

User's Guide

VirusScan for Windows 3.1x

McAfee, Inc.

2710 Walsh Avenue
Santa Clara, CA 95051-0963

Phone: (408) 988-3832
Monday - Friday
6:00 A.M. - 6:00 P.M.

FAX: (408) 970-9727
BBS: (408) 988-4004

COPYRIGHT

Copyright © 1996 by 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.

TRADEMARK NOTICES

McAfee, McAfee Associates, VirusScan, NetShield, and Site Meter are registered trademarks of McAfee Associates, Inc. WebScan, SiteExpress, BootShield, ServerStor, ScreenScan, PCCrypto, WebCrypto, Remote Desktop 32, eMail-It, WebShield, GroupScan, GroupShield, NetCrypto, and NetRemote are trademarks of McAfee Associates, Inc. All other products or services mentioned in this document are identified by the trademarks or service marks of their respective companies or organizations.

“SABRE” is a trademark of American Airlines, Inc. and is licensed for use to McAfee. Saber Software is not affiliated with American Airlines, Inc. or SABRE Travel Information Network. All trademarks are the property of their respective owners.

FEEDBACK

McAfee appreciates your comments and reserves the right to use any information you supply in any way it believes appropriate without incurring any obligations whatsoever. Please address your comments to: McAfee, Inc., Documentation, 2710 Walsh Avenue, Santa Clara, CA 95051-0963, or send a fax to McAfee Documentation at (408) 653-3143.

Table of Contents

Chapter 1. Introducing VirusScan.....	5
What is VirusScan?.....	5
How To Contact Us	8
Chapter 2. Installing VirusScan.....	11
Before You Start.....	11
Installation Procedure	12
Chapter 3. On-access Scanning.....	14
What is On-access Scanning?.....	14
Starting VShield	15
Configuring On-access Scanning	17
Chapter 4. On-demand Scanning.....	25
What is On-demand Scanning?	25
Starting VirusScan	26
Selecting Items To Scan	29
Selecting On-demand Scanning Options.....	31
Setting Up and Using Profiles.....	41
Scheduling Scans	44
Using the VirusScan Activity Log	46
Displaying the Virus List.....	47
Chapter 5. Removing a Virus.....	49
If You Suspect You Have a Virus	49

If VirusScan Detects a Virus	51
Appendix A. Preventing Virus Infection	53
Keys to a Secure System Environment	53
Detecting New and Unknown Viruses.....	55
Making a Clean Start-up Diskette	58
Write Protecting a Diskette	61
Appendix B. Understanding Viruses	63
Computer Virus Primer	63
McAfee Virus Information Library.....	68
Appendix C. Testing Your Installation	69
Appendix D. McAfee Support Services	70
Customer Service Programs.....	71
Professional Services Programs.....	74
Appendix E. Reference	77
VirusScan Command-line Options.....	77
VirusScan DOS Error Levels	88
VSH File Format	90
Glossary	99
Index	105

Introducing VirusScan

What is VirusScan?

VirusScan is McAfee's powerful desktop anti-virus solution. Once installed, VirusScan continuously monitors your system for virus activity using its on-access component, VShield. If a virus is detected, you can automatically take action to remove the virus, move infected files to another location, or delete the infected files. VirusScan can also be user-initiated to scan a file, folder, disk, or volume.

VirusScan is an important element of a comprehensive security program that includes a variety of safety measures, such as regular backups, meaningful password protection, training, and awareness. We urge you to set up and comply with such a security program as a preventive measure to protect against future infection. For tips on creating a secure environment, see [Appendix A, "Preventing Virus Infection."](#)

Main Features

- NCSA-certified scanner assures detection of more than 90% of the viruses identified by the National Computer Security Association and 100% of the viruses found "in the wild." See the NCSA website, www.NCSA.com, for certification status.
- VShield, VirusScan's on-access scanner, provides real-time identification of both known and unknown viruses upon file access, create, copy, rename, and run; and system startup.
- On-demand scanning provides for user-initiated detection of known boot, file, multi-partite, stealth, encrypted, and polymorphic viruses located within files, drives, and diskettes.

- Code Trace™, Code Poly™, and Code Matrix™ Scanning employ McAfee's proprietary technologies for pinpoint virus identification accuracy.
- VirusScan can be configured for an automated response on virus detection, including logging, deletion, isolation, or cleaning.
- VirusScan for Windows 3.1x includes a scheduler to set up daily, weekly, or monthly scans.
- Monthly updates of virus signatures and product upgrades are included with the purchase of a McAfee subscription license to assure the best detection and removal rates.

How virus detection works

VirusScan monitors your computer and searches for characteristics (sequences of code) unique to each known virus. If a virus is detected, VirusScan alerts you of its presence. For viruses that are encrypted or mutated, VirusScan uses algorithms for detection that rely on statistical analysis, heuristics, and code disassembly.

When should I scan for viruses?

VirusScan's on-access scanner will perform automatic scans of your system every time you access, create, copy, rename, or run a file, or start up your system. It also protects your system against viruses when you upload and download from networks.

For maximum protection, you should also use VirusScan's on-demand scanning feature to scan for viruses whenever you add files to your system. If you copy files from a diskette or download files from an online service, you should run VirusScan to ensure that a virus has not been introduced.

Scan when you insert an unknown diskette

Every time you insert an unknown diskette in your drive, scan it before executing, installing, or copying its files.

Scan when you install or download new files

Every time you install new software on your hard drive or download executable files from an online service, run VirusScan to check the files before you use them.

Scan on a regular basis

Perform on-demand scans of your system regularly, from as frequently as once a day to once a month, depending on how susceptible your system is to virus infection. Schedule scans of your most vulnerable system areas for maximum security.

How To Contact Us

Customer service

To order products or obtain product information, we invite you to contact our Customer Care department at (408) 988-3832 or at the following address:

McAfee, Inc.
2710 Walsh Avenue
Santa Clara, CA 95051-0963
U.S.A.

Technical support

McAfee is famous for its dedication to customer satisfaction. McAfee has continued this tradition by investing considerable time and effort to make our website a valuable resource for updating McAfee software and obtaining the latest news and information. For technical support information and issues, we encourage you to visit our website first.

World Wide Web <http://www.mcafee.com>

If you do not find what you need or do not have access to the Web, try one of McAfee's automated services.

Automated Voice (408) 988-3034
and Fax Response
System

Internet support@mcafee.com

McAfee BBS (408) 988-4004
1200 bps to 28,800 bps
8 bits, no parity, 1 stop bit
24 hours, 365 days a year

CompuServe GO MCAFEE

America Online	keyword MCAFEE
Microsoft Network (MSN)	MCAFEE

If the automated services did not solve your problem, you may contact McAfee Monday through Friday between 6:00 A.M. and 6:00 P.M. Pacific time.

Phone	(408) 988-3832
Fax	(408) 970-9727

To speed the process of helping you use our products, please note the following before you call:

- Product name and version
- Computer brand, model, and any additional hardware
- Operating system type and version
- Network type and version
- Contents of your AUTOEXEC.BAT, CONFIG.SYS, and system LOGIN script
- Specific steps to reproduce the problem, if applicable

McAfee training

For information about scheduling on-site training for any McAfee product, call (800) 338-8754.

International contact information

To contact McAfee outside the United States, use the addresses and numbers below.

McAfee Canada

178 Main Street
Unionville, Ontario
Canada L3R 2G9
Phone: (905) 479-4189
Fax: (905) 479-4540

McAfee Europe B.V.

Orlyplein 81 - Busitel 1
1043 DS Amsterdam
The Netherlands
Phone: (0) 31 20 6815500
Fax: (0) 31 20 6810229

McAfee France S.A.

50 rue de Londres
75008 Paris
France
Phone: 33 1 44 908733
Fax: 33 1 45 227554

McAfee Deutschland GmbH

Industriestrasse 1
D-82110 Germering
Germany
Phone: 49 89 8943560
Fax: 49 89 89435699

McAfee (UK) Ltd.

Hayley House, London
Road
Bracknell, Berkshire
RG12 2TH United Kingdom
Phone: 44 1344 304730
Fax: 44 1344 306902

2

Installing VirusScan

Before You Start

Take the steps below to prepare for installation of VirusScan and minimize the risk of spreading viruses that may already be present on your system.


Step	Action
1.	Review the system requirements for VirusScan.
2.	Ensure that your system is virus-free. If you suspect that your system is already infected, follow the procedure for cleaning it before beginning the installation procedure. See “If You Suspect You Have a Virus” on page 49.

System requirements

- IBM-compatible personal computer running Windows 3.1x: 386 or better
- 2MB hard drive space
- 8MB of available memory

Installation Procedure

Follow the procedure below to install VirusScan for Windows 3.1x on your system.

 *If you suspect that your system is already infected by a virus, see “If You Suspect You Have a Virus” on page 49 before beginning this installation procedure.*

Step	Action
1.	Start your computer.
2.	Take one of the following steps: <ul style="list-style-type: none">■ If you are installing from diskette or compact disc, insert the VirusScan for Windows 3.1x installation diskette or the CD-ROM.■ If you are installing from files downloaded from a BBS or the McAfee Web Site, decompress the zipped files into a directory on your local drive or the network.
3.	Select Run from the File menu. <ul style="list-style-type: none">■ If you are installing from diskette, type: <code>x:\setup.exe</code> where <i>x</i> is the drive that contains the diskette. Click OK.■ If you are installing from compact disc, type: <code>x:\win3x\setup.exe</code> where <i>x</i> is the drive that contains the CD-ROM. Click OK.■ If you are installing from downloaded files, type: <code>x:\path\setup.exe</code>

where *x:\path* is the location of the files. Click OK.

Response: The Welcome screen is displayed.

4. Click Next to continue.
5. Take one of the following steps:
 - Select Typical to perform a complete installation of VirusScan with the most common options.
 - Select Compact to install VirusScan with the minimum required options.
 - Select Custom to install VirusScan with user-definable options. You will be prompted to Select Components you wish to install.
6. Select a destination directory for your VirusScan files. Enter the directory in the text box provided, or click Browse to navigate to a specific directory. Click Next to continue.
7. When prompted, review your settings and click Next to continue.

Response: VirusScan files are copied to the hard drive.

8. Click Yes to review the What's New text file for information on VirusScan's new features.
9. Review the modifications made to files on your system and click Next.
10. Select Yes to restart your computer for VirusScan to be available and for on-access scanning protection to take effect. Click Finish.

Response: The system restarts. All changes are enabled. VirusScan is now running.

Testing your installation

For information on how to use the Eicar Standard AntiVirus Test File to test your installation of VirusScan, see [Appendix C, "Testing Your Installation."](#)

What is On-access Scanning?

On-access scanning works through a memory-resident program, VShield, which uses a series of VxD (dynamically loaded virtual device driver) modules to provide real-time protection for your system. On-access scanning helps to prevent virus infection by automatically checking programs—such as files, directories, drives, and any media—as they are accessed.

In this chapter, you will find procedures for starting and configuring VShield, VirusScan's on-access scanning component.


Starting VShield

VShield, VirusScan's on-access scanner, is memory resident and, if configured to load at startup, is active in the background when you start up your system. There are two easy methods for ensuring that VShield is active:

- By double-clicking on the VShield Configuration Manager icon, and making sure that the Load VShield at Startup checkbox is selected.
- By double-clicking on VSHWIN.EXE in the installation directory.

Using the VShield Status window

When VShield is enabled, you can configure your scanning options or view the status of files scanned from the VShield Status window (Figure 3-1). To display this window, double-click on the VShield icon on the Desktop.

 *This method requires that the VShield icon is visible on the Desktop. If your VShield icon is not displayed, double-click the VShield Configuration Manager in the Program Manager, and check the box next to Show Icon on the Desktop. VShield options can also be configured directly from this Configuration Manager.*

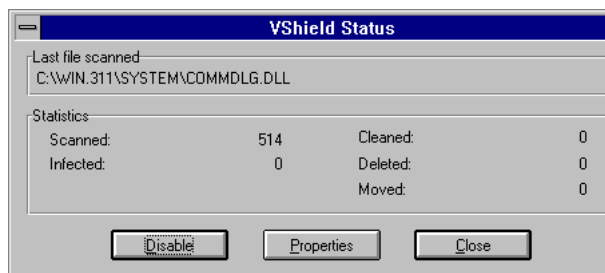


Figure 3-1. VShield Status Window

The VShield Status window displays the name of the last file scanned, information about the number of files that have been scanned, the number of infected files, and any files that have been cleaned, deleted or moved.

In addition, the following options are available:

- **Disable/Enable:** Click this button to either activate (Enable) or deactivate (Disable) on-access scanning during the current Windows session.
- **Properties:** Click this button to configure the detection, action, and reporting settings of on-access scanning. See [“Configuring On-access Scanning” on page 17](#) for more information.
- **Close:** Click this button to close the VShield Status window.

Configuring On-access Scanning

On-access scanning can be configured using the VShield Configuration Manager. Use the following procedure to set up your on-access scanning options.

- | Step | Action |
|------|---|
| 1. | <p>Open the VShield Configuration Manager by taking one of the following steps:</p> <ul style="list-style-type: none">Double-click the VShield Configuration Manager icon.Select Properties from the VShield Status Window. See “Using the VShield Status window” on page 15 for details on displaying this window.Click the VShield icon from the Desktop and select Properties. |



Response: The VShield Configuration Manager is displayed, with the Detection property page on top (Figure 3-2).




**Figure 3-2. VShield Configuration Manager
(Detection Property Page)**

Configuring VShield detection

Use the Detection property page (Figure 3-2) to configure which items should be scanned and when scanning should take place. Take the following steps to configure your detection options:

- | Step | Action |
|------|--|
| 1. | Use the Scan Files On section to select when VShield should scan files. Checkmarks indicate that a scan will be launched when a user attempts to Run, Create, Copy, and/or Rename files. |
| 2. | Use the Scan Disks On section to select when VShield should scan disks. A checkmark indicates that VShield will scan disks on Access. |
| |  <i>McAfee recommends selecting all items in these two sections for maximum protection.</i> |
| 3. | <p>Select which files VShield should scan.</p> <ul style="list-style-type: none"> ■ If you select All Files, all files will be scanned, regardless of file extension. ■ If you select Program Files Only, all files with the extensions specified in the Program Files window will be scanned. <p> <i>Click Program Files to edit the list of file extensions that VShield scans. The default file types are .386 , .BIN, .COM, .EXE, .DLL, .DRV, .VXD, .OVL, .SYS, .DOC, and .DOT.</i></p> |
| 4. | Check the Compressed Files checkbox if you want files compressed with LZEXE and PKLite to be scanned. |
| 5. | <p>Configure your general preferences.</p> <ul style="list-style-type: none"> ■ Select Load VShield at Startup to activate on-access scanning when you start up your system. ■ Select VShield Can Be Disabled if you want to allow for disabling of on-access scanning. |

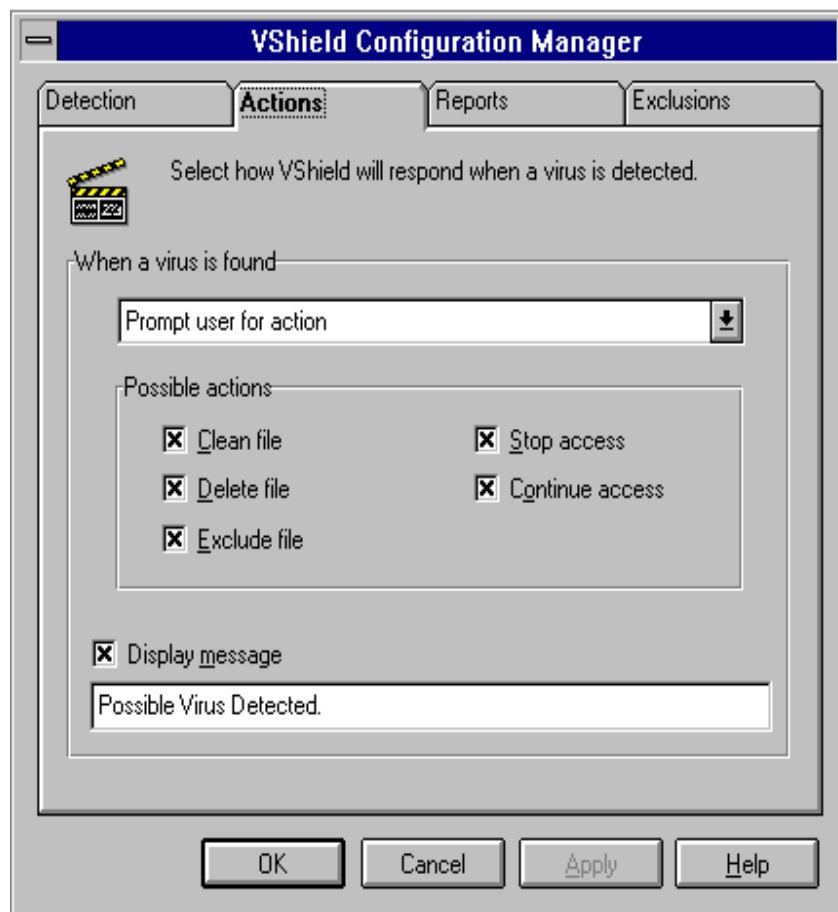
- Select Show Icon on the Desktop if you want to be able to select VShield properties from a desktop icon.

 *McAfee recommends choosing all items. However, if you are a system administrator and want to ensure that VShield remains enabled on your users' systems, do not check the VShield Can Be Disabled and Show Icon on the Desktop boxes when configuring their software.*

6. Click Apply to save your changes. To save your changes and exit VShield Configuration Manager, click OK. To exit VShield Configuration Manager without saving your changes, click Cancel.

Configuring VShield actions

Use the Actions property page (Figure 3-3) to select what actions VShield should take if a virus is detected.





**Figure 3-3. VShield Configuration Manager
(Actions Property Page)**

Take the steps outlined below to configure these settings:

Step

Action

1. In When a Virus is Found, select one of the following actions:

- Prompt User for Action (recommended for attended systems)
 - Use the Possible Actions checkboxes to configure which actions are available at the prompt. Actions include: Clean File, Delete File, Exclude File, Stop Access, and Continue Access.
 - To display a message upon virus detection, check the Display Message checkbox and type your custom message in the text box provided.
 -  *You can use this function to add a customized message that will help users better respond to a virus. For example, you can direct users to a virus response center or technical support, or instruct users to contact a specific person.*
- Move Infected Files to a Folder
 - Specify a path in the Folder To Move To box or choose Browse to locate a folder. This path can be relative. For example, if you type `\Infected` in the text box, an Infected folder will be created on the drive where the infected file was found, and the infected file will be moved there.
 -  *If an infected file cannot be cleaned or if VShield does not have the proper file access, file access will be denied.*
- Clean Infected Files Automatically
- Delete Infected Files Automatically
 - If you select this option, you must restore a clean copy of the deleted file from backups.
- Deny Access to Infected Files and Continue (recommended for systems left unattended)

2. Click Apply to save your changes. To save your changes and exit VShield Configuration Manager, click OK. To exit VShield Configuration Manager without saving your changes, click Cancel.

Configure VShield reports

Use the Reports property page (Figure 3-4) to configure the logging of virus activity and to determine which information will be included in the log entry.

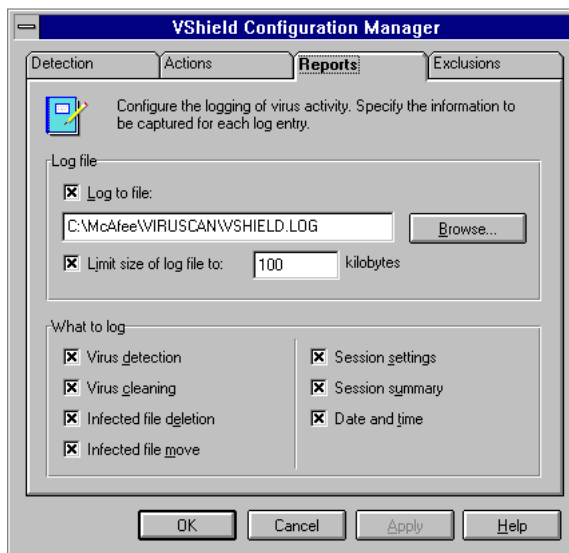



Figure 3-4. VShield Configuration Manager (Reports Property Page)

Take the steps outlined below to configure these settings.

Step

Action

1. Click the Log to File checkbox and enter a path and file in the text box (or choose a path by clicking on the Browse button) to enable logging. Limit the size of the log file by selecting the Limit Size checkbox and specifying a size between 10KB and 999KB.

 *The default path for the log file is C:\McAfee\Viruscan\VShield.log.
The default log file size is 100KB.*

2. Select from the checkboxes provided to specify what information should be included in the log file. Options include: Virus Detection, Virus Cleaning, Infected File Deletion, Infected File Move, Session Settings, Session Summary, and Date and Time.

3. Click Apply to save your changes. To save your changes and exit VShield Configuration Manager, click OK. To exit VShield Configuration Manager without saving your changes, click Cancel.

Configuring VShield exclusions

Use the Exclusions property page (Figure 3-5) to define which items should be excluded from scans.

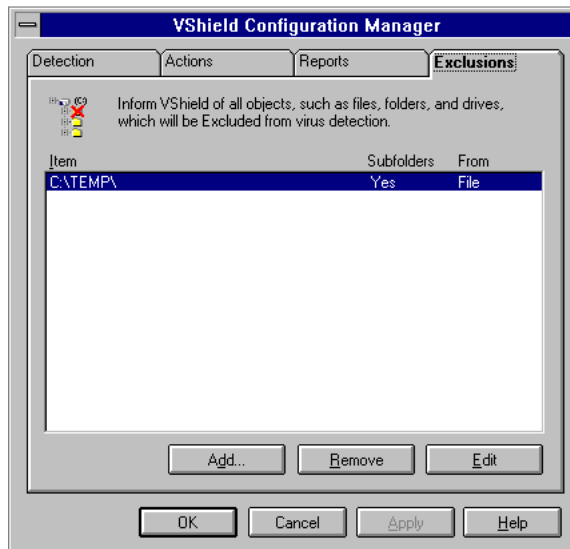


Figure 3-5. VShield Configuration Manager (Exclusions Property Page)


Take the following steps to change these settings:

Step	Action
------	--------

1. To add an object to the exclusion list, click Add.

Response: The Exclude Item dialog box is displayed.

- Type the path to the folder you wish to exclude from scanning, or click Browse to locate the folder.

 *The Exclude Item dialog box only excludes folders. To exclude files, manually type the filename of the file you want to exclude.*

- Click Include Subfolders if you want to exclude all subfolders within the selected folder.
 - Indicate whether you want the folder excluded from a File Scan or a Boot Sector Scan by placing checkmarks in the boxes provided.
 - Click OK.
2. To remove an object from the list, select it and click Remove.
 3. To edit an object on the list, select it and click Edit.
 4. Click Apply to save your changes. To save your changes and exit VShield Configuration Manager, click OK. To exit VShield Configuration Manager without saving your changes, click Cancel.

What is On-demand Scanning?

As described in the previous chapter, “On-access Scanning,” VShield provides constant protection of your system by scanning for viruses as you access files and drives. Using the on-demand component of VirusScan, you can also perform immediate scans of specific items while you’re working or schedule scans to take place daily, weekly, or monthly.

VirusScan’s on-demand scanner allows you to scan new media or specific files to determine whether a computer virus is present. VirusScan immediately detects known boot, file, multi-partite, stealth, encrypted, and polymorphic viruses located within files, drives, and diskettes.

In this chapter, you’ll find procedures for starting VirusScan’s on-demand component, as well as steps you need to take to configure and customize scanning functions.

Starting VirusScan

To start VirusScan, double-click on the VirusScan icon from the Program Manager. As it loads, VirusScan performs a self-check of its program files to ensure that they are virus-free. Once the self-check is complete, the McAfee VirusScan for Windows main window (Figure 4-1) is displayed.

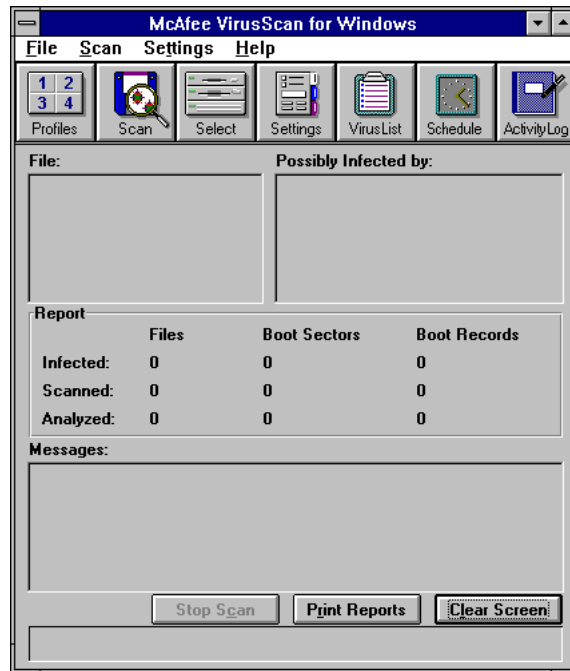



Figure 4-1. McAfee VirusScan Main Window

 If VirusScan fails the self-check, or if it exits Windows while loading, you should turn off your computer and run the VirusScan command-line program from the Emergency Diskette included with CD-ROM versions of the VirusScan product or a clean start-up diskette. See [“Making a Clean Start-up Diskette” on page 58](#) for instructions on making a clean boot diskette.

From this main window, you can establish scan settings and schedules, start an on-demand scan, view the activity log and virus list, print reports, and view scan results.

Using the menu bar

The VirusScan menu bar contains the following menus, all of which are described in detail within this chapter. Most of the menu bar actions also can be performed using the toolbar buttons, described in the following section.

- From the File menu, you are given the following options: Load Settings, Save Settings, Run Profile, Select Items to Scan, Print Setup, Print, and Exit.
- From the Scan menu, you can Start a Scan, Schedule a Scan, and view the Activity Log or Virus List.
- From the Settings menu, you can configure your on-demand scan according to the specifications that best meet your needs. Options available include: Controls, Actions, Reports, Validations, and Exceptions.
- From the Help Menu, you can select Contents for in-depth online help on the VirusScan product, Product Support for technical support details, or About VirusScan for more information about this product and McAfee.

Using the toolbar

You can use the toolbar to quickly start a task without using the menu bar. The toolbar contains the following icons, which are described in detail later in this chapter.



Click the Profiles button to run scans according to pre-established, customized settings. See [page 41](#) for details on setting up and using Profiles.



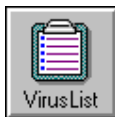
Click the Scan button to start a scan according to the options you have established.



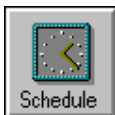
Click the Select button to configure which drives, directories, and files you would like to include in the scan.



Click the Settings button to select your scanning configuration, including controls, actions, reports, validations, and exceptions.



Click the Virus List button to view details on the viruses that VirusScan detects.



Click the Schedule button to schedule automatic scans of your system at regular intervals.



Click the Activity Log button to view the log of VirusScan's activity.

Selecting Items To Scan

Before scanning or cleaning your system with VirusScan, you must first specify what items should be included in the scan. Using VirusScan's on-demand scanner, you can scan both local and network drives.

You can specify up to 26 scan items. By default, drive C is selected.

To select drives, directories, or files for scanning, follow the procedure described below.

Step

Action

1. Start VirusScan.



Response: The McAfee VirusScan main window is displayed (See [Figure 4-1 on page 26](#)).

2. Click Select, or select Select Items to Scan from the File menu.

Response: The Select Items to Scan dialog box is displayed (Figure 4-3).

Use the Select button to specify drives, directories, or files to include in the scan.

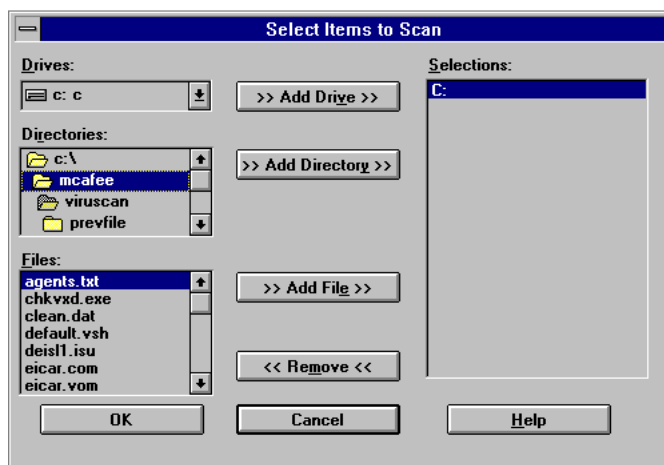




Figure 4-2. Select Items to Scan Dialog Box

3. Drives, directories, and files can be selected for scanning. To add a scan item, take one of the following steps:
 - To add a drive to the Selections list, select it from the Drives list, then click Add Drive.

 *If a drive is selected, all directories and subdirectories on the drive will be scanned.*
 - To add a directory to the Selections list, select it from the Directories list, and click Add Directories.

 *If you want all subdirectories within this directory to be scanned, you must select the Subdirectories checkbox in the Settings Notebook.*
 - To add a file to the Selections list, select it from the Files list and click Add File.

Response: The items you selected appear in the Selections list.

4. To remove an item from the list to be scanned, select it from the Selections list, and click Remove.
5. If you wish to save these selections in a settings file, see [“Using scan settings files” on page 39](#).

Selecting On-demand Scanning Options

You can configure VirusScan's scan settings to increase security, reduce scanning time, or perform specific tasks. Use the following procedure to configure an on-demand scan of your system.

Step	Action
------	--------

- | | |
|----|------------------|
| 1. | Start VirusScan. |
|----|------------------|

Response: The McAfee VirusScan main window is displayed (See [Figure 4-1 on page 26](#)).

- | | |
|----|--|
| 2. | Click Settings, or select any option from the Settings menu. |
|----|--|

Response: The Settings notebook is displayed (Figure 4-3).



Use the Settings button to configure your on-demand scanning settings.

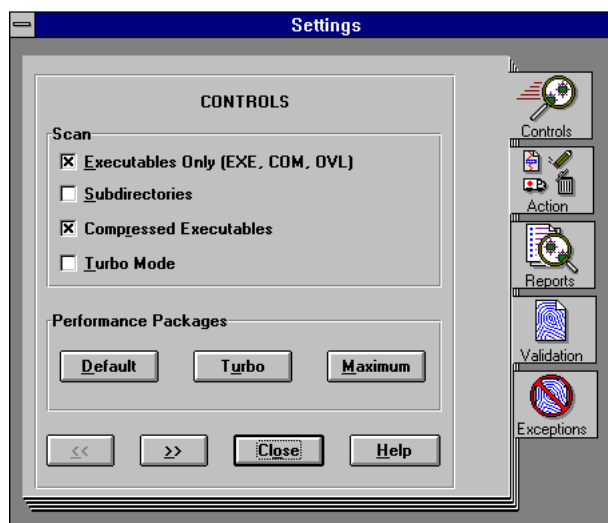


Figure 4-3. Settings Notebook (Controls Property Page)

To close the Settings Notebook at any time, click Close. To move from tab to tab, click the tab for the appropriate page or click the >> or << buttons. For online help on using the product, click Help.

Controlling the scope of the scan

Follow the procedure outlined below to configure which types of files to check and how many system resources you want to use while scanning.

Step

Action

1. From the Settings notebook, select the Controls tab.

Response: The Controls property page appears ([Figure 4-3 on page 31](#)).

2. Select the types of files you wish to include in the scan by checking the desired boxes in the Scan area. Options include: Executables Only, Subdirectories, Compressed Executables, and Turbo Mode.

- **Executables Only** reduces scanning time when a full system scan is unnecessary, limiting scans to executable files with .EXE, .COM, .SYS, .BIN, .DLL, and .OVL extensions. These are the types of files most commonly infected by viruses.
- **Subdirectories** instructs VirusScan to scan the subdirectories of selected directories. See [“Selecting Items To Scan” on page 29](#) for details on selecting directories for scanning. If this option is not selected, VirusScan does not scan within subdirectories.



You do not need to select this option if you are scanning an entire drive or individual files.

- **Compressed Executables** instructs VirusScan to scan inside executable, or self-decompressing, files that have been created using LZEXE or PKLITE. If this option is not selected, VirusScan does not check inside compressed files for viruses, but can check for modifications if the validation options are used. See [“Validating program files” on page 36](#) for details on validation.
- **Turbo Mode** reduces scan time by examining more files, but a smaller portion of each. If you suspect your system is infected by a virus, you should not use this option.

3. If you wish to use a predefined set of scanning options, use the Performance Packages section and select a package.

- For the recommended typical scan, click Default. Using this package, VirusScan will search for viruses in all executable files, including compressed executables.
- For maximum protection but a slower scan, click Maximum. Using this option, VirusScan searches for viruses within all types of files, including compressed executables. Using the Maximum setting, VirusScan will also check subdirectories of selected directories.
- For the fastest scan, click Turbo. This package instructs VirusScan to check executable files and subdirectories, using the Turbo Mode option.

Selecting VirusScan's actions

The Actions property page allows you to determine what actions VirusScan will take when it finds a virus. Follow the steps below to configure these settings.

Step

Action

1. From the Settings notebook, select the Actions tab.

Response: The Actions property page appears (see Figure 4-4).

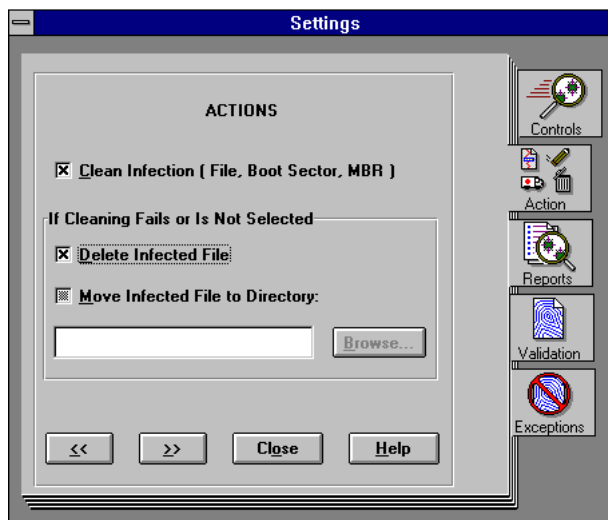




Figure 4-4. Settings Notebook (Actions Property Page)

2. Select an action for VirusScan to take if a virus is found. Options are:

- Clean Infection, which will automatically attempt to clean the infected file. Select this option to allow for removal of boot sector and Master Boot Record viruses; these types of viruses cannot be deleted or moved to another directory.

 *If you select this option and VirusScan cannot safely clean the infected file, VirusScan will either delete the infected file or move it to a directory, depending on which option you specify. McAfee recommends that you select Clean Infection in conjunction with one of the options below.*

- Delete Infected File, which will automatically delete the infected file. If you select this option, you must recover a clean copy of the file from backups.

 *Be sure to take note of the filenames so you know what to restore from backups. If the infected files resides on a network drive, you must have rights to delete files on that drive to use this option.*

- Move Infected File to Directory, which will automatically move the infected file to the directory you specify. To specify a directory, type its complete path in the text box provided, or click Browse to navigate to its location.

Generating a scan report

The Reports property page is used to save scan results in a report file, which you can view or print out for future reference. The VirusScan report file includes information on the items scanned, infections found, and infections cleaned. It also can include information on corrupted or modified files and system errors. In addition to the report file, VirusScan can generate an activity log, which includes such information as the date and time a scan is run. To generate a scan report or activity log, follow the procedures outlined below.

Step

Action

1. From the Settings notebook, select the Reports tab.


Response: The Reports property page (Figure 4-5) is displayed.



Figure 4-5. Settings Notebook (Reports Property Page)


2. If you would like to create a report of your scanning activity, type the full path and filename of an existing report file in the text box provided, or click Browse to navigate to the desired location. If a report file does not exist, you will be given the option of creating one.
 - Select Append to Report File if you want the file to include all reports. If this option is not selected, the report file will only include details from the most recent scan.
 - Select Include Corrupted Files if you wish to include details on corrupted files VirusScan encounters.
 - Select Include Modified Files if you wish to include details in the report on validated files that have been modified. See [“Validating program files” on page 36](#) for information on validation.
 - Select Include System Errors if you wish to keep a record of all errors that occur while scanning.
3. If you wish to save the time and date that a scan is run and any scan results in an activity log, select the Maintain Activity Log checkbox.

4. If you wish to limit the activity log to most recent scans, click the Keep Last *n* Events checkbox.

 *The number of events can be modified by editing the KeepLogOnly setting in the WSCAN.INI file.*

Validating program files

VirusScan includes a validation feature, which you can use to track any modification to executable files on your hard disk—a sign of possible virus activity. By appending codes to executable files or storing codes in a separate external file, you can increase your protection against virus infection. Follow the procedures described in this section to validate your program files.

 *VirusScan cannot validate files on the boot sector or Master Boot Record.*

Step

Action

1. Select the Validation tab.

Response: The Validations property page (Figure 4-6) is displayed.

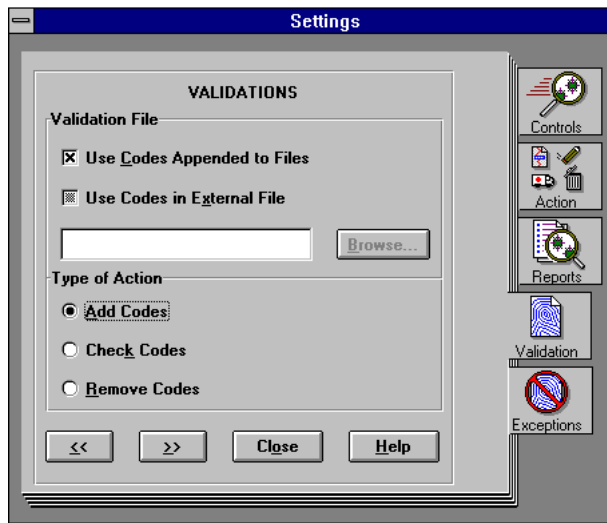



Figure 4-6. Settings Notebook (Validations Property Page)

2. Select the type of validation you would like to use.
 - Select Use Codes Appended to Files to add validation codes to all standard executable files. This method adds approximately 98 bytes to each validated file.
 - Select Use Codes in External File to store validation codes in an external database file. If you select this option, you must type in a filename and complete path or click Browse to navigate to a file's location. Using this method, the external file size increases approximately 95 bytes for each file validated.
3. Select the type of action you wish to perform.
 - To add codes to files or the external database, check Add Codes.
 - To check codes that have previously been added to files or the external database, select Check Codes. If a file has been modified, VirusScan reports the change.

 *You can save this information in a report by selecting the Include Modified Files checkbox on the Reports property page. See [“Generating a scan report” on page 34](#).*
 - To remove codes from files or the external database, check Remove Codes.
4. To exclude files from validation, see the following section, [“Excluding files from validation.”](#)

Excluding files from validation

VirusScan's validation feature uses codes to help you identify executable files that have been modified, which is a common sign of virus infection. Using the Exceptions property page, you can exclude from validation self-modifying files that might generate false alarms.

VirusScan offers two methods for excluding files from validation:

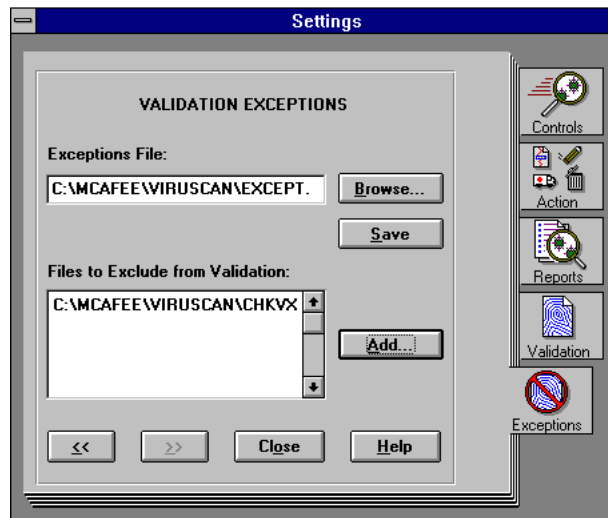
- Creating an exceptions file and directing VirusScan to the file using the Exceptions File section of the property page
- Listing all files in the Files to Exclude from Validation text box.

Follow the procedure below to exclude files from validation.

Step	Action
-------------	---------------


1. Select the Exceptions tab.

Response: The Validation Exceptions property page (Figure 4-7) is displayed.




**Figure 4-7. Settings Notebook
(Validation Exceptions Property Page)**

2. To exclude files from validation using an external exceptions file, type the filename and complete path of the exceptions file in the Exceptions File text box, or click Browse and navigate to the location.

 *Exceptions files can be created using a text editor such as Notepad.exe. For information on creating an exceptions file, see [“Creating an exceptions file” on page 39](#).*

3. To exclude files individually, type the name and path of the file to exclude in the Files to Exclude from Validation text box, or click Add and select it from the list provided.

 *To delete an entry, select it and press Delete on your keyboard.*

Creating an exceptions file

If you would like to create an exceptions file listing all files to exclude from validation, follow the steps outlined below.

Step	Action
1.	Open any word processing program that can read and save ASCII text files, such as Notepad.
2.	Type a list of the drives, directories, and files (including the file paths) that should be excluded from validation. Each line in the file should contain the path and filename of one file.

Example:

```
C:\clipper\bin\clipper.exe
```

```
C:\123\123.com
```

```
C:\DOS\setver.exe
```

3. Save the profile in the same directory as WSCAN.EXE under a name of your choice.

Using scan settings files

To use the scan settings files, save the scan settings and the selected items in a WSCAN.INI file. This will enable the scanning options to load automatically, saving you the task of selecting scanning options and items individually every time you want to scan.

Saving scan settings

To save scan settings, follow the steps outlined below.

Step	Action
1.	Start VirusScan Response: The McAfee VirusScan main window is displayed (See Figure 4-1 on page 26).
2.	Select Save Settings from the File menu.
3.	Select a file type from Save File as Type.
4.	Type or select the name of the settings file to save.
5.	Save the settings file in a VirusScan subdirectory. Click OK.

Loading scan settings

To load a scan settings file, follow the steps outlined below.

Step	Action
1.	Start VirusScan. Response: The McAfee VirusScan main window is displayed (See Figure 4-1 on page 26).
2.	Select Load Settings from the File menu.
3.	Select the file type to load the scan settings file from the List File of Type area.
4.	Under File Name, type or select the name of the settings file. Click OK. Response: The scan settings file is loaded and a scan is initiated using the options specified in the settings file.

Setting Up and Using Profiles

VirusScan's Profiles option allows you to scan your system with the click of a button, using options you have previously specified. Profiles automate repetitive scanning tasks and make it easier for you to scan your system.

Setting up profiles

Follow the procedures outlined in this section to set up profiles.

- | Step | Action |
|------|--|
| 1. | Open any word processing program that can read and save ASCII text files, such as Notepad. |
| 2. | Type a list of the drives, directories, files (including the file paths), and any command-line options desired. See “VirusScan Command-line Options” on page 77 for details on available command-line options. |

Example:

A:

C:\Windows /sub /all

C:\DOS

VirusScan scans in the order of the list that you create. In the example profile above, VirusScan will scan the A: drive first, then the Windows directory, and finally the DOS root directory.

- | | |
|----|---|
| 3. | Save the profile in the same directory as WSCAN.EXE as a .prf file under a name of your choice. |
|----|---|

Example:

```
filename = PROFILE3.PRF
```

4. With the word processing program still open, open WSCAN.INI. Profile 1 will read `Label = Hard disk` and Profile 2 will read `Label= Floppy disks`; Profile 3 and 4 will read `Label = Unavailable`.
5. To activate personal profiles, edit area 3 to reference the new profile.

Example:

```
[Profile 3]
```

```
Label = (profile name)
```

```
Description = (profile description)
```

```
File = (profile filename)
```

Save changes and close. A new button will appear in the run Profile dialog box with the new profile attached. Click the profile button to test the new profile.



PROFILE1.PRF and PROFILE2.PRF have already been created. Multiple profiles can be written, however only four can be used within WSCAN.INI at any given time.

Using profiles

Follow the steps outlined below for using profiles.

Step

Action

1. Start VirusScan.

Response: The McAfee VirusScan main window is displayed (See [Figure 4-1 on page 26](#)).



Use the Profiles button to quickly scan your system using customized settings.

2. Click Profiles, or select Profiles from the File menu.

Response: The Run Profile dialog box is displayed (Figure 4-8).



Figure 4-8. Run Profile Dialog Box

3. Run a profile by clicking on the appropriate profile button.

- To scan the hard disk, click the Hard Disk button.
- To scan floppy disks, click the Floppy Disks button.



Newly created profiles and descriptions are listed below the Floppy Disk profile button and description.

Scheduling Scans

VirusScan can be configured to run customized scans of your system at scheduled times. Once a schedule is established, the scan will run automatically at the specified time. Scheduled scans can be configured to run daily, weekly, or monthly, with the scanning options you specify.

For scans to take place as scheduled, the workstation must be running and VirusScan must be loaded. Multiple scheduled scans can be configured on one system; VirusScan saves the information for each scheduled scan in WSCAN.INI.

Use the Schedule button on your task bar and follow the procedures below to set up scheduled scanning.

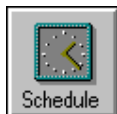
Step	Action
------	--------

- | | |
|----|------------------|
| 1. | Start VirusScan. |
|----|------------------|

Response: The McAfee VirusScan main window is displayed (See [Figure 4-1 on page 26](#)).

- | | |
|----|--|
| 2. | Click Schedule, or select Schedule from the Scan menu. |
|----|--|

Response: The Schedule dialog box is displayed (Figure 4-3).



Use the Schedule button to set up scheduled scans of your system: daily, weekly, or monthly.

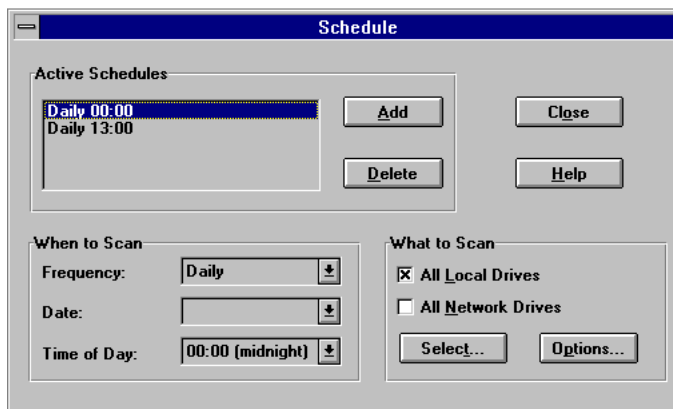


Figure 4-9. Schedule Dialog Box

3. In the When to Scan area, click the coinciding arrow button to choose the frequency, date, and time of day you want to implement a scan.
4. Click Add in the Active Schedules area to add the new schedule settings.

Response: The new schedule appears in the Active Schedules box.

5. Click on the new schedule listed in the Active Schedules box to access the What to Scan area.
6. Check the All Local Drives and/or All Network Drives checkbox in the What to Scan area to scan all local drives and/or all network drives.



You can select files and drives to scan and modify the scan options by clicking on the Select and Options button in the What to Scan area.

Using the VirusScan Activity Log

The VirusScan Activity Log keeps track of the dates and times you scan your system, as well as, associated messages regarding the items scanned and infections found. You can view details of the scan activity in VirusScan's Activity Log by following the steps outlined below:

Step	Action
------	--------

1. Start VirusScan.

Response: The McAfee VirusScan main window is displayed (See [Figure 4-1 on page 26](#)).

2. Click Activity Log, or select Activity Log from the Scan menu.

Response: The Activity Log dialog box is displayed (Figure 4-10).



Use the Activity Log button to view the log of your scanning activity.

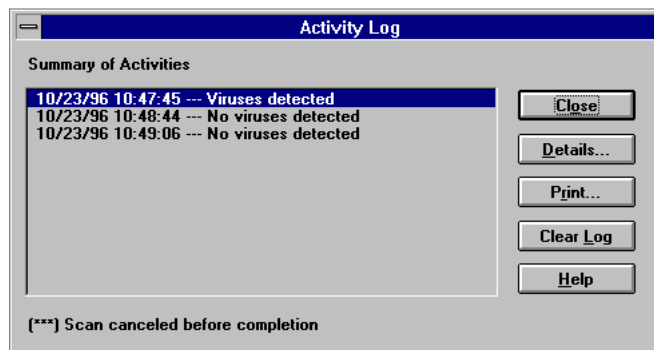


Figure 4-10. Activity Log Dialog Box

3. To display details of a specific scan, select the date and time of the scan from the Summary of Activities box in the Activity Log.

Response: Additional details of the scan is displayed.

4. To print

Displaying the Virus List



The Virus List is a comprehensive list of viruses detected by VirusScan. The list provides a description of the viruses, including the infector type, virus characteristics, virus size, and cleaning status. To display and use the Virus List, follow the instructions outlined below.

Use the Virus List button to view details on the viruses that VirusScan detects.

Step

Action

1. Start VirusScan.

Response: The McAfee VirusScan main window is displayed (See [Figure 4-1 on page 26.](#))

2. Click the Virus List button or select Virus List from the Scan menu.

Response: The Virus List dialog box is displayed (Figure 4-11).

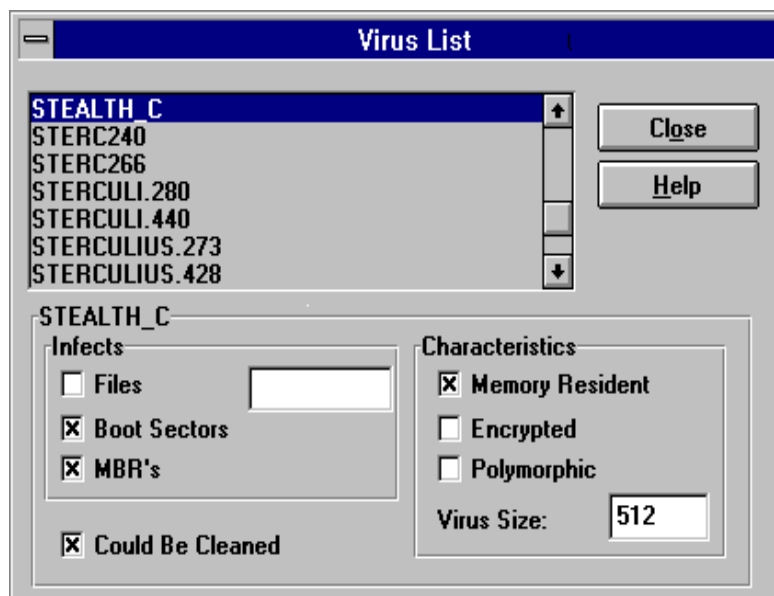



Figure 4-11. Virus List Dialog Box

3. To display information on a specific virus, scroll through the list of viruses using the scroll bars to select the virus.


 *Once you have selected a virus from the list, you can use your keyboard to type the first letter of a virus to scroll directly to a specific section.*

- The Infects section describes what the selected virus infects:
 - Files, if selected, indicates that the virus infects files. If the virus targets files with specific extensions or files of a specific type, the extensions appear to the right of the checkbox.
 - Boot Sectors, if selected, indicates that the virus infects the boot sector.
 - MBRs, if selected, indicates that the virus infects the Master Boot Record.
- Could Be Cleaned, if selected, indicates that a remover for the virus is available.
- The Characteristics section describes the behavior of the selected virus:
 - Memory Resident, if selected, indicates that the virus is a memory resident program that acts similar to a TSR or a device driver and remains active in memory while the computer is running.
 - Encrypted, if selected, indicates that the virus attempts to evade detection by self-encrypting.
 - Polymorphic, if selected, indicates that the virus attempts to evade detection by changing its internal structure or its encryption techniques.
 - Virus Size describes the amount, in bytes, that the virus increases the size of a file it infects.

 *The default size for an MBR or boot sector virus is 512.*

If You Suspect You Have a Virus

If you have or suspect you have a virus before installing VirusScan, you should follow this procedure to create a virus-free environment.

Step	Action
1.	Turn off your computer.  <i>Do not reboot using the reset button or CTRL+ALT+DELETE; if you do, some viruses might remain intact.</i>
2.	Place the McAfee Emergency Diskette that accompanied your VirusScan product or a clean start-up (boot) diskette into the A: drive. See “Making a Clean Start-up Diskette” on page 58 for details on creating a virus-free boot diskette.
3.	Turn on your computer.
4.	Follow the on-screen instructions and remove any viruses found.

If viruses were removed

If VirusScan successfully removes all the viruses, shut down your computer and remove the diskette. Begin the installation procedure described in [Chapter 2, “Installing VirusScan.”](#)

To find and eliminate the source of infection, scan your diskettes immediately after installation.

If viruses were not removed

If VirusScan cannot remove a virus, you will receive the message:

Virus could not be removed.

If you receive this message, refer to documents related to manually removing viruses on the McAfee Web Site. For contact information, see [“How To Contact Us” on page 8](#).

If VirusScan Detects a Virus

Viruses attack your computer system by infecting files—usually executable program or Word document files. Often, these files are damaged during the infection. VirusScan can safely remove most viruses from infected files and repair any damage done to the files by the virus. Some viruses, however, are designed to damage your files beyond repair. These irreparably damaged files, called “corrupted” files, can be moved by VirusScan to a quarantine directory or deleted to prevent another virus infection of your system.

Removing a virus found in a file

If VirusScan detects a virus in a file, it will take the action you specified during configuration. See [“Selecting On-demand Scanning Options” on page 31](#).

Removing a virus found in memory

If VirusScan detects a virus on your system, you should immediately clean your system to prevent the virus from spreading throughout your PC or network. You can remove viruses from files if you know or suspect that infection has occurred.

However, if a virus is resident in memory, or if the virus has infected the Master Boot Record (MBR) or boot sector, the most secure way to clean your system is to shut down your computer. Then, reboot from a clean start-up diskette (boot disk) and remove the virus using VirusScan DOS commands. For more information, see [Appendix E, “Reference.”](#) Be sure you only use the DOS commands to clean your system if a virus was detected in memory.

Understanding False Alarms

A false alarm is a report of a virus in a file or in memory when a virus does not actually exist. False alarms are more likely if you are using more than one brand of virus detection software, because some anti-virus programs store their virus signature strings unprotected in memory. As a result, VirusScan may “detect” them falsely as a virus. Your system’s BIOS, use of validation codes, and other factors may also produce false alarms.

Always first assume that any virus found by VirusScan is real and dangerous, and take necessary steps to remove it from your system. If, however, you have reason to believe that VirusScan is generating a false alarm (for example, it has detected a virus in only one file that you have been using safely for years), refer to the list of potential sources below:

- VirusScan may report a false alarm if more than one anti-virus program is running. Set up your computer so that only one anti-virus program is running at a time. Remark out lines in the AUTOEXEC.BAT file that refer to other anti-virus programs. Turn off your computer, wait a few seconds, and turn it on again to make sure that all code from other anti-virus programs is cleared from memory.
- Some BIOS chips include an anti-virus feature that could be the source of false alarms. Refer to your computer's reference manual for details.
- If you set up validation/recovery codes, subsequent scans can detect changes in validated files. This can trigger false alarms if the executable files are self-modifying or self-checking. When using validation codes, specify an exceptions list to exclude such files from checking.
- Some older Hewlett-Packard and Zenith PCs modify the boot sector each time the system is booted. VirusScan may detect these modifications as a possible infection, even though no virus may be present. Check your computer's reference manual to determine if your PC has self-modifying boot code. To solve this problem, save validation/recovery information to the executable files themselves; this method does not save information about the boot sector or Master Boot Record.
- VirusScan may report viruses in the boot sector or Master Boot Record of certain copy-protected diskettes.


Preventing Virus Infection

Keys to a Secure System Environment

VirusScan is an effective tool for preventing, detecting, and recovering from virus infection. It is most effective, however, when used in conjunction with a comprehensive computing security program that includes a variety of safety measures, such as regular backups, meaningful password protection, user training, and awareness.

To create a secure system environment and minimize your chance of infection, McAfee recommends that you take the following steps:

1. Follow the installation procedures as outlined in [Chapter 2, "Installing VirusScan."](#) If you suspect you have a virus, take steps to clean your system before installing VirusScan. For this procedure, see ["If You Suspect You Have a Virus" on page 49.](#)
2. Configure your AUTOEXEC.BAT file to load VShield automatically at start-up.

 *Your AUTOEXEC.BAT is automatically modified if you followed the recommended installation procedures.*
3. Create a start-up diskette containing the VirusScan program and DOS by following the procedure outlined in ["Making a Clean Start-up Diskette" on page 58.](#) Make sure the diskette is write protected so that it cannot become infected.
4. Make frequent backups of important files. Even with VirusScan, some viruses (as well as fire, theft, or vandalism) can render a disk unrecoverable without a recent backup.

Outlining a full security program is beyond the scope of this manual. However, by following the steps provided in this appendix and reading the information provided in [Appendix B, “Understanding Viruses,”](#) you can gain a clearer understanding of what viruses are, how they affect your system, and what you can do to prevent an infection.

Detecting New and Unknown Viruses

There are two ways for you to deal with new and unknown viruses that may infect your system:

- Update your VirusScan data files
- Validate the VirusScan program files

Updating your VirusScan data files

To offer the best virus protection possible, McAfee continually updates the files VirusScan uses to detect viruses. After a certain time period, you are notified that you need to update the virus definition database. McAfee recommends that you update these files on a regular basis for maximum protection.


What is a data file?

The files CLEAN.DAT, NAMES.DAT, and SCAN.DAT all provide virus information to the VirusScan software. These are the data files we're referring to in this section.

Why would I need a new data file?



New viruses are discovered at a rate of more than 100 per month. Often, these new viruses are not detected using older data files. The data files that came with your copy of VirusScan might not be able to help VirusScan detect a virus that was discovered months after you bought the product.

McAfee's virus researchers are working constantly to update the data files with more and newer virus definitions. The new data files are released approximately every four to six weeks.

 *McAfee offers online virus signature file updates for the life of your product. However, we cannot guarantee backward compatibility of the virus signature files with a previous version's software. By subscribing to a maintenance plan and upgrading your VirusScan software, you ensure complete virus protection for at least one year after your VirusScan purchase.*

How to apply the data file

To update your data files, take the following steps.


- | Step | Action |
|-------------|--|
| 1. | <p>Download the data file (for example, DAT-9611.ZIP) from one of McAfee's electronic services. On most services, it is located in the anti-virus area.</p> <p> <i>Please note that your ability to access these updates is legally restricted by the maintenance terms outlined in the README.1ST file accompanying the software and detailed in the software license agreement.</i></p> |
| 2. | Copy the file to a new directory. |
| 3. | <p>The file is in a compressed format. Decompress the file using any PKUNZIP-compatible decompressing software. If you don't have the decompressing software, you can download PKUNZIP (shareware) from McAfee electronic sites.</p> |
| 4. | <p>Locate the directories on your hard drive where your VirusScan software is currently loaded. Typically, the files are stored in C:\McAfee\VirusScan. This varies depending on the version of the software you have and on whether or not a different directory was specified during installation.</p> |
| 5. | <p>Copy the new files into these directory or directories, overwriting the old data files.</p> <p> <i>There might be part of the software in more than one directory. If so, place the updated files in each directory.</i></p> |
| 6. | Reboot your computer so that changes take place immediately. |

Validating the VirusScan program files


When you download a file from any source other than the McAfee bulletin board or other McAfee service, it is important to verify that it is authentic, unaltered, and uninfected. McAfee anti-virus software includes a utility program called Validate that you can use to ensure that your version of VirusScan is authentic. When you receive a new version of VirusScan, run Validate on all of its program files. For details on the Validate program, see the README.1ST text file that accompanied your software.

Making a Clean Start-up Diskette

In case your system becomes infected, you should have a clean start-up (boot) diskette. This section describes how to create that boot diskette.

 *Your system must be virus-free to make a boot diskette. Any virus residing in your system could be transferred to your boot diskette and reinfect your system. If your computer is infected, go to another computer, scan it, and if it is virus-free, follow the steps below.*

If you are working in DOS, start this procedure from a DOS prompt (C:\>). If you are in Windows, you must open a DOS box to get the DOS prompt.

Step	Action
1.	Insert a blank diskette in drive A:.
2.	Format the diskette by typing the following command at the C:\> prompt: <pre>format a: /s /u</pre> This overwrites any information already on the diskette.  <i>If you are using DOS 5.0 or an earlier version of DOS, do not type the /u. If you are unsure of which version you are using, type ver at the C:\> prompt for version information.</i>
3.	When the system prompts you for a volume label, enter an appropriate name using no more than eleven characters.
4.	Change to the VirusScan directory by typing the following command at the C:\> prompt: <pre>cd \mcafee\viruscan</pre>
5.	Copy the DOS version of VirusScan to the diskette by typing the following commands at the C:\mcafee\viruscan prompt: <pre>copy scan.exe a:</pre>

```
copy scan.dat a:
```

```
copy clean.dat a:
```

```
copy names.dat a:
```

6. Change back to the root directory by typing the following command at the `c:\mcafee\viruscan` prompt:


```
cd\
```

7. Copy useful DOS programs to the diskette by typing the following command at the `C:\` prompt:

```
copy c:\dos\chkdsk.* a:
```

8. Repeat the last step for any other useful programs you want to add to the diskette. Here are some programs you might want:

- `debug.*`
- `diskcopy.*`
- `fdisk.*`
- `format.*`
- `label.*`
- `mem.*`
- `sys.*`
- `unerase.*`
- `xcopy.*`


 *If you use a disk compression utility, be sure to copy the drivers required to access the compressed diskettes onto the clean boot diskette. See the documentation for that utility for more information about those drivers.*

9. Label and write protect this diskette, then store it in a secure place.
See [“Write Protecting a Diskette” on page 61](#) for more information.

Write Protecting a Diskette

Floppy diskettes are convenient, portable devices for storage and retrieval of computer data. Diskettes are used to save files (write) and recover files (read). They are also the most common vehicle viruses use to invade your computer's system.

One way to help avoid infection via floppy diskette is to *write protect* diskettes for read only data. If your system does become infected with a virus, the write-protection feature keeps your clean diskettes from also becoming infected, preventing reinfection after your system is cleaned.

 *Any diskettes that are not write protected should be scanned and cleaned before you write protect them.*

Write protecting 5.25" floppy diskettes

- | Step | Action |
|------|---|
| 1. | <p>Position the diskette face up with the label facing away from you.</p> <p>The notch on the upper right hand side is called the <i>write-protect</i> notch. When you can see this notch, you can read and write data to and from the diskette. When the notch is covered with an adhesive tab, you can no longer write to the diskette. This stops you from accidentally changing data on the disk. It also prevents viruses from infecting the diskette.</p> |
| 2. | <p>Cover the notch with an adhesive tab or tape to write protect the diskette.</p> |

Write protecting 3.5" floppy diskettes

- | Step | Action |
|------|---|
| 1. | <p>Position the diskette face down with the metal slide facing you.</p> <p>Examine the small rectangular hole on the upper left side. There should be a square, plastic tab that you can slide up and down across the hole.</p> |
| 2. | <p>To write protect the diskette, slide the plastic tab upward toward the edge of the diskette so that the hole is open.</p> |



Understanding Viruses

Computer Virus Primer

Your computer posted an unusual message, changed screen colors, is missing files, has no hard disk space left, or just plain won't work. Is this a virus? In many cases, the answer is no. These are all symptoms of viruses and viral damage. However, the problems actually may be caused by a faulty system battery, a keyboard error, a practical joke, fragmented disks, or even reboot corruption. Unless you use anti-virus software, it is difficult to determine if computer anomalies are caused by viruses.

Typical Signs of Virus Infection

- Unusual messages
- Missing files or increased file size
- Slow system operation
- No more disk space
- No more disk access

Every month, more than 100 new viruses are added to the worldwide viral pool of more than 8,500. The threat from these viruses is real: According to a National Computer Security Association March 1996 survey of 2,300 North American companies with 500 or more PCs:

- Approximately 90% of companies experience a virus encounter or incident each month.
- Approximately 90% believe that the virus problems are the same as or worse than last year.

- The Word.Concept macro virus appears to be the fastest growing virus and seems to travel to a large extent by e-mail and other network connections.
- Virus encounters average 1 per 100 PCs per month.
- Over 70% of infections occur through diskette distribution.
- More than 80% of infections result in lost productivity, and 35% result in lost data.
- Over 46% of infections require more than 19 days to completely recover.
- More than 35% of incidents cost \$2,000 or more.
- Less than 35% of companies use the full-time protection capabilities of their anti-virus software.
- Over 20% of viruses reported were received through electronic distribution.
- The average server virus incident takes over 5.5 hours for recovery.

What is a virus?

A computer virus is a program that replicates itself, attaches to other programs, and performs unsolicited, if not malicious, actions when executed. The two fundamental virus categories are “boot” and “file” viruses.

Boot viruses are programs that become active upon system start-up. They dwell within the boot sector of a system’s infected floppy or hard disk. Most often, the boot virus spreads as it becomes memory resident, replicating and attaching onto other available logical disks. Subsequent use allows the virus to spread to other disks.

File viruses are programs that become active only when executed—these include .EXE, .COM, .DLL, and other executable files. The file virus spreads upon execution as it typically becomes memory resident, then replicates and attaches to other executable programs.

Other viral classifications also exist. *Multi-partite viruses*, for example, are viruses that have both file and boot virus characteristics. *Stealth viruses* hide their actions either generically or against specific anti-virus products. *Encrypted viruses* actually encrypt their viral code, further hiding from detection. *Polymorphic viruses* use mutation engines to randomize their signature. Today, the most common widespread virus is a classification called a *macro virus*. Macro viruses use an application's macro language to spread to other documents within that application and perform unsolicited actions. The Word macro virus is obtained by opening macro-infected Microsoft Word document (.doc) or Word template (.dot) files.

How do viruses spread?

Incident reports indicate that the majority of viruses are introduced innocently to end-user environments from unsuspecting employees, family, and friends. Depending on a site's software security standards, it is even possible to contract a computer virus when sending your PC to a repair service center, utilizing re-packaged software, or using new software.

How One Receives a Computer Virus

- Diskette and file sharing
- File exchange from e-mail, online services, the Internet, and bulletin board systems
- Re-packaged software and repair services

It is not uncommon to believe that you just received a computer virus and it caused immediate damage. Today's computer viruses, however, are designed to spread among computers before causing enough damage to evoke publicity. If a virus were to make itself known immediately—by displaying an impolite message on your screen, for example—you would instantly know that something was wrong. Additionally, if a virus immediately corrupted your machine (making it inoperable), the virus would not be able to transfer to other disks and computers. Therefore, the most common viruses are designed to replicate without users' knowledge.

When a virus does present itself, it typically is well after the point of original infection. Generally, a virus monitors for a *trigger event*, or a computer condition that causes a payload to be delivered. Trigger events include dates, time, keyboard strokes, number of file saves, number of disk accesses, file sizes, file types, and more. *Payloads*, whether designed intentionally or not, always waste productivity or harm data. Some payloads deliver “amusing” or political messages, such as the Nuclear macro virus asking for a ban on French nuclear testing. Others cause the disruption of computer processes, such as AntiCMOS preventing the user access to his or her drives. An inadvertent payload is the operation of a stealth boot virus overwriting data as it attempts to write pre-infected boot information to another part of the disk. The most lethal type of payload is inconspicuous activity and minute data damage spread across long periods of time. This is considered lethal since ultimately one may be using corrupt or irrecoverable data.

How does anti-virus software work?

Anti-virus software use a variety of counteractions to detect and remove computer viruses. Most solutions rely on three primary detection components: on-access scanning, on-demand scanning, and checksumming.

On-access scanning is similar to an automatic fire sprinkler system: A virus scan is automatically initiated on file access, such as when a disk is inserted, a file is copied, or a program is executed.

On-demand scanning is similar to a fire extinguisher: A virus scan is user initiated. On-demand scans can be performed immediately, at scheduled intervals, or at system start-up on a particular file, directory, or volume. Both on-access and on-demand scanning rely on a scanning engine, which typically utilizes a monthly updated signature file to accurately pinpoint known, generic, and even new virus signatures and characteristics.

Checksumming, also known as *integrity checking*, is a method by which an anti-virus product determines that a file has changed. Since viral code physically attaches to another file, one can determine such modification by keeping pre-infection file information. Checksumming is generally accurate and does not require any particular upgrades. Nevertheless, checksummers will not provide the virus name or type. More importantly, checksummers assume that the user has the ability to maintain a virus-free file database. Unlike scanning engines, the user must submit a virus-free file to update the checksum database registry—leaving the possibility for an infected file to be marked as valid.

Additional viral counteractions also have been added to the anti-virus arsenal. Because a virus performs an unsolicited action, such as attaching to another file without the user's knowledge, a virus must make system calls (requesting functions through computer system's interrupts) to operate discretely. *Interrupt monitoring* attempts to locate and prevent interrupt calls that may indicate viral action. However, a thorough monitoring of interrupts usually is obtrusive—negatively affecting system resource utilization and possibly preventing “legal” system functions. *Memory detection* depends on the recognition of a known virus's location and code while in memory. While generally successful, this too can constrain system resources and may prevent “legal” memory use. Lastly, a new generation of virus scanning engine has been introduced under various names including *heuristics*, *rules-based scanning*, *expert systems*, or *neural nets*. These engines use a set of rules to more efficiently parse through a file and more quickly identify suspect code. While operating much faster than traditional scanners, these engines can falsely identify virus-free files.

Due to the number of virus types, effective products leverage a combination of counteraction methods. Also, the anti-virus field is constantly evolving: Involvement in virus counteraction steadily increases the knowledge base of virus research and anti-virus software vendors. This enables the refinement of detection and cure methods as well as the creation of entirely new techniques for the future.

How can I minimize my chance of infection?

McAfee's anti-virus solutions offer a convenient and effective way to minimize the possibility of virus infection, providing optimal protection with minimal intrusion. Once VirusScan is installed, we suggest you scan your system frequently.

Because more than 100 new viruses are introduced each month, McAfee updates its solutions regularly. Our maintenance subscription enables you to conveniently obtain our monthly product updates to make sure your system has the most current barrier to infection.

Implementing other safe computing practices daily can further ensure virus-free operation. See “[Keys to a Secure System Environment](#)” on page 53 for tips on creating and maintaining a virus-free environment.

McAfee Virus Information Library

The McAfee Virus Information Library is a comprehensive database containing more than 250 technical documents and information about more than 1,000 viruses. The library offers detailed information concerning computer viruses, their methods of infection, their effect on computers, instructions on removing viruses, and methods to prevent virus infection.

The McAfee Virus Information Library is available on the CD-ROM version of this software in the Windows 3.1x help file format or through the McAfee Web Site.

The Virus Information Library is continuously being updated through our website to offer the most comprehensive, up-to-date information available. For more information on reaching the McAfee Web Site, see [“How To Contact Us” on page 8](#).

C

Testing Your Installation

The Eicar Standard AntiVirus Test File is a combined effort by anti-virus vendors throughout the world to come up with one standard by which customers can verify their anti-virus installations. To test your installation, copy the following line into its own file and name it EICAR.COM.

```
X5O!P%@AP[4\PZX54(P^)7CC)7)$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

When finished, you will have a 69- or 70-byte file.

When VirusScan is applied to this file, it will report finding the EICAR-STANDARD-AV-TEST-FILE virus.

It is important to know that THIS IS NOT A VIRUS. However, users often have the need to test that their installations function correctly. The anti-virus industry, through the European Institute for Computer Antivirus Research, has adopted this standard to facilitate this need.


Delete the file when installation testing is completed so unsuspecting users are not unnecessarily alarmed.

D

McAfee Support Services

McAfee is pleased to offer many different types of technical assistance to customers. These flexible support programs are designed to meet the needs of individuals and businesses at any level. By offering support solutions that range from a complimentary 90-day introductory technical support program to an optional one-year personal online maintenance and support program, McAfee helps to ensure that you receive the level of technical assistance you require.

McAfee also offers a variety of technical assistance plans designed to meet the needs of business customers, including training, consulting, enterprise support, and a Jump Start program. Please review each of the different support service plans and benefits listed in this appendix and pick the one best suited for you.

 *The term update refers only to the virus definition files; the term upgrade refers to product version revisions, executables, and definition files. McAfee offers free online virus signature file updates (.DATs) for the life of your product. However, we cannot guarantee backward compatibility of the signature files with previous versions' executable files (.EXEs). By upgrading your software to the latest product version and latest .DAT files, you ensure complete virus protection for the term of your software subscription or maintenance plan.*

Customer Service Programs

Free 90-day introductory support program

All registered owners of single-node (one computer) products, such as those purchased at local retail stores or those downloaded from McAfee Store on our website, are entitled to:

- Free online virus updates (new .DAT files)
- One free online product upgrade (product version revision) with the newest features
- Free support services listed below

Support services

- Electronic and online support, available 24 hours a day, seven days a week on each of the forums listed below:
 - Automated voice and fax system: (408) 988-3034
 - McAfee BBS (electronic bulletin board system): (408) 988-4004
 - World Wide Web site: <http://www.mcafee.com>
 - CompuServe: GO MCAFEE
 - Microsoft Network: MCAFEE
 - America Online: keyword MCAFEE
- Technical support phone assistance, available during regular business hours, 6:00 A.M.– 6:00 P.M. Pacific time, Monday through Friday, from our professionally-trained support representatives at (408) 988-3832.

To receive your free one-time online upgrade, please contact our Customer Care department at (408) 988-3832. Please supply your proof of purchase when you request the upgrade. You will be given a password to the upgrade area on either the McAfee BBS, FTP site, or World Wide Web site so that you can download a registered version of the latest product. This password is valid for one access only.

Free subscription maintenance and support program


McAfee offers all registered owners of licensed multiple-node (ten computers or more) subscription products the following free support services and maintenance during the two-year term of the software subscription.

 *You must be registered to receive these services.*

Support services

- Electronic and online support, available 24 hours a day, seven days a week on each of the forums listed below:
 - Automated voice and fax system: (408) 988-3034
 - McAfee BBS (electronic bulletin board system): (408) 988-4004
 - World Wide Web site: <http://www.mcafee.com>
 - CompuServe: GO MCAFEE
 - The Microsoft Network: MCAFEE
 - America Online: keyword MCAFEE
- Technical support phone assistance during regular business hours, 6:00 A.M.–6:00 P.M. Pacific time, Monday through Friday, from our professionally trained support representatives at (408) 988-3832.
- Two years of free online product upgrades with the newest features and virus definition data. If you upgrade your operating system, you can also extend the upgrade of your McAfee product to the new platform.

Optional support plans

 *Contact McAfee for current pricing structures.*

Option 1: One-year personal online maintenance and support


program

For registered owners of single-node products who want to extend their support coverage, this plan allows you to call in for unlimited technical support, download the latest virus protection updates each month, and periodically download upgrades from any of McAfee's registered online services—all for a full year. If you upgrade your operating system, you can also upgrade your product program to the new platform.

Option 2: One-year quarterly disk/CD-ROM maintenance and support programs

This plan is for registered owners of either single- or multiple-node subscription products. It offers all the features of Option 1, while adding a quarterly mailing of software upgrade diskettes or CD-ROMs (depending on the product) and a quarterly update newsletter. With this option, you can update your product to include the latest features and virus data files without having to download from an online service.

Each optional support plan begins as soon as you purchase the product and is good for one year, at which time you can renew your support program through McAfee's Customer Care department at (408) 988-3832.

 *McAfee reserves the right to change part or all of its Customer Service Programs at any time without notice.*

Professional Services Programs

McAfee Professional Services provide a wide range of on-site services. Whether for short-term assistance or long-term strategic planning, a highly qualified consultant can help you achieve positive results. McAfee consultants are trained on NetWare, Microsoft NT Advanced Server, Windows 95, and a multitude of desktop applications.

Before work begins, a project manager discusses the project scope and objective with you and comes to a mutual agreement on the job objective. When the consultant leaves the site, you can be sure that the objective has been achieved.

Training

McAfee's expertise and experience is available to your personnel, allowing an organization to take full advantage of its computing resources. McAfee offers on-site training on all McAfee products, network management seminars, anti-virus seminars, customized curriculums for site-specific applications as well as product and personnel certification. McAfee's consultants provide extensive training with curriculum tailored to your organization's needs.

Consulting

McAfee Professional Services offer a number of hourly and daily consulting services including:

- Troubleshooting an existing installation
- Writing PowerScript or SaberBASIC scripts
- Planning and designing networks
- Installing and configuring McAfee products
- Configuring Windows 95
- One-on-one consulting

McAfee Professional Services are available on a quotable time and materials basis to perform project management, product research, and a number of other consulting services.

Jump Start program

This fixed-fee consulting program is designed to get clients up and running on McAfee products as soon as possible. It includes training, installation, and configuration services as needed on a single server. It is designed to demonstrate how to connect various PCs to the LAN, train administrators how to use the program, and master the roll-out process.

Enterprise support

McAfee's Enterprise Support Program provides customers with the highest level of support possible. This fee-based program is designed for those customers who need a higher level of personal service.

The Enterprise Support Program offers the following features:

- Direct pager number to your assigned senior Enterprise Support Program analyst
- Extended support hours: 7:00 A.M. to 7:00 P.M. central time, Monday through Friday
- Five designated McAfee contacts
- Proactive support, providing updated company and product information as it becomes available
- On-site services at a 25% discount
- VIP issues review list
- Beta site (if desired)

Every Enterprise Support Representative calls clients each week. This phone call is used to forward any information such as technical notes and application anomalies of which you should be aware. This call also ensures that you have no unresolved problems or complications with the product. Enterprise Support representatives will return your page on the day it is received.

Optional 7 x 24 enterprise support


Frequently, customers are responsible for their own LANs, which run 24 hours a day, seven days a week. This feature offers round-the-clock support for clients requiring support outside normal business hours.





McAfee reserves the right to change part or all of its Professional Services Programs at any time without notice.



VirusScan Command-line Options


The following table lists all of the VirusScan options you can use when you're running the program from the command line. To run VirusScan from the command line, first use the `cd` command to change directories to the directory in which VirusScan was installed. Then, type `scan /?` to display a list of options and descriptions of how they can be used.

 *When specifying a filename as part of a command-line option, you must include the full path to the file if it is not located in the directory in which VirusScan is installed.*

Command-line Option	Description
<code>/?</code> or <code>/HELP</code>	Does not scan. Instead, displays a list of VirusScan command-line options with a brief description of each. Use either of these options alone on the command line (with no other options).
<code>/ADL</code>	Scans all local drives (including compressed, CD-ROM, and PCMCIA drives, but not diskettes), in addition to those specified on the command line. To scan both local and network drives, use <code>/ADL</code> and <code>/ADN</code> together in the same command line.
<code>/ADN</code>	Scans all network drives for viruses, in addition to those specified on the command line. To scan both the local drives and network drives, use <code>/ADL</code> and <code>/ADN</code> together in the same command line.

Command-line Option	Description
/AF filename	<p>Stores validation/recovery codes in <i>filename</i>.</p> <p>Helps you detect new or unknown viruses. /AF logs validation and recovery data for executable files, the boot sector, and Master Boot Record on a hard disk or diskette in a file you specify. The log file is about 89 bytes per file validated.</p> <p>You must specify a <i>filename</i>, which can include the full path. If the target path is a network drive, you must have rights to create and delete files on that drive. If <i>filename</i> exists, VirusScan updates it. /AF adds about 300% more time to scanning.</p> <p> <i>/AF performs the same function as /AV, but stores its data in a separate file rather than changing the executable files themselves.</i></p> <p><i>The /AF option does not store any information about the Master Boot Record or boot sector of the drive being scanned.</i></p>
/ALL	<p>Overrides the default settings by scanning all files.</p> <p>This option substantially increases the scanning time required. Use it if you have found a virus or suspect one.</p> <p> <i>The list of extensions for standard executables has changed from previous releases of VirusScan.</i></p>
/APPEND	<p>Used in conjunction with /REPORT, appends the report message text to the specified report file, if it exists. Otherwise, the /REPORT option overwrites the specified report file, if it exists.</p>

Command-line Option	Description
/AV	<p>To help you detect and recover from new or unknown viruses, /AV adds recovery and validation data to each standard executable file (.EXE, .COM, .SYS, .BIN, .OVL, and .DLL), increasing the size of each file by 98 bytes. To update files on a shared network drive, you must have update access rights.</p> <p>To exclude self-modifying or self-checking files, and damaged files that might cause false alarms, use the /EXCLUDE option. Using any of the /AV, /CV, or /RV options together in the same command line returns an error.</p> <p> <i>The /AV option does not store any information about the Master Boot Record or boot sector of the drive being scanned.</i></p>
/BOOT	<p>Scans only the boot sector and Master Boot Record on the specified drive.</p>
/CF filename	<p>Helps you detect new or unknown viruses. Checks validation data stored by the /AF option in <i>filename</i>. If a file or system area has changed, VirusScan reports that a viral infection may have occurred. The /CF option adds about 250% more time to scanning.</p> <p>Using any of the /AF, /CF, or /RF options together in a command line returns an error.</p> <p> <i>Some older Hewlett-Packard and Zenith PCs modify the boot sector each time the system is booted. If you use /CF, VirusScan continuously reports that the boot sector has been modified even though no virus may be present. Check your computer's reference manual to determine whether your PC has self-modifying boot code.</i></p>

Command-line Option	Description
<code>/CONTACTFILE filename</code>	<p>Identifies a file containing a message string to display when a virus is found. This option is especially useful in network environments, because you can easily maintain the message text in a central file rather than on each workstation.</p> <p>Any character is valid except a backslash (\). Messages that begin with a slash (/) or a hyphen (-) should be placed in quotation marks.</p>
<code>/CV</code>	<p>Helps you detect new or unknown viruses. Checks validation data added by the <code>/AV</code> option. If a file is modified, VirusScan reports that a viral infection may have occurred. The <code>/CV</code> option adds about 50% more time to scanning.</p> <p>Using any of the <code>/AV</code>, <code>/CV</code>, or <code>/RV</code> options together in the same command line returns an error.</p> <p> <i>The <code>/CV</code> option does not check the boot sector for changes.</i></p>
<code>/EXCLUDE filename</code>	<p>Excludes any files listed in <i>filename</i> from the scan. This option allows you to exclude files from <code>/AF</code> and <code>/AV</code> validation and <code>/CF</code> and <code>/CV</code> checking. Self-modifying or self-checking files can cause a false alarm during a scan.</p>
<code>/FAST</code>	<p>Speeds up the scan.</p> <p>Reduces scanning time by about 15%. Using the <code>/FAST</code> option, VirusScan examines a smaller portion of each file for viruses.</p> <p>Using <code>/FAST</code> might miss some infections found in a more comprehensive (but slower) scan. Do not use this option if you have found a virus or suspect one.</p>

Command-line Option	Description
<code>/FREQUENCY hours</code>	<p>The number of hours that must occur between subsequent successful scans (Example: <code>/FREQUENCY 1</code>).</p> <p>In environments where the risk of viral infection is very low, use this option to prevent unnecessary or too-frequent scans. The lower the number of <i>hours</i> specified, the greater the scan frequency and the greater your protection against infection.</p>
<code>/LOAD filename</code>	<p>Performs a scan using the information saved in <i>filename</i>.</p> <p>You can store all custom settings in a separate configuration file (an ASCII text file), then use <code>/LOAD</code> to load those settings from that file.</p>
<code>/LOCK</code>	<p>Halts the system to stop further infection if VirusScan finds a virus.</p> <p><code>/LOCK</code> is appropriate in highly vulnerable network environments, such as open-use computer labs. If you use <code>/LOCK</code>, we recommend you use it with <code>/CONTACTFILE</code> to tell users what to do or whom to contact if a virus is found and the system locks up.</p>
<code>/LOG</code>	<p>Stores the time and date VirusScan is being run by updating or creating a file called <code>SCAN.LOG</code> in the root of the current drive.</p>


Command-line Option	Description
/MANY	<p>Scans multiple diskettes consecutively in a single drive. VirusScan prompts you for each diskette. Once you have established a virus-free system, use this option to check multiple diskettes quickly.</p> <p>The VirusScan program should reside on a disk that will not be removed during the scan.</p> <p>For example, if you are scanning disks in the computer's A: drive, and you are running the program from a disk in the A: drive, the program will become unavailable as soon as you remove the diskette to put another in. The following command causes an error during execution:</p> <pre>a:\scan a: /many</pre>
/MEMEXCL	<p>Exclude memory area from scanning. (The default is A000-FFFF, 0000=Scan all.)</p> <p>This command-line option has been added to prevent VirusScan from checking areas in upper memory which might contain memory-mapped hardware and might cause false alarms.</p>
/MOVE directory	<p>Moves all infected files found during a scan to the specified directory. To preserve drive and directory structure, this option has no effect if the Master Boot Record or boot sector is infected, since these are not actually files.</p>
/NOBEEP	<p>Disables the tone that sounds whenever VirusScan finds a virus.</p>
/NOBREAK	<p>Disables CTRL-C and CTRL-BREAK during scans.</p> <p>Users will not be able to halt scans in progress using CTRL-C or CTRL-BREAK. Use this option in conjunction with /LOG to create a meaningful audit trail of regularly scheduled scans.</p>

Command-line Option	Description
/NOCOMP	<p>Skips checking of compressed executables created with the LZEXE or PKLITE file-compression programs.</p> <p>Reduces scanning time when a full scan is not needed. Otherwise, by default, VirusScan checks inside executable, or self-decompressing, files that have been created using the LZEXE or PKLITE file-compression programs. VirusScan decompresses each file in memory and checks for virus signatures, which takes time but results in a more thorough scan. If you use /NOCOMP, VirusScan does not check inside compressed files for viruses, although it can check for modifications to those files if they have been validated using validation/recovery codes.</p>
/NODDA	<p>No direct disk access.</p> <p>Prevents VirusScan from accessing the boot record. This feature has been added to allow VirusScan to run under Windows NT.</p> <p>You might need to use this option on some device-driven drives.</p>
/NOEMS	<p>Prevents VirusScan from using expanded memory (LIM EMS 3.2), ensuring that EMS is available to other programs.</p>
/NOEXPIRE	<p>Disables the “expiration date” message if the VirusScan data files are out of date.</p>

Command-line Option	Description
/NOMEM	<p>Reduces scan time by omitting all memory checks for viruses. Use /NOMEM only when you are absolutely certain that your computer is virus-free.</p> <p>VirusScan can check system memory for all critical known computer viruses that can inhabit memory. In addition to main memory from 0kB to 640kB, VirusScan checks system memory from 640kB to 1088kB that can be used by computer viruses on 286 and later systems. Memory above 1088kB is not addressed directly by the processor and is not presently susceptible to viruses.</p>
/PAUSE	<p>Enables screen pause.</p> <p>If you specify /PAUSE, the “Press any key to continue” prompt appears when VirusScan fills up a screen with messages (for example, when you’re using the /SHOWLOG or /VIRLIST options). Otherwise, by default, VirusScan fills and scrolls a screen continuously without stopping, which allows VirusScan to run on PCs with many drives or that have severe infections without requiring you to attend.</p> <p>We recommend that you omit /PAUSE when keeping a record of VirusScan’s messages using the report options (/REPORT, /RPTCOR, /RPTMOD, and /RPTERR).</p>
/PLAD	<p>Preserve last access dates (on proprietary drives only).</p> <p>Prevents changing the last access date attribute for files stored on a network drive in a proprietary network. Normally, proprietary network drives update the last access date when VirusScan opens and examines a file. However, some tape backup systems use this last access date to decide whether to back up the file. Use /PLAD to ensure that the last access date does not change as the result of scanning.</p>


Command-line Option	Description
<code>/REPORT filename</code>	<p>Creates a report of infected files and system errors.</p> <p>Saves the output of VirusScan to <i>filename</i> in ASCII text file format. If <i>filename</i> exists, /REPORT erases and replaces it (or, if you use /APPEND, adds the report information to the end of the existing file).</p> <p>You can include the destination drive and directory (such as D:\VSREPT\ALL.TXT), but if the destination is a network drive, you must have rights to create and delete files on that drive. You can also use /RPTALL, /RPTCOR, /RPTMOD, and /RPTERR to add scanned files, corrupted files, modified files, and system errors to the report.</p>
<code>/RF filename</code>	<p>Removes recovery and validation data from <i>filename</i> created by the /AF option.</p> <p>If <i>filename</i> resides on a shared network drive, you must be able to delete files on that drive. Using any of the /AF, /CF, or /RF options together in the same command line returns an error.</p>
<code>/RPTALL</code>	<p>Adds list of files scanned to the report file (used with /REPORT).</p>
<code>/RPTCOR</code>	<p>When used in conjunction with /REPORT, adds the names of corrupted files to the report file.</p> <p>A corrupted file may be a file that has been damaged by a virus. You can use /RPTCOR with /RPTMOD and /RPTERR on the same command line.</p> <p>✍ <i>There may be false readings in some files that require an overlay or another executable to run properly (that is, a file that is not executable on its own).</i></p>

Command-line Option	Description
/RPTERR	<p>Adds a list of system errors to the report file. This option is used in conjunction with /REPORT.</p> <p>System errors include problems reading or writing to a diskette or hard disk, file system or network problems, problems creating reports, and other system-related problems. You can use /RPTERR with /RPTCOR and /RPTMOD on the same command line.</p>
/RPTMOD	<p>Adds list of modified files to the report file. This option is used in conjunction with /REPORT.</p> <p>VirusScan identifies modified files when the validation/recovery codes do not match (using the /CF or /CV options). You can use /RPTMOD with /RPTCOR and /RPTERR on the same command line.</p>
/RV	<p>Removes validation and recovery data from files validated with the /AV option.</p> <p>To update files on a shared network drive, you must have access rights to update them. Using any of the /AV, /CV, or /RV options together in the same command line returns an error.</p>
/SHOWLOG	<p>Displays the contents of SCAN.LOG.</p> <p>SCAN.LOG stores the time and date VirusScan is being run by updating or creating a file called SCAN.LOG in the current directory and the date and time of previous scans that have been recorded in the SCAN.LOG file using the /LOG switch.</p> <p>The SCAN.LOG file contains text and some special formatting. To pause when the screen fills with messages, specify the /PAUSE option.</p>

Command-line Option	Description
/SUB	<p>Scans subdirectories inside a directory.</p> <p>By default, when you specify a directory to scan rather than a drive, VirusScan will examine only the files it contains, not its subdirectories. Use /SUB to scan all subdirectories inside any directories you have specified. Do not use /SUB if you are scanning an entire drive.</p>
/VIRLIST	<p>Displays the name and a brief description of each virus that VirusScan detects. To pause when the screen fills with messages, specify the /PAUSE option. Use /VIRLIST alone or with /PAUSE on the command line.</p> <p>You can save the list of virus names and descriptions to a file by redirecting the output of the command. For example, in DOS, enter:</p> <pre>scan /virlist > filename.txt</pre> <p> <i>Because VirusScan can detect many viruses, this file is more than 250 pages long.</i></p>

VirusScan DOS Error Levels

When you run VirusScan in the DOS environment, a DOS error level is set. You can use the ERRORLEVEL in batch files to take different actions based on the results of the scan.

 See your DOS operating system documentation for more information.

VirusScan can return the following error levels:

ERRORLEVEL	Description
0	No errors occurred; no viruses were found.
1	Error occurred while accessing a file (reading or writing).
2	A VirusScan data file is corrupted.
3	An error occurred while accessing a disk (reading or writing).
4	An error occurred while accessing the file created with the /AF option; the file has been damaged.
5	Insufficient memory to load program or complete operation.
6	An internal program error has occurred (out of memory error).
7	An error occurred in accessing an international message file (MCAFEE.MSG).
8	A file required to run VirusScan, such as SCAN.DAT, is missing.
9	Incompatible or unrecognized option(s) or option argument(s) specified in the command line.
10	A virus was found in memory.
11	An internal program error occurred.

ERRORLEVEL	Description
12	An error occurred while attempting to remove a virus, such as no CLEAN.DAT file found, or VirusScan was unable to remove the virus.
13	One or more viruses were found in the Master Boot Record, boot sector, or files.
14	The SCAN.DAT file is out of date; upgrade VirusScan data files.
15	VirusScan self-check failed; it may be infected or damaged.
16	An error occurred while accessing a specified drive or file.
17	No drive, directory, or file was specified; nothing to scan.
18	A validated file has been modified (/CF or /CV options).
19-99	Reserved.
100+	Operating system error; VirusScan adds 100 to the original number.
102	CTRL+C or CTRL+BREAK was used to interrupt the Scan. (You can disable CTRL+C or CTRL+BREAK with the /NOBREAK command-line option.)

VSH File Format

The VSH file is a configuration text file, formatted similarly to the Windows INI file, which outlines VShield's settings. Each variable in the file has a name followed by the equal (=) sign and a value. The values define which settings have been selected for VShield configuration. The variables are arranged in five groups: DetectionOptions, ActionOptions, ReportOptions, General, and ExcludedItems. To edit the VSH file, right-click on the filename and select Edit.



In Boolean variables, possible values are 0 and 1. The 0 value instructs VirusScan to disable the setting, while 1 indicates that the setting is enabled.

DetectionOptions

Variable	Description
szProgramExtensions	Type: String Defines extensions to be scanned Default value: EXE COM DO?
szDefaultProgramExtensions -	Type: String Defines extensions to be used as default program extensions during scan configuration Default value: EXE COM DO?
bScanOnExecute	Type: Boolean (1/0) Instructs VShield to scan when files are run Default value: 1
bScanOnOpen	Type: Boolean (1/0) Instructs VShield to scan when files are opened Default value: 1
bScanOnCreate	Type: Boolean (1/0) Instructs VShield to when files are created Default value: 1
bScanOnRename	Type: Boolean (1/0) Instructs VShield to when files are renamed Default value: 1
bScanOnBootAccess	Type: Boolean (1/0) Instructs VShield to scan the boot record of a disk drive the first time it is accessed Default value: 1
bScanAllFiles	Type: Boolean (1/0) Instructs program to scan inside all files Default value: 0

Variable	Description
bScanCompressed	Type: Boolean (1/0) Instructs program to scan inside compressed files (PkLite, LZEXE) Default value: 1

ActionOptions

Variable	Description
szCustomMessage	Type: String Defines custom message to be displayed upon virus detection if action is set to Prompt for Action Default value: Possible Virus Detected
szMoveToFolder	Type: String Defines folder to which infected files should be moved Default value: \Infected
uVshieldAction	Type: Integer (1-5) Instructs VShield to take the action specified when a virus is detected Possible values: 1 - Prompt for action 2 - Move infected files to a folder 3 - Clean infected files automatically (Deny access if files can't be cleaned) 4 - Delete infected files automatically 5 - Deny access to infected files Default value: 1
bButtonClean	Type: Boolean (1/0) Instructs VShield to give user option of cleaning file if Prompt for Action is selected and a virus is detected Default value: 1

Variable	Description
bButtonDelete	Type: Boolean (1/0) Instructs VShield to give user option of deleting file if Prompt for Action is selected and a virus is detected Default value: 1
bButtonExclude	Type: Boolean (1/0) Instructs VShield to give user option of excluding file if Prompt for Action is selected and a virus is detected Default value: 1
bButtonStop	Type: Boolean (1/0) Instructs VShield to give user option of denying access to the infected file if Prompt for Action is selected and a virus is detected Default value: 1
bButtonContinue	Type: Boolean (1/0) Instructs VShield to give user option of continuing the intercepted event if Prompt for Action is selected and a virus is detected Default value: 1
bDisplayMessage	Type: Boolean (1/0) Defines if custom message should be displayed in the Prompt for Action dialog box upon virus detection Default value: 0

ReportOptions

Variable	Description
szLogFileName	Type: String Defines log file name Default value: C:\McAfee\Virus- can\VShield.log
bLogToFile	Type: Boolean (1/0) Defines if scan results should be logged into log file Default value: 1
bLimitSize	Type: Boolean (1/0) Defines if size of the log file should be limited Default value: 1
uMaxKilobytes	Type: Integer (10-999) Defines maximum size of the log file in kilobytes Default value: 100
bLogDetection	Type: Boolean (1/0) Defines if scanning results should be logged Default value: 1
bLogClean	Type: Boolean (1/0) Defines if cleaning results should be logged Default value: 1
bLogDelete	Type: Boolean (1/0) Defines if infected file delete operations should be logged Default value: 1

Variable	Description
bLogMove	Type: Boolean (1/0) Defines if infected file move operations should be logged Default value: 1
bLogSettings	Type: Boolean (1/0) Defines if session settings should be logged on shutdown Default value: 1
bLogSummary	Type: Boolean (1/0) Defines if session summary should be logged on shutdown Default value: 1
bLogDateTime	Type: Boolean (1/0) Defines if time and date of an event should be logged Default value: 1
bLogUserName	Type: Boolean (1/0) Defines if user name should be logged Default value: 1

General

Variable	Description
bLoadAtStartup	Type: Boolean (1/0) Defines if VShield should be loaded at system start-up Default value: 256
bCanBeDisabled	Type: Boolean (1/0) Defines if VShield can be disabled Default value: 1
bShowTaskbarIcon	Type: Boolean (1/0) Defines whether VShield taskbar icon is displayed Default value: 257
bNoSplash	Type: Boolean (1/0) Instructs VShield to not show splash screen when program is launched Default value: 0

ExcludedItems

Variable	Description
NumExcludedItems	Type: Integer (0-n) Defines the number of items excluded from on-access scanning Default value: 0

ExcludedItem_x, where x is a zero- based index	<p>Type: String</p> <p>Instructs VShield to exclude the item from on-access scanning</p> <p>Default value: \Recycled *.* 1 1 *</p> <p>* The string is separated into fields using the pipe () character:</p> <p>Field 1 - Folder portion of item to exclude. Leave blank for a single file anywhere on the system.</p> <p>Field 2 - File portion of the item to exclude. Leave blank if a folder is excluded without a filename.</p> <p>Field 3 - Integer (1-3)</p> <p>Possible values:</p> <ul style="list-style-type: none">1 - Exclude from file-access scanning2 - Exclude from boot-record scanning3 - Exclude from both boot-record and file-access scanning <p>Field 4 - Boolean (1/0)</p> <p>Possible values:</p> <ul style="list-style-type: none">1 - Instructs VShield to exclude subfolders of the excluded item2 - Instructs VShield to not exclude subfolders
--	---



Glossary

The following list defines some terms you might encounter while using VirusScan to guard your computer against viruses.

BIOS

A read-only memory chip that contains the coded instructions for using hardware such as a keyboard or monitor. Always present in portable computers, a BIOS (boot ROM) is not susceptible to infection (unlike the boot sector on a disk). Some BIOS chips contain anti-virus features that can generate a false alarm, installation failure, and other problems.

boot

To start a computer. The computer will load start-up instructions from a disk's boot ROM (BIOS) or boot sector. See also “cold boot” and “warm boot.”

boot sector

A portion of a disk that contains the coded instructions for the operating system to start the computer.

boot sector infection

Contamination of the boot sector by a virus. A boot sector infection is particularly dangerous because information in the boot sector is loaded into memory first, *before* virus protection code can be executed. The only certain way to eliminate a boot sector infection is to start your computer from a clean start-up diskette, then remove the infection using VirusScan.



boot disk

A write-protected diskette that contains the computer's system and start-up files. You can use this diskette to start up your computer. It is important to use a virus-free boot disk to guarantee that a virus is not introduced into the computer.

cold boot

To turn on a computer, or to restart a computer by turning it off, waiting a few seconds, and turning it on again. Other methods of restarting (such as pressing a reset button or pressing CTRL+ALT+DEL) may not remove all traces of a virus infection from memory. See also “boot” and “warm boot.”

compressed executable

A file that has been compressed using a file compression utility such as LZEXE or PKLITE. See also “compressed file.”

compressed file

A file that has been compressed using a file compression utility such as PKZIP. See also “compressed executable.”

conventional memory

Up to 640KB (1MB) of main memory in which DOS executes programs.

corrupted file

A file that has been irreparably damaged, by a virus for example.

detection

Scanning memory and disks for clues that a virus may be present. Some detection methods include searching for common viral patterns or strings, comparing suspicious file activity with known virus activity, and monitoring files for unauthorized changes.



disinfect

To eradicate a **virus** so that it can no longer spread or cause damage to a system.

exception list

List of files to which **validation codes** should not be added because they have built-in virus detection, contain self-modifying code, or are unlikely to be infected by a virus. Such files are usually skipped in validation checking because they may trigger a **false alarm**.

executable (file)

A file containing coded instructions to be executed by the computer. Executable files include programs and overlays (auxiliary program code which cannot be executed directly by the user).

expanded memory

Computer memory above the DOS 1MB limit of **conventional memory** that is accessed by memory paging. You need special software, conforming to an expanded memory specification, to take advantage of expanded memory.

extended memory

Linear memory above the DOS 1MB limit of **conventional memory**. Often used for RAM disks and print spoolers.

false alarm

Reporting a viral infection when none is present.

fast

A scanning option that is faster than normal but less comprehensive (because it checks a smaller portion of each file).

infected file

A file contaminated by a **virus**.



Master Boot Record (MBR)

A portion of a hard disk that contains a partition table that divides the drive into “chunks,” some of which may be assigned to operating systems other than DOS. The MBR accesses the **boot sector**.

memory

A storage medium where data or program code are kept temporarily while being used by the computer. DOS supports up to 640KB of **conventional memory**. Beyond that limit may be accessed as **expanded memory**, **extended memory**, or an **upper memory block (UMB)**.

memory infection

Contamination of **memory** by a **virus**. The only certain way to eliminate memory infection is to *shut down your computer*, restart from a **clean start-up diskette**, and clean up the source of the infection using VirusScan.

modified file

A file that has changed after **validation codes** have been added, possibly by a **virus**.

overlay infection

Virus contamination of a file containing auxiliary program code that is loaded by the main program.

polymorphic virus

A virus that attempts to evade detection by changing its internal structure or its encryption techniques.

read operation

Any operation in which information is read from a disk, including a hard drive, floppy diskette, CD-ROM, or network drive. DOS commands that perform read operations include DIR (directory listing), TYPE (display contents of a file), and COPY (copy files). See also “**write operation**.”



recovery codes

Information that VirusScan records about an executable file in order to recover (repair) it if it is damaged by a virus. See also “[validation codes](#).”

self-modifying program

Software that changes its own program files, often to protect against viruses or illegal copying. These programs should be included in an [exception list](#) to prevent these modifications from being reported as a [false alarm](#) by VirusScan.

system errors

Errors that can prevent VirusScan from completing its job successfully. System error conditions include disk format errors, media errors, file system errors, network errors, device access errors, and report failures.

unknown virus

A virus not yet identified and listed in SCAN.DAT. VirusScan can detect unknown viruses by observing changes in files that could result from infection.

upper memory block (UMB)

Memory in the range 640KB to 1024KB, just above the DOS 640KB limit of [conventional memory](#).

validate

To check that a file is authentic and has not been altered. Most validation methods rely on computing a statistic based on all the data in the file, which is unlikely to remain constant if the file itself is changed.

validation codes

Information that VirusScan records about an executable file in order to detect subsequent infection by a virus. See also “[recovery codes](#).”



virus

A software program that attaches itself to another program on a disk or lurks in a computer's memory, and spreads from one program to another. Viruses may damage data, cause computers to crash, display messages, and so on.

warm boot

To restart (reset) a computer by pressing CTRL+ALT+DEL. See also [“boot”](#) and [“cold boot.”](#)

write operation

Any operation in which information is recorded to a disk. Commands that perform write operations include those that save, move, or copy files. See also [“read operation.”](#)

write protection

A mechanism to protect files or disks from being changed. A file may be write protected by changing its system attributes. A diskette may be write protected by sliding its movable corner tab so that the square hole is open (3.5" diskettes) or by covering its corner notch with a write-protect tab (5.25" diskettes).

A

America Online 9

B

BBS 8

Boot diskette
making a 58

Boot record
preventing VirusScan
from accessing 83

Boot sector
limiting scan to 79

Bulletin Board Sys-
tem 8

C

Cleaning viruses
from memory 51

Compressed files
skipping during virus
scans 83

CompuServe 8

Consulting 74

Control Break
disabling during scans
82

Control C
disabling during scans
82

Customer Care
department 8

Customer service
8
programs 71

D

Data files
updating 55

Dates
preventing VirusScan
from changing 84

Default settings
creating multiple con-
figuration files 81

DEFAULT.CFG
using a different config-
uration file 81

Direct drive access
disabling with VirusS-
can 83

Directories
scanning 87

Diskettes
scanning multiple 82
write protecting 61

Displaying list of
detected viruses
with VirusScan 87

DOS error levels
VirusScan 88

Drives
scanning local 77
scanning network 77

E

EMS
preventing VirusScan
from using 83

Enterprise sup-
port 75

Excluding files
during virus scans 80

Expanded memory
preventing VirusScan
from using 83

Expiration date
message
disabling 83

F

File types
determining which are
scanned 78

Files
moving infected files
82
preventing VirusScan
from changing last
access dates 84

Floppy diskettes
scanning multiple 82

Frequency
determining for VirusS-
can 81

G

Glossary 99

H

Help
displaying 77

I

Infected files
moving 82
Installation 11
testing 69
Internet support 8

L

Last access date
preventing VirusScan
from changing 84
Library
virus information 68
Local drives
scanning 77
Locking the system
if a virus is found 81
Log file
creating with VirusS-
can 81
displaying 86
LZEXE
and VirusScan 83

M

McAfee
BBS 8
enterprise support 75
jump start program 75
support 8
support services 70
Virus Information
Library 68
website 8
Memory
excluding area from
scans 82
omitting from scans 84
preventing VirusScan
from using expanded
83
Messages
displaying when a virus
is found 80
pausing when display-
ing 84
Microsoft Network
(MSN) 9
Moving
infected files 82

N

Network drives
scanning 77

O

On-access scan-
ning 14
configuring 17
On-demand scan-
ning 25
configuring 31

P

Pausing
when displaying
VirusScan messages
84
PKLITE
and VirusScan 83
Preventing infec-
tion 53
Professional ser-
vices
programs 74
R
Recovery codes
using with VirusScan
78
Recovery data
adding to executable
files 79
removing 85, 86
Reference 77, 99
Removing a virus
from memory 51
Reports
adding names of cor-
rupted files to 85
adding names of modi-
fied files to 86
adding names of
scanned files to 85
adding system errors
to 86
generating with VirusS-
can 78, 85
Requirements
system 11

S

Scan

- virus detection method 6

SCAN.LOG

- creating a log 81
- displaying 86

Scanning

- when to scan 6

Start-up diskette

- making a 58

Subdirectories

- scanning 87

Support

- enterprise 75
- international 10
- programs 71

System require-

- ments 11

T

Technical support

- 8
- contacting 8
- international 10

Training 74

- scheduling 9

V

Validate 57

Validating VirusS-

- can 57
- Validation codes
 - using with VirusScan 78

Validation data

- adding to executable files 79
- checking 80
- checking during virus scans 79
- removing 85, 86

Virus

- defined 104
- infections 65
- McAfee Information Library 68
- new and unknown 55
- preventing infection 53
- protection against 66
- types and classifica-tions 64
- understanding 63
- updating data files 55
- what is a 64

Virus removal

- from memory 51

Virus scanning

- excluding files 80
- excluding the memory area 82
- file types scanned 78
- including subdirecto-ries 87
- moving infected files 82
- multiple diskettes 82
- network drives 77
- preventing users from halting 82
- skipping compressed files 83
- speeding up 80
- system memory 84

Viruses

- displaying list of detected 87
- locking the system if found 81

VirusScan

- and expanded mem-ory 83
- command-line exam-ples 88
- command-line options 77
- disabling expiration date message 83
- displaying a message when a virus is found 80
- displaying list of detected viruses 87
- DOS error levels 88
- excluding files 80
- excluding memory area from scans 82
- generating a report file 78, 85, 86
- installing 11
- introducing 5
- locking the system 81
- multiple diskettes 82
- preventing users from halting 82
- scanning only the boot sector 79
- setting the scan fre-quency 81
- speeding the scan 80
- validation 85

VirusScan com-	/SHOWLOG 86
mand-line options	/SUB 87
/? or /HELP 77	/VCV 80
/ADL 77	/VIRLIST 87
/ADN 77	VirusScan95
/AF 78	configuring 31
/ALL 78	using 25
/APPEND 78	VSH file format 90
/AV 79	VShield
/BOOT 79	actions 20
/CF 79	configuring 17
/CONTACTFILE 80	detection 18
/EXCLUDE 80	exclusions 23
/FAST 80	reports 22
/FREQUENCY 81	starting 15
/LOAD 81	using 14
/LOCK 81	
/LOG 81	
/MANY 82	
/MEMEXCL 82	
/MOVE 82	
/NOBEEP 82	
/NOBREAK 82	
/NOCOMP 83	
/NODDA 83	
/NOEMS 83	
/NOEXPIRE 83	
/NOMEM 84	
/PAUSE 84	
/PLAD 84	
/REPORT 85	
/RPTALL 85	
/RPTCOR 85	
/RPTERR 86	
/RPTMOD 86	
/RRF 85	
/RV 86	

W

World Wide Web 8
Write protecting
diskettes 61