



User Guide



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, 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, INC. OR THE PLACE OF PURCHASE FOR A FULL REFUND.

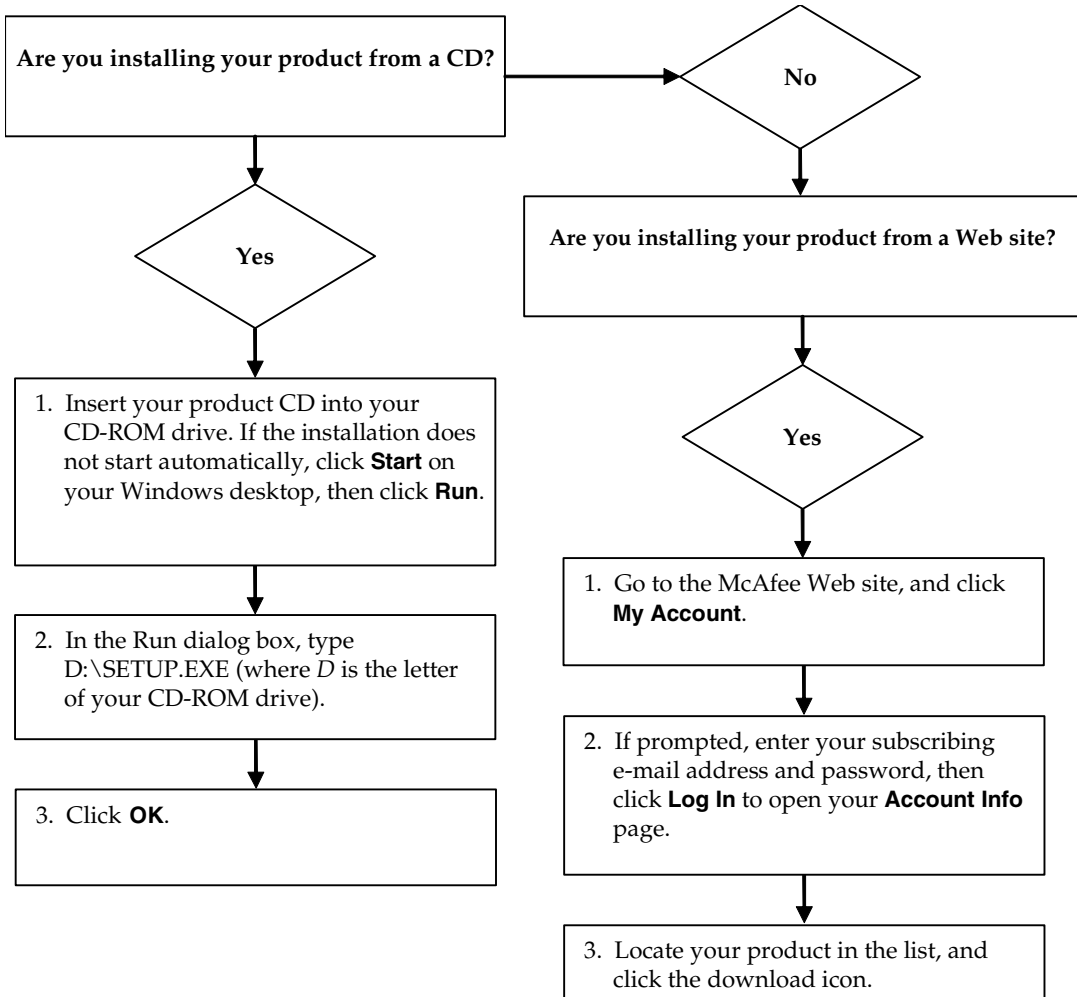
Attributions

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, Inc. 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 Stellent Chicago, Inc. and/or Outside In[®] HTML Export, © 2001 Stellent 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	7
New features	7
System requirements	8
Testing VirusScan	9
Testing ActiveShield	9
Testing Scan	9
Using McAfee SecurityCenter	11
2 Using McAfee VirusScan	13
Using ActiveShield	13
Enabling or disabling ActiveShield	13
Configuring ActiveShield options	14
Understanding security alerts	23
Manually scanning your computer	26
Manually scanning for viruses and other threats	26
Automatically scanning for viruses and other threats	29
Understanding threat detections	31
Managing quarantined files	32
Creating a Rescue Disk	34
Write-protecting a Rescue Disk	35
Using a Rescue Disk	35
Updating a Rescue Disk	35
Automatically reporting viruses	35
Reporting to the World Virus Map	36
Viewing the World Virus Map	37
Updating VirusScan	38
Automatically checking for updates	38
Manually checking for updates	38
Index	41

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.

System requirements

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

NOTE

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

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

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 23 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 31](#) for details.


Using McAfee SecurityCenter

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

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


NOTE

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

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

If one or more of the McAfee 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 VirusScan feature:


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

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 2-1 on page 14](#)).

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 2-1), which is accessible via the McAfee icon  in your Windows system tray.

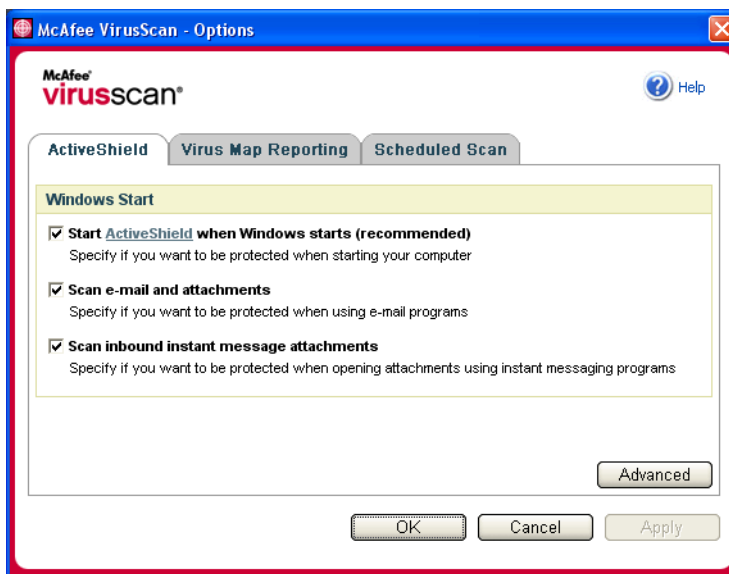




Figure 2-1. ActiveShield Options

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 2-1 on page 14).
- 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 2-1 on page 14).
- 2 Deselect the **Start ActiveShield when Windows starts (recommended)** checkbox, then click **Apply** to save your changes.
- 3 Click **OK** to confirm, then click **OK**.

Scanning e-mail and attachments

By default, e-mail scanning and automatic cleaning are enabled via the **Scan e-mail and attachments** option (Figure 2-1 on page 14).

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 2-2 on page 17) 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 2-2).
- 3 Deselect **Inbound e-mail messages** or **Outbound e-mail messages**, then click **OK**.

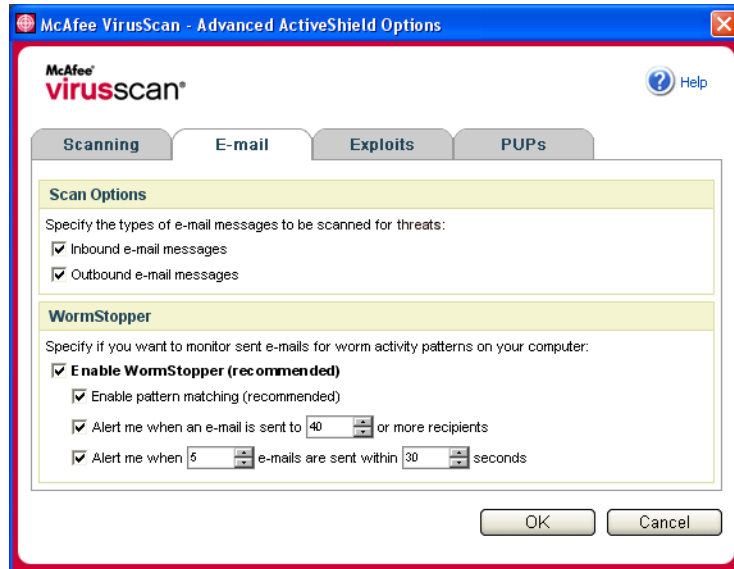


Figure 2-2. Advanced ActiveShield Options - E-mail tab

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 2-3).

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 24 for details):

- ◆ Automatic blocking of suspect outbound e-mails

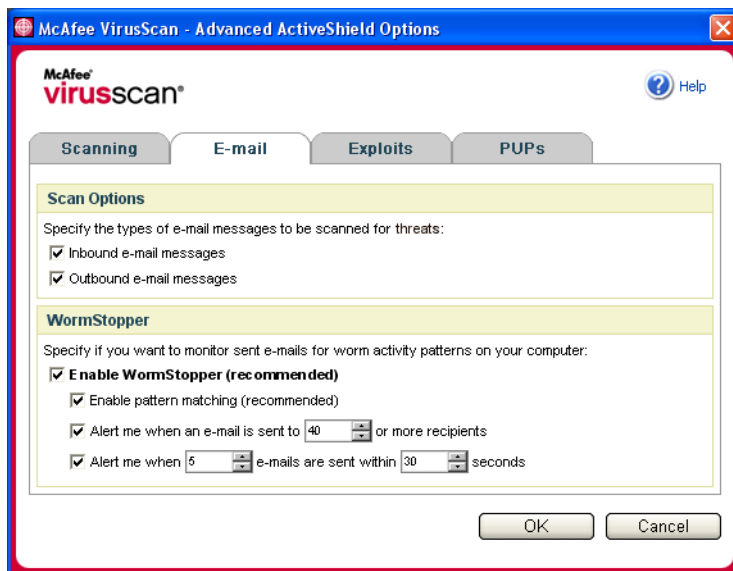


Figure 2-3. Advanced ActiveShield Options - E-mail tab

Scanning inbound instant message attachments

By default, scanning of instant message attachments is enabled via the **Scan inbound instant message attachments** option (Figure 2-1 on page 14).

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 2-4 on page 20).
- 3 Click **All files (recommended)**, then click **OK**.

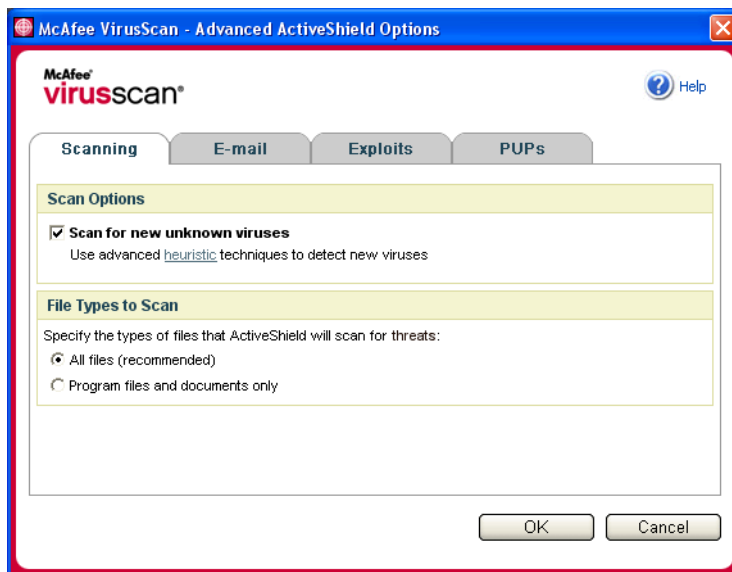


Figure 2-4. Advanced ActiveShield Options - Scanning tab

Scanning program files and documents only

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

- 1 Right-click the McAfee icon, point to **VirusScan**, and then click **Options**.
- 2 Click **Advanced**, then click the **Scanning** tab (Figure 2-4).
- 3 Click **Program files and documents only**, then click **OK**.

Scanning for new unknown viruses

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

To set ActiveShield to scan for new unknown viruses:

- 1 Right-click the McAfee icon, point to **VirusScan**, and then click **Options**.
- 2 Click **Advanced**, then click the **Scanning** tab (Figure 2-4).
- 3 Click **Scan for new unknown viruses (recommended)**, then click **OK**.

Scanning for scripts

VirusScan monitors your computer for 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 2-5).
- 3 Click **Enable ScriptStopper (recommended)**, then click **OK**.

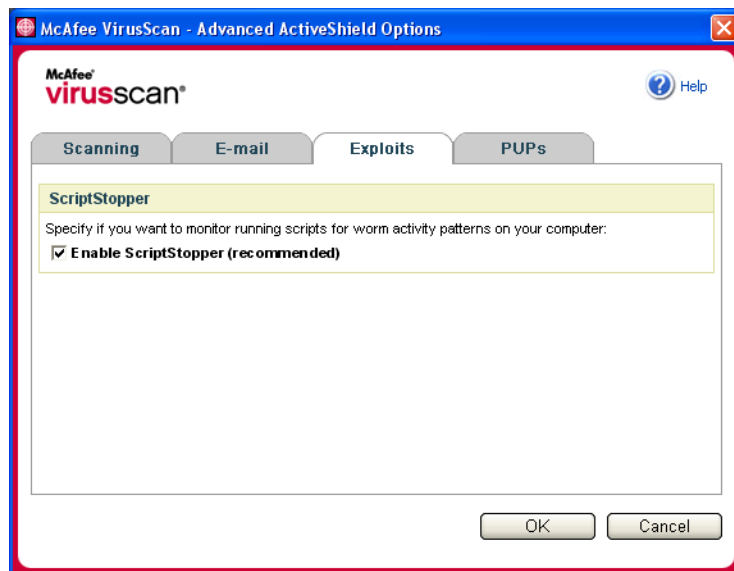


Figure 2-5. Advanced ActiveShield Options - Exploits tab

Scanning for Potentially Unwanted Programs (PUPs)

NOTE

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

If you set ActiveShield to use the default **Scan Potentially Unwanted Programs (recommended)** option in the **Advanced Options** dialog box, Potentially Unwanted Program (PUP) protection quickly detects, blocks, and removes spyware, adware, and other 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 2-6).
- 3 Click **Scan Potentially Unwanted Programs (recommended)**, then click **OK**.

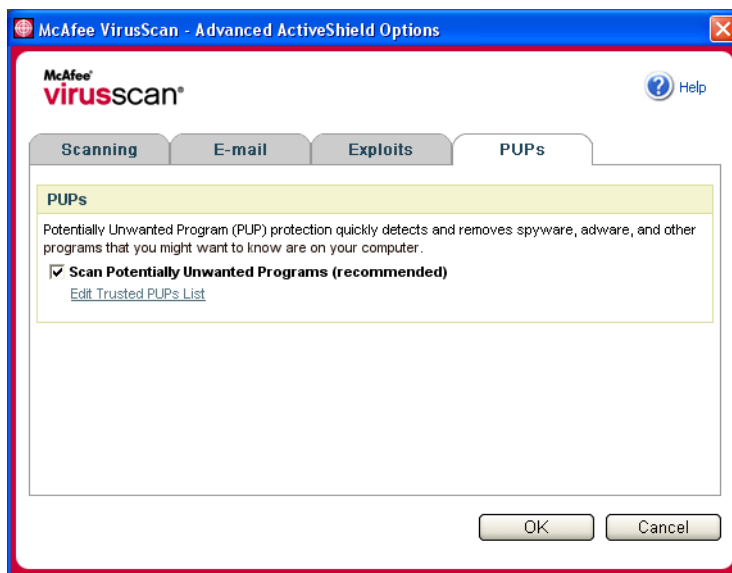


Figure 2-6. Advanced ActiveShield Options - PUPs tab

Understanding security alerts

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

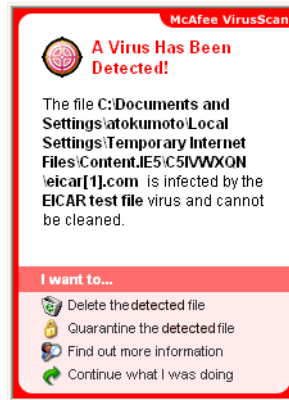


Figure 2-7. Virus alert

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 2-8).



Figure 2-8. 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 2-8):
 - ◆ **Scan subfolders** — Use this option to scan files contained in your subfolders. Deselect this checkbox to allow checking of only the files visible when you open a folder or drive.

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

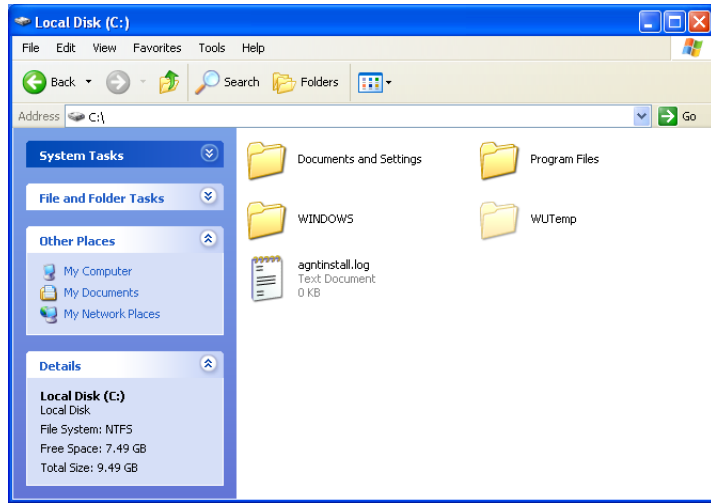


Figure 2-9. Local disk contents

- ◆ **Scan all files** — Use this option to allow the thorough scanning of all file types. Deselect this checkbox to shorten the scanning time and allow checking of program files and documents only.
- ◆ **Scan within compressed files** — Use this option to reveal hidden 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 2-10).

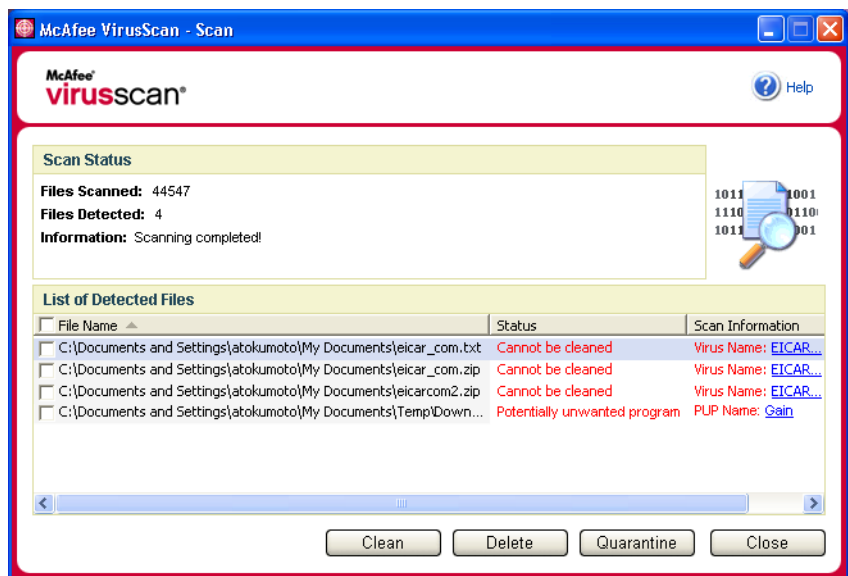


Figure 2-10. Scan results

NOTE

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

- 6 If Scan finds no viruses or 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 31](#).

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 2-8 on page 26](#)).

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 2-8 on page 26](#)).

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 2-11 on page 30](#)).

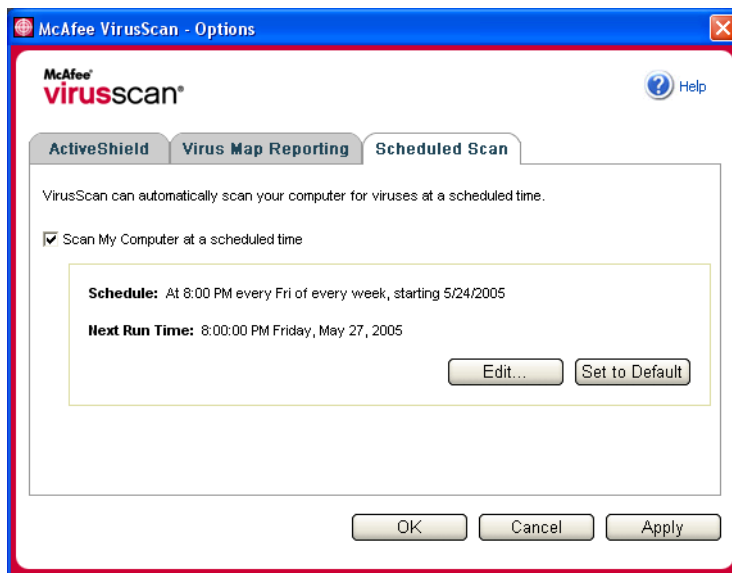


Figure 2-11. Scheduled Scan Options

- 3 Select the **Scan My Computer at a scheduled time** checkbox to enable automatic scanning.
- 4 Specify a schedule for automatic scanning:
 - ◆ To accept the default schedule (8PM every Friday), click **OK**.
 - ◆ To edit the schedule:
 - a. Click **Edit**.
 - b. Select how often to scan your computer in the **Schedule Task** list, and then select additional options in the dynamic area below it:
 - Daily** - Specify the number of days between scans.
 - Weekly** (the default) - Specify the number of weeks between scans as well as the names of the day(s) of the week.
 - Monthly** - Specify which day of the month to scan. Click **Select Months** to specify which months to scan, and click **OK**.
 - Once** - Specify which date to scan.

NOTE

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

- c. Select the time of day to scan your computer in the **Start time** box.
- d. To select advanced options, click **Advanced**.

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

- i. Specify a start date, end date, duration, end time, and whether to stop the task at the specified time if the scan is still running.
 - ii. Click **OK** to save your changes and close the dialog box. Otherwise, click **Cancel**.
- 5 Click **OK** to save your changes and close the dialog box. Otherwise, click **Cancel**.
 - 6 To revert to the default schedule, click **Set to Default**. Otherwise, click **OK**.

Understanding threat detections

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

To manage a virus or potentially unwanted program:

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

NOTE

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

- 2 If the file is a Potentially Unwanted Program, you can click **Clean** to try to clean it.
- 3 If Scan cannot clean the file, you can click **Quarantine** to encrypt and temporarily isolate suspect files in the quarantine directory until an appropriate action can be taken. (See [Managing quarantined files on page 32](#) 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 34](#) 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 2-12](#)).

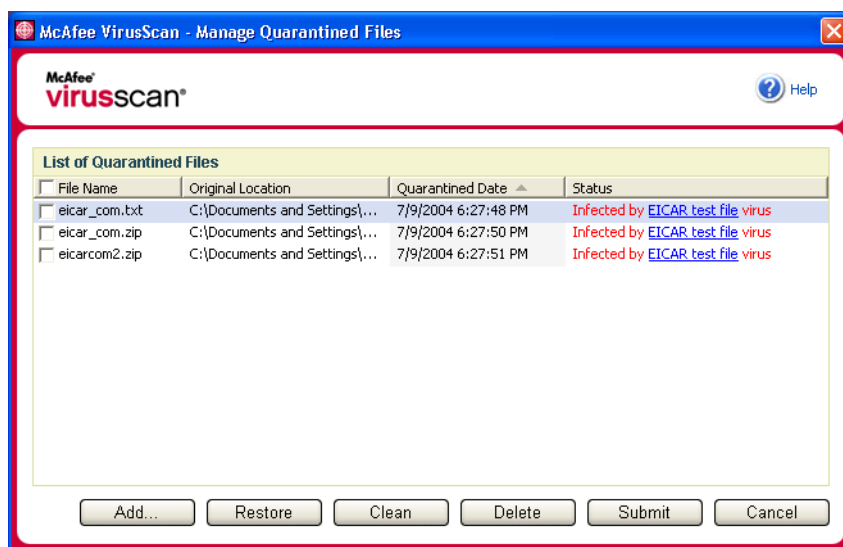


Figure 2-12. Manage Quarantined Files dialog box

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

NOTE

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

Or, click **Add**, select a 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 26](#) for details.)
- 2 Right-click the McAfee icon, point to **VirusScan**, then click **Create Rescue Disk**.

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

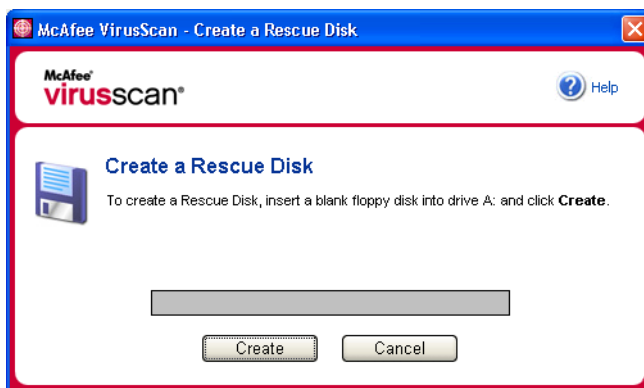


Figure 2-13. Create a Rescue Disk dialog box

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

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

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

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

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

- 5 When the message "Rescue disk created" appears, click **OK**, then close the **Create Rescue Disk** dialog box.
- 6 Remove the Rescue Disk from the drive, write-protect it, and store it in a safe location.

Write-protecting a Rescue Disk

To write-protect a Rescue Disk:

- 1 Turn the floppy disk label-side down (the metal circle should be visible).
- 2 Locate the write-protect tab. Slide the tab so the hole is visible.

Using a Rescue Disk

To use a Rescue Disk:

- 1 Turn off the infected computer.
- 2 Insert the Rescue Disk into the drive.
- 3 Turn the computer on.

A gray window with several options appears.
- 4 Choose the option that best suits your needs by pressing the Function keys (for example, F2, F3).

NOTE

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

Updating a Rescue Disk

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

Automatically reporting viruses

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

Reporting to the World Virus Map

To automatically report virus information to the World Virus Map:

- 1 Right-click the McAfee icon, point to **VirusScan**, then click **Options**.
The **VirusScan Options** dialog box opens.
- 2 Click the **Virus Map Reporting** tab (Figure 2-14).

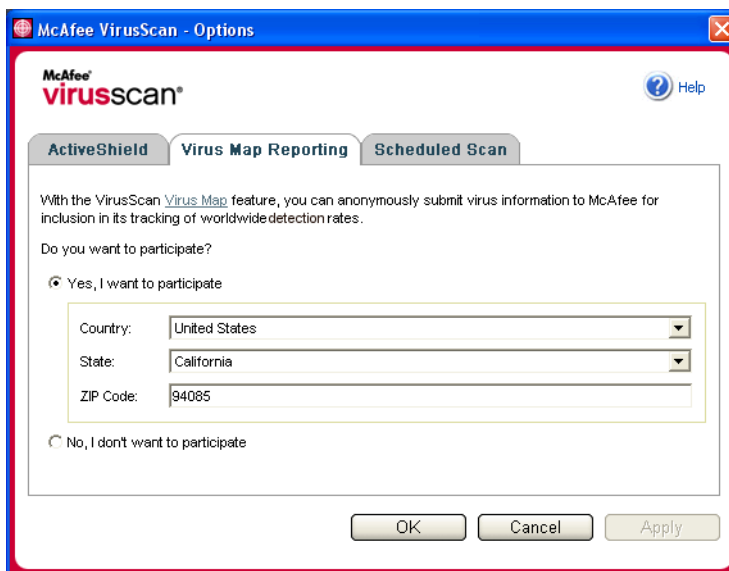


Figure 2-14. Virus Map Reporting Options

- 3 Accept the default **Yes, I want to participate** to anonymously send your virus information to McAfee for inclusion in its World Virus Map of worldwide 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 2-15).

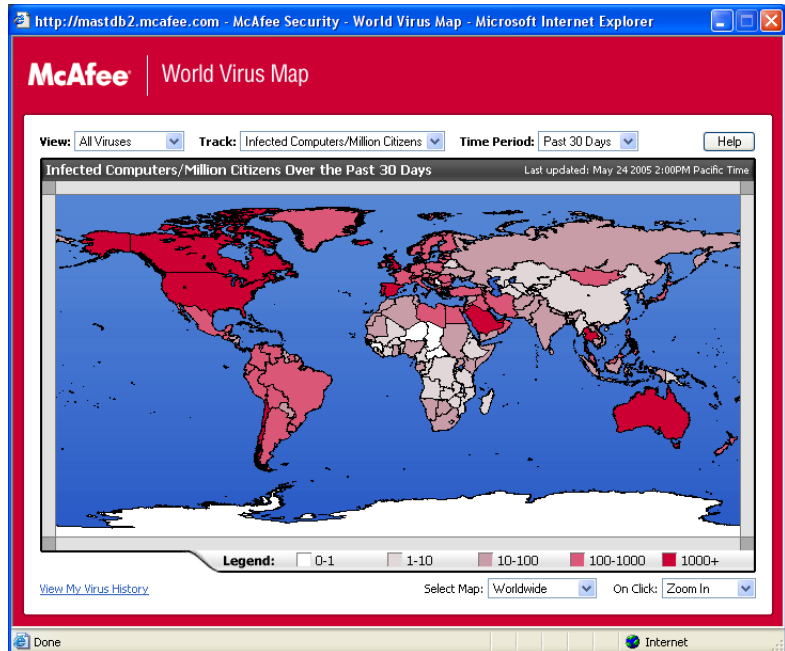


Figure 2-15. World Virus Map

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 2-16 on page 39](#)). 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.

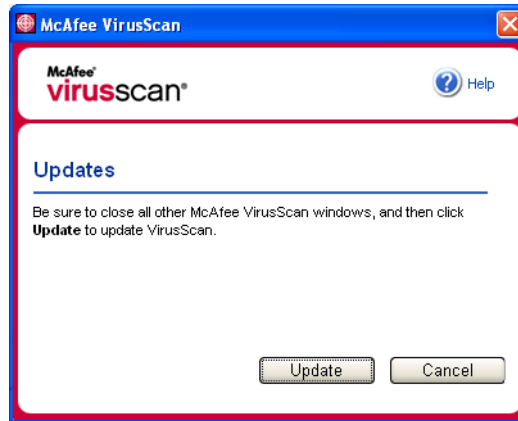


Figure 2-16. Updates dialog box

- 4 Log on to the web site if prompted. The **Update Wizard** installs the update automatically.
- 5 Click **Finish** when the update is finished installing.

NOTE

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

Index

A

- ActiveShield
 - cleaning a virus, 23
 - default scan setting, 15, 17 to 22
 - disabling, 14
 - enabling, 13
 - scan options, 14
 - scanning all file types, 19
 - scanning all files, 19
 - scanning e-mail and attachments, 15
 - scanning for new unknown viruses, 20
 - scanning for Potentially Unwanted Programs (PUPs), 22
 - scanning for scripts, 21
 - scanning for worms, 17
 - scanning inbound instant message attachments, 19
 - scanning program files and documents only, 20
 - starting, 15
 - stopping, 15
 - testing, 9

alerts

- for detected e-mail, 24
- for detected files, 23
- for potential worms, 24
- for PUPs, 25
- for suspect scripts, 24
- for viruses, 23

AVERT, submitting suspect files to, 33

C

- configuring
 - VirusScan
 - ActiveShield, 13
 - Scan, 26
- creating a Rescue Disk, 34

E

- editing whitelists, 25
- e-mail and attachments
 - auto-cleaning
 - enabling, 15
 - scanning
 - disabling, 16
 - enabling, 15
 - errors, 16

G

getting started with VirusScan, 7

I

- inbound instant message attachments
 - auto-cleaning, 19
 - scanning, 19

L

list of detected files (Scan), 28, 31

M

- McAfee SecurityCenter, 11
- Microsoft Outlook, 29

N

new features, 7

P

- Potentially Unwanted Programs (PUPs), 22
 - alerts, 25
 - cleaning, 31
 - deleting, 32
 - detecting, 31
 - quarantining, 31
 - removing, 25
 - trusting, 25

Q

Quarantine

- adding suspect files, 32
- cleaning files, 32 to 33
- deleting files, 32
- deleting suspect files, 33
- managing suspect files, 32
- restoring cleaned files, 32 to 33
- submitting suspect files, 33

Quick Start Card, iii

R

Rescue Disk

- creating, 34
- updating, 35
- using, 32, 35
- write-protecting, 35

S

Scan

- automatic scanning, 29
 - cleaning a virus or Potentially Unwanted Program, 31
 - deleting a virus or Potentially Unwanted Program, 32
 - manual scanning, 26
 - manual scanning via Microsoft Outlook toolbar, 29
 - manual scanning via Windows Explorer, 29
 - quarantining a virus or Potentially Unwanted Program, 31
 - Scan all files option, 27
 - Scan for new unknown viruses option, 27
 - Scan for Potentially Unwanted Programs option, 28
 - Scan subfolders option, 26
 - Scan within compressed files option, 27
 - testing, 9 to 10
- Scan all files option (Scan), 27
 - Scan for new unknown viruses option (Scan), 27
 - Scan for Potentially Unwanted Programs option (Scan), 28

scan options

- ActiveShield, 14, 19 to 20
- Scan, 26

Scan subfolders option (Scan), 26

Scan within compressed files option (Scan), 27

scanning

- all files, 19, 27
- compressed files, 27
- for new unknown viruses, 27
- for Potentially Unwanted Programs (PUPs), 22
- for scripts, 21
- for worms, 17
- program files and documents only, 20
- scheduling automatic scans, 29
- subfolders, 26
- via Microsoft Outlook toolbar, 29
- via Windows Explorer, 29

scheduling scans, 29

scripts

- alerts, 24
- allowing, 24
- stopping, 24

ScriptStopper, 21

submitting suspect files to AVERT, 33

system requirements, 8

T

technical support, 32

testing VirusScan, 9

Trojans

- alerts, 23
- detecting, 31

Trusted PUPs List, 25

U

Update Wizard, 15

updating

- a Rescue Disk, 35
- VirusScan
 - automatically, 38
 - manually, 38

using a Rescue Disk, 35

V

viruses

- alerts, 23
- allowing suspect scripts, 24
- cleaning, 23, 31
- deleting, 23, 31
- deleting detected files, 23
- detecting, 31
- detecting with ActiveShield, 23
- quarantining, 23, 31
- quarantining detected files, 23
- removing PUPs, 25
- reporting automatically, 35, 37
- stopping potential worms, 24
- stopping suspect scripts, 24

VirusScan

- getting started, 7
- reporting viruses automatically, 35, 37
- scanning via Microsoft Outlook toolbar, 29
- scanning via Windows Explorer, 29
- scheduling scans, 29
- testing, 9
- updating automatically, 38
- updating manually, 38

W

whitelisted programs, 25

whitelisting

- PUPs, 25

Windows Explorer, 29

World Virus Map

- reporting, 35
- viewing, 37

worms

- alerts, 23 to 24
- detecting, 23, 31
- stopping, 24

WormStopper, 17

write-protecting a Rescue Disk, 35