting from another computer.

If other computers are not available, unprotect the network from the computer that already has access, and protect the network from the computer that did not have access. Then, join the network from the computer that originally protected the network.

Granting access to an unknown computer

When you receive a request from an unknown computer to grant access, verify that they are familiar. Someone might be trying to illegitimately access your network.

Connecting to a network or the Internet

This section explains how to troubleshoot problems when connecting to a network or the Internet.

Bad connection to the Internet

If you cannot connect, try accessing your network using a cable, and then connect to the Internet. If you still cannot connect, verify the following:

- your modem is turned on
- your PPPoE (see [Glossary on page 39](#)) settings are correct
- your DSL or Cable line is active

Connectivity problems such as speed and signal strength can also be caused by wireless interference. Try changing the channel of your cordless telephone, eliminate possible sources of interference, or change the location of your wireless router, access point, or computer.

Connection briefly stops

When your connection briefly stops (for example, during an online game), the key rotation might be causing brief network delays: Momentarily suspend key rotation. McAfee recommends that you resume key rotation as soon as you can to ensure that your network is fully protected from hackers.

Devices (not your computer) losing connection

If some devices are losing their connection when you are using McAfee Wireless Home Network Security, suspend the key rotation.

Prompted to enter the WEP or WPA key

If you have to enter a WEP or WPA key to connect to your network, you probably did not install the software on your computer. To function correctly, Wireless Home Network Security must be installed on every wireless computer in your network. See [Protecting or configuring your network on page 32](#).

Unable to connect

If you are unable to connect, try the following. Note that each procedure is independent.

- If you are not connecting to a protected network, verify that you have the correct key and enter it again.
- Unplug the wireless adapter and plug it in again, or disable it and re-enable it.

- Turn off the router or access point, and turn it on again, then try connecting.
- Verify that your wireless router or access point is connected, and repair the security settings (see [Repairing security settings on page 24](#)).

If the repair fails, see [Unable to repair on page 33](#).

- Restart your computer.
- Update your wireless adapter or buy a new one. To update your adapter, see [Updating your wireless adapter on page 35](#). For example, your network could be using WPA-PSK TKIP security, and your wireless adapter might not support the network's security mode (the networks show WEP, even though they are set to WPA).
- If you are unable to connect after you upgraded your wireless router or access point, you might have upgraded it to an unsupported version. Verify that the router or access point is supported. If it is not supported, downgrade it to a supported version, or wait until a Wireless Home Network Security update is available.

Updating your wireless adapter

To update your adapter, follow these steps.

- 1 From your desktop, click **Start**, point to **Settings**, and then select **Control Panel**.
- 2 Double-click the **System** icon. The **System Properties** dialog box appears.
- 3 Select the **Hardware** tab, and then click **Device Manager**.
- 4 In the Device Manager list, double-click your adapter.
- 5 Select the **Driver** tab and note the driver you have.
- 6 Go to the Web site of the adapter's manufacturer and see if an update is available. Drivers are usually found in the Support or Downloads section.
- 7 If a driver update is available, follow the instructions on the Web site to download it.
- 8 Go back to the **Driver** tab and click **Update Driver**. A Windows wizard appears.
- 9 Follow the on-screen instructions.

Weak signal level

If your connection drops or is slow, your signal level might not be strong enough. To improve your signal, try the following.

- Ensure that your wireless devices are not blocked by metal objects such as furnaces, ducts, or large appliances. Wireless signals do not travel well through these objects.
- If your signal is going through walls, make sure that it does not have to cross at a shallow angle. The longer the signal travels inside a wall, the weaker it gets.
- If your wireless router or access point has more than one antenna, try moving the two antennas perpendicular to each other (one upright and one horizontal, at a 90 degree angle).
- Some manufacturers have high-gain antennas. Directional antennas provide longer range, while omni-directional antennas offer the most versatility. Consult your manufacturer's installation instructions for installing your antenna.

If these steps are not successful, add an Access Point to your network that is closer to the computer you are trying to connect to. If you configure your second AP with the same network name (SSID) and a different channel, your adapter automatically finds the strongest signal and connects through the appropriate AP.

Windows cannot configure your wireless connection

When you get a message saying that Windows cannot configure your wireless connection, you can ignore it. Use Wireless Home Network Security to connect to, and configure wireless networks. In the Windows Wireless Network Connection Properties dialog box, under the Wireless Networks tab, ensure that the **Use Windows to configure my wireless network setting** box is clear.

Windows showing no connection

If you are connected, but the Windows Network icon is showing an X (no connection), ignore this. You have a good connection.

Other issues

This section explains how to troubleshoot problems with other issues.

Network name is different when using other programs

If the name of the network is different when viewed through other programs (for example, `_SafeAaf` is part of the name), this is normal. Wireless Home Network Security marks networks with a code when they are protected.

Problems configuring wireless routers or access points

If an error appears when configuring your router or access point or adding multiple routers on the network, verify that all the routers and access points have a distinct IP address.

If the name of your wireless router or access point appears in the Protect Wireless Router or Access Point dialog box, but you get an error when you configure it: Verify that your router or access point is supported. To view a list of supported routers or access points, go to <http://www.mcafee.com/router>.

If your router or access point is configured, but does not seem to be on the correct network (for example, you cannot see other computers attached to the LAN), verify that you configured the appropriate router or access point, and not your neighbor's. Unplug the power from the router or access point, and ensure that the connection drops. If the wrong router or access point was configured, unprotect it and then protect the correct router or access point.

If you are unable to configure or add your router or access point, but it is supported, some changes you performed might be preventing it from being properly configured.

- Follow the manufacturer's directions to configure your wireless router or access point to DHCP, or to configure the correct IP address. In some cases, the manufacturer provides a configuration tool.
- Reset your router or access point to factory defaults and try repairing your network again. You might have changed the administration port on the router or access point, or turned off wireless administration. Ensure that you are using the default configuration, and that wireless configuration is enabled. Another possibility is that the http administration is disabled. In this case, verify that the http administration is enabled.
- If your wireless router or access point does not appear in the list of wireless routers or access points to protect or connect to, enable broadcast SSID and verify that the router or access point is enabled.
- If you get disconnected, or cannot establish a connection, MAC filtering might be enabled. Disable MAC filtering.

- If you cannot perform network operations (for example, share files or print to shared printers) across two computers with wireless connection to the network, verify that you have not enabled AP Isolation. AP Isolation prevents wireless computers from being able to connect to each other over the network.

Replacing computers

If the computer that protected the network has been replaced and there are not any computers that have access (you cannot access the network), reset the wireless router or access point to its factory defaults and protect your network again.

Software not working after upgrading operating systems

If Wireless Home Network Security does not work after upgrading operating systems, uninstall it and then reinstall it.

Glossary

802.11

A set of IEEE standards for wireless LAN technology. 802.11 specifies an over-the-air interface between a wireless client and a base station or between two wireless clients. Several specifications of 802.11 include 802.11a, a standard for up to 54 Mbps networking in the 5GHz band, 802.11b, a standard for up to 11 Mbps networking in the 2.4 GHz band, 802.11g, a standard for up to 54 Mbps networking in the 2.4 GHz band, and 802.11i, a suite of security standards for all wireless Ethernets.

802.11a

An extension to 802.11 that applies to wireless LANs and sends data at up to 54 Mbps in the 5GHz band. Although the transmission speed is faster than 802.11b, the distance covered is much smaller.

802.11b

An extension to 802.11 that applies to wireless LANs and provides 11 Mbps transmission in the 2.4 GHz band. 802.11b is currently considered the wireless standard.

802.11g

An extension to 802.11 that applies to wireless LANs and provides up to 54 Mbps in the 2.4 GHz band.

802.1x

Not supported by Wireless Home Network Security. An IEEE standard for authentication on wired and wireless networks, but is most notably used in conjunction with 802.11 wireless networking. This standard provides strong, mutual authentication between a client and an authentication server. In addition, 802.1x can provide dynamic per-user, per-session WEP keys, removing the administrative burden and security risks surrounding static WEP keys.

A

Access Point (AP)

A network device that allows 802.11 clients to connect to a local area network (LAN). APs extend the physical range of service for a wireless user. Sometimes referred to as wireless router.

Authentication

The process of identifying an individual, usually based on a user name and password. Authentication ensures that the individual is who he or she claims to be, but says nothing about the access rights of the individual.

B

Bandwidth

The amount of data that can be transmitted in a fixed amount of time. For digital devices, the bandwidth is usually expressed in bits per second (bps) or bytes per second. For analog devices, the bandwidth is expressed in cycles per second, or Hertz (Hz).

Brute-Force Attack

Also known as brute force cracking, a trial and error method used by application programs to decode encrypted data such as passwords through exhaustive effort (using brute force) rather than employing intellectual strategies. Just as a criminal might break into, or crack, a safe by trying many possible combinations, a brute force cracking application proceeds through all possible combinations of legal characters in sequence. Brute force is considered to be an infallible, although time-consuming, approach.

C

Cipher Text

Data that has been encrypted. Cipher text is unreadable until it has been converted into plain text (decrypted) with a key.

Client

An application that runs on a personal computer or workstation and relies on a server to perform some operations. For example, an e-mail client is an application that enables you to send and receive e-mail.

D

Denial of Service

On the Internet, a denial of service (DoS) attack is an incident in which a user or organization is deprived of the services of a resource they would normally expect to have. Typically, the loss of service is the inability of a particular network service, such as e-mail, to be available or the temporary loss of all network connectivity and services. In the worst cases, for example, a Web site accessed by millions of people can occasionally be forced to temporarily cease operation. A denial of service attack can also destroy programming and files in a computer system. Although

usually intentional and malicious, a denial of service attack can sometimes happen accidentally. A denial of service attack is a type of security breach to a computer system that does not usually result in the theft of information or other security loss. However, these attacks can cost the target person or company a great deal of time and money.

Dictionary Attack

These attacks involve trying a host of words from a list to determine someone's password. Attackers don't manually try all combinations but have tools that automatically attempt to identify someone's password.

E

Encryption

The translation of data into a secret code. Encryption is the most effective way to achieve data security. To read an encrypted file, a person must have access to a secret key or password that enables them to decrypt it. Data that is not encrypted is called plain text; encrypted data is referred to as cipher text.

ESS (Extended Service Set)

A set of two or more networks that form a single subnetwork.

F

Firewall

A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially an intranet. All messages entering or leaving the intranet pass through the firewall. The firewall examines each message and blocks those that do not meet the specified security criteria. A firewall is considered a first line of defense in protecting private information. For greater security, data can be encrypted.

G

H

Hotspot

A specific geographic location in which an access point (AP) provides public wireless broadband network services to mobile visitors through a wireless network. Hotspots are often located in heavily populated places such as airports, train stations, libraries, marinas, conventions centers, and hotels. Hotspots typically have a short range of access.

I

Integrated Gateway

A device that combines the functions of an access point (AP), router, and firewall. Some devices may also include security enhancements and bridging features.

IP Address

An identifier for a computer or device on a TCP/IP network. Networks using the TCP/IP protocol route messages based on the IP address of the destination. The format of an IP address is a 32-bit numeric address written as four numbers separated by periods. Each number can be zero to 255. For example, 192.168.1.100 could be an IP address.

IP Spoofing

Forging the IP addresses in an IP packet. This is used in many types of attacks including session hijacking. It is also often used to fake the e-mail headers of SPAM so they cannot be properly traced.

J

K

Key

A series of letters and/or numbers used by two devices to authenticate their communication. Both devices must have the key. See also WEP and WPA-PSK.

L

LAN (Local Area Network)

A computer network that spans a relatively small area. Most LANs are confined to a single building or group of buildings. However, one LAN can be connected to other LANs over any distance via telephone and radio waves. A system of LANs connected in this way is called a wide-area network (WAN).

Most LANs connect workstations and personal computers generally through simple hubs or switches. Each node (individual computer) in a LAN has its own CPU with which it executes programs, but it also is able to access data and devices (e.g., printers) anywhere on the LAN. This means that many users can share expensive devices, such as laser printers, as well as data. Users can also use the LAN to communicate with each other, for example, by sending e-mail or engaging in chat sessions.

M**MAC (Media Access Control or Message Authenticator Code)**

For the former, see MAC Address. The latter is a code that is used to identify a given message (e.g., a RADIUS message). The code is generally a cryptographically strong hash of the contents of the message which includes a unique value to insure against replay protection.

MAC Address (Media Access Control Address)

A low-level address assigned to the physical device accessing the network.

Man-in-the-Middle Attack

The attacker intercepts messages in a public key exchange and then retransmits them, substituting their own public key for the requested one, so that the two original parties still appear to be communicating with each other directly. The attacker uses a program that appears to be the server to the client and appears to be the client to the server. The attack may be used simply to gain access to the messages, or enable the attacker to modify them before transmitting them again. The term is derived from the ball game where a number of people try to throw a ball directly to each other while one person in between attempts to catch it.

N**Network**

A collection of Access Points and their associated users, equivalent to an ESS. Information about this network is maintained in McAfee Wireless Home Network Security. See ESS.

NIC (Network Interface Card)

A card that plugs into a laptop or other device and connects the device to the LAN.

O**P****PCI Wireless Adapter Cards**

Connects a desktop computer to a network. The card plugs into a PCI expansion slot inside the computer.

PPPoE

Point-to-Point Protocol Over Ethernet. Used by many DSL providers, PPPoE supports the protocol layers and authentication widely used in PPP and enables a point-to-point connection to be established in the normally multipoint architecture of Ethernet.

Plain Text

Any message that is not encrypted.

Protocol

An agreed-upon format for transmitting data between two devices. From a user's perspective, the only interesting aspect about protocols is that their computer or device must support the right ones if they want to communicate with other computers. The protocol can be implemented either in hardware or in software.

Q

R

RADIUS (Remote Access Dial-In User Service)

A protocol that provides for authentication of users, usually in the context of remote access. Originally defined for use with dial-in remote access servers, the protocol is now used in a variety of authentication environments, including 802.1x authentication of a WLAN user's Shared Secret.

Roaming

The ability to move from one AP coverage area to another without interruption in service or loss in connectivity.

Rogue Access Points

An access point that a company does not authorize for operation. The trouble is that a rogue access points often don't conform to wireless LAN (WLAN) security policies. A rogue access point enables an open, insecure interface to the corporate network from outside the physically controlled facility.

Within a properly secured WLAN, rogue access points are more damaging than rogue users. Unauthorized users trying to access a WLAN likely will not be successful at reaching valuable corporate resources if effective authentication mechanisms are in place. Major issues arise, however, when an employee or hacker plugs in a rogue access point. The rogue allows just about anyone with an 802.11-equipped device on the corporate network. This puts them very close to mission-critical resources.

Router

A network device that forwards packets from one network to another. Based on internal routing tables, routers read each incoming packet and decide how to forward it. To which interface on the router outgoing packets are sent may be determined by any combination of source and destination address as well as current traffic conditions such as load, line costs, bad lines. Sometimes referred to as access point (AP).

S

Shared Secret

See also RADIUS. Protects sensitive portions of RADIUS messages. This shared secret is a password that is shared between the authenticator and the authentication server in some secure manner.

SSID (Service Set Identifier)

Network name for the devices in a wireless LAN subsystem. It is a clear text 32-character string added to the head of every WLAN packet. The SSID differentiates one WLAN from another, so all users of a network must supply the same SSID to access a given AP. An SSID prevents access by any client device that does not have the SSID. By default, however, an access point (AP) broadcasts its SSID in its beacon. Even if SSID broadcasting is turned off, a hacker can detect the SSID through sniffing.

SSL (Secure Sockets Layer)

A protocol developed by Netscape for transmitting private documents via the Internet. SSL works by using a public key to encrypt data which is transferred over the SSL connection. Both Netscape Navigator and Internet Explorer use and support SSL, and many Web sites use the protocol to obtain confidential user information, such as credit card numbers. By convention, URLs that require an SSL connection start with https: instead of http:

T

TKIP (Temporal Key Integrity Protocol)

A quick-fix method to overcome the inherent weaknesses in WEP security, especially the reuse of encryption keys. TKIP changes temporal keys every 10,000 packets, providing a dynamic distribution method that significantly enhances the security of the network. The TKIP (security) process begins with a 128-bit temporal key shared among clients and access points (APs). TKIP combines the temporal key with the (client machine's) MAC address and then adds a relatively large 16-octet initialization vector to produce the key that encrypts the data. This procedure ensures that each station uses different key streams to encrypt the data. TKIP uses RC4 to perform the encryption. WEP also uses RC4.

U

USB Wireless Adapter Cards

Provide an expandable Plug and Play serial interface. This interface provides a standard, low-cost wireless connection for peripheral devices such as keyboards, mice, joysticks, printers, scanners, storage devices, and video conference cameras.

V

VPN (Virtual Private Network)

A network constructed by using public wires to reunite nodes. For example, there are a number of systems that enable you to create networks using the Internet as the medium for transporting data. These systems use encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted.

W

Wardriver

Interlopers armed with laptops, special software, and some makeshift hardware, who drive through cities, suburbs and business parks in order to intercept wireless LAN traffic.

WEP (Wired Equivalent Privacy)

An encryption and authentication protocol defined as part of the 802.11 standard. Initial versions are based on RC4 ciphers and have significant weaknesses. WEP attempts to provide security by encrypting data over radio waves so that it is protected as it is transmitted from one end point to another. However, it has been found that WEP is not as secure as once believed.

Wi-Fi (Wireless Fidelity)

Used generically when referring to any type of 802.11 network, whether 802.11b, 802.11a, dual-band, etc. The term is used by the Wi-Fi Alliance.

Wi-Fi Certified

Any products tested and approved as Wi-Fi Certified (a registered trademark) by the Wi-Fi Alliance are certified as interoperable with each other, even if they are from different manufacturers. A user with a Wi-Fi Certified product can use any brand of access point (AP) with any other brand of client hardware that also is certified. Typically, however, any Wi-Fi product using the same radio frequency (for example, 2.4GHz for 802.11b or 11g, 5GHz for 802.11a) works with any other, even if not Wi-Fi Certified.

Wi-Fi Alliance

An organization made up of leading wireless equipment and software providers with the mission of (1) certifying all 802.11-based products for inter-operability and (2) promoting the term Wi-Fi as the global brand name across all markets for any 802.11-based wireless LAN products. The organization serves as a consortium, testing laboratory, and clearinghouse for vendors who want to promote inter-operability and the growth of the industry.

While all 802.11a/b/g products are called Wi-Fi, only products that have passed the Wi-Fi Alliance testing are allowed to refer to their products as Wi-Fi Certified (a registered trademark). Products that pass are required to carry an identifying seal on their packaging that states Wi-Fi Certified and indicates the radio frequency band used. This group was formerly known as the Wireless Ethernet Compatibility Alliance (WECA) but changed its name in October 2002 to better reflect the Wi-Fi brand it wants to build.

Wireless adapter

Contains the circuitry to enable a computer or other device to communicate with a wireless router (attach to a wireless network). Wireless adapters can either be built into the main circuitry of a hardware device or they can be a separate add-on that can be inserted into a device through the appropriate port.

WLAN (Wireless Local Area Network)

See also LAN. A local area network using a wireless medium for connection. A WLAN uses high-frequency radio waves rather than wires to communicate between nodes.

WPA (Wi-Fi Protected Access)

A specification standard that strongly increases the level of data protection and access control for existing and future wireless LAN systems. Designed to run on existing hardware as a software upgrade, WPA is derived from, and is compatible with, the IEEE 802.11i standard. When properly installed, it provides wireless LAN users with a high level of assurance that their data remains protected and that only authorized network users can access the network.

WPA-PSK

A special WPA mode designed for home users who do not require strong enterprise-class security and do not have access to authentication servers. In this mode, the home user manually enters the starting password to activate Wi-Fi Protected Access in Pre-Shared Key mode, and should change the pass-phrase on each wireless computer and access point regularly. See also TKIP.

X

Y

Z

Welcome to McAfee VirusScan.

McAfee VirusScan is an anti-virus 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, suspect scripts, hybrid attacks, and other threats.

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 other threats in hard drives, floppy disks, and individual files and folders.

Quarantine — Encrypt and temporarily isolate suspect 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 suspect 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 threats 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 suspect mass-mailing behaviors and stops viruses and worms from spreading through e-mail to other computers.
- **Script monitoring for worm-like activity**
ScriptStopper™ monitors suspect 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 detected files to see how ActiveShield handles possible threats. See *Understanding security alerts* on page 63 for details.

Testing Scan

Before you can test Scan, you must disable ActiveShield to prevent it from detecting the test 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**.
- 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. 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** 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 detected files to see how Scan handles possible threats. See [Understanding threat detections on page 71](#) for details.


Using McAfee VirusScan


This section explains how to use VirusScan.

Using ActiveShield

When ActiveShield is started (loaded into computer memory) and enabled, it is constantly protecting your computer. ActiveShield scans files when they are accessed by either you or your computer. When ActiveShield detects a file, it automatically tries to clean it. 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  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  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 .

If ActiveShield is still configured to start when Windows starts, a message tells you that you are now protected from threats. Otherwise, a dialog box appears that lets you configure ActiveShield to start when Windows starts ([Figure 3-1 on page 54](#)).

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 .

If ActiveShield is still configured to start when Windows starts, your computer will be protected from threats 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 3-1), which is accessible via the McAfee icon  in your Windows system tray.

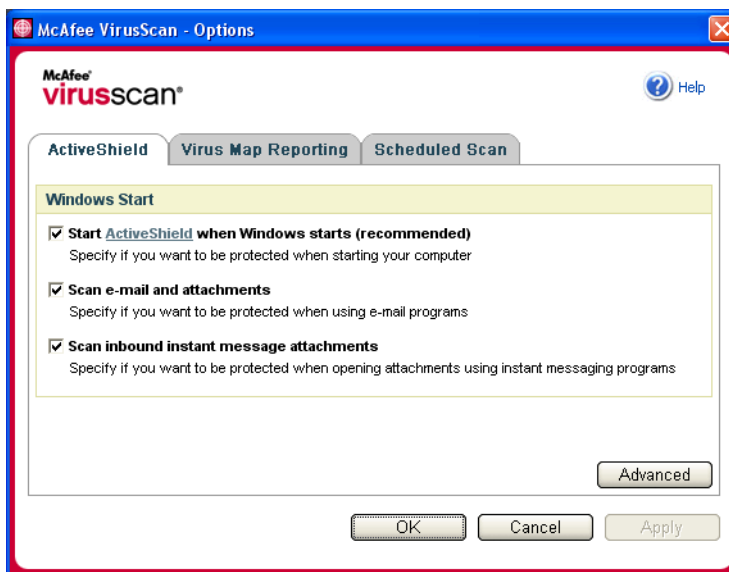




Figure 3-1. ActiveShield Options

Starting ActiveShield

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

If ActiveShield is stopped (denoted by black ), 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 3-1 on page 54).
- 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 threats. 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 3-1 on page 54).
- 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 3-1 on page 54).

When this option is enabled, ActiveShield automatically scans and attempts to clean inbound (POP3) and outbound (SMTP) detected 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 3-2 on page 57) 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 detected, ActiveShield performs the following steps:

- Tries to clean the detected 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 possible threat

Outbound e-mail

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

- Tries to clean the detected 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 3-2).
- 3 Deselect **Inbound e-mail messages** or **Outbound e-mail messages**, then click **OK**.

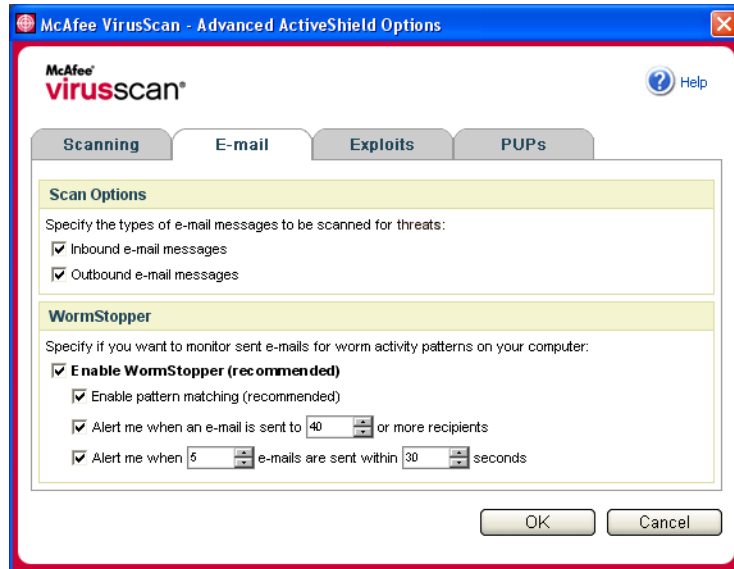


Figure 3-2. Advanced ActiveShield Options - E-mail tab

Scanning for worms

VirusScan monitors your computer for suspect activity that might indicate a threat is present on your computer. While VirusScan cleans viruses and other threats, WormStopper™ 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 suspect activity. Suspect 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 suspect 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 3-3).

By default, the following detailed options are enabled:

- ◆ Pattern matching to detect suspect 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 64 for details):

- ◆ Automatic blocking of suspect outbound e-mails

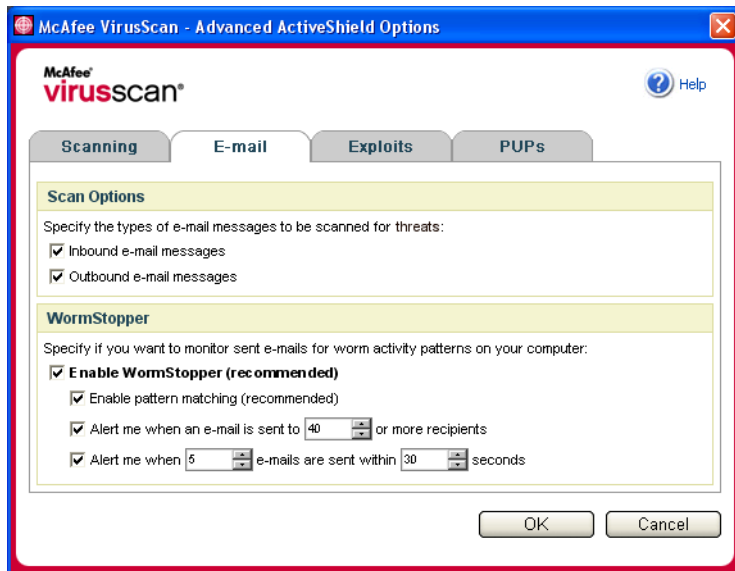


Figure 3-3. Advanced ActiveShield Options - E-mail tab

Scanning inbound instant message attachments

By default, scanning of instant message attachments is enabled via the **Scan inbound instant message attachments** option (Figure 3-1 on page 54).

When this option is enabled, VirusScan automatically scans and attempts to clean inbound detected 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 detected, VirusScan performs the following steps:

- Tries to clean the detected 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 3-4 on page 60).
- 3 Click **All files (recommended)**, then click **OK**.

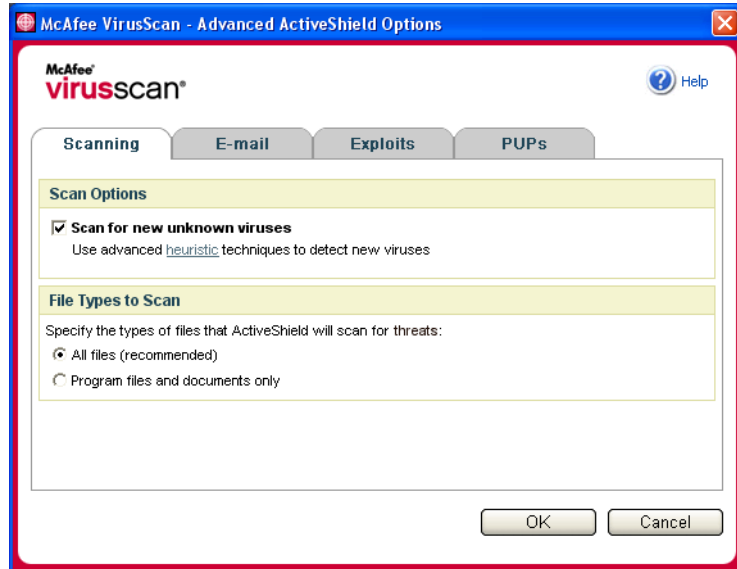


Figure 3-4. Advanced ActiveShield Options - Scanning tab

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 3-4).
- 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 3-4).
- 3 Click **Scan for new unknown viruses (recommended)**, then click **OK**.

Scanning for scripts

VirusScan monitors your computer for suspect activity that might indicate a threat is present on your computer. While VirusScan cleans viruses and other threats, ScriptStopper™ prevents Trojan horses from running scripts that spread viruses further.

A “Trojan horse” is a suspect 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 suspect activity. Suspect 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 suspect 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 3-5).
- 3 Click **Enable ScriptStopper (recommended)**, then click **OK**.

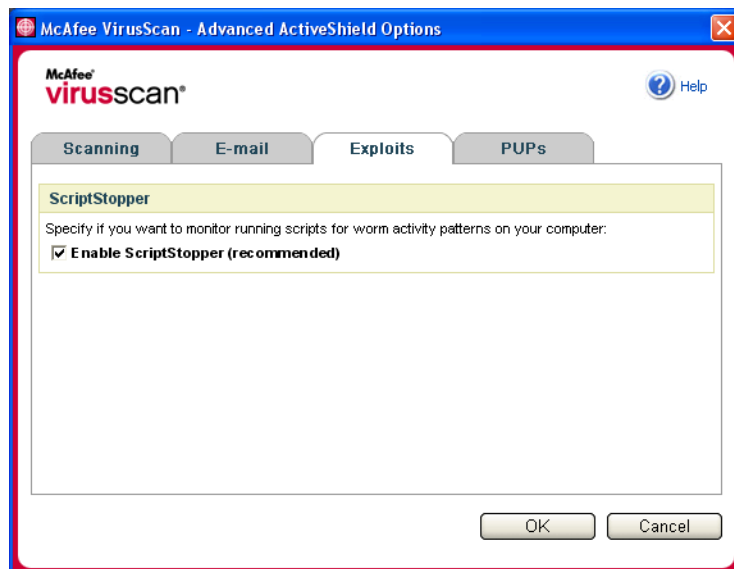


Figure 3-5. Advanced ActiveShield Options - Exploits tab

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 programs that gather and transmit 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 3-6).
- 3 Click **Scan Potentially Unwanted Programs (recommended)**, then click **OK**.

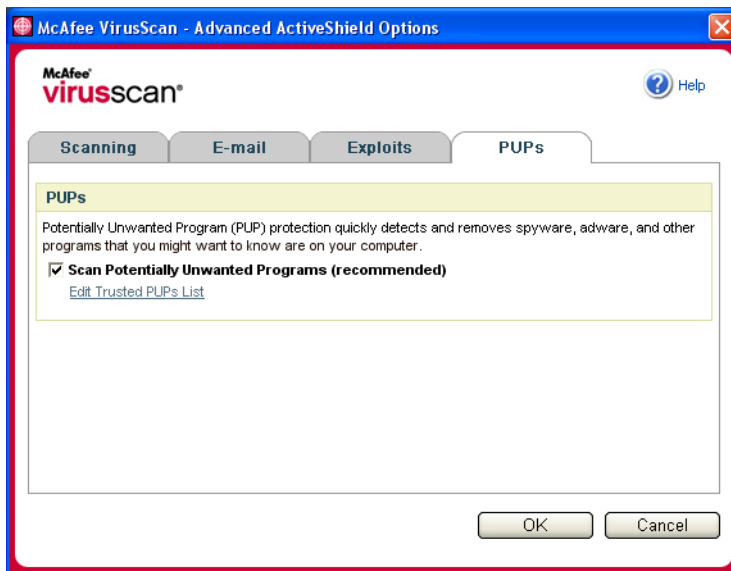


Figure 3-6. Advanced ActiveShield Options - PUPs tab

Understanding security alerts

If ActiveShield finds a virus, a virus alert similar to [Figure 3-7](#) 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.

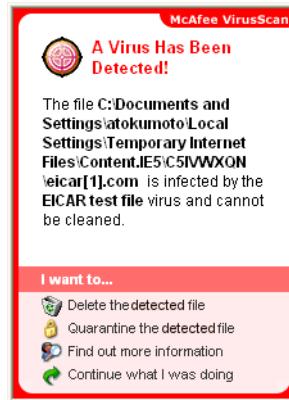


Figure 3-7. Virus alert

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

For added protection, whenever ActiveShield detects a suspect 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 detected 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 detected file.
 - ◆ Click **Continue what I was doing** to ignore the alert and close it.
- 2 If ActiveShield cannot clean the file, click **Quarantine the detected file** to encrypt and temporarily isolate suspect files in the quarantine directory until an appropriate action can be taken.

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

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

Managing detected e-mail

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

Managing suspect scripts

If ActiveShield detects a suspect 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 suspect script.
- ◆ Click **Stop this script** to prevent the suspect 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 suspect activity associated with the detected e-mail message.
- ◆ Click **Stop this e-mail** to prevent the suspect 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 other threats on hard drives, floppy disks, and individual files and folders. When Scan finds a suspect 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**.

The **Scan** dialog box opens (Figure 3-8).

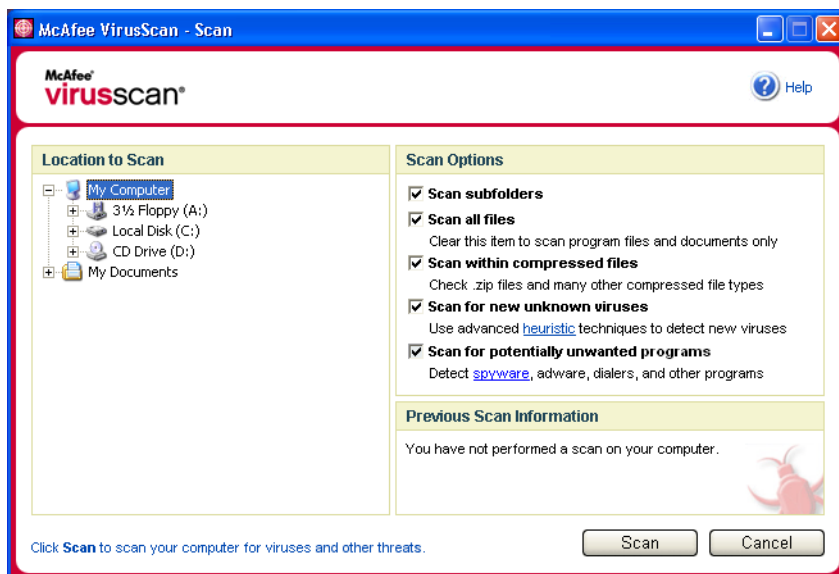


Figure 3-8. Scan dialog box

- 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 3-8):
 - ◆ **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 3-9](#) 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.

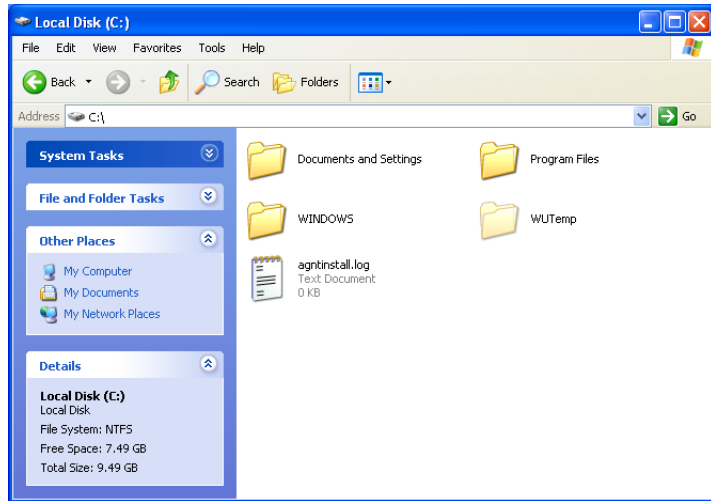


Figure 3-9. Local disk contents

- ◆ **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 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 anti-virus 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, and other programs that gather and transmit your private data without your permission.

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** dialog box (Figure 3-10).

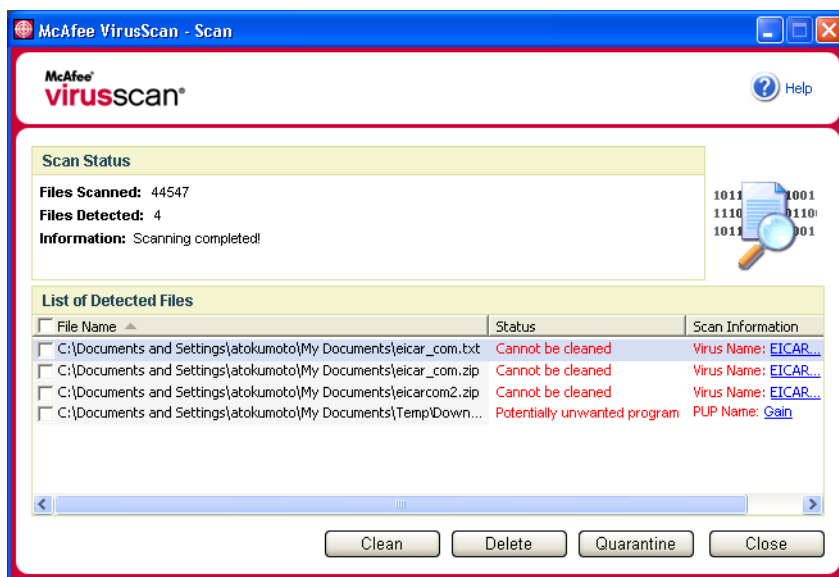


Figure 3-10. Scan results

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 other threats, 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 71](#).

Scanning via Windows Explorer

VirusScan provides a shortcut menu to scan selected files, folders, or drives for viruses and other threats 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**.

The **Scan** 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 3-8 on page 66](#)).

Scanning via Microsoft Outlook

VirusScan provides a toolbar icon to scan for viruses and other threats 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 3-8 on page 66](#)).

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 other threats 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 3-11 on page 70](#)).

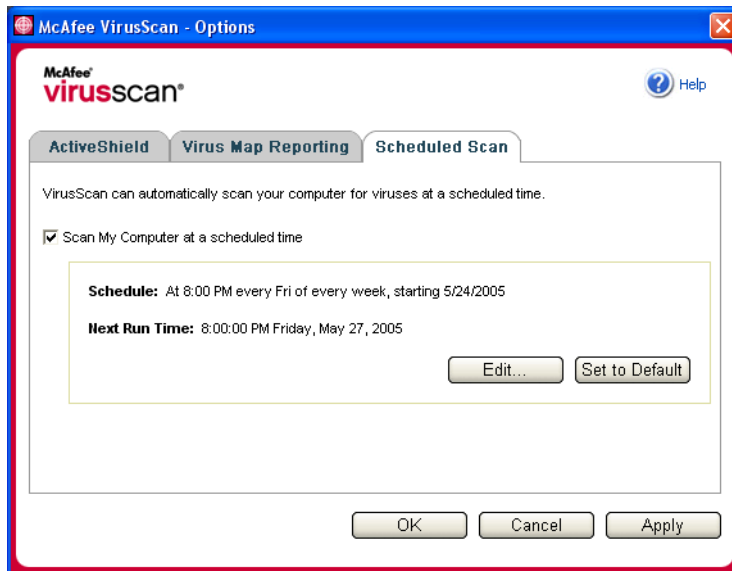


Figure 3-11. Scheduled Scan Options

- 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 suspect files in the quarantine directory until an appropriate action can be taken. (See [Managing quarantined files on page 72](#) 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 74](#) for details.

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

Managing quarantined files

The Quarantine feature encrypts and temporarily isolates suspect 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 3-12).

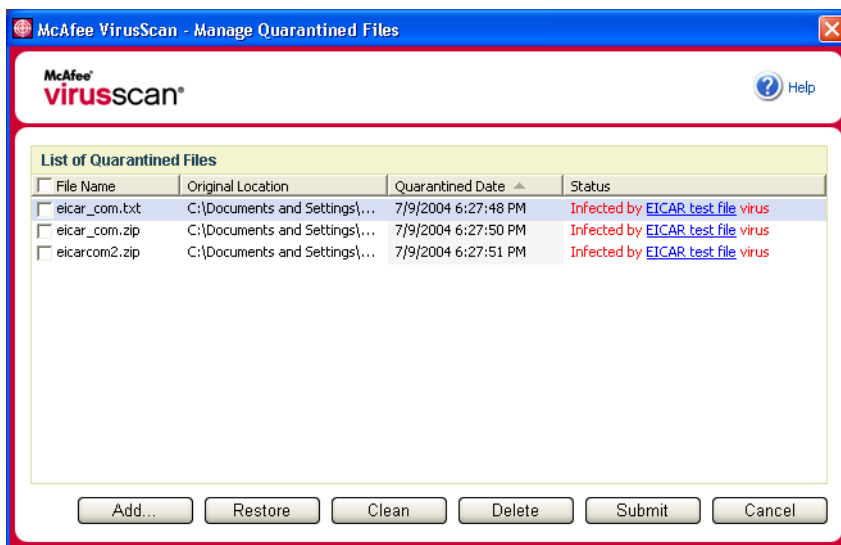


Figure 3-12. Manage Quarantined Files dialog box

- 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 suspect 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™) 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 66 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 3-13).

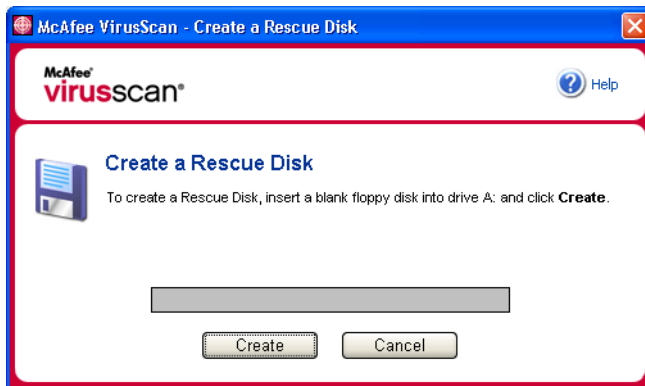


Figure 3-13. Create a Rescue Disk dialog box

- 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 3-14).

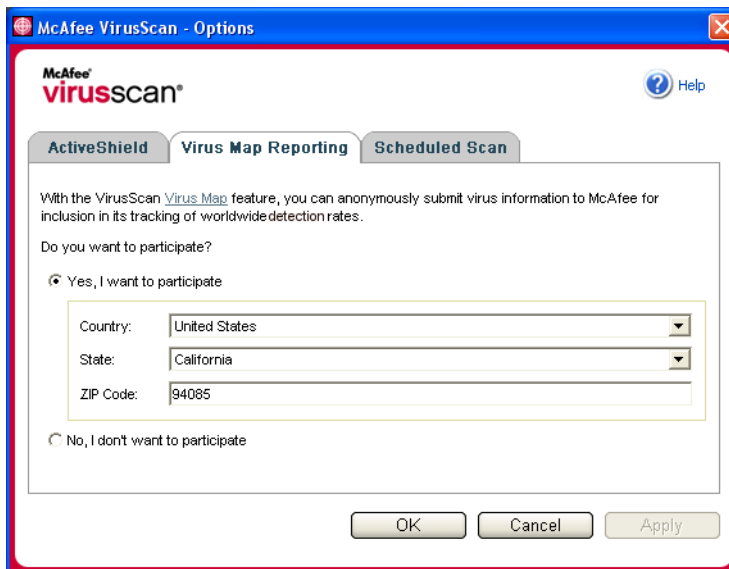


Figure 3-14. Virus Map Reporting Options

- 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 detection 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 detection 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 3-15).

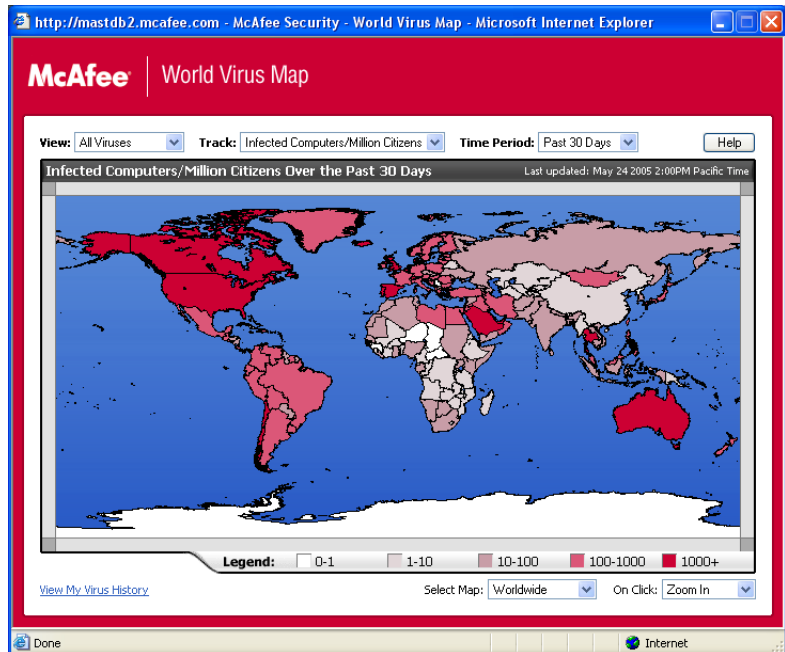


Figure 3-15. World Virus Map

By default, the World Virus Map shows the number of detected 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 detected 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, detected files, and detected 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 3-16 on page 79](#)). 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.



Figure 3-16. 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.

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

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.

Uninstalling other firewalls

Before you install McAfee Personal Firewall Plus software, you must uninstall 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  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 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  in the Windows system tray, and select **Test Firewall**.

Personal Firewall opens Internet Explorer and goes to <http://www.hackerwatch.org/>, a web site maintained by McAfee. Please follow the directions on the Hackerwatch.org Probe page to test Personal Firewall.

Using McAfee Personal Firewall Plus

To open Personal Firewall:

- Right-click the McAfee icon  in the Windows system tray, point to **Personal Firewall**, and select a task.

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 4-1).



Figure 4-1. 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.
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  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	<p>Active Applications shows the bandwidth use of your computer's most active applications during the last twenty-four hours.</p> <p>Application—The application accessing the Internet.</p> <p>%—The percentage of bandwidth used by the application.</p> <p>Permission—The type of Internet access that the application is allowed.</p> <p>Rule Created—When the application rule was created.</p>
What's New?	What's New? shows the latest application that was granted full access to the Internet.
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.

Item	Description
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 4-2).

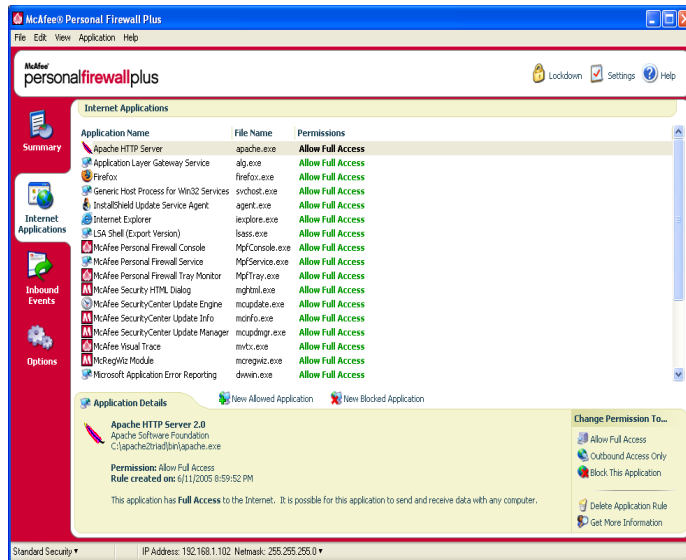


Figure 4-2. Internet Applications page

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  in the Windows system tray, point to **Personal Firewall**, then select **Inbound Events** (Figure 4-3).

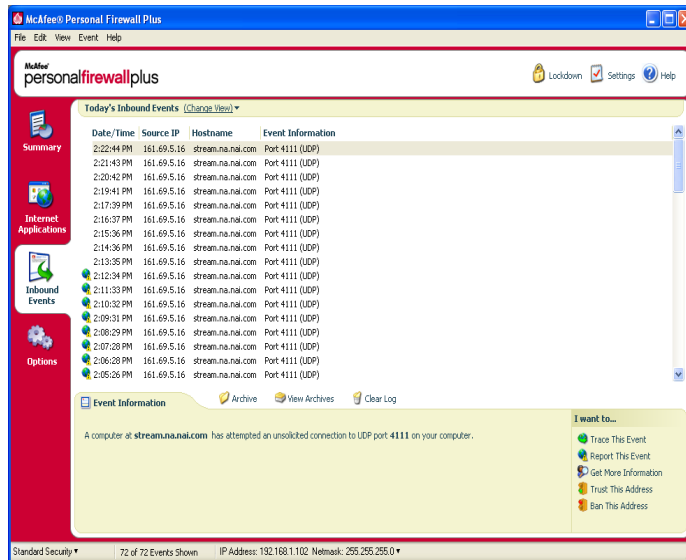


Figure 4-3. Inbound Events page

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

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

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

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 Address**.
- 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 4-4), 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.

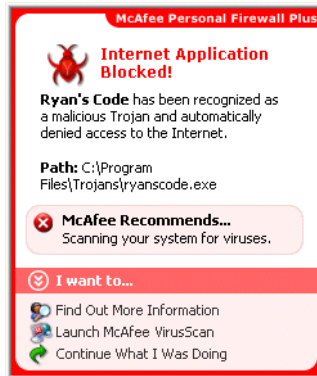


Figure 4-4. Internet Application Blocked alert

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 93](#) 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 4-5) when it detects Internet or network connections for new or modified applications.



Figure 4-5. 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 4-6).

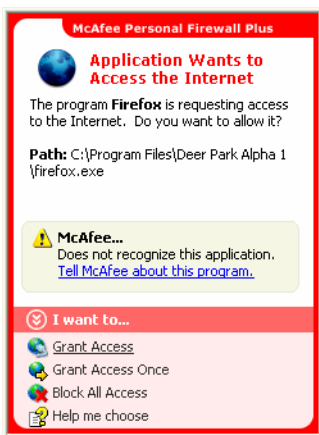


Figure 4-6. Unrecognized Application alert

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 4-7) 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.

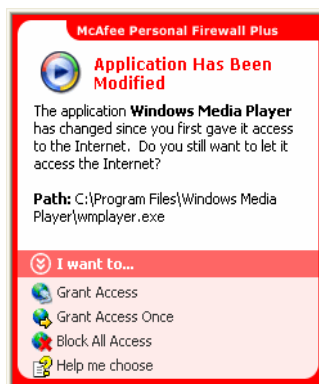


Figure 4-7. Application Has Been Modified alert

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 4-8) when it detects that an application you have previously allowed to access the Internet has requested Internet access as a server.

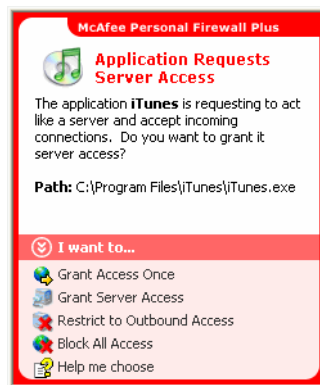


Figure 4-8. Application Requests Server Access alert

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 4-9).

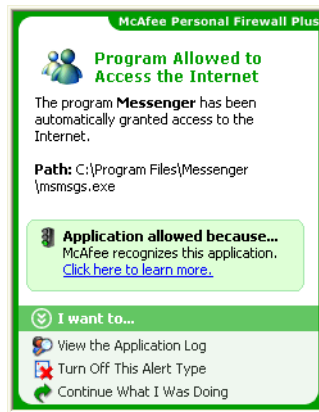


Figure 4-9. Program Allowed to Access the Internet

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 91* 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 91](#) 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 4-10) when it blocks unwanted Internet or network traffic.

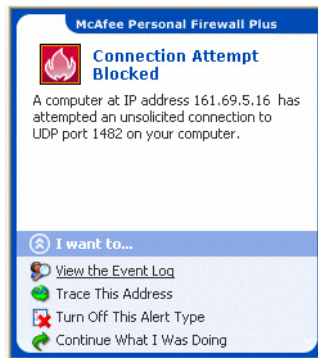


Figure 4-10. Connection Attempt Blocked alert

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 93](#) 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

Index

A

ActiveShield

- cleaning a virus, 63
- default scan setting, 55, 57 to 62
- disabling, 54
- enabling, 53
- scan options, 54
- scanning all file types, 59
- scanning all files, 59
- scanning e-mail and attachments, 55
- scanning for new unknown viruses, 60
- scanning for Potentially Unwanted Programs (PUPs), 62
- scanning for scripts, 61
- scanning for worms, 57
- scanning inbound instant message attachments, 59
- scanning program files and documents only, 60
- starting, 55
- stopping, 55
- testing, 51

advanced settings

- alerts, 23
- other, 23
- security, 23

alerts, 28

- Application Has Been Modified, 104
- Application Requests Internet Access, 104
- Application Requests Server Access, 104
- Connection Attempt Blocked, 111
- for detected e-mail, 64
- for detected files, 63
- for potential worms, 64
- for PUPs, 65
- for suspect scripts, 64
- for viruses, 63
- Internet Application Blocked, 104

New Application Allowed, 109

Available Wireless Networks page, 20

AVERT, submitting suspect files to, 73

C

configuration wizard, using, 17

configuring

VirusScan

- ActiveShield, 53
- Scan, 66

connection, viewing, 18

creating a Rescue Disk, 74

D

default firewall, setting the, 83

E

editing whitelists, 65

e-mail and attachments

- auto-cleaning
 - enabling, 55
- scanning
 - disabling, 56
 - enabling, 55
 - errors, 56

Event Log

- about, 93
- managing, 102
- viewing, 102

events

- about, 93
- archiving the Event Log, 102
- clearing the Event Log, 102
- copying, 103
- deleting, 103
- exporting, 103
- from 0.0.0.0, 94

- from 127.0.0.1, 94
- from computers on your LAN, 95
- from private IP addresses, 95
- HackerWatch.org advice, 98
- loopback, 94
- more information, 98
- reporting, 99
- responding to, 98
- showing
 - all, 96
 - from one address, 97
 - one day's, 97
 - this week's, 96
 - today's, 96
 - with same event info, 98
- tracing
 - understanding, 93
 - viewing archived Event Logs, 102

events, viewing, 22

F

features, 15

G

getting started with VirusScan, 49

H

HackerWatch.org

- advice, 98
- reporting an event to, 99
- signing up, 99

I

inbound instant message attachments

- auto-cleaning, 59
- scanning, 59

Internet applications

- about, 91
- allowing and blocking, 92
- changing application rules, 92

IP addresses

- about, 94
- banning, 100

trusting, 99

K

keys, rotating, 25

L

list of detected files (Scan), 68, 71

M

McAfee SecurityCenter, 11

Microsoft Outlook, 69

N

network

- connecting, 20
- disconnecting, 21
- protecting, 26
- revoking access, 24
- unprotecting, 26
- viewing, 19

new features, 49, 81

O

options

- advanced, 21
- configuring, 22

Options page, 22

options, configuring, 22

P

Personal Firewall

- testing, 86
- using, 86

Potentially Unwanted Programs (PUPs), 62

- alerts, 65
- cleaning, 71
- deleting, 72
- detecting, 71
- quarantining, 71
- removing, 65
- trusting, 65

protecting computers, 25

Q

Quarantine

- adding suspect files, 72
- cleaning files, 72 to 73
- deleting files, 72
- deleting suspect files, 73
- managing suspect files, 72
- restoring cleaned files, 72 to 73
- submitting suspect files, 73

Quick Start Card, iii

R

reporting an event, 99

Rescue Disk

- creating, 74
- updating, 75
- using, 72, 75
- write-protecting, 75

S

Scan

- automatic scanning, 69
- cleaning a virus or Potentially Unwanted Program, 71
- deleting a virus or Potentially Unwanted Program, 72
- manual scanning, 66
- manual scanning via Microsoft Outlook toolbar, 69
- manual scanning via Windows Explorer, 69
- quarantining a virus or Potentially Unwanted Program, 71
- Scan all files option, 67
- Scan for new unknown viruses option, 67
- Scan for Potentially Unwanted Programs option, 68
- Scan subfolders option, 66
- Scan within compressed files option, 67
- testing, 51 to 52

Scan all files option (Scan), 67

Scan for new unknown viruses option (Scan), 67

Scan for Potentially Unwanted Programs option (Scan), 68

scan options

ActiveShield, 54, 59 to 60

Scan, 66

Scan subfolders option (Scan), 66

Scan within compressed files option (Scan), 67

scanning

- all files, 59, 67
- compressed files, 67
- for new unknown viruses, 67
- for Potentially Unwanted Programs (PUPs), 62
- for scripts, 61
- for worms, 57
- program files and documents only, 60
- scheduling automatic scans, 69
- subfolders, 66
- via Microsoft Outlook toolbar, 69
- via Windows Explorer, 69

scheduling scans, 69

scripts

- alerts, 64
- allowing, 64
- stopping, 64

ScriptStopper, 61

settings, repairing, 24

showing events in the Event Log, 96

submitting suspect files to AVERT, 73

Summary Page, 86

Summary page, 18, 20

system requirements, 9

T

technical support, 72

testing Personal Firewall, 86

testing VirusScan, 51

tracing an event, 98

Trojans

- alerts, 63
- detecting, 71

troubleshooting, 30

Trusted PUPs List, 65

U

uninstalling

- other firewalls, 83

Update Wizard, 55

updating

 a Rescue Disk, 75

 VirusScan

 automatically, 78

 manually, 78

updating Wireless Home Network Security

 automatically checking for updates, 26

 manually checking for updates, 26

using a Rescue Disk, 75

V

viruses

 alerts, 63

 allowing suspect scripts, 64

 cleaning, 63, 71

 deleting, 63, 71

 deleting detected files, 63

 detecting, 71

 detecting with ActiveShield, 63

 quarantining, 63, 71

 quarantining detected files, 63

 removing PUPs, 65

 reporting automatically, 75, 77

 stopping potential worms, 64

 stopping suspect scripts, 64

VirusScan

 getting started, 49

 reporting viruses automatically, 75, 77

 scanning via Microsoft Outlook toolbar, 69

 scanning via Windows Explorer, 69

 scheduling scans, 69

 testing, 51

 updating automatically, 78

 updating manually, 78

W

whitelisted programs, 65

whitelisting

 PUPs, 65

Windows Automatic Updates, 104

Windows Explorer, 69

Windows Firewall, 83

Wireless Home Network Security

 introduction, 14

 using, 13

World Virus Map

 reporting, 75

 viewing, 77

worms

 alerts, 63 to 64

 detecting, 63, 71

 stopping, 64

WormStopper, 57

write-protecting a Rescue Disk, 75