User's Guide

VirusScan for Windows 95

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, GroupScan, GroupShield, PCCrypto, WebCrypto, Remote Desktop 32, eMail-It, WebShield, 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.

Issued October 1996/VirusScan v2.0.6

Table of Contents

1 Introducing VirusScan

What is VirusScan?

VirusScan is McAfee's powerful desktop anti-virus solution. Once installed, VirusScan continuously monitors your system for virus activity. 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.
- VirusScan95 is a native Windows 95 application, providing true 32-bit implementation, long filename support, Windows 95 context-sensitive help, and unobtrusive memory scanning.
- VShield, VirusScan's on-access scanner, provides real-time identification of both known and unknown viruses upon file access, create, copy, rename, and run; disk insert; system startup; and system shut down.

- On-demand scanning provides for user-initiated detection of known boot, file, mutation, 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 notification, logging, deletion, isolation, or cleaning.
- The VirusScan Scan Window, Activity Log, and VirusInfo provide details of scan results, as well as information about detected viruses.
- Monthly updates of virus signatures are included with the purchase of a McAfee subscription license to assure the best detection and removal rates. See Appendix D, "McAfee Support Services," for details.

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, insert a diskette, start up your system, or shut down. It also protects your system against viruses when you upload and download from networks or receive files electronically.

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 can 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.

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 and Fax Response System	(408) 988-3034
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 43.
3.	Confirm that your Date/Time settings are accurate.

✍ *Windows 95 does not require DOS memory managers. If you choose to use them, VirusScan95 may falsely detect viruses in memory. To eliminate this possibility, remove the memory manager command lines from your CONFIG.SYS file.*

System Requirements

- IBM-compatible personal computer running Windows 95
- 486 with at least 8MB of memory, 2.5MB of free hard drive space

✍ *VirusScan95 is a native Windows 95 application. As such, Windows 95 must be functioning properly in order to install and use this software. You cannot install VirusScan95 onto a Windows 3.1x system.*

Installation Procedure

Follow the procedure outlined below to install VirusScan.

✍ *If you suspect that your system is already infected by a virus, see "If You Suspect You Have a Virus" on page 43 before beginning this procedure.*

Step	Action

1. Start your computer.

2. Do one of the following:

- If you are installing from diskette or compact disc, insert it into your floppy disk drive or CD-ROM drive.
- If you are installing from files downloaded from a BBS or the McAfee Web Site, decompress the zipped files into a directory on the network or your local drive.

3. Select Run from the Start menu.

- If you are installing from diskette, type:

  `x:\setup.exe`

  where *x* is the drive in which you placed the diskette. Click OK.

- If you are installing from compact disc, type:

  `x:\win95\setup.exe`

  where *x* is the drive in which you placed the CD-ROM. Click OK.

- If you are installing from downloaded files, type:

  `x:\path\setup.exe`

  where *x:**path* is the location of the files (for example, C:\DOWN-LOAD\SETUP.EXE). Click OK.

Response: The Welcome screen is displayed.

Action: Click Next to continue.

4. 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.

   ✍ *The Typical installation meets must users' needs.*

5. 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.

   Response: The Confirm Installation Settings screen is displayed.

   Action: Review your settings and click Next to continue

   Response: Installation begins and VirusScan checks your system for viruses.

6. When the scan is complete, take one of the following steps:

   - If a virus is found, VirusScan will display the infected files. Right-click on the infected file and select Virus Info.

     - If the Memory-resident checkbox is selected, cancel the installation. For step-by-step instructions on removing the virus, see "Removing a memory-resident virus found during installation" on page 45.

     - If the Memory-resident checkbox is not selected, McAfee recommends that you delete the infected file and recover a clean copy from backups. Right-click on the infected file and click Delete. You can then continue installation of VirusScan.

   - If no infected files are found, click OK. VirusScan continues copying files to the hard disk drive.

7. Click Yes to review the What's New text file.

8. Review the modifications made to files on your system and click Next.

9. Select Yes to restart your computer. Click Finish.

   Response: The system restarts. VirusScan is now running.

10. Click Yes to review the What's New text file for information on VirusScan's new features.

11. Review the modifications made to files on your system and click Next.

12. Select Yes to restart your computer for VirusScan to be available and for on-access scanning protection to take effect. Click Finish.

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."

3 On-access Scanning

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 three easy methods for ensuring that VShield is active:

- By selecting Programs, McAfee VirusScan95, VShield Configuration Manager from the Start menu, and making sure that the Load VShield at Startup checkbox is selected.
- By double-clicking on VSHWIN.EXE in the installation directory.
- By double-clicking on the VShield icon in the task bar (the Shield next to the clock) and ensuring that the Enable/Disable button is set to Disable. This indicates that VShield is enabled.

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). There are two methods for displaying this window:

- By double-clicking on the VShield icon in the task bar (the Shield next to the clock).
- By right-clicking on the VShield icon and selecting Status.

✍ *Both of these methods require that the VShield icon is visible on the task bar. If your VShield icon is not displayed, select Programs, McAfee VirusScan95, VShield Configuration Manager from the Start menu, and check the box next to Show Icon on the Taskbar. VShield options can also be configured directly from this Configuration Manager.*

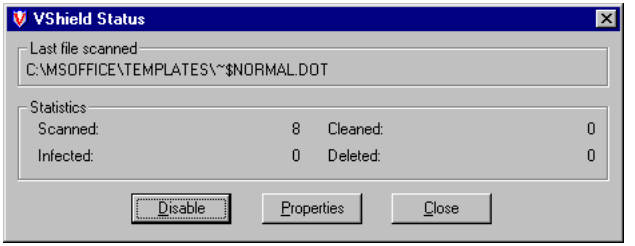

Figure 3-1. VShield Status Window

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 or deleted. 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 95 session. If you select Disable, on-access scanning is disabled during the current session and reactivated when you restart your computer.

- **Properties**: Click this button to configure the detection, action, and reporting settings of on-access scanning. See "Configuring On-access Scanning" on page 18 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. Open the VShield Configuration Manager by taking one of the following steps:

- Select Programs, McAfee VirusScan95, VShield Configuration Manager from the Start Menu.
- Select Properties from the VShield Status Window. See "Using the VShield Status window" on page 16 for details on displaying this window.
- Right-click on the VShield icon in the task bar and select Properties.

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

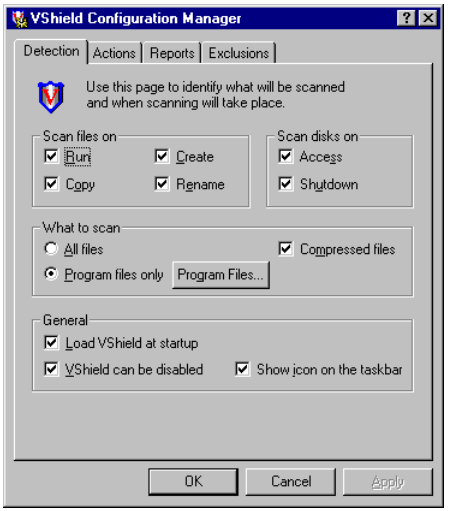

Figure 3-2. VShield Configuration Manager (Detection Property Page)

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. Checkmarks indicate that VShield will scan disks on Access and on Shutdown.

✍ *McAfee recommends selecting all items in these two sections for maximum protection.*

3. Select which files VShield should scan.

- 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. Click Program Files to edit the list of file extensions that VShield scans.

✍ *The default file types are .COM, .EXE, and .DO?. When the DO? extension is selected, VirusScan scans Microsoft Word documents and templates for macro viruses.*

4. Check the Compressed Files checkbox if you want files created with LZEXE and PKLite to be scanned.

5. Configure your general preferences.

- 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 Taskbar if you want to be able to start VShield from the Shield 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 Taskbar boxes when configuring the users' 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.

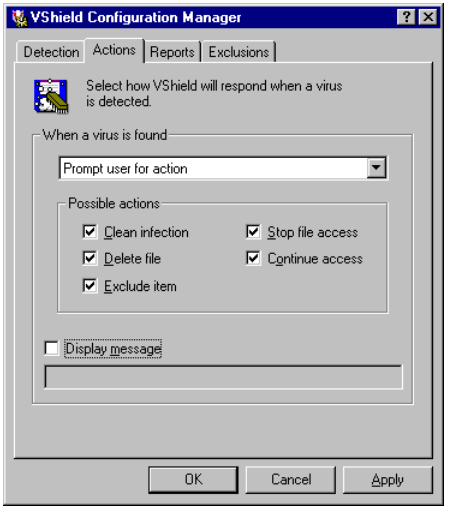

Figure 3-3. VShield Configuration Manager (Actions Property Page)

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 Infection, Delete File, Exclude Item, Stop File Access, and Continue Access.

    ✍ *By unchecking all Possible Actions, network administrators can configure VShield to "lock" users' computers upon virus detection. If using this feature, you should also select Display Message and type a custom message in the text box informing users of whom to contact for assistance.*

- To display a message upon virus detection, click the Display Message checkbox and type a 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 infected files will be moved there.

    ✍ *When this option is selected, VirusScan automatically generates a text file called INFECTED.LOG in the specified folder, which logs the name of the file and where it was found.*

- Clean Infected Files Automatically

  ✍ *VirusScan can repair files damaged by many viruses, but some viruses damage files beyond repair. If VirusScan cannot safely remove the virus, a message is displayed indicating the name of the unrecoverable file.*

- 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.

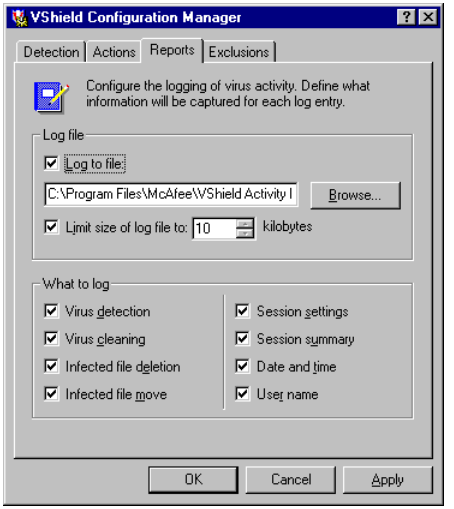

Figure 3-4. VShield Configuration Manager (Reports Property Page)

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 using the scroll buttons to specify a size between 10KB and 999KB.
	✍ *The default path for the log file is C:\Program Files\McAfee\VirusScan95\VShield Activity Log.txt. 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, Date and Time, and User Name.

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.

Exclusions will not be scanned by VirusScan's on-access scanner and should be avoided whenever possible.

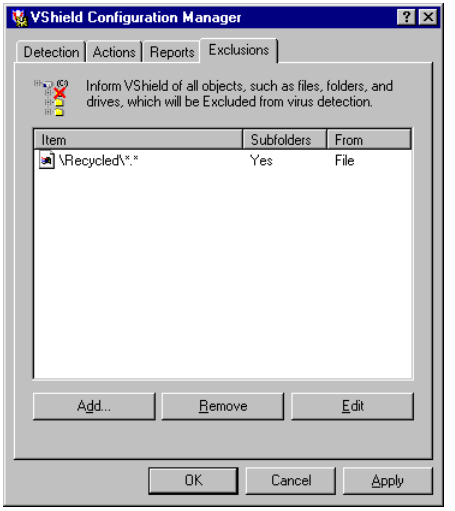

Figure 3-5. VShield Configuration Manager (Exclusions Property Page)

Take the following steps to change these settings:

Step **Action**

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

Response: The Exclude Item dialog box is displayed.

- Type the path to the item or folder you wish to exclude from scanning, or click Browse to navigate to its location.
  - If you enter a filename without a path, such as `MCAFEE.TXT` or `MCAFEE.*`, all files with that description will be excluded, regardless of location.

    ✍ *The wildcard (*) character indicates that all files with the MCAFEE. description should be excluded, regardless of extension. A wildcard can also be used in place of a description, as in `*.TXT`, which indicates that all .TXT files should be excluded.*
  - If you enter a folder, all files in the folder are excluded. `\MCAFEE` indicates that folders on the root named MCAFEE should be excluded, regardless of drive location. Click Include Subfolders if you want to exclude all subfolders within a selected folder.
- Indicate whether you want the item excluded from a File Scan or a Boot Sector Scan by placing checkmarks in the boxes provided.
- Click OK.

2. To remove an item from the list, select it and click Remove.

3. To edit an item on the list, select it and click Edit.

✍ *The default setting excludes the recycled bin.*

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.

✍ *All VShield settings are stored in C:\Program Files\Mcfee\VirusScan95\DEFAULT.VSH. Please see Appendix E, "Reference" for the VSH file format.*

4 On-demand Scanning

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 VirusScan95, you can also perform immediate or scheduled on-demand scans of specific items while you're working.

VirusScan95's on-demand scanner allows you to scan new media or specific files to determine whether a computer virus is present. VirusScan95 immediately detects known boot, file, multi-partite, stealth, encrypted, and polymorphic viruses located within files, drives, and diskettes. Using VirusScan in conjunction with Microsoft Plus!, you can also set up scheduled scans to meet your needs.

In this chapter, you'll find procedures for starting VirusScan95, as well as steps you need to take to configure and customize on-demand scanning functions.

Starting VirusScan95

There are two easy methods for starting on-demand scanning in VirusScan95:

- By selecting Programs, McAfee VirusScan95, VirusScan95 from the Start menu.
- By right-clicking on any drive, folder, or executable file and selecting Scan for Viruses.

The VirusScan main window (Figure 4-1) is displayed whenever you start on-demand scanning.

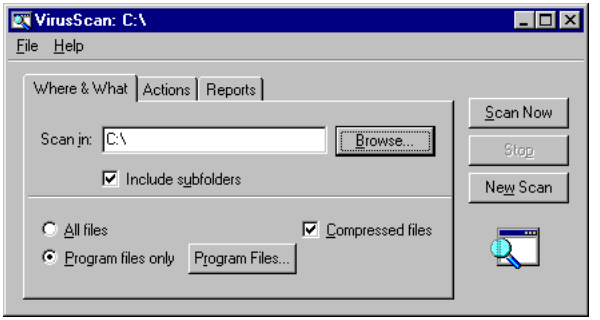

Figure 4-1. VirusScan Main Window (Where & What Property Page)

A description of the basic menus and buttons is provided below.

- The File Menu offers three choices: Save Settings, View Activity Log, and Close. For more information about saving and using settings, see "Using settings files" on page 34. For more information about the activity log, see "Configuring On-demand Scanning" on page 30. Choosing Close exits the program.

  ✍ *In certain circumstances, additional options are added to the File menu. These additional commands are described in detail later in this manual.*

- From the Help Menu, you can choose Help Topics to gain access to online help information; What's This? for context-sensitive help; and About for more information about this product and McAfee.

  ✍ *For context-sensitive help, you also can right-click on any control and select What's This?.*

- The Scan Now button initiates a scan.

- The Stop button halts a scan in progress.

- The New Scan button resets VirusScan95 to its default settings.

Property pages

The VirusScan main window has three tabbed property pages:

- The Where & What property page is used to define the scope of a scan.

- The Actions property page is used to define VirusScan's response if a virus is detected.

- The Reports property page is used to determine VirusScan's notification, reporting, and logging options.

These pages are described in detail in "Configuring On-demand Scanning" on page 30.

Configuring On-demand Scanning

Use the following procedure to configure an on-demand scan of your system.

Step **Action**

1. Start VirusScan95.

Response: The main VirusScan window is displayed, with the Where & What property page on top. (See Figure 4-1 on page 28.)

- In the Scan In text box, enter the path of the drive, folder, or individual file you want VirusScan to scan, or choose Browse to navigate to the location.

  ✍ *If you would like to scan multiple local or network drives, enter* `LocalDrives` *or* `NetworkDrives` *in the text box.*

  If you would like to scan multiple items, create a text file that lists the scan items, one item to a line. Then, type `<x:\path\filename.txt>`*, including the brackets, (where x:\path is the path to the file and filename is the name of the file you created) in the Scan In text box. All items listed in the text file will be scanned.*

- Select Include Subfolders to indicate that all subfolders within the folder you just selected should be scanned. Otherwise, only the selected folder will be scanned.

- Click the All Files button if you want VirusScan to check all files in the selected folder, or select Program Files Only to scan executable and Microsoft Word files in the selected folder. If you select Program Files Only, click the Program Files button to edit the types of files VirusScan will examine.

  ✍ *The default settings are .COM, .DO?, and .EXE. When the DO? extension is selected, VirusScan scans Microsoft Word documents and templates for macro viruses.*

- Select Compressed Files if you want files compressed with PKZIP, PKLite, and LZEXE to be scanned.

2. Select the Actions tab.

Response: The Actions property page is displayed (Figure 4-2).

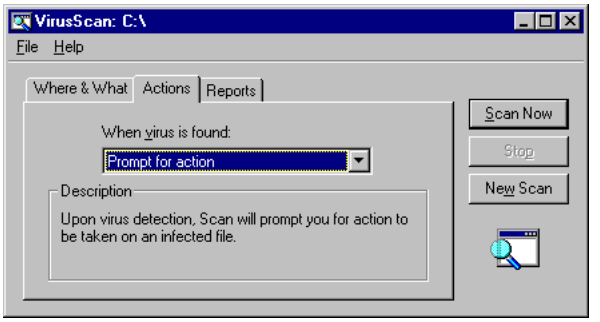

Figure 4-2. VirusScan Main Window (Actions Property Page)

- Select an action for VirusScan95 to take if a virus is found. Options are:
  - Continue Scanning
  - Prompt for Action
  - Move Infected Files to a Folder
  - Clean Infected File
  - Delete Infected File

A description for each action is displayed when the action is selected. For additional information on these options and virus removal, see Chapter 5, “Removing a Virus.”

3. Select the Reports tab.

Response: The Reports property page (Figure 4-3) is displayed.

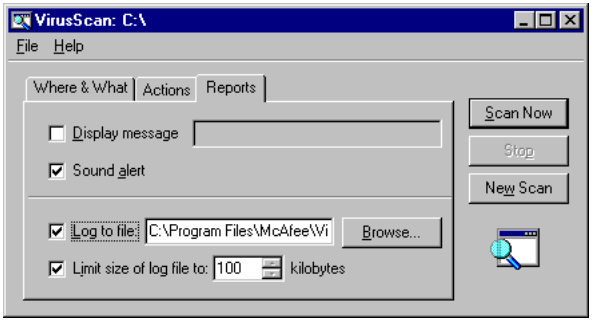

Figure 4-3. VirusScan Main Window (Reports Property Page)

- If you selected Prompt for Action from the Actions property page tab, VirusScan95 can display a custom message to alert users or administrators that a virus has been detected.

  ✍ *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.*

- If you would like VirusScan to sound an alert when a virus is detected, click the Sound Alert checkbox.

  ✍ *This option requires a sound card.*

- If you would like to create a record of your scanning activity, select Log to File. VirusScan will automatically record its activity in the default location, C:\Program Files\McAfee\VirusScan95 \VSLOG.TXT. If you want to select another location, you must enter the path of the drive or folder, or Browse to navigate to the location. Your selection will appear in the Log to File text box.

Select Limit Size of Log File and enter a number between 10KB and 999KB to change the maximum size of the log file.

✍ *The default activity log size is 100KB.*

4. Select Save Settings from the File menu to retain custom settings. See "Using settings files" on page 34 for more information on this feature.

5. Click the Scan Now icon button to begin scanning.

Response: VirusScan checks the drives, folders, and/or files you have selected. Any status or warning messages are displayed in the VirusScan main window, and the names of folders being scanned are displayed in the status bar.

✍ *If you wish to stop scanning before the scan is completed, click Stop.*

6. Upon scan completion, take one of the following steps:

   - If VirusScan reports that no files are infected, your scanned files are most likely virus-free. Select Close from the File menu.

     ✍ *VirusScan's ability to detect viruses must be maintained through regular upgrades of the VirusScan data files. For more information about updating VirusScan, see "Updating your VirusScan data files" on page 53.*

   - If VirusScan detects a virus, it will display the infected files and take the action you specified during configuration. See "If VirusScan Detects a Virus" on page 45 for instructions on how to proceed.

7. McAfee recommends that you regularly back up or copy any important or critical files to fresh diskettes or tape backup so you will have current, clean files should a virus later infect your system and damage your data.

Creating Custom On-demand Scans

VirusScan95 allows you to establish preferred scan settings, which you can save in a settings file. That way, you do not need to select scanning options and items individually every time you want to scan.

✍ *VirusScan95 uses the default settings file C:\Program Files\McAfee\VirusScan95\DEFAULT.VSC when you perform an on-demand scan. Please see Appendix E, "Reference" for the VSC file format.*

VirusScan95 also offers an Administrator Mode that allows system administrators to lock down VirusScan settings on users' systems, and scheduled scanning for users who have Microsoft Plus!. Follow the procedures in this section to customize your scanning options and use these features.

Using settings files

If you are likely to use the same scanning settings frequently, you should save your configuration in a settings file by following the procedure below.

Step	Action
1.	Start VirusScan95.
2.	Configure VirusScan to your preferred settings. See "Configuring On-demand Scanning" on page 30 for details on configuration.
3.	Select Save Settings from the File menu. **Response:** The Save Settings dialog box is displayed.
4.	Select one of the following options: ▪ To retain these settings as an individual custom configuration file, save the .VSC file to the Desktop, under a name of your choice. ▪ To establish your settings as the default, save the new settings by overwriting the default, C:\Program Files\McAfee\VirusScan95\DEFAULT.VSC

Reconfiguring your settings file

Once you have created a custom settings file, you can alter the file's settings by following the steps below.

You can also modify your settings in DEFAULT.VSC by taking these steps.

Step	Action

1. Right-click on the file or Desktop icon and select Properties.

Response: The Properties window is displayed with the General property page on top (Figure 4-4).

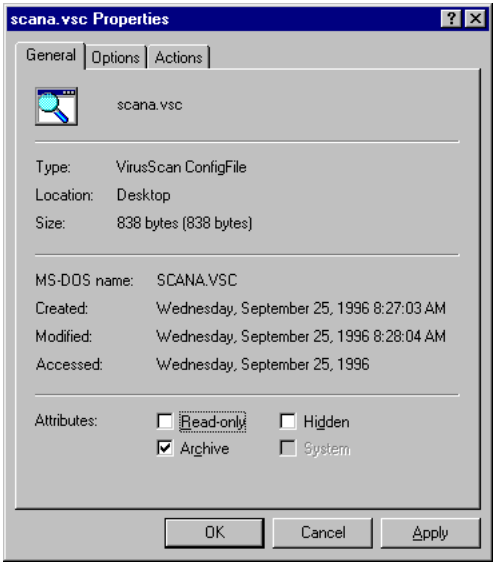

Figure 4-4. Properties Window (General Properties Page)

- Review the information on this page for details on the settings file.
- If you wish to change the file's Attributes, check the appropriate boxes.

2. Select the Options tab.

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

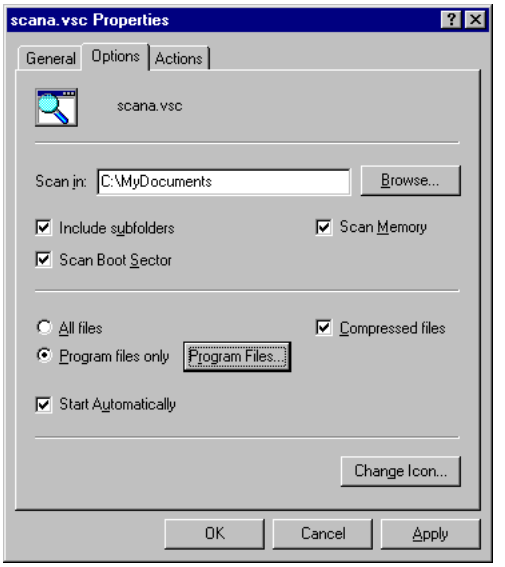

Figure 4-5. Properties Window (Options Property Page)

- In the Scan In text box, enter the path of the drive, folder, or individual file you want VirusScan to scan, or choose Browse to navigate to the location.

  ✍ *If you would like to scan multiple local or network drives, enter* `LocalDrives` *or* `NetworkDrives` *in the text box.*

- Select Include Subfolders to indicate that all subfolders within the folder you just selected should be scanned. Otherwise, only the selected folder will be scanned.

- Click Scan Boot Sector and/or Scan Memory if you want VirusScan to include these areas in its scan.

- Click the All Files button if you want VirusScan to check all files in the selected folder, or select Program Files Only to scan selected program files only. If you select Program Files Only, click the Program Files button to edit the types of files VirusScan will examine.

  ✍ *The default settings are .COM, .DO?, and .EXE. When the DO? extension is selected, VirusScan scans Microsoft Word documents and templates for macro viruses.*

- Select Compressed Files if you want files compressed with PKZIP, PKLite, and LZEXE to be scanned.

- Click Start Automatically if you want the scan to start immediately after the file is launched, without having to click Scan Now.

  ✍ *The Start Automatically option must be selected if this settings file will be used for scheduled scans. See "Setting up scheduled scans" on page 40.*

3. Select the Actions tab.

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

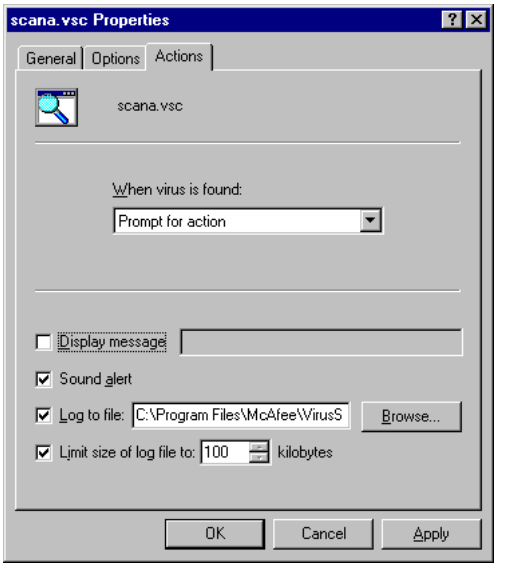

Figure 4-6. Properties Window (Actions Property Page)

- Select an action for VirusScan95 to take if a virus is found. Options are:

  - Continue Scanning
  - Prompt for Action
  - Clean Infected File
  - Delete Infected File

  For additional information on these options and virus removal, see Chapter 5, “Removing a Virus.”

- If you selected Prompt for Action, VirusScan95 can display a custom message to alert users or administrators that a virus has been detected. Click Display Message and type a 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.*

- If you would like VirusScan to sound an alert when a virus is detected, click the Sound Alert checkbox.

  ✍ *This option requires a soundcard.*

- If you would like to create a record of your scanning activity, select Log to File. VirusScan will automatically record its activity in the default location, C:\Program Files\McAfee\VirusScan95\VSLOG.TXT. If you want to select another location, you must enter the path of the drive or folder, or Browse to navigate to the location. Your selection will appear in the Log to File text box.

Select Limit Size of Log File and enter a number between 10KB and 999KB to change the maximum size of the log file.

✍ *The default activity log size is 100KB.*

4. Click Apply to save changes. Click OK to save changes and exit the settings file Properties window. To exit the window without saving changes, click Cancel.

Using Administrator Mode

The Administrator Mode feature allows system administrators to lock VirusScan95 configurations on users' systems to prevent accidental changes to the scan settings. To use this feature, take the following steps:

Step	Action

1. Start VirusScan95.

2. Press and hold the CTRL+SHIFT+ALT keys and double-click the magnifying glass icon.

   Response: New Administrator Mode options appear in the File menu.

3. Select Administrator Mode from the File menu.

   Response: You are prompted for a password.

   - If this is the first time you are using Administrator Mode, enter a new password. Type it a second time for confirmation.

   - If you have used Administrator Mode previously, you will be prompted to enter your password. Type it in as originally entered.

4. Choose your configurations from the What & Where, Actions, and Reports tabs.

5. Select one of the following options:

   - To retain these settings as an individual custom configuration file, save the file to the Desktop or location of choice, under a name of your choice.

   - To establish your configuration as the default setting, save the new settings by overwriting the default: C:\Program Files\McAfee\VirusScan95\DEFAULT.VSC

     ✍ *Context-sensitive scanning (right-clicking and selecting Scan for Viruses) will draw upon the DEFAULT.VSC configuration file.*

6. Leave Administrator Mode by closing VirusScan95 or selecting Leave Administrator Mode from the File menu.

   ✍ *After leaving administrator mode, the optional settings will be locked and cannot be altered from the VirusScan main window without knowledge of the access keys, hotspot, and established password.*

7. To view and confirm your changes, take one of the following steps:

   - If you overwrote the DEFAULT.VSC file, restart VirusScan95.
   - If you saved these as settings as an individual custom configuration file, click on the shortcut you created.

8. To alter your configuration settings or make additional changes, repeat this process.

✍ *To change a password, enter Administrator Mode, then select Administrator Mode a second time from the File Menu. Enter a new password, confirm your new password, and click OK. To remove password protection from the .VSC file, leave both fields blank. You must overwrite your .VSC file to permanently save this change.*

Setting up scheduled scans

VirusScan works with Microsoft Plus! to provide scheduled scanning. If your system has the Microsoft Plus! pack and you would like to set up a scheduled scan of your system, follow the steps below.

Step	Action

1. Following the procedures outlined in “Using settings files” on page 34, create a custom configuration file, saving it under a name of your choice.

2. Right-click on the icon or file and select Properties. Under the Options tab, ensure that Start Automatically is selected.

3. From the Start menu, select Programs/Accessories/System Tools/System Agent.

4. Select Schedule a New Program from the Program menu.

   Response: The Schedule a New Program dialog box appears.

5. In the Program text box, enter the path to Scan95.EXE, followed by the path and filename of the custom configuration file you created in Step 1. Click Browse to navigate to the program (Scan95.EXE) and manually enter the .VSC file location. For example: “C:\Program Files\McAfee\VirusScan95\Scan95.EXE” “C:\Windows\Desktop\Scan for Viruses.VSC”

   ✍ *The default location for Scan95.EXE is “C:\Program Files\McAfee\VirusScan95\Scan95.EXE.” In order for System Agent to properly read the long directory names, quotation marks must be used.*

6. Select your scan options, including when you wish the scan to run.

7. When you have finished configuring the scheduled scan, click OK.

   Response: VirusScan95 will run automatically at the scheduled time.

Scanning Your Diskettes

Although the on-access scanning component of VirusScan (VShield) will monitor your system for viruses, it is recommended that you scan all diskettes you use on your PC. Most viruses invade your system when you boot or attempt to boot from an infected diskette or when you copy, run, or install programs or files that are infected.

✍ *Always make sure your diskette drives are empty before turning on your computer. A diskette does not have to be bootable in order for you to catch a boot sector virus from it.*

Whenever you insert unknown diskettes in your drive—including diskettes received from friends, co-workers, and salespeople—you should run VirusScan on them before executing, installing, or copying their files. Use the procedure below to scan your diskettes.

Step	Action

1. Start VirusScan95.

Response: The VirusScan main window is displayed, with the Where & What property page on top (See Figure 4-1 on page 28).

2. Enter the drive letter for the diskette you wish to scan in the Scan In text box, or click Browse and navigate to the drive you want to scan.

3. Insert the first diskette you wish to scan in the selected drive and choose Scan Now.

Response: The diskette is scanned and the names of any infected files are displayed.

✍ *If VirusScan detects a virus on this diskette, it will take the action you specified during configuration. See "Removing a virus found in a file" on page 46 for details on virus removal.*

4. Repeat this procedure for all the diskettes you wish to scan.

5 Removing a Virus

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.
	✍ *Do not reboot using the reset button or* CTRL+ALT+DELETE*; if you do, some viruses might remain intact or their drop destructive payloads.*
2.	Place the McAfee Emergency Diskette that accompanied your VirusScan product into the floppy disk drive.
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. For information on scanning your diskettes, see “Scanning Your Diskettes” on page 42.

If viruses were not removed

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

```
Virus could not be removed.
```

If the virus was found in a file and cannot be removed by VirusScan, you should delete the file and repeat the steps described above under “If You Suspect You Have a Virus” on page 43. If the virus was found in the Master Boot Record, refer to documents on the McAfee Web Site related to manually removing viruses. 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 files or Microsoft Word documents and templates. 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 memory-resident virus found during installation

If VirusScan discovers a virus during installation, you should follow the steps outlined below to create a virus-free environment before completing the installation procedure:

Step	Action
1.	Turn off your computer.
	✍ *Do not reboot using the reset button or* CTRL+ALT+DELETE*; if you do, some viruses might remain intact or drop their destructive payloads.*
2.	Place the McAfee Emergency Diskette that accompanied your VirusScan product into the floppy disk drive.
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 again, as described in Chapter 2, “Installing VirusScan.”

To find and eliminate the source of infection, scan your diskettes immediately after installation. For information on scanning your diskettes, see “Scanning Your Diskettes” on page 42.

If viruses were not removed

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

```
Virus could not be removed.
```

If the virus was found in a file and cannot be removed by VirusScan, you should delete the file and repeat the steps described above under “If You Suspect You Have a Virus” on page 43. If the virus was found in the Master Boot Record, refer to documents on the McAfee Web Site related to manually removing viruses. For contact information, see “How To Contact Us” on page 8.

Removing a virus found in a file

If VirusScan detects a virus in a file, it will display the infected files and take the action you specified during configuration. See “Configuring On-demand Scanning” on page 30.

- If you selected Prompt for Action from the When Virus Is Found text box, VirusScan will display the Virus Found dialog box upon virus detection (Figure 5-1).

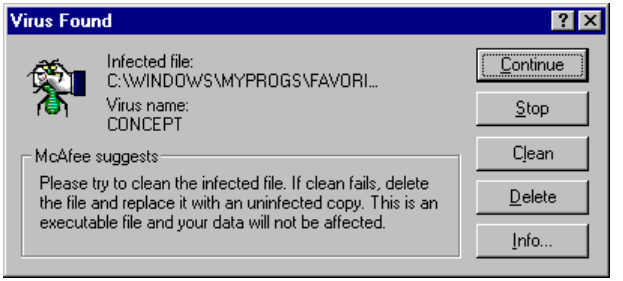

Figure 5-1. Virus Found Dialog Box

From this prompt, you have the following choices:

- Continue. Select this option if you want VirusScan to continue until all files have been scanned. You can then respond to the infection or infections by following the steps described in "Responding to a virus infection" on page 48.
- Stop. Select this option to end the scan session.
- Clean. Select this option to repair the file.
- Delete. Select this option to delete and permanently overwrite the infected file.

✍ *Click Info for more information about the virus discovered.*

As you act upon these files, icons are displayed in the VirusScan main window that correspond to the action you have taken (Figure 5-2).

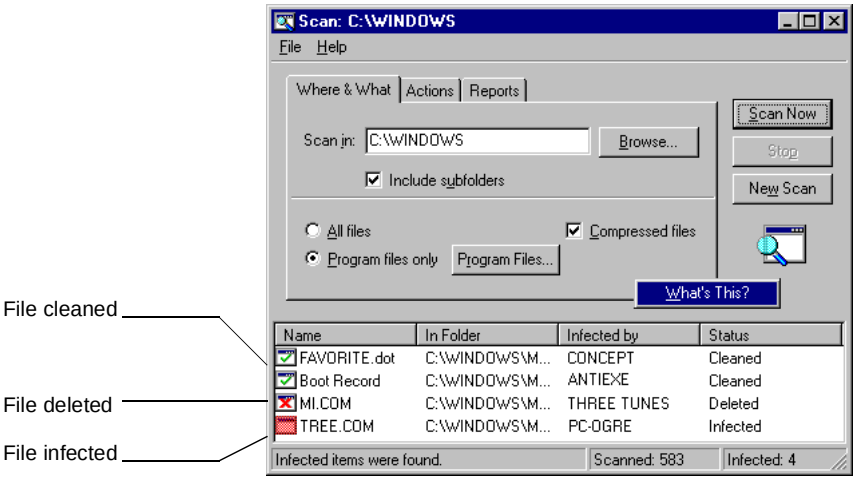

Figure 5-2. VirusScan Main Window (displaying icons for infected files, cleaned files, and deleted files)

- If you selected Move Infected Files to a Folder, Clean Infected File, or Delete Infected File during configuration, VirusScan will automatically perform the action when it finds a virus. Files acted upon will be displayed in the VirusScan main window (see Figure 5-2 on page 47).

- If you selected Continue Scanning during configuration, VirusScan will continue until all the files have been scanned. When the scan is finished, any infected files found will be listed in the VirusScan main window (see Figure 5-2 on page 47). You can then respond to the infection by following the steps below.

Responding to a virus infection

To respond to a virus infection, highlight the infected file. Then go to the File menu or right-click on the infected file and take the following steps:

Step	Action

1. Select Virus Info to view basic information about the virus infecting your file. To view detailed information, go to the McAfee Virus Information Library, which is described in "McAfee Virus Information Library" on page 66.

2. Select File Info to view basic information on the infected file.

3. Select the response you would like VirusScan to take to the infected file. Options include: Clean File, Delete File, or Move To.

   ✍ *If you select Move To, specify a path or choose Browse to navigate to the desired destination.When this option is selected, VirusScan automatically generates a text file called INFECTED.LOG in the specified folder, which logs the name of the file and where it was found.*

4. Repeat this process for all infected files.

VirusScan can repair files damaged by many viruses, but some viruses damage infected files beyond repair. If VirusScan cannot safely remove the virus, a message is displayed indicating the name of the unrecoverable file.

✍ *If* VirusScan *reports that it could not remove the virus from the infected file (the infected file is corrupted beyond repair), take note of the filename so that you know what to restore from backups. Clean your system again, this time selecting the Delete Infected File checkbox to delete the infected file.*

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.

If VirusScan for DOS is unable to remove a virus from the Master Boot Record, refer to documents on the McAfee Web Site related to manually removing viruses. For contact information, see “How To Contact Us” on page 8.

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 protection 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.

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 false alarms (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.

A 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:

Step	Action
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 43.
2.	Create a DOS start-up diskette containing the VirusScan command-line program by following the procedure outlined in "Making a Clean Start-up Diskette" on page 56. Make sure the diskette is write protected so that it cannot become infected.
3.	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.
4.	Scan all the diskettes you use. See "Scanning Your Diskettes" on page 42.

5. Never start your computer from an unchecked diskette. Always make sure your disk drives are empty before starting your computer.

6. Re-scan whenever you introduce new programs onto your computer. If you download or install software from a network server, bulletin board, or online service, run VirusScan on the directory you placed the new files in before running the software.

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 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.*

Using the Electronic Update feature

McAfee's new feature, Electronic Update, will inform you when your data files are dangerously out of date or your evaluation copy of VirusScan is expired. With this feature, you can easily update your data files or register your software electronically. When prompted, click Update or Purchase and follow the on-screen instructions to use Electronic Update and ensure the highest level of virus protection.

Applying the data file manually

To update your McAfee data files manually, without using Electronic Update, take the following steps.

Step	Action
1.	Download the data file (for example, DAT-9609.ZIP) from one of McAfee's electronic services. On most services, it is located in the anti-virus area.
	✍ *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.*
2.	Copy the file to a new directory.
3.	The file is in a compressed format. Decompress the file using any PKUNZIP-compatible decompression software. If you don't have the decompression software, you can download PKUNZIP (shareware) from McAfee electronic sites.
4.	Locate the directories on your hard drive where your VirusScan software is currently loaded. Typically, the files are stored in C:\Program Files\McAfee\VirusScan95.
5.	Copy the new files into the directory or directories, overwriting the old data files.
	✍ *There might be part of the software in more than one directory. If so, place the updated files in each directory.*

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 on 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.*

Start this procedure from a command prompt (`C:\>`). If you are in Windows, you must open a DOS shell to get the prompt. Then take the following steps.

Step	Action
1.	Insert a blank diskette in drive A:.
2.	Format the diskette by typing the following command at the `C:\>` prompt: `format a: /s /u` This overwrites any information already on the diskette. ✍ *If you are using DOS 5.0 or earlier, do not type the* `/u`. *If you are unsure of which version you are using, type* `ver` *at the* `C:\>` *prompt for version information.*
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: `cd Program Files\McAfee\VirusScan95`

5. Copy the command-line version of VirusScan to the diskette by typing the following commands at the prompt:

```
copy scan.exe a:

copy scan.dat a:

copy clean.dat a:

copy names.dat a:
```

6. Change back to the root directory by typing `cd\` at the `C:\Program Files\McAfee\VirusScan95` prompt.

7. Copy useful command-line programs to the diskette by typing one of the following commands at the `C:\>` prompt:

   `copy c:\dos\chkdsk.* a:` (for systems that have been upgraded from Windows 3.1x to Windows 95)

   `copy c:\windows\command\chkdsk.* a:` (for Windows 95 systems that have not been upgraded from Windows 3.1x)

8. Repeat the last step for any other useful programs, including:

   - `debug.*`
   - `diskcopy.*`
   - `fdisk.*`
   - `format.*`
   - `label.*`
   - `mem.*`
   - `sys.*`
   - `xcopy32.*`

✍ *If you use a disk compression utility, be sure to copy the drivers required to access the compressed drives 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 59 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* the diskettes you are using for read-only data. If your system does become infected with a virus, the write-protection feature keeps your 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.	Position the diskette face up with the label facing away from you. The notch on the upper right hand side is called the *write-protect* 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.
2.	Cover the notch with an adhesive tab or tape to write protect the diskette.

Write protecting 3.5” floppy diskettes

Step	Action
1.	Position the diskette face down with the metal slide facing you.
2.	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.
3.	To write protect the diskette, slide the plastic tab upward toward the edge of the diskette so that the hole is open.

✍ *If there is no tab and the hole is open, the diskette is permanently write protected.*

B 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 51 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 95 help file format or through the McAfee Web Site.

The Virus Information Library is continuously being updated through our web-site 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.

✍ *Because the Eicar Standard AntiVirus Test File is not a true virus infection, you will not be able to clean or repair the infected file.*

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.*

E

Reference

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 VirusScan95 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 VirusScan95 is installed.*

Command-line Option	Description
`/?` or `/HELP`	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).
`/ADL`	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 /ADL and /ADN together in the same command line.
`/ADN`	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 /ADL and /ADN together in the same command line.

Command-line Option	Description
`/AF filename`	Stores validation/recovery codes in *filename.* 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. You must specify a *filename*, 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 *filename* exists, VirusScan updates it. /AF adds about 300% more time to scanning. ✍ */AF performs the same function as /AV, but stores its data in a separate file rather than changing the executable files themselves.* *The /AF option does not store any information about the Master Boot Record or boot sector of the drive being scanned.*
`/ALL`	Overrides the default settings by scanning all files. This option substantially increases the scanning time required. Use it if you have found a virus or suspect one. ✍ *The list of extensions for standard executables has changed from previous releases of VirusScan.*
`/APPEND`	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.

Command-line Option	Description
/AV	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. 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. ✍ *The /AV option does not store any information about the Master Boot Record or boot sector of the drive being scanned.*
/BOOT	Scans only the boot sector and Master Boot Record on the specified drive.
/CF filename	Helps you detect new or unknown viruses. Checks validation data stored by the /AF option in *filename*. 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. Using any of the /AF, /CF, or /RF options together in a command line returns an error. ✍ *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.*

Command-line Option	Description
`/CONTACTFILE filename`	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. Any character is valid except a backslash (\). Messages that begin with a slash (/)or a hyphen (-) should be placed in quotation marks.
`/CV`	Helps you detect new or unknown viruses. Checks validation data added by the /AV option. If a file is modified, VirusScan reports that a viral infection may have occurred. The /CV option adds about 50% more time to scanning. Using any of the /AV, /CV, or /RV options together in the same command line returns an error. ✍ *The /CV option does not check the boot sector for changes.*
`/EXCLUDE filename`	Excludes any files listed in *filename* from the scan. This option allows you to exclude files from /AF and /AV validation and /CF and /CV checking. Self-modifying or self-checking files can cause a false alarm during a scan.
`/FAST`	Speeds up the scan. Reduces scanning time by about 15%. Using the /FAST option, VirusScan examines a smaller portion of each file for viruses. Using /FAST 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.

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

Command-line Option	Description
/MANY	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. The VirusScan program should reside on a disk that will not be removed during the scan. 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: `a:\scan a: /many`
/MEMEXCL	Exclude memory area from scanning. (The default is A000-FFFF, 0000=Scan all.) 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.
/MOVE directory	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.
/NOBEEP	Disables the tone that sounds whenever VirusScan finds a virus.
/NOBREAK	Disables CTRL-C and CTRL-BREAK during scans. 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.

Command-line Option	Description
/NOCOMP	Skips checking of compressed executables created with the LZEXE or PKLITE file-compression programs. 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.
/NODDA	No direct disk access. Prevents VirusScan from accessing the boot record. This feature has been added to allow VirusScan to run under Windows NT. You might need to use this option on some device-driven drives.
/NOEMS	Prevents VirusScan from using expanded memory (LIM EMS 3.2), ensuring that EMS is available to other programs.
/NOEXPIRE	Disables the “expiration date” message if the VirusScan data files are out of date.

Command-line Option	Description
/NOMEM	Reduces scan time by omitting all memory checks for viruses. Use /NOMEM only when you are absolutely certain that your computer is virus-free. 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.
/PAUSE	Enables screen pause. 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. We recommend that you omit /PAUSE when keeping a record of VirusScan’s messages using the report options (/REPORT, /RPTCOR, /RPTMOD, and /RPTERR).
/PLAD	Preserve last access dates (on proprietary drives only). 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.

Command-line Option	Description
`/REPORT file-name`	Creates a report of infected files and system errors. Saves the output of VirusScan to *filename* in ASCII text file format. If *filename* exists, /REPORT erases and replaces it (or, if you use /APPEND, adds the report information to the end of the existing file). You can include the destination drive and directory (such as `D:\VSREPRT\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.
`/RF filename`	Removes recovery and validation data from *filename* created by the /AF option. If *filename* 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.
`/RPTALL`	Adds list of files scanned to the report file (used with /REPORT).
`/RPTCOR`	When used in conjunction with /REPORT, adds the names of corrupted files to the report file. 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. ✍ *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).*

Command-line Option	Description
/RPTERR	Adds a list of system errors to the report file. This option is used in conjunction with /REPORT. 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.
/RPTMOD	Adds list of modified files to the report file. This option is used in conjunction with /REPORT. 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.
/RV	Removes validation and recovery data from files validated with the /AV option. 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.
/SHOWLOG	Displays the contents of SCAN.LOG. 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. The SCAN.LOG file contains text and some special formatting. To pause when the screen fills with messages, specify the /PAUSE option.

Command-line Option	Description
/SUB	Scans subdirectories inside a directory. 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.
/VIRLIST	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. 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: `scan /virlist > filename.txt` ✍ *Because VirusScan can detect many viruses, this file is more than 250 pages long.*

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.)

VSC File Format

The VSC file is a configuration text file, formatted similarly to the Windows INI file, which outlines VirusScan'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 VirusScan configuration. The variables are arranged in three groups: ScanOptions, AlertOptions, and ActivityLogOptions. To edit the VSC 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.*

ScanOptions

Variable	Description
szProgramExtensions	Type: String Defines extensions to be scanned Default value: COM DO? EXE
szDefaultProgramExtensions	Type: String Defines extensions to be used as default program extensions during scan configuration Default value: COM DO? EXE
szMoveToFolder	Type: String Defines folder to which infected files should be moved Default value: \Infected
bIncludeSubFolders	Type: Boolean (1/0) Instructs VirusScan to search for viruses inside subfolders Default value: 1
bScanAllFiles	Type: Boolean (1/0) Instructs VirusScan to scan inside all files Default value: 0
bScanCompressed	Type: Boolean (1/0) Instructs VirusScan to scan inside compressed files Default value: 1

Variable	Description
uScanAction	Type: Integer (1-5) Instructs VirusScan 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 4 - Delete infected files automatically 5 - Continue scanning Default value: 2
bAutoStart	Type: Boolean (1/0) Instructs VirusScan to start scanning immediately as it is launched Default value: 0
bAutoExit	Type: Boolean (1/0) Instructs VirusScan to exit upon scan completion if no viruses are found Default value: 0
bAlwaysExit	Type: Boolean (1/0) Instructs VirusScan to always exit upon scan completion Default value: 0
bSkipMemoryScan	Type: Boolean (1/0) Instructs VirusScan to skip memory scan Default value: 0
bSkipBootScan	Type: Boolean (1/0) Instructs VirusScan to skip boot sector scan Default value: 0

Variable	Description
bSkipSplash	Type: Boolean (1/0) Instructs VirusScan to not display the initial splash screen when the application is launched Default value: 0
nPriority	Type: Integer (0-5) Specifies the scanning threads priority. Possible values: 0 - Normal (default) thread priority 1 - Lowest thread priority 2 - Below normal thread priority 3 - Normal thread priority 4 - Above normal thread priority 5 - Highest thread priority Default value: 0
szScanItem	Type: String Defines item to be scanned Default value: C:\

AlertOptions

Variable	Description
szCustomMessage	Type: String Defines custom message to be displayed upon virus detection Default value: Your custom message
szSuggestMessage	Type: String Instructs VirusScan to display this message in place of the McAfee suggested message in the prompt display box Default value: Your custom message
bDisplayMessage	Type: Boolean (1/0) Defines if custom message should be displayed upon virus detection Default value: 0
bSoundAlert	Type: Boolean (1/0) Instructs VirusScan to sound an alert when a virus is detected Default value: 1

ActivityLogOptions

Variable	Description
szLogFileName	Type: String Defines log file name Default value: VSLOG.TXT
bLogToFile	Type: Boolean (1/0) Defines if scan results should be logged into log file Default value: 0

Variable	Description
bLimitSize	Type: Boolean (1/0) Defines if size of the log file should be limited Default value: 1
uMaxKilobytes	Type: Integer Defines maximum size of the log file in kilobytes Default value: 100
bLogDetection	Type: Boolean (1/0) Defines if scan results should be logged Default value: 1
bLogClean	Type: Boolean (1/0) Defines if clean results should be logged Default value: 1
bLogDelete	Type: Boolean (1/0) Defines if file delete operations should be logged Default value: 1
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

Variable	Description
bLogDateTime	Type: Boolean (1/0) Defines if date and time of an event should be logged Default value: 1
bLogUserName	Type: Boolean (1/0) Defines if user name should be logged Default value: 1

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
bScanOnShutdown	Type: Boolean (1/0) Instructs VShield to scan the boot record of drive A: when system is shut down Default value: 1

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

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: Your custom message
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:\Program Files\McAfee\VShield Activity Log.txt
bLogToFile	Type: Boolean (1/0) Defines if scan results should be logged into log file Default value: 0
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-tup Default value: 1
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: 1
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: 1
ExcludedItem_x, where x is a zero-based index	Type: String Instructs VShield to exclude the item from on-access scanning Default value: \Recycled|*.*|1|1 * * The string is separated into fields using the pipe (|) character: Field 1 - Folder portion of item to exclude. Leave blank for a single file anywhere on the system. Field 2 - File portion of the item to exclude. Leave blank if a folder is excluded without a filename. Field 3 - Integer (1-3) Possible values: 1 - Exclude from file-access scanning 2 - Exclude from boot-record scanning 3 - Exclude from both boot-record and file-access scanning Field 4 - Boolean (1/0) Possible values: 1 - Instructs VShield to exclude subfolders of the excluded item 2 - 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).

Index

G

H

I

L

M

N

O

P

R

S

T

V

W