User's Guide

VirusScan for Windows 3.x and 95, DOS, and OS/2

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

Phone: (408) 988-3832
Monday - Friday
6:00 am - 5:00 pm

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

(For international contact information, see the following page.)

TRADEMARK NOTICES

McAfee is a registered trademark of McAfee, Inc. SiteMeter, SiteExpress, ServerStor, and NetRemote are trademarks of McAfee, 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 Saber Software Corporation, a wholly owned subsidiary of 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

A Reader's Comment Form is provided in the back of this publication. 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. If the form has been removed, please address your comments to: McAfee, Inc., Documentation, P.O. Box 9088, Dallas, Texas 75209.

SUPPORT

For fast and accurate help, please have the following ready when you contact McAfee:

- Program name and version number
- Type and brand of your computer, hard drive, and any peripherals
- DOS type and version
- Network name, operating system, and version
- Contents of your AUTOEXEC.BAT, CONFIG.SYS, and system LOGIN script
- Specific steps to reproduce the problem.

INTERNATIONAL CONTACT INFORMATION

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

McAfee Europe B.V.
Orlyplein 81 - Busitel 1
1043 DS Amsterdam
The Netherlands
Voice: (0) 31 20 6815500
Fax: (0) 31 20 6810229

McAfee (UK) Ltd.
Hayley House, London Road
Bracknell, Berkshire
RG12 2TH United Kingdom
Voice: 44 1344 304730
Fax: 44 1344 306902

McAfee France S.A.
50 rue de Londres
75008 Paris
France
Voice: 33 1 44 908733
Fax: 33 1 45 227554

McAfee Deutschland GmbH
Weltenburger Strasse 70
81677 Munich
Germany
Voice: 49 89 92404214
Fax: 49 89 92404211

Issued March 1996

Table of Contents

1 About This Document

Who Should Read This Document

Anyone responsible for protecting computer data against possible viruses should read this manual. Whether you're responsible for maintaining a large network with multiple servers and workstations, or you're using your computer at home, this manual is written for you.

This manual provides instructions for using McAfee's award-winning VirusScan software to detect, remove, and prevent computer viruses. VirusScan is designed to protect IBM-PC or 100% compatible personal computers (PCs) that use DOS, Windows 3.x, Windows 95, and OS/2. VirusScan helps you protect one of your most important assets—the information on your computer.

Read the next section to get a quick view of what you'll find in this book.

It's not necessary to read this entire document at once; therefore, you'll want to look at the introductory material first to decide which tasks are most important to you. The next section outlines the chapters and indicates what major tasks are covered.

What You'll Find in This Book

This user's guide contains information you need for using the product components. VirusScan documentation provides a clear and easy path to information you need to use the product effectively.

✍ *The manual gives you full product details and procedures. Release Notes contain last minute updates made to the product.*

The following topics are covered:

Introduction

Chapter 1, "About This Document." Tells you how this book is organized and describes the notation and symbols used in this book.

Chapter 2, "Introducing VirusScan." Describes the main features and gives recommendations for using VirusScan to protect your computer from viruses.

Detecting viruses with VirusScan

Chapter 3, "Getting the Basics." Explains how to run VirusScan, use the tool bar and menu bar in Windows, and customize the On-Access Scanning feature.

Chapter 4, "Advanced Functions." Provides procedures for performing on-demand scanning to detect viruses. It also tells you how to repair virus-damaged files and how to maintain an "audit trail" of scanning activity and results.

Reference information

Appendix A, "VirusScan DOS and OS/2 Command Options." Lists and describes the VirusScan command options you can use in the DOS and OS/2 operating environments.

Appendix B, "Creating a Secure System Environment." Provides recommendations for creating and maintaining a virus-free computer environment.

"Glossary." Defines special terms that are used throughout this manual.

Notation and Symbols

In this section, we've illustrated and described all the conventions we've used throughout the book. Our style eliminates clutter so that you can focus on the important task of protecting your data. Take a look now, before you begin using the guidelines, so that you'll know how to interpret the information in this book.

Procedures

Procedures begin with a feature description followed by step-by-step procedures. Specific commands you are to type are shown in capital letters. Placeholders for items such as file names or command parameters are shown in lowercase letters.

We assume you have a working knowledge of your operating system. For example, we do not tell DOS users to press ENTER after every command.

The following paragraphs show how procedures appear:

Step **Action**

1. Numbered steps tell you what action to take.

Response: Tells how the system responds to the actions you take.

Action: Tells what further action, if necessary, you need to perform to complete the step.

Information references

Key notation. This notation represents a key on the keyboard. In a step-by-step instruction, we instruct you to press one key or a combination of keys to perform a function.

For example, press the ENTER key. Or, press SHIFT+F10

This note contains important information for all users.

Author note. The author note emphasizes information about any of the following:

- Options
- Functions
- Procedures
- References to information in the current chapter, a different chapter, or another manual.

Text note. The text note emphasizes supplemental information that provides tips about options, functions, or procedures.

This is a note that emphasizes Windows-specific information.

Windows note. The Windows note emphasizes that the accompanying command or setting affects only or is restricted to Windows programs or applications.

This note emphasizes OS/2-related information.

OS/2 note. The OS/2 note emphasizes that the accompanying command or setting affects only or is restricted to OS/2 programs or applications.

This note emphasizes DOS-related information.

DOS note. The DOS note emphasizes that the accompanying command or setting affects only or is restricted to DOS programs or applications.

Terminology and Tips

This section provides information and tips that will help you understand and perform the tasks and instructions in this book. The tips provided assume that you are familiar with and are using a mouse.

Entering commands

Instructions in this book refer to entering commands in Windows, DOS, and OS/2. In Windows, this means you make selections using your mouse and keyboard. In DOS and OS/2, this means you enter the command at the DOS or OS/2 prompt.

Selecting elements

The following information assumes that you are using a mouse. “Element” is used here to represent menus, menu items, icons, or items listed in a dialog.

To select, position the mouse pointer on the element you want and click the left mouse button.

To deselect, position the mouse pointer in white space that isn’t occupied by an element and click the left mouse button.

2 Introducing VirusScan

What Is VirusScan?

VirusScan is McAfee's powerful and advanced desktop anti-virus solution. Once installed, VirusScan continuously monitors machines running DOS, Windows 3.x, Windows 95, and OS/2 for virus activity. If a virus is detected, you can use VirusScan to remove the virus, move virus-infected files to another location, or delete them. VirusScan helps protect one of your most important assets—the information on your personal computer.

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 in your organization. For tips on how to do this, refer to Appendix B, "Creating a Secure System Environment."

Main features

VirusScan provides these main features for machines running Windows 3.x, Windows 95, DOS, and OS/2:

- Continuous monitoring of the computer to detect virus activity through the VirusScan memory-resident program VShield.
- On-access scanning. Use this feature to detect viruses whenever files are opened or saved on your computer.

- On-demand scanning. Use this feature to scan your system periodically to determine whether a computer virus is present.

Scheduled scanning is offered in Windows 3.x and 95

- Scheduled scans. Use this feature to run automatic scans of your system for periodic virus checks in Windows 3.x, Windows 95 and OS/2.
- Virus removal. Use this feature to repair virus-infected files.

How virus detection works

VirusScan monitors your computer operations and detects known viruses by searching the system for characteristics (sequences of code) unique to each computer virus and reports their presence. For viruses that are encrypted (secured), Scan uses detection algorithms that work by statistical analysis, heuristics, and code disassembly.

To obtain a list of all the viruses that VirusScan detects, run the Scan command with the /VIRLIST option. See Appendix A, "VirusScan DOS and OS/2 Command Options," for a full list of the VirusScan command options.

When should I scan for viruses?

Using VirusScan allows you to maintain a virus-free environment. After you install the product and perform an initial scan of your machine's local drives as well as any diskettes you normally use (see "Getting the Basics" on page 11) you have created a virus-free environment. However, this virus-free environment can only be maintained if you are sure that new programs, diskettes, and files introduced into your system are also virus free.

Viruses can be introduced if you startup your computer using an infected "boot" (startup) diskette. Or viruses can be introduced to your system if you install, copy, or run programs that have virus-infected files. Therefore, we recommend that you use VirusScan's On-Demand scan feature to check your system whenever you add files to your system. For example, if you copy files from a diskette or download files from an online service, you should run VirusScan to ensure that a virus has not been introduced to your system.

Scan when you insert an unchecked diskette

Every time you insert an unchecked diskette in your drive, run VirusScan on 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

You should scan your system regularly, from as frequently as once a day to as infrequently as once a month, depending on how susceptible your system is to virus infection.

How to Contact Us

To order or for more information about our products, we invite you to contact our Customer Service department at (408) 988-3832. Or you can contact us at the following address:

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

McAfee's customer and technical support

McAfee is famous for its dedication to customer satisfaction. McAfee's customer support, technical support, and product development departments provide real-time technical support and problem resolutions.

Use the following information to contact McAfee Technical Support.

Phone	(408) 988-3832
FAX	(408) 970-9727
FAX-back automated response system	(408) 988-3034
Hours	6 a.m. to 5 p.m. PST Monday through Friday
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
Internet	support@mcafee.com
America On-line	Keyword MCAFEE
MicroSoft Network (MSN)	MCAFEE

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

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

McAfee training

For more information about scheduling onsite training for any McAfee product, call Customer Service at (800) 338-8754.

3 Getting the Basics

What You Can Do

Once you install VirusScan, your computer is automatically checked for viruses each time it is powered on. You can further customize the scan functions to best suit your individual needs. VirusScan will scan floppy diskettes to detect viruses before they infect your hard drive.

This chapter provides the following procedures:

- Customizing the on-access scanning functions.
- Scanning floppy diskettes to detect viruses.

What Is On-Access Scanning?

On-access scanning works through a memory-resident program, VShield. On-access scanning helps to prevent virus infection by checking programs as they are loaded into your computer's memory. VirusScan is directly incorporated into the Windows 95 interface by means of Context Menus. Once enabled, VirusScan' on-access scanning component VShield will provide real-time protection against contracting and spreading viruses.

On-access scanning in Windows 95

VirusScan uses a series of VXD (dynamically loaded virtual device driver) modules to provide "on-access" protection. VirusScan checks programs, the master boot record, boot sector, system files, and itself for virus signatures (the pattern of code unique to each virus). If on-access scanning (VShield) finds an infection, it prevents programs from running. It also prevents warm boots CTRL+ALT+DEL from infected disks.

There is one way to infect your computer that VirusScan cannot prevent—only you can. Never start your computer from an unknown diskette. That's how 80 percent of all viruses are passed! VShield checks diskettes if you reset your computer, but cannot check a diskette if you turn on your computer with the diskette in the disk drive. Always make sure your diskette drives are empty before you turn your computer on.

VShield can be accessed at any time through the VShield icon on the taskbar.

✍ *On-access scanning is automatically enabled when you restart your system if you choose this setting during the installation.*

When you double-click on the VShield icon on the taskbar, the VShield Status window is displayed. This window displays the file 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.

VShield will scan your system according to the configuration options you have set. For instructions on configuring on-access scanning, refer to "Setting up on-access scanning in Windows 95" on page 16.

On-access scanning in Windows 3.x

On-access scanning works through a memory-resident program, VShield. On-access scanning helps to prevent virus infection by checking programs as they are loaded into your computer's memory. Instructions on how to configure on-access scanning can be found in "Setting up on-access scanning in DOS, Windows 3.x, or OS/2" on page 19.

On-access scanning features include:

- Checking master boot records, boot sectors, system files, and itself for viruses when you turn on or reset your PC.
- Checking program files for viruses as your computer executes them.
- Checking files for viruses as you copy them (optional).
- Checking for viruses whenever your computer accesses a disk (optional).

If at any time a virus is detected, you will hear three beeps and a message similar to the following will be displayed:

```
Found the Jerusalem Virus in memory.
```

If a virus is detected, follow the instructions in "Cleaning the computer system in Windows" on page 49 to use VirusScan to remove the virus and repair any virus-damaged files.

On-access scanning in DOS and OS/2

On-access scanning in DOS and OS/2 is enabled through a memory-resident program, VShield. On-access scanning helps to prevent virus infection by checking programs as they load into your computer's memory. Instructions on how to configure on-access scanning to your system can be found in "Setting up on-access scanning in DOS, Windows 3.x, or OS/2" on page 19.

In OS/2, on-access scanning is active in DOS and Win-OS/2 sessions only, because viruses can operate only in those sessions. On-access scanning does not run in native OS/2 sessions. This function is only available when you're running a temporary DOS session (DOS box) and when you're running a Win-OS/2 session.

On-access scanning features include:

- Checking master boot records, boot sectors, system files, and itself for viruses when you turn on or reset your PC.
- Checking program files for viruses as your computer executes them.
- Checking files for viruses as you copy them (optional).
- Checking for viruses whenever your computer accesses a disk (optional).

If at any time a virus is detected, you will hear three beeps and a message similar to the following is displayed:

```
Found the Jerusalem Virus in memory.
```

If a virus is detected, follow the instructions in "Cleaning the computer system in DOS and OS/2" on page 54 to use VirusScan to remove the virus and repair any virus-damaged files.

We recommend using the command line option /FILEACCESS in OS/2. This option checks standard executable files whenever the file is executed and prevents the execution of infected programs.

Setting Up On-Access Scanning (VShield)

VirusScan's on-access scanning component, VShield, can help prevent viruses from infecting your system. In DOS, Windows 3.x, and OS/2, VShield runs as a "Terminate-and-Stay-Resident" (TSR) program, remaining in memory and scanning and intercepting programs as they are executed. In Windows 95, VShield uses a series of VXD (dynamically loaded virtual device driver) modules to provide this "on-access" scanning independent of the DOS environment.

VirusScan's on-access scanning feature enables it to check programs, the master boot record, boot sector, system files, and the VirusScan program files themselves for virus signatures, the pattern of code unique to each virus. If VirusScan finds an infection, it prevents programs from running. It also prevents warm boots (CTRL+ALT+DEL) from infected disks.

There is one way to infect your computer that VirusScan cannot prevent—only you can. Never start your computer using a boot disk that has not been checked for viruses. VirusScan's on-access scanning function can check a diskette when you reset your computer, but diskettes are not checked when you turn on your computer with a diskette in the disk drive.

About false alarms

Due to the nature of anti-virus software, there is a possibility that VShield may report a virus in a file or in memory, even if a virus does not exist. This can be more likely if you are using more than one brand of virus protection software, especially if the virus is reported in memory rather than on the boot disk.

Always assume that the virus is genuine. Follow the procedures outlined in "Removing Viruses" on page 49. Then upload any files which you suspect are generating false alarms to our bulletin board system at (408) 988-4004.

Setting up on-access scanning in Windows 95

For more information about VShield, refer to "On-demand scanning in Windows 95" on page 37.

Windows 95

When you double-click on the VShield icon on the taskbar, the VShield Status window will be displayed. This window displays the file name of the last file scanned, information about the number of files that have been scanned, the number of infected files, and any files which have been cleaned or deleted.

The following buttons are also available:

- *Disable.* Choose this button to deactivate on-access scanning from the current Windows 95 session. On-access scanning is reactivated when you restart your computer.
- *Properties.* Choose this button to configure the detection, action, and reporting settings of on-access scanning. Refer to the next section, "Configuring on-access scanning in Windows 95," for more information.
- *Close.* Choose this button to close the VShield Status window. To re-open this window, double-click on the VShield icon from the taskbar.

Configuring on-access scanning in Windows 95

On-access scanning can be configured through the graphic interface (VShield Configuration Manager), or by editing a text file which contains its default options.

Use the following procedure to edit on-access scanning through the VShield Configuration Manager.

Step	Action
1.	Double-click on the VShield icon on the Taskbar.
	Response: The VShield Status window is displayed.

2. Choose Properties.

   Response: The VShield Configuration Manager is displayed.

3. Use the Detection property page to identify what will be scanned and when scanning will take place.

   - Scan files on. A checkmark indicates that VirusScan will scan files when a user attempts to ‘Run,’ ‘Create,’ ‘Copy,’ and/or ‘Rename’ the files.

   - Scan disks on. A checkmark indicates that VShield will scan disks on ‘Access’ and/or ‘Shutdown.’

   - What to scan. If selected, either ‘All files’ (all executable and MS-Word document files regardless of file extension) or ‘Program files only’ (all files with the extensions specified in the Program Files window) are scanned. A checkmark in the ‘Compressed files’ box indicates that self-decompressing files created with LZEXE or PKLITE file compression programs are scanned.

     ✍ *Choose Program Files to edit the list of file extensions that VirusScan will scan if you have selected Program files only. The default file types are .BIN, .COM, .EXE, .OVL, .SYS, and .DO?.*

   - General. Configure on-access scanning by choosing ‘Load VShield at startup,’ ‘VShield can be disabled,’ and/or ‘Show icon on the taskbar.’

4. Use the Actions property page to select what actions VirusScan should take if a virus is detected.

   - When a virus is found. Choose one of the following actions from the pull-down list box: ‘Prompt user for action’ (recommended for attended systems); ‘Move infected files to a folder’ (specify a path in the ‘Folder to move to’ box or choose Browse to select a folder); ‘Clean infected files automatically;’ ‘Delete infected files automatically;’ or ‘Deny access to infected files and continue’ (recommended for systems left unattended).

- If 'Prompt user for action' is selected, you can configure what actions the user may take with the 'Possible actions' check boxes. You can also display a message if a virus is detected by selecting the 'Display message' check box and typing a message in the text box provided.

5. Use the Reports property page to configure the logging of virus activity and to determine which information will be included in the log entry.

   - Log file. Select the 'Log to file' check box and enter a path 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' check box and using the scroll buttons to specify a size between 10 and 999 Kb.

     ✍ *The default path for the log file is C:\Program Files\McAfee\VShield Activity log.txt. The default log file size is 100 KB.*

   - What to log. Select from the check boxes provided to specify what information should be included in the Log file: 'Virus detection,' 'Virus cleaning,' 'Infected file deletion,' 'Infected file move,' 'Session settings,' 'Session summary,' 'Date and time,' 'User name.'

6. The Exclusions property page is used to define which objects (files, folders, and/or drives) that should be excluded from scans.

   - To add an object to the exclusion list, choose Add. To remove an object from the exclusion list, select it and choose Remove. To edit an object in the exclusion list, select it and choose Edit.

7. Choose Apply to save your changes. To save your changes and exit VShield Configuration Manager, choose OK. To exit VShield Configuration Manager without saving your changes, choose Cancel.

On-access scanning options can also be edited through a text file. This text file is stored in C:\Program Files\McAfee\DEFAULT.VSH. This is a standard text file with line items associated with each option in the VShield Configuration Manager. All items in the DEFAULT.VSH file are directly referenced in the VShield Configuration Manager (through the Properties button). When you apply these changes through the User Interface, the DEFAULT.VSH file is updated immediately.

Setting up on-access scanning in DOS, Windows 3.x, or OS/2

VShield in DOS, Windows 3.x, and OS/2 is the memory-resident component of VirusScan that helps to prevent virus infection by checking programs as they load into your computer's memory, or "on-access" scanning.

On-access scanning runs under DOS, Windows 3.x, OS/2 Virtual DOS Machine, and WIN-OS/2 sessions.

✍ *For more information about on-access scanning in DOS or OS/2, refer to "On-access scanning in DOS and OS/2" on page 13. For information about using on-access scanning in Windows 3.x, refer to "On-access scanning in Windows 3.x" on page 13.*

System requirements and performance

VShield is a Terminate-and-Stay-Resident (TSR) program, which remains in memory while you run other programs. VShield tries to optimize memory usage and minimize conflicts with other TSRs. However, if you do encounter problems using on-access scanning, it may be due to conflicts with other TSR programs in your system, or with other programs that monitor disk access.

VShield minimizes the use of conventional memory by attempting to load into extended, expanded, upper memory, or a combination thereof, before using conventional memory. If you have less than 640 KB, you can use the /SWAP option to reduce memory requirements to 8 KB, although this significantly decreases the speed of on-access scanning.

If you have more than 640 KB, VShield tries to load as much of itself as possible above conventional memory, first into expanded memory (EMS), into extended memory (XMS), then into upper memory blocks (640 KB to 1024 KB, or UMB). If you have sufficient high memory available, VShield and VShieldCRC use no conventional memory.

✍ *You can control where VShield loads by using the /NOUMB, /NOEMS, and /NOXMS options.*

Launching on-access scanning in DOS, Windows 3.x, and OS/2

The VirusScan installation program gives you the option of adding a line to your AUTOEXEC.BAT file which automatically activates on-access scanning whenever you start or restart your computer. To activate on-access scanning at any time, complete the following procedures.

In DOS and Windows 3.x, restart your computer. In OS/2, restart all DOS and Win-OS/2 windows. If you have not changed the path statement in your AUTOEXEC.BAT file, you need to include its location (usually C:\MCAFEE\VIRUSCAN) in the command, or change to that directory.

✍ *We recommend using the command line option /FILEACCESS in OS/2. This option checks standard executable files whenever the file is executed and prevents the execution of infected programs.*

OS/2

Setting up VShieldCRC in DOS, Windows 3.x, or OS/2

VShieldCRC in DOS, Windows 3.x, and OS/2 offers less protection than VShield, but requires little system memory. VShieldCRC does not check for virus signatures or prevent infection, but it does check for infection and will inform you if a virus has been detected.

To use VShieldCRC, first run Scan with the /AF or /AV options. (For instructions on how to do this, refer to "Validation and recovery in Windows 3.x" on page 67 or "Validation and recovery in DOS and OS/2" on page 69.) Then type:

```
vshldcrc options
```

where:

vshldcrc	runs the application.
options	VShieldCRC's command line switches. Refer to the options listed in the table below. For specific information about a VShieldCRC option, see "Setting up on-access scanning in DOS, Windows 3.x, or OS/2" on page 19.

✍ *For a full list and description of the VirusScan command options, see Appendix A, "VirusScan DOS and OS/2 Command Options."*

Using CheckVShield in DOS, Windows 3.x, or OS/2

CheckVShield allows network administrators to make sure that workstations are running VShield or VShieldCRC before users can log onto a network.

To load CheckVShield with options, use the following syntax:

```
chkvshld options
```

where:

chkvshld	runs the application.
options	include the following:

/? or /HELP displays the list of valid CheckVShield options.

/DEBUG displays the version of VShield or VShieldCRC resident in memory and the DOS ERRORLEVEL on the screen.

/QUIET suppresses CheckVShield messages (quiet mode) so users do not see the messages.

/V "*xxxx*" tells CheckVShield to look for a specific version (2.00 or higher) of the VShield or VShieldCRC program in memory. For example, /v "2.00" instructs CheckVShield to look for VShield or VShieldCRC version 2.00 or higher.

Customizing the On-Access Scan Feature

VirusScan allows you to customize the on-access scan feature. You can save the scan settings and selected items in a settings file or a scanning profile. That way, you do not need to select scanning options and items individually every time you want to scan; you can just load the appropriate profile or have the default settings configured to your system's needs.

- A settings file configures VirusScan's default settings every time you scan.
- A scanning profile can be used to automate specific scanning procedures; for example, you could have a Floppy Disks profile, a Local Drives profile, and a Network Drives profile, changing the profile for whichever target you want to scan.

Using settings files in Windows

If you are likely to use the same scanning settings every time you save, you should save this configuration in a settings file so VirusScan will use them as the default settings.

To save a settings file in Windows, use the following procedure:

Step	Action
1.	Configure VirusScan to the scanning settings that you will most often use.
	✍ *Refer to "On-demand scanning in Windows 95" on page 37 or "On-access scanning in Windows 3.x" on page 13 for information about configuring VirusScan scanning settings.*
2.	Choose **File/Save Settings**.
	Response: The Save Settings dialog box is displayed.
3.	Select a different file type, if needed.

4. Type a new name for the settings file you want to save. In Windows 3.x, save this file with the .INI extension.


Windows 95

Saving your settings in the Desktop in Windows 95 creates a new desktop icon. Saving your settings to the Startup group makes the scan job execute upon Windows 95 startup.

To load a settings file, use the following procedure:

Step	Action

1. Choose **File/Load Settings**.

   Response: The Load Settings dialog box is displayed.

2. Select a different file type, if needed.

3. Type or select the name of the settings file you want to use.

Using settings files in DOS and OS/2

If you use the same Scan command line options often, you can save your settings in a configuration file, called DEFAULT.CFG. VirusScan checks for the existence of this file and, if it exists, loads the options specified in this file as its default.

To create the configuration file, use the following procedure:

Step	Action

1. Using a word processor or text editor such as Windows Write, create a new file.

2. Put all the options on the same command line or put each option (with its parameter) on its own line, separated by a hard carriage return and line feed, as shown in the following examples.

Sample configuration file with all options on the same command line:

```
c:\chris c:\craig /all /sub /report d:\virus.rpt
```

Sample configuration file with each option on a separate command line:

```
c:\chris
c:\craig
/all
/sub
/report d:\virus.rpt
```

✍ *In both examples, VirusScan will scan the directories "CHRIS" and "CRAIG" and their associated subdirectories on the C: drive. All executable and MS-Word document files are scanned. A report file, called "VIRUS.RPT," is saved to the D: drive.*

3. Save the file as "DEFAULT.CFG" as an ASCII or DOS Text file in the same directory that VirusScan is stored in.

   Response: After you create the configuration file, VirusScan defaults to the selected drive(s) and command line options specified in the DEFAULT.CFG file.

4. Create the configuration file using the above procedure, ensuring that it is saved in the same directory as SCAN.EXE and that it is saved as an ASCII or DOS Text file.

5. At the system prompt, type:

   ```
   scan
   ```

   Response: Scan initiates a virus check using the drives and command line options specified in the file, DEFAULT.CFG. Using the above example, Scan examines all executable and MS-Word document files in the directories C:\CHRIS and C:\CRAIG and their associated sub-directories. A report file, called "VIRUS.RPT," is saved to the D: drive.

Using scanning profiles in Windows

If there are several scanning profiles you are likely to use (i.e., one for floppy drives, another for networks, and one for local drives only), you should use VirusScan's scanning profiles feature to create quick-access "buttons" to launch a particular scanning configuration in Windows 3.x or you can create settings icons to launch scans in Windows 95.

Using scanning profiles in Windows 95

In Windows 95, you can create a scanning profile using the procedure outlined below, then run the desired settings file either through Windows Explorer or automatically at Windows 95 start-up.

To run a scanning profile from Windows Explorer, use the following procedure:

Step	Action
1.	Navigate to the drive or folder that you would like to scan.
2.	Click the right mouse button on this location to display the Context Menu.
3.	Choose Scan for viruses from the context menu.
4.	Select the desired options from the property pages.
5.	Click Scan Now.

To run a scanning profile automatically at Windows startup, follow the procedure below:

Step	Action
1.	Create a scanning profile following the procedure above and save it to the Startup group, or copy an existing scanning profile to the Startup group.

2. Through Windows Explorer, right-click on the scanning profile and choose Properties.

   Response: The Scan for viruses Properties box is displayed.

3. Click on the Options tab to display the Options property page.

4. Choose the Start Automatically check box.

   Response: VirusScan scans for viruses whenever you restart your computer.

   ✍ *You may have more than one scanning profile in your Startup program to perform scans on multiple targets. Configure each .VSC file by right-clicking on the scanning profile icon and changing the settings on the General, Options, and Actions property pages.*

Using scanning profiles in Windows 3.x

Before you can select profiles from the Run Profile dialog box, the profiles must be defined in the WSCAN.INI file. Once defined, you must restart VirusScan for your changes to take effect.

✍ *Refer to your Windows user's manual for more information about modifying .INI files.*

To create a scanning profile in Windows 3.x use the following procedure:

Step	Action

1. Open the WSCAN.INI file using an ASCII text editor.

2. Edit the Header variables section of the WSCAN.INI file.

   For example:

   ```
   Header1=Profile Engine v1.0
   Header2=Select a profile to run, please
   ```

3. Edit the [Profile*n*] section of the WSCAN.INI file.

For example, you can change the first button in the Run Profile dialog box to “My Drive,” which will scan the C: drive:

```
[Profile1]
Label=My Drive
Description=Scan disk C:
File=c:\mcafee\profile1.prf
```

- [Profile1] begins the section for the first button (the next button is Profile2, and so on).
- Label is the short word or phrase that appears in the button. This label should not exceed 13 characters.
- Description is the text that provides additional information about the profile and appears to the right of the button. This description should not exceed 29 characters.
- File identifies the name and path of the settings file. If VirusScan cannot locate the specified file, the button is dimmed (unavailable).

  You can specify these settings for up to four profiles.

✍ *You can refer to the two default files provided with VirusScan, Profile1.PRF and Profile2.PRF as templates to “build” other profiles from.*

For more information about the WSCAN.INI file, including other settings, refer to the “WSCAN.INI” topic in the on-line help.

After creating a profile, use the following procedure to load and run the preselected settings:

Step	Action
1.	Choose **File/Run Profile** or click the Profiles icon.
	Response: The Run Profile dialog box is displayed.

2. Choose the profile you want.

   Response: VirusScan loads the associated profile, then scans your system using those settings.

Using scanning profiles in DOS and OS/2

You can create a scanning profile in VirusScan by creating an ASCII text file, then use the /LOAD option to load the scanning profile.

To use a scanning profile in DOS and OS/2, use the following procedure:

Step	Action

1. Use a text editor to create a new ASCII text file.

2. Enter the options you want included in this scanning profile.

   You can put all the options on the same command line or put each option (with its parameter) on its own line, separated by a hard carriage return and line feed. For an example of a configuration file, refer to "Using settings files in DOS and OS/2" on page 23.

   ✍ *Be sure to save this file as ASCII text only.*

3. After creating the scanning profile, run the profile using the /LOAD option. For example, if you created a profile with the name FLOPPY.CFG, enter the following in DOS and Windows environments:

   ```
   scan /load floppy.cfg
   ```

   In OS/2, type:

   ```
   os2scan /load floppy.cfg
   ```

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 the diskettes you use on your PC. Most viruses invade your system either by booting from, or attempting to boot from, an infected diskette or by copying, running, or installing programs that contain infected files.

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.

✍ *DOS users can use the /ANYACCESS option of VirusScan to scan diskettes automatically. For more information about on-access scanning, refer to "Setting Up On-Access Scanning (VShield)" on page 15.*

When should I scan diskettes?

Whenever you insert an unchecked diskette in your drive, you should run VirusScan on it before executing, installing, or copying its files. This includes any diskettes received from friends, co-workers, salespeople, and even your own diskettes if they have been used on another PC.

How do I scan my diskettes?

Use the procedures below to scan your diskettes. Refer to "On-Demand Virus Scanning in Windows" on page 37 for more information about scanning and cleaning.

Scanning your diskettes in Windows 95

Step	Action
1.	Right-click on the Start menu and choose **Scan for Viruses**.
	Response: VirusScan is loaded and the main window is displayed.
2.	Select the Where & What property page.

3. Enter A: in the 'Scan in' text box, or click Browse and navigate to the diskette drive you want to scan.

4. Insert the first diskette you'd like to scan in drive A: and choose Scan Now.

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

   ✍ *If VirusScan detects a virus on this diskette, refer to "Removing a virus in Windows 95" on page 50 to clean the diskette.*

5. Repeat this procedure for all the diskettes you normally use.

Scanning your diskettes in Windows 3.x

Step	Action

1. Launch VirusScan by double-clicking the VirusScan icon in the McAfee program group.

2. Click on the Select icon.

   Response: The Select Items to Scan dialog box is displayed.

3. Select the A: drive from the Drives list, then choose Add Drive.

   Response: The A: drive appears in the Selections list.

4. Choose OK to return to the VirusScan Main Window.

5. Insert the first diskette you would like to scan and click on the Scan icon.

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

   ✍ *If VirusScan detects a virus on this diskette, refer to "Removing a virus in Windows 3.x" on page 52 to clean the diskette.*

6. Repeat this procedure for all the diskettes you normally use.

Scanning in DOS and OS/2

Step	Action

1. Change to the directory in which the VirusScan program files are located.

2. Insert the first diskette into the A: drive.

3. Scan the diskette by entering on of the following commands.

In DOS, type:

scan a: / many

In OS/2, type:

os2scan a: /many

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

✍ *If VirusScan detects a virus on this diskette, refer to "Cleaning the computer system in DOS and OS/2" on page 54 to clean the diskette.*

4. VirusScan prompts you to enter the next diskette. Continue scanning until you have checked all the diskettes you use.

4 Advanced Functions

In addition to the continual virus checks of your computer's hard drive provided by VirusScan's automatic on-access scans, you can also perform periodic scans (called on-demand scanning) while you're working. This chapter provides the following procedures:

- Performing on-demand scans of your system to detect viruses. You'll find instructions for performing periodic scans in the Windows 3.x and 95, DOS, and OS/2 environments.
- Customizing on-demand scanning functions
- Scheduling automatic scans in Windows
- Cleaning a virus-infected file
- Using the Validate feature for virus detection and recovery
- Viewing virus scan results
- Updating the VirusScan database to ensure that the product always detects the latest viruses.

Starting VirusScan

There are four easy methods to start VirusScan in Windows 95: through the Start menu, Windows Explorer, by creating a shortcut (icon) on your desktop, or by right-clicking on any drive, folder, or executable file.

In Windows 3.x, VirusScan can be started through the Program Manager. To start VirusScan in DOS or OS/2 environments, enter the appropriate VirusScan command at the command prompt.

In Windows 95

The main VirusScan window automatically appears whenever you scan for viruses in Windows 95. A description of the basic menus and buttons is provided below:

- *File Menu.* This menu has three choices: Save Settings, View Activity Log, and Close. For more information about saving and using settings, refer to "Using settings files in Windows" on page 22. For more information about the activity log, refer to "Viewing Scan Results" on page 58. Choosing Close exits the program.

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

- *Scan Now.* This button initiates a scan.

- *Stop.* This button halts a scan in progress.

- *New Scan.* This button resets VirusScan to its default settings.

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

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

- *Reports.* This property page is used to determine VirusScan's notification, reporting, and logging options. For more information, refer to "Viewing Scan Results" on page 58.

Getting help

VirusScan provides on-line help for all of its features. You can obtain context-sensitive help for menus, icons, and dialog box objects, as well as general help for conceptual and background information.

- To get general help, choose **Help/Topics**. The Topics page of the on-line help system is displayed.
- For context-sensitive help, right mouse-click on any control and select **What's This**.
- To get more information about this product, choose **Help/About**.

In Windows 3.x

The VirusScan window contains the following elements when you're running Windows 3.x:

- The menu bar contains the following menus:

Menu	Commands
File	Load Settings, Save Settings, Run Profile, Select Items to Scan, Print Setup, Print, Exit
Scan	Start Scan, Schedule Scan, Activity Log, Virus List
Settings	Controls, Actions, Reports, Validations, Exceptions
Help	Contents, Product Support, About VirusScan

- The VirusScan tool bar is used to quickly start a task without navigating the menu. The tool bar contains the following icons:

Button	Description
	Choose this button to load a scanning configuration file (scanning profile). For more information about using profiles, refer to "Using scanning profiles in Windows" on page 25.

Choose this button to begin scanning your system for viruses. For more information about scanning with VirusScan, refer to "On-Demand Virus Scanning in Windows" on page 37.

This button enables you to select the drives, directories, and/or files you want to scan or clean. For more information about scanning with VirusScan, refer to "Getting the Basics" on page 11.

Use this button to configure the VirusScan Notebook, where you can define scanning, reporting, and validation options.

Click here to display a list of the many viruses VirusScan can detect and remove.

Use this button to schedule automatic scans. For more information about scheduling scans, refer to "Scheduling Virus Scans in Windows 3.x" on page 47.

Choose this button to save an activity log of scanning dates and results. For more information, refer to "Viewing Scan Results" on page 58.

Getting help

VirusScan provides extensive on-line help for all of its features. You can obtain context-sensitive help for menus, icons, and dialog box objects, as well as general help for conceptual and background information.

- To get general help, choose **Help/Help Topics**. The Contents page of the on-line help system is displayed.
- To get general help for a dialog box or window, choose its Help button.

In DOS and OS/2

To start VirusScan in the DOS and OS/2 environments, simply enter the appropriate VirusScan command. See “On-Demand Scanning in DOS and OS/2.”

On-Demand Virus Scanning in Windows

This section gives you instructions for using VirusScan in Windows 3.x and Window 95 to perform periodic scans of your system to detect viruses.

On-demand scanning in Windows 95


Windows 95

There are four easy methods to start VirusScan in Windows 95: through the Start menu, Windows Explorer, by creating a shortcut (icon) on your desktop, or by right-clicking on any drive, folder, or executable file.

- From the Programs option on the Start menu, choose **McAfee VirusScan95**, or right-click on the Start button and choose the Scan for Viruses button.
- From Windows Explorer, locate the Windows/Program files folder and then locate the McAfee/VirusScan folder and double-click on the VirusScan program.
- From your desktop, create a VirusScan shortcut. For information about creating shortcuts with Windows 95, refer to your Windows 95 manual or online help.
- To launch VirusScan with your mouse, right-click on any drive, folder, or executable file (those with .EXE, .COM, or .DOC extensions) and choose the Scan for Viruses button from the menu displayed.

Use the following procedure to scan your system, including local and/or floppy drives, in Windows 95:

Step	Action
1.	Select the Where & What property page tab.
2.	Enter the path of the drive, folder, or individual file you want VirusScan to scan, or choose Browse to navigate to the location. Your selection will appear in the ‘Scan in’ text box.

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

- Choose ‘All files’ if you want VirusScan to check all executable and Microsoft Word files in the selected folder, or select ‘Program files only’ to scan only executable and MS-Word files of a specific type.

  ✍ *Click on the Program Files button to edit the type of executable and MS-Word document files that VirusScan will examine. The default settings are: .386, .BIN, .COM, .DLL, .DO?, .DRV, .EXE, .FON, .OVL, .SYS, and .VXD.*

- Select ‘Compressed files’ if you want files compressed with PKLITE or LZEXE to be scanned.

3. Click the Scan Now icon button.

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

- **Files infected**: Indicates how many infected files VirusScan has found.

- **Files scanned**: Indicates how many files VirusScan has scanned for viruses. If you are using the default scanning settings, VirusScan will only check executable files. To change the scanning settings, return to Step 2.

- **Files analyzed**: Indicates how many executable or MS-Word files VirusScan has found on your system.

4. Do one of the following:

   - If VirusScan reports that no files are infected, congratulations—most likely your system is currently virus-free. Go to Step 5.

     ✍ *VirusScan's ability to detect viruses must be maintained through regular upgrades of the VirusScan data files. For more information about updating VirusScan, refer to "Updating the VirusScan Database" on page 75.*

   or

   - If VirusScan does detect a virus, do not panic, even if the virus has infected many files.

     - If VirusScan finds a virus in a file, refer to "Removing a virus in Windows 95" on page 50 for instructions on how to proceed.
     - If VirusScan finds a virus in memory, the Master Boot Record (MBR), or boot sector, shut down your computer. Then reboot from a clean write-protected start-up diskette or a Windows recovery diskette, and follow the procedures outlined in "Cleaning the computer system in DOS and OS/2" on page 54.

5. We recommend that you 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 work.

On-demand scanning in Windows 3.x

Use the following procedure to scan your system, including local and floppy drives, in Windows 3.x:

Step	Action

1. To start VirusScan in Windows 3.x, use the Run command to start the program WSCAN.EXE (during installation, the program is stored in the directory \MCAFEE\VIRUSCAN).

   Response: VirusScan checks your computer's hard disk to determine whether a virus exists.

2. Select the items you want to scan by choosing **File/Select Items to Scan** or by clicking the Select icon.

   Response: The Select Items to Scan dialog box is displayed.

   - Use the following procedure to select drives, directories, and files:
     - To add a drive to the Selections list, select it from the Drives list, then choose Add Drive. This selects all files in all directories and subdirectories on that drive for scanning.
     - To add a directory, select it from the Directories list, then choose Add Directory. This selects all files in this directory, but not files listed in subdirectories. To add a subdirectory, select it from the Directories list and choose Add Directory.
     - To add a file, select it in the Files list, then choose Add File.
   - The item you have added appears in the Selections list.

     ✍ *You can also identify directories and files to scan by dragging them from the Windows File Manager (right window only) to the* VirusScan *main window. To scan a single directory or file, drag it from the right window in the File Manager to the* VirusScan *window.*

   - Choose OK to return to the VirusScan Main Window.

3. Choose **Scan/Start Scan** or click the Scan icon.

   Response: VirusScan will check the drives, directories, and/or files you have selected. The names of files being scanned are displayed in the status bar and any status or warning messages are displayed in the VirusScan main window.

   - **Files infected**: Indicates how many infected files VirusScan has found.

- **Files scanned**: Indicates how many files VirusScan has scanned for viruses. If you are using the default scanning settings, VirusScan only checks executable and MS-Word files with the extensions .COM, .EXE, .SYS, .BIN, .OVL, .DLL, .DOC, and .DOT. To change the scanning settings, refer to "Using Scanning Packages" on page 46.

- **Files analyzed**: Indicates how many executable type or MS-Word document files VirusScan has found on your system.

4. Do one of the following:

- If VirusScan reports that no files are infected, congratulations—most likely your system is currently virus-free. Go to Step 5.

  ✍ *VirusScan's ability to detect viruses must be maintained through regular upgrades of the VirusScan data files. For more information about updating VirusScan, refer to "Updating the VirusScan Database" on page 75.*

- If VirusScan does detect a virus, do not panic, even if the virus has infected many files.

  - If VirusScan finds a virus in a file, refer to "Cleaning the computer system in Windows" on page 49 for instructions on how to proceed.

  - If VirusScan finds a virus in memory, the Master Boot Record (MBR), or boot sector, exit Windows and shut down your computer. Then reboot from the clean start-up diskette you created in Chapter 2, and follow the procedures outlined in "Cleaning the computer system in DOS and OS/2" on page 54.

5. We recommend that you 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 work.

On-Demand Scanning in DOS and OS/2

This section gives you instructions for using VirusScan in the DOS and OS/2 operating environments to perform periodic scans of your system to detect viruses.

On-demand scanning in DOS and OS/2

Start from the system prompt (C> or [C:\]). If you are running Windows 3.x or an application program, exit from it to display the prompt. If you are running OS/2, close all DOS and Win-OS/2 sessions. Then open the Command Prompts folder in the OS/2 system folder and click the OS/2 Full Screen or OS/2 Window icon.

To perform a scan in the DOS and OS/2 environments, use the following procedure:

Step	Action

1. Navigate to the directory where VirusScan was installed.

✍ *The default directory is* C:\MCAFEE\VIRUSCAN.

2. Scan your C drive for known viruses by entering the following command.

- In the DOS or Windows environments, type:
  `scan c: /all`

or

- In OS/2, type:
  `os2scan c: /all`

where:

Scan (or os2scan)	runs the application.
C:	specifies the hard drive (C:\) as the target of the scan.
/ALL	this option instructs VirusScan to scan all files, not standard executables and MS-Word documents.

If you have more than one hard drive, add them to the scan in the same manner. For example, if you have C and D drives, type:

```
scan c: d: /all
```

In OS/2, type:

```
os2scan c: d: /all
```

You can also scan all local drives (including compressed, CD-ROM and PCMCIA drives but not diskettes) using the /ADL option. For example:

```
scan /adl /all
```

In OS/2, type:

```
os2scan /all
```

3. It may take several minutes for the VirusScan program to check for viruses in memory, then on the system and user portions of your drives. VirusScan keeps you informed of its progress. Read the information on the screen carefully. On the next page is a sample of what VirusScan reports when checking a drive for viruses.

```
Scan V.2.2.5 Copyright (c) McAfee, Inc. 1994, 1995.
All rights reserved.
(408) 988-3832 LICENSED COPY - Aug 16, 1995

Virus data file V9508 created 08/16/95 12:02:37
No viruses found in memory.
Scanning C: [MS-DOS_6]
Summary report on C:
File(s)
   Analyzed:..............3601
   Scanned:...............680
   Possibly infected:..... 0
Master Boot Record(s):..... 1
   Possibly infected:..... 0
Boot Sector(s):............ 1
   Possibly infected:..... 0
Time: 00:01.34
```

- **Analyzed** indicates how many files executable or MS-Word files VirusScan has found on your system.

- **VirusScanned** indicates how many files VirusScan has VirusScanned for viruses. If you are using the default VirusScanning settings, VirusScan only checks executable files and MS-Word documents with standard executable or document file extensions (i.e., .COM, .EXE, .SYS, .BIN, .OVL, .DLL, .DOC, .DOT). To check all executable and MS-Word document files, use the /ALL command line option.

- **Possibly infected** indicates how many infected files VirusScan has found.

4. Do one of the following:

- If VirusScan reports “No viruses found,” congratulations—most likely your system is currently virus-free. Go to Step 6.

  ✍ *VirusScan’s ability to detect viruses must be maintained through regular upgrades of the VirusScan data files. For more information about updating VirusScan, refer to “Updating the VirusScan Database” on page 75.*

- If VirusScan finds one or more viruses, a message similar to the following is displayed:

  ```
  Scanning C:
  Scanning file C:\DOS\ATTRIB.EXE
  Found the Jerusalem Virus
  ```

  Do not panic, even if the virus has infected many files. At the same time, do not run any other programs, especially if the virus is found in memory. Refer immediately to “Cleaning the computer system in DOS and OS/2” on page 54.

5. To display a list of the Scan command-line options on screen, run Scan with the /? option.

6. 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 work.

Customizing On-Demand Options in Windows

You can customize the VirusScan On-Demand scan options available in Windows 3.x and Windows 95.

Using Scanning Packages

The Controls property page of the Notebook allows you to determine the scope of the scan by offering you several choices of scanning “packages.”

- **Executables Only** reduces scan time when a full scan is not needed by checking only executable and MS-Word document files with the extensions .COM, .EXE, .SYS, .BIN, .OVL, .DLL, .DOC, and .DOT. These are the files more commonly infected by viruses. If this option is **not** selected, VirusScan checks all executables and MS-Word files on the selected drives and directories, which increases scan time. Do not use this option if you are scanning an entire drive or individual files.

- **Subdirectories** includes the subdirectories of selected directories. If this option is **not** selected, VirusScan ignores subdirectories of selected directories. You do not need to select this option if you are scanning an entire drive or individual files.

- **Compressed Executables** tells VirusScan to check inside executable or self-decompressing files that have been created using LZEXE or PKLITE file compression programs. If selected, VirusScan decompresses each file in memory and checks for virus signatures, which takes more time but results in a more thorough scan. If this option is **not** selected, VirusScan does not check *inside* compressed files for viruses, although it can check for modifications if validation checking is used (refer to “Validation and recovery in Windows 3.x” on page 67).

- **Turbo Mode** reduces scan time by examining a smaller portion of each file, although it examines more files overall. This takes less time but might miss some infections found in a more comprehensive scan. Do not use this option if you have found a virus or suspect one.

- **Maximum Mode** performs the most thorough scan, but it takes the longest time. VirusScan will check all subdirectories, all files (not just standard executables), and all compressed executables.

Scheduling Virus Scans in Windows 3.x

You can schedule automatic virus scans in the Windows 3.x environment. VirusScan searches the drives, directories, or specific files you have selected. The scheduled scan occurs “in the background,” so you can continue your work if you’re using another application when the scan begins. Using the scheduled scanning feature, you can ensure that scanning will occur on a regular basis.

Windows 95

To schedule scans in Windows 95, use the Microsoft PlusPack scheduling agent. For more information, refer to your Windows 95 PlusPack manual.

To schedule a scan using VirusScan, use the following procedure:

Step	Action

1. Choose **Scan/Schedule**, or click on the Schedule icon.

Response: The Schedule dialog box is displayed.

- **Active Schedules** contains a list of scheduled scans stored in separate .VSS files. To add the currently selected items and settings to the Active Schedules list, click the Add button, which creates a new .VSS file in the Windows directory. To remove a scheduled scan, select it in the Active Schedules list, then click the Delete button, which deletes the associated .VSS file.

- **When to Scan** configures VirusScan’s frequency, date, and time information:

  - **Frequency** is the regular interval (Daily, Weekly, or Monthly) at which you want WScan to perform automatic scanning.

  - **Date/Day of Week/Month** is the day on which you want to scan. If the selected Frequency is Weekly, select the day of the week (Sunday through Saturday). If the Frequency is Monthly, select the day of the Month (1 through 31). If the Frequency is Daily, this list is unavailable.

  - **Time of Day** is the time of day at which the automatic scan will occur (midnight to 11:00 pm).

- **What to Scan** configures the scope of the scheduled scan:
  - **All Local Drives** configures VirusScan to select all local drives (including compressed, CD-ROM, and PCMCIA drives, but not diskette drives) on the workstation during the automatic scan.
  - **All Network Drives** will scan all network drives attached to the workstation during the scheduled scan.
  - **Select** displays the Scanning Selection dialog box from which you can select drives, directories and files for the currently selected scheduled scan.
  - **Options** displays the VirusScan Notebook, from which you can select scanning options for the currently selected scheduled scan.

    ✍ *Selecting items from within the Scheduler dialog box or the* VirusScan *Notebook does not change the items currently selected for scanning in the main application.*

Removing Viruses

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. If a virus is detected in memory, immediately shut down your computer, reboot from the clean start-up diskette (boot disk) you received in the VirusScan product.

Viruses attack your computer system by infecting files, usually executable program files, and 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. However, some viruses 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 by VirusScan to prevent another virus infection of your system.

About false alarms

Due to the nature of anti-virus software, there is a possibility that VirusScan may report a virus in a file or in memory, even if a virus does not exist. This can be more likely if you are using more than one brand of virus protection software, especially if the virus is reported in memory rather than on the boot disk.

Always assume that the virus is genuine. Follow the procedures outlined in “Cleaning the computer system in Windows” on page 49 or “Cleaning the computer system in DOS and OS/2” on page 54. Then upload any files that you suspect are generating false alarms to our bulletin board system at (408) 988-4004. For more information, refer to “How to Contact Us” on page 9.

Cleaning the computer system in Windows

If you are a Windows 95 or Windows 3.x user, 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, reboot from a clean start-up diskette, and remove the virus using VirusScan DOS commands. See “Cleaning the computer system in DOS and OS/2” on page 54 for instructions . Be sure you only use the DOS commands to clean your system if a virus was detected in memory.

You should use VirusScan to clean infections only if:

- You are *absolutely sure* your operating system is virus-free (VirusScan reported no viruses found in memory), and
- You are *absolutely sure* that all files on your system are virus free.

If VirusScan detects a virus in memory, you must use VirusScan's DOS commands to remove the virus. To use VirusScan to clean up infected files, the CLEAN.DAT file must be present in the subdirectory containing the VirusScan program files. By default, this file is stored in the VirusScan installation directory (\MCAFEE\VIRUSCAN).

If the virus was detected in memory, the master boot record, the boot sector, a VirusScan file, or an operating system file, you use VirusScan DOS commands to clean your system.

Use the following procedure to reboot your system in a clean DOS or OS/2 environment:

Step	Action
1.	Shut down your computer. ▪ In Windows 3.x, exit Windows and turn off your computer. ▪ In Windows 95, choose **Shut Down** from the Start menu. Turn off your computer when Windows informs you it is safe to do so.
2.	Reboot from the clean DOS or OS/2 start-up diskette.
3.	Follow the procedures outlined in "Cleaning the computer system in DOS and OS/2" on page 54 to remove the virus using VirusScan.

Removing a virus in Windows 95

If you perform a scan with either 'Clean infected file' or 'Delete infected file' as a pre-defined setting, VirusScan will respond automatically. When the scan is completed, the Virus Notification extension is displayed updating you on the status of all infected files found. You can also configure VirusScan to alert you when a virus is detected, and to prompt you for action.

✍ *You can configure on-access scanning (VShield95) to remove detected viruses automatically. For more information about configuring on-access scanning, refer to "Setting up on-access scanning in Windows 95" on page 16.*

To remove a virus in Windows 95 using VirusScan, begin by following the procedures outlined in "On-demand scanning in Windows 95" on page 37.

Step	Action

1. Before choosing the Scan Now button, click on the Actions tab.

Response: The Actions property page is displayed.

2. Use this property page to define VirusScan's action if infected files are detected.

- **Continue Scanning**: Continues scanning after virus detection occurs.
- **Prompt for Action**: Displays a dialog window which prompts you for action if a virus is determined.

  ✍ *Do not use this option if you perform scans when your system or workstation is unattended!*

  When a virus is detected, VirusScan will offer you the following choices:

  - Choose Continue if you want VirusScan to continue scanning until all files have been searched for viruses.
  - Choose Stop to end the scan session.
  - Choose Clean to repair the file.
  - Choose Delete to delete and overwrite the infected file.

- **Clean Infected File**: Attempts to repair any infected files detected. This is the recommended setting.

- **Delete Infected File**: Deletes infected files upon detection.

  ✍ *Files deleted with this option cannot be restored except from backups. Use the Reporting option (refer to "Validation and recovery in Windows 3.x" on page 67) so you know which files have been deleted.*

3. Select 'Clean Infected File' so VirusScan will repair any virus-damaged files.

   - VirusScan checks the drives, directories and/or files you have selected. The names of files being scanned are displayed in the status bar and any status or warning messages are displayed in the VirusScan main window.

   - If a virus is detected, VirusScan attempts to restore the boot sector and any infected files. VirusScan can repair files damaged by many viruses, but some viruses damage the infected file 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 file name so that you know what to restore from backups. Clean your system again, this time selecting the Delete Infected File check box to remove the file. Be sure to take note of the file names of any deleted files so you can restore them from backups.*

4. Most virus infections are introduced by booting from (or attempting to boot from) an infected diskette, or by accessing files on an infected diskette. Follow the procedures outlined in "Scanning your diskettes in Windows 95" on page 29 to scan and clean your diskettes.

Removing a virus in Windows 3.x

Use the following procedure to clean virus-infected files in Windows 3.x:

Step	Action
1.	Follow the procedures outlined in "On-demand scanning in Windows 3.x" on page 39.

2. Before choosing the Start Scan button, click on the Actions tab of the Notebook, or by choosing **Settings/Actions**.

   Response: The Actions page of the Notebook is displayed.

3. Use this property page to define VirusScan's action if infected files are detected.

   - Clean Infection (File, Boot Sector, MBR): Attempts to repair any infected files detected. This is the recommended setting.

   - Delete Infected File: Deletes infected files upon detection.

     ✍ *Files deleted with this option cannot be restored except from backups. Use the Reporting option (refer to "Validation and recovery in Windows 3.x" on page 67) so you know which files have been deleted.*

   - Move Infected File to Directory: Copies the infected file to the specified directory and deletes the original infected file upon detection.

     ✍ *Infected files can be uploaded to the McAfee BBS for expert inspection and disinfection. Select the Browse button to search for a directory. Be sure this is a restricted-access ("quarantine") directory to prevent re-infection. For more information about the McAfee BBS, refer to "How to Contact Us" on page 9.*

   - Select the Clean Infection (File, Boot Sector, MBR) check box on the Action page of the Notebook.

   - Click OK to return to the VirusScan main window.

4. Choose **Scan/Start Scan** or click the VirusScan icon.

   - VirusScan checks the drives, directories, and/or files you have selected. The names of files being scanned are displayed in the status bar and any status or warning messages are displayed in the VirusScan main window.

- If a virus is detected, VirusScan attempts to restore the boot sector and any infected files. VirusScan can safely remove many viruses from infected files, but some viruses will damage the infected file beyond repair. If VirusScan cannot safely remove the virus, a message is displayed indicating the name of the unrecoverable file.

  ✍ *If* VirusScan *reports that an infected file is corrupted beyond repair, take note of the file name so that you know what to restore from backups or the original diskettes. Consider cleaning your system again, this time selecting either the 'Delete Infected File' check box (to remove the file) or the 'Move Infected File to Directory' check box (to save it in a quarantine directory). For more information, refer to Step 3.*

5. Most virus infections are introduced by booting from or using infected diskettes. Follow the procedures outlined in "Scanning Your Diskettes" on page 29 to scan and clean your diskettes.

Cleaning the computer system in DOS and OS/2

Clean your system with VirusScan whenever you know or suspect that a virus infection has occurred. VirusScan can be used by DOS or OS/2 users, or Windows 3.x users who exit Windows to return to DOS. Windows 95 users can use DOS VirusScan by rebooting their system from a DOS start-up diskette.

Windows users must use VirusScan DOS commands if a virus is resident in memory, the master boot record (MBR), or the boot sector. Do not run VirusScan from Windows to remove a virus in memory, the master boot record, or the boot sector.

To use VirusScan to clean up infected files, the CLEAN.DAT file must be present in the subdirectory containing the VirusScan program files. If you do not have the CLEAN.DAT file, first verify whether you should contact your system administrator or information systems staff directly for virus clean-up. Otherwise, you can download the CLEAN.DAT file from the McAfee BBS at (408) 988-4004. For more information about McAfee, refer to "How to Contact Us" on page 9.

Start from the system prompt (C> or [C:\]). If you are running Windows 3.x or an application program, exit from it to display the prompt. If you are running OS/2, close all DOS and Win-OS/2 sessions; then open the Command Prompts folder in the OS/2 system folder and click the OS/2 Full Screen or OS/2 Window icon. If you are using Windows 95, shut down your computer and reboot from the DOS start-up diskette you created.

After typing each entry on the command line, press ENTER.

To remove the virus and repair any virus-infected files, use the following procedure:

Step	Action
1.	Navigate to the directory where VirusScan was installed. ✍ *The default directory is* C:\MCAFEE\VIRUSCAN. If the virus was found in memory, reboot from the clean, write-protected start-up diskette you created in "Getting Started."
2.	Eliminate the virus and repair any virus-infected files by typing: **`scan /adl /all /clean`** In OS/2, type: **`os2scan /adl /all /clean`**

where:

Scan (or os2scan)	runs the application.
/ADL	is used to scan and clean all local drive(s) (including hard drives, compressed, and CD-ROM drives, but not diskette drives).
/ALL	instructs VirusScan to scan all files, not standard executables and MS-Word documents.
/CLEAN	repairs any virus-infected files, if possible. Most files can be safely used again after using this option.

Response:

- If the virus is removed and all infected files are repaired, VirusScan informs you that the virus has been removed successfully.

or

- If one or more infected files cannot be repaired, VirusScan informs you with the message “Virus cannot be removed from this file.”

  Action: Take note of the file name(s) and proceed to Step 4.

3. If VirusScan successfully repaired all infected files, restart your computer and scan your system again. Your system should now be virus-free.

✍ *One common source of virus infection is diskettes. After you have successfully scanned your system, use VirusScan to examine and disinfect all the disks you use, following the procedures outlined in* *“Scanning Your Diskettes” on page 29**.*

4. If the virus-infected file is corrupted beyond repair, you need to delete the file and restore it from backup. Then run VirusScan again with the /ALL and /DEL options to delete any virus-corrupted files.

   Do not use DOS commands (e.g., DEL, FORMAT) to delete virus-infected files. This can result in the loss of all data and/or use of the infected disks.

Viewing Scan Results

You should create and maintain a record of your scanning activity. This allows you to monitor scanning activity and, if a virus later infects your PC, to possibly detect when and where the system initially entered your system.

- A report includes information about the items scanned, infections found, infections cleaned, and optional details about corrupted files, modified files, and system errors.
- A log keeps track of the dates and times you scan your system, as well as information regarding the items scanned and infections found.
- Notification is used to immediately warn users and/or administrators that a virus has been detected.

The following sections include information about creating, viewing, and printing report files and activity logs in Windows, DOS, and OS/2, and about how to set up notification in VirusScan.

Reporting and logging in Windows 95

To save scanning results to a report file in Windows 95, use the following procedure:

Step	Action
1.	Choose the Reports tab. **Response:** The Reports property page is displayed.
2.	Select Log to File to record virus activity information to a log file. ✍ *By selecting Log to File, VirusScan will automatically record its activity log in the default location, C:\Program Files\McAfee. If you want to select another location then 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.*

✍ *VirusScan supports long file names and Universal Naming Convention (UNC).*

3. Select ‘Limit size of log file to’ to change the maximum size of the log file.

✍ *The default activity log size is 100 KB. The value must be between 10 and 999 KB.*

Setting up notification in Windows 95

Notification can be used to alert users and/or administrators that a virus has been detected.

Use the following procedure to activate notification in Windows 95:

Step	Action

1. Select Display Message to add a message that, upon virus detection, will be displayed in the bottom of the Virus Found window.

✍ *You can use this message to add a customized note which will help users better respond to a virus. For example, you can direct users to a virus response center or technical support.*

Response: The Virus Found window is displayed.

✍ *This window is available when the Actions property page is set to Prompt for Action.*

2. Select Sound Alert to be notified by an electronic beep when a virus is detected.

Reporting and logging in Windows 3.x

Use the following procedure to save scanning results to a report file in Windows 3.x:

Step	Action

1. Display the Reports page of the VirusScan Notebook by choosing **Settings/Reports** from the menu bar or by clicking on the Settings icon and choosing the Reports tab:

   - **Report File Name** is the name of the report file you want to create or update. Type a file name, including the path, in the entry field, or choose Browse to select one from a list. If the target path is on a network drive, you must have sufficient rights to create, update, and delete files on that drive. The default file extension is .VSS.

   - **Append to Report File** instructs VirusScan to write the new information at the end of the specified report file, if the file already exists. If this check box is not selected, VirusScan will overwrite the old report file with the new report if the file names are the same.

   - **Include Corrupted Files** adds information about corrupted (non-recoverable) files to the report file. Between 10 and 20 percent of all viral infections result in files that are corrupted beyond repair. These files must be moved or deleted in order to prevent re-infection.

   - **Include Modified Files** adds information about validated files that have been modified to the report file.

     ✍ *For more information about validation checking, refer to* *"Validation and recovery in Windows 3.x" on page 67**.*

   - **Include System Errors** adds information to the report about errors that occurred during the scan, such as network problems, read/write errors, and so on.

- **Maintain Activity Log** tells VirusScan to save the time and date at which a scan is run, as well as any results of the scan, by updating or creating an activity log file. The default file name is SCAN.LOG, and the default path is the current directory.

  ✍ *For more information about the Scan Activity Log, refer to* *"Using the Scan Activity Log in Window" on page 61**.*

- **Keep Last *n* Events** tells VirusScan to retain log entries for the most recent scans only. By default, you can keep the 10 most recent events, but you can adjust this setting by changing the KeepLogOnly setting in the WSCAN.INI file. You can save from 1 to 100 events.

  ✍ *For more information, refer to the WSCAN.INI topic in the on-line help.*

Using the Scan Activity Log in Window

Use the following procedure to create a scan activity log in VirusScan.

Step	Action

1. Display the Reports page of the VirusScan Notebook by choosing **Settings/Reports** from the menu bar, or by clicking on the Settings icon and choosing the Reports tab.

2. Select the Maintain Activity Log check box. If this feature is enabled (i.e., the Maintain Activity Log check box is marked), VirusScan maintains an activity log of scanning dates, times, and results.

3. Do either of the following:

   - To view the activity log, choose **Scan/Activity Log** or click the Activity Log icon.

     Response: The Activity Log dialog box is displayed.

- To see details about scans and scanning results for a specific scan, select the entry in the Summary of Activities list and choose Details.

  Response: The Activity Log - Details dialog box is displayed.

4. You can print, view, or edit the activity log by opening the file through a text editor such as Microsoft Word or Notepad.

   ✍ *The default file name is VSCAN.LOG. To specify a different default file name for the Scan Activity Log, change the LogFile variable in the [Maintain] section of the WSCAN.INI file.*

Reporting and logging in DOS and OS/2

Use the following procedure to save scanning results to a report file in the DOS and OS/2 program, Scan.

Start from the system prompt (C> or [C:\]). If you are running Windows 3.X or an application program, exit from it to display the prompt. If you are running OS/2, close all DOS and Win-OS/2 sessions; then open the Command Prompts folder in the OS/2 system folder and click the OS/2 Full Screen or OS/2 Window icon.

To activate logging and reporting in DOS and OS/2, use the following procedure:

1. Navigate to the directory where VirusScan was installed.

   ✍ *The default directory is* C:\MCAFEE\VIRUSCAN.

2. Scan your C drive for known viruses and create a report with the file name C:\VIRUS.LOG by typing:

   ```
   scan c: /report c:\virus.log
   ```

   In OS/2, type:

   ```
   os2scan c: /report c:\virus.log
   ```

where:

Scan (or os2scan)	runs the application.
C:	specifies the target of the scan, in this case the hard drive (C:\).
/report c:\virus.log	instructs VirusScan to save the scanning results to a file, VIRUS.LOG, which is saved to the root directory.

✍ *If you have a program that uses special or nonstandard start-up functions, VirusScan may report some files as corrupt even though they are not.*

3. The following options for the report file are also available in VirusScan:

- /APPEND instructs VirusScan to write the new information at the end of the specified report file, if the file already exists. If this option is **not** specified, VirusScan will overwrite the old report file with the new report, if the file names are the same.
- /RPTALL adds the names of all files scanned to the report file.
- /RPTCOR adds the names of non-executable files to the report file. These files may have once been executable files that have been damaged by a virus and are no longer executable; however, they may also require overlay files or other programs in order to execute. Compare the results of /RPTCOR to previous reports to see if a file that was once executable is now listed as non-executable, which could be evidence of a virus-corrupted file.
- /RPTERR adds information to the report about errors that occurred during the scan, such as network problems, read/write errors, and so on.
- /RPTMOD adds information about validated files that have been modified to the report file.

  ✍ *For more information about validation checking, refer to "Validation and recovery in DOS and OS/2" on page 69.*

- /LOG tells VirusScan to save the time and date at which a scan is run, as well as any results of the scan, by updating or creating an activity log file. The default file name is SCAN.LOG, and the default path is the current directory.

✍ *For more information about the Scan Activity Log, refer to "Using the Scan Activity Log in VirusScan" on page 64.*

Using the Scan Activity Log in VirusScan

Use the following procedure to create a scan activity log in VirusScan:

Step	Action

1. Scan your C drive for known viruses and create a Scan Activity Log by typing:

```
scan a: /log
```

In OS/2, type:

```
os2scan a: /log
```

where:

Scan (or os2scan)	runs the application.
a:	specifies the target of the scan, in this case the diskette drive (A:\).
/log	saves the date and time of the scan to the Scan Activity Log, with the file name SCAN.LOG, in the current directory. If this file already exists, VirusScan updates the file with the new information.

2. To view the activity log, use the /SHOWLOG option instead of /LOG.

```
scan /adl /showlog /pause
```

In OS/2, type:

```
os2scan /adl /showlog /pause
```

You can print, view, or edit the activity log by opening the file through a text editor such as Microsoft Word or the DOS utility Edit.

✍ *The default file name is SCAN.LOG.*

Setting up notification in DOS and OS/2

Use notification to alert the user(s) that a virus has been detected. Follow this procedure to enable notification during a scan:

Step **Action**

1. Using a text editor, such as Microsoft Write, create a message that will be displayed to when a virus has been detected.

✍ *Be sure to save this message as text-only.*

2. Scan your network drives for known viruses and activate notification by typing:

```
scan /adn /contactfile c:\redalert.txt
```

In OS/2, type:

```
os2scan /adn /contactfile c:\redalert.txt
```

where:

Scan (or os2scan)	runs the application.
/adn	specifies the target of the scan, in this case all attached network drives.
/contactfile c:\redalert.txt	displays the text message saved in c:\redalert.txt, if a virus is detected.

3. Another notification option available in VirusScan is /LOCK. This option halts the system to stop further infection if VirusScan finds a virus. This option is useful in highly vulnerable network environments, such as open-use computer labs.

✍ *If you use /LOCK, use /CONTACTFILE to tell users what to do or whom to contact if a virus is found and the system locks up.*

Using Validate for Virus Detection and Recovery

VirusScan's validation and recovery options are powerful tools used to detect and disinfect viruses. Validation checking is a method of virus detection that routinely records information about files (file size, type, and so on) and then examines each file's "history" to detect suspicious activity. Using this technique, VirusScan is able to detect viruses that haven't been written yet! The recovery options are used to restore files that have been damaged by these new viruses.

✍ *Validation and recovery is not applicable to VirusScan for Windows 95.*

Validation and recovery in Windows 3.x

The Validation page of the Notebook lets you save validation information, scan using this information, and delete validation codes in order to update validation information after installing or upgrading software.

Access the Validation page of the Notebook by clicking on the Validation tab.

- **Use Codes Appended to Files** instructs VirusScan to store validation and recovery codes in the scanned files themselves, adding about 98 bytes to each file validated. This method validates files (but not the master boot record or boot sector) on a hard disk or diskette. If the files reside on a network disk. You must have sufficient rights to update them.

- **Use Codes in External File** stores validation and recovery codes in an external file you specify. If you select this option, type the file name in the entry field, or choose Browse to select one from a list. The data file size increases by about 95 bytes for each file validated. This method validates files on a hard disk or diskette as well as system areas. If the file resides on a network drive, you must have sufficient rights to update it. McAfee recommends using this method to store validation and recovery codes.

  ✍ *You can select either Use Codes Appended to Files or Use Codes in External File, but not both in the same scan.*

- **Add Codes** adds validation and recovery codes during the next scan. If you selected Use Codes Appended to Files, VirusScan adds the information to each executable and MS-Word document file scanned. If you chose Use Codes in External File, the information will be saved to the file specified in the entry field.

- **Check Codes** tells VirusScan to check validation and recovery codes during the next scan.

- **Remove Codes** deletes the validation and recovery code file (if Use Codes in External File is selected), or delete the validation and recovery code information from the modified executable and MS-Word document files.

If you install new software on your system, including a new DOS or Windows version, you will need to update validation codes to include these files. The only way to do this is to Remove Codes first, then scan your system using Add Codes.

Excluding files from validation

The Validation Exceptions page of the Notebook contains a list of files to exclude from the validation checking options you selected on the Validation page. You can also create the exception file as an ASCII file using a text editor, with each line of the text file the path and file name of a file to exclude from validation.

If you set up validation codes, subsequent scans can detect changes in validated files. This can trigger false alarms if the executable files are self-modifying or self-checking (most programs that do this will tell you to turn of your antivirus software before running them). Therefore, when using validation codes, specify an exception list to identify such files and exclude them from validation checking.

- **Exceptions File** is the name of the file containing the list of files to exclude. Type the file name and path in the text box, or choose Add and select it from a list.

- **Files to Exclude from Validation** is the list in the exceptions file of self-modifying or self-checking files to exclude. To add a new file to the exceptions list, type the name and path in the data entry box, or choose Add and select it from a list. To delete an entry, select it in the list and press DEL.

Validation and recovery in DOS and OS/2

These options are used to detect and recover from new or unknown viruses.

There are two methods to storing validation and recovery codes:

- The “F” options (/AF, /CF, /RF) store validation and recovery codes in a separate file. The “F” options are slow but do not edit the actual files themselves. The “F” options can also be used to detect changes in the boot sector and master boot record. McAfee recommends that you use this method.

- The “V” options (/AV, /CV, /RV) store validation and recovery codes in the files themselves. The “V” options save their information directly to the executable or MS-Word document file, so they are faster than the “F” options, but some self-modifying files (such as PKZIP or WordStar) may report “false alarms” using this method. These options do not look for changes in the boot sector or master boot record.

For more information about validation and recovery codes, refer to “Validation and recovery in DOS and OS/2” on page 69.

Using the /AF, /CF, and /RF options

The /AF, /CF, and /RF options store validation and recovery information in a separate file. These options are slower than the /AV, /CV, and /RV options but they do not modify the files themselves. In addition, the /AF, /CF, and /RF options check for changes in the boot sector and master boot record.

✍ *Using any of the /AF, /CF, or /RF options together in the same command line returns an error.*

You may want to use /CV instead of /CF if the following applies:

- 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 system's reference manual to determine whether your PC has self-modifying boot code. If it does, use /CV instead.

- OS/2 dual boot systems change the boot sector between DOS and OS/2 depending on which operating system is active. This causes VirusScan to report that the boot sector has been modified. Use /CV instead, which does not check the boot sector for modifications.

OS/2

To store validation and recovery codes in a separate file, using the following procedure:

Step	Action

1. Navigate to the directory where VirusScan was installed.

✍ *The default directory is* C:\MCAFEE\VIRUSCAN.

2. Perform a scan on all local drives and save the validation and recovery codes to a file by typing:

```
scan /adl /af c:\valcodes.vsc
```

In OS/2, type:

```
os2scan /adl /af c:\valcodes.vsc
```

where:

Scan (or os2scan)	runs the application.
C:	specifies the hard drive (C:\) as the target of the scan.
/ADL	instructs VirusScan to scan all local drives.
/AF C:\VAL-CODES.VSC	saves the validation and recovery codes to a file (VALCODES.VSC) saved in the root directory of C: drive.

✍ *If the target path is a network drive, you must have rights to create and delete files on that drive. If {filename} already exists, VirusScan updates it. /AF adds about 300 percent more time to scanning. The validation and recovery code file created is about 89 bytes per file validated.*

To scan and clean using validation and recovery codes saved to a separate file, follow the procedure below:

Step **Action**

1. Navigate to the directory where VirusScan was installed.

   ✍ *The default directory is* C:\MCAFEE\VIRUSCAN.

2. Perform the above procedure to save the validation and recovery information to a file.

3. Scan all local drives using the validation and recovery information by typing:

   ```
   scan /adl /cf c:\valcodes.vsc
   ```

   In OS/2, type:

   ```
   os2scan /adl /cf c:\valcodes.vsc
   ```

   ✍ */CF adds about 250 percent more time to scanning.*

4. If Scan reports a virus has been detected, perform another scan using the /CF and /CLEAN options (refer to "Cleaning the computer system in DOS and OS/2" on page 54) to repair any virus-damaged files using the recovery codes.

If you install new software or upgrade your existing software, you will have to update the validation and recovery codes. Delete the validation and recovery code file by using DOS commands (e.g., DEL C:\VALCODES.VSC) or use the following procedure to delete validation and recovery codes through VirusScan:

Step	Action

1. Navigate to the directory where VirusScan was installed.

   ✍ *The default directory is* C:\MCAFEE\VIRUSCAN.

2. Delete the validation and recovery codes from the file by typing:

   ```
   scan /adl /rf c:\valcodes.vsc
   ```

   In OS/2, type:

   ```
   os2scan /adl /rf c:\valcodes.vsc
   ```

Using the /AV, /CV, and /RV options

The /AV, /CV, and /RV options are faster than the /AF, /CF, and /RF options because they store the validation and recovery information in the actual file, not in a separate file. However, the /AV, /CV, and /RV options may create a "false alarm" on self-modifying programs. In addition, the /AV, /CV, and /RV options do not check the boot sector or master boot record for changes.

Some files are self-modifying or self-checking and will therefore produce "false alarms" if you use this method of validation and recovery checking. Most self-modifying or self-checking programs will tell you to turn off your anti-virus software before running them.

VirusScan provides you with the /EXCLUDE option so you can still use validation checking even if some of your programs are self-checking. To create an exception list and use it with the /EXCLUDE option, refer to "Using Validate for Virus Detection and Recovery" on page 67.

✍ */AV adds information to every executable and MS-Word file scanned. Each file adds about 98 bytes per file inspected.*

To store validation and recovery codes in the same file, use the following procedure:

Step **Action**

1. Navigate to the directory where VirusScan was installed.

✍ *The default directory is* C:\MCAFEE\VIRUSCAN.

2. Perform a scan on all local drives and save the validation and recovery codes to the checked files by typing:

```
scan /adl /av
```

In OS/2, type
```
os2scan /adl /av
```

where:

Scan (or os2scan)	runs the application.
C:	specifies the hard drive (C:\) as the target of the scan.
/ADL	instructs VirusScan to scan all local drives.
/AV	saves the validation and recovery codes to the file being inspected.

To scan and/or clean using validation and recovery codes:

Step **Action**

1. Navigate to the directory where VirusScan was installed.

✍ *The default directory is* C:\MCAFEE\VIRUSCAN.

2. Perform the above procedure to save the validation and recovery information to the inspected executable files.

3. Scan all local drives using the validation and recovery information by typing:

   `scan /adl /cv`

   In OS/2, type:
   `os2scan /adl /cv`

4. If VirusScan reports a virus has been detected, perform another scan using the /CV and /CLEAN options (refer to "Cleaning the computer system in DOS and OS/2" on page 54) to repair any virus-damaged files using the recovery codes.

If you install new software or upgrade your existing software, you will have to update the validation and recovery codes. Delete the validation and recovery codes from the executable and MS-Word files with the following procedure:

Step	Action

1. Navigate to the directory where VirusScan was installed.

   ✍ *The default directory is* C:\MCAFEE\VIRUSCAN.

2. Delete the validation and recovery codes by typing:

   `scan /adl /rv`

   In OS/2, type:
   `os2scan /adl /rv`

Updating the VirusScan Database

To offer the best virus protection possible, McAfee continually updates the files VirusScan uses to detect the most current viruses. After a certain time period, you are notified that you need to update the virus definition database.

To update this database, you can go to the McAfee Store located at this Internet World Wide Web address:

http://www.mcafee.com

Once you have received the new files, unzip them and copy them into the VirusScan installation directory.

A VirusScan DOS and OS/2 Command Options

VirusScan Command Options

The following table lists all of the VirusScan command options you can use when you're running the program in DOS and OS/2.

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 more files. By default, Scan checks files with .COM, .EXE, .SYS, .BIN, .OVL, .DLL, .DOC, and .DOT extensions, which are the files most likely to be infected by a virus. 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. 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	Uses the VirusScan settings stored in *filename.* VirusScan gets its settings from the default configuration file, DEFAULT.CFG, which is delivered with BootShield. You can specify any additional options on the command line. Alternatively, 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. Use the /LOAD *filename* command-line option to perform a scan using the information saved in this file. For example, if you have created a configuration file called FLOPPY.CFG, enter: **scan /load floppy.cfg** The above command line initiates a scan using its internal default settings plus any options specified in FLOPPY.CFG.
/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. ✍ *Scan does not check compressed files, such as .ZIP and .ARC files.*
/NODDA	No direct disk access. Prevents VirusScan from accessing the boot record. This feature has been added to allow Scan 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 50 pages long.*

Scan command option examples

The following examples show the VirusScan command using various option settings. Remember that you can use the DEFAULT.CFG file to specify the commands used each time VirusScan is run.

These examples show how to scan all files, not just the boot sector.

- To scan your computer's C: drive:

  `scan c:`

  VirusScan checks executable files on C:, plus the boot sector and boot master record and RAM memory file viruses.

- To scan the computer's boot sector and master boot record:

  `scan c: /boot`

This command also scans memory.

- To scan executable files on drive F:, a network drive:

  ```
  scan f:
  ```

- To scan executable files on multiple diskettes on drive A:

  ```
  scan a: /many
  ```

  VirusScan checks the diskette in drive A:, then prompts the user to insert more disks to continue checking. This command also scans the diskette's boot sectors.

- To scan all local and network drives (including compressed, CD-ROM, and PCMCIA drives, but not diskettes):

  ```
  scan c: /adl /adn
  ```

- To scan for viruses in files and add validation codes to executable files on drives C:, D:, and E:

  ```
  scan c: d: e: /av /all
  ```

- To scan for viruses on network drive M: and create a log file of infections, corruptions, and errors in the file INFECTN.RPT on drive D:

  ```
  scan m: /report d:\infectn.rpt /rptcor /rpterr /append
  ```

  If D:\INFECTN.RPT already exists, VirusScan appends the new information to the existing report file.

- To scan files in the directories USER\MAC, USER\BILL, and USER\DAVE:, including their associated subdirectories, on drive E:

  ```
  scan e:\user\mac e:\user\bill e:\user\dave /sub /all
  ```

- To quickly scan drives C:, D:, and E: and report any executable files that have associated validation codes and have been modified:

  ```
  scan c: d: e: /fast /cv
  ```

- To scan a single file, in this case COMMAND.COM:

  ```
  scan c:\command.com
  ```

On-Access Scanning Command Options (VShield)

The following table lists the VShield command options you can use when you run the command in DOS, Windows 3.x, and OS/2.

Command-Line Option	Type	Description
/? or **/HELP**	General	Display a list of valid command line options.
/ANYACCESS	Target	Scan the boot sector whenever a diskette is accessed (read and write); scan executables; scan any newly created files.
/BOOTACCESS	Target	Scan the boot sector for viruses whenever a diskette is accessed (including read/write operations).
/CERTIFY	Validation/ Recovery	Prevent files without validation codes from running.
/CF filename	Validation/ recovery	Check validation/recovery codes stored by VirusScan /AF in {filename}.
/CONTACT message	Notification	Display specified message when a virus is found.
/CONTACTFILE filename	Notification	Display message stored in {filename} if a virus is detected.
/CV	Validation/ recovery	Check validation/recovery data stored in files by VirusScan /AV.
/EXCLUDE filename	Validation/ recovery	Do not check files listed in {filename} for validation codes (/CV option).
/FILEACCESS	Target	Scan executable files when they are accessed on a diskette, but do not check the boot sector.
/HELP or /?	General	Display help screen.

Command-Line Option	Type	Description
/IGNORE drive(s)	Target	Do not check programs loaded from the specified drive(s).
/LOCK	Notification	Halt the system if a virus is detected.
/NOEMS	Memory	Do not use expanded memory (EMS).
/NOMEM	Target	Disable memory checking.
/NOREMOVE	General	Prevent VShield from being removed from memory with the /REMOVE switch.
/NOUMB	Memory	Do not use upper memory blocks (UMB).
/NOWARMBOOT	Target	Do not check the diskette boot sector for viruses during warm boot (system reset or (CTRL+ALT+DEL).
/NOXMS	Memory	Do not use extended memory (XMS).
/ONLY drive(s)	Target	Check only programs loaded from the specified drive(s).
/POLY	Target	Check for polymorphic viruses.
/RECONNECT	General	Restore on-access scanning after certain drivers or TSRs have disabled it.
/REMOVE	General	Unload VShield from memory.
/SAVE	General	Save the command line options to the VSHIELD.INI file.
/SWAP pathname	Memory	Load VShield kernel (8 Kb) only; swap the rest to [pathname].
/XMSDATA	Memory	Loads VShield data files into XMS memory.

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 database (*.DAT) 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 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) were 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 was found in the master boot record, boot sector, or file(s).
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	Multiple viruses were found and cleaned.
20	/FREQUENCY option prevents scanning again.
21-99	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.)

VShield DOS Error Levels

VShield error levels

When on-access scanning (VShield) is activated, a DOS error level is set. You can use the returned ERRORLEVEL in AUTOEXEC.BAT or another batch file to take different actions based on whether VShield has loaded in memory. Refer to your DOS manual for more information.

ERRORLEVEL	Description
0	VShield successfully loaded into memory with all options operational.
9	VShield not loaded correctly. Abnormal termination (program error).

VShield alerts you to problems by beeping once for system errors, twice for validation errors, or three times if a virus is found.

CheckVShield DOS Error Levels

When you run CheckVShield in the DOS environment, a DOS error level is set. Use the ERRORLEVEL in batch files to take different actions based on the results of CheckVShield's ERRORLEVEL.

The following table describes the CheckVShield error levels.

ERRORLEVEL	Description
0	VShield or VShieldCRC is resident or, if /V is used, the version specified is resident in memory.
1	VShield or VShieldCRC is resident but does not match the version specified in /V.
2	VShield or VShieldCRC not resident in memory.
3	Abnormal termination (program error).

See Chapter 3, "Getting the Basics." for instructions on entering the Check-VShield command.

B Creating a Secure System Environment

Keys to a Secure System Environment

VirusScan is an effective way to prevent, detect, and/or recover from viral infection. VirusScan is most effective when it is used in a virus-free environment, the "sterile field" that was discussed in "*Getting Started*." This appendix contains information that should help you create and maintain a virus-free working environment.

McAfee recommends that you do the following to ensure a secure system environment:

- Be sure to follow the installation procedures as outlined in "*Getting Started*."
- Configure your AUTOEXEC.BAT file to load VShield automatically at start-up.

Windows 95

✍ *VShield for Windows 95 is automatically loaded if you followed the recommended installation procedures.*

- Scan all the diskettes you use by using Scan with the /MANY option (refer to "Scanning Your Diskettes" on page 29).
  - Never start your computer from an unchecked diskette. Always make sure your disk drive(s) are empty before turning on or starting your computer.
  - Rescan whenever you introduce new programs onto your computer.
  - Run VirusScan on an unknown diskette before executing, installing, or copying its files.

- If you download or install software from a network server, bulletin board, or on-line service, run VirusScan on the directory you placed the new files in before executing them.

- Create a start-up diskette containing the Scan program and DOS by following the procedure outlined in *Getting Started*.

  ✍ *Make sure the diskette is write-protected so that it cannot become infected.*

VirusScan is an effective virus-preventive measure when used in a conscientiously applied program of network security and regular professional care.

VirusScan is one important element of a comprehensive computing security program that includes a variety of safety measures, such as regular backups, meaningful password protection, user training, and awareness. Even with VirusScan, some viruses (as well as fire, theft, or vandalism) can render a disk unrecoverable without a recent backup.

Although outlining a full security program is beyond the scope of this manual, refer to *Getting Started*.

If you are a network administrator, we urge you to implement security procedures to safeguard your organization's data and productivity. If you are a network user, please support and comply with such a program.

Detecting New and Unknown Viruses

There are two ways of dealing with new and unknown viruses that may infect your system:

- Update the VirusScan database (.DAT) files
- Store and check validation and recovery information about your files.

Update the VirusScan database files (.DAT)

To offer the best virus protection possible, McAfee continually updates the files VirusScan uses to detect the most current viruses. After a certain time period, you are notified that you need to update the virus definition database.

To update this database, you can go to the McAfee Store located at this Internet World Wide Web address:

http://www.mcafee.com

Once you have received the new files, unzip them and copy them into the VirusScan installation directory.

Using validation/recovery information

If your environment is highly vulnerable to viruses, or if you require unusual security against them, you should make use of VirusScan's validation and recovery options. VirusScan checks for new or unknown viruses by comparing files against previously recorded validation data. If a file has been modified, it will no longer match the validation data, and VirusScan reports that the file may have become infected. Scan has two levels of validation, which are stored in two separate ways:

- It can store the enhanced code in a separate recovery file, which can be stored off-line (for example, on a diskette) for recovery purposes. This is the preferred method.

- It can append a simple 98-byte validation code to executable files. You can create an exceptions list to exclude some executables from this method. This method does not store information about the master boot record or boot sector. This option is primarily useful for companies that distribute software to their customers or employees, and want to incorporate an additional level of virus protection.

McAfee recommends that you save the validation/recovery information to a separate file. This method is more effective because you can keep a backup of the validation/recovery information on a diskette, network drive, or tape drive so you can recover from viral infections. And because this method does not alter the executable programs themselves, you can avoid triggering false-alarms in self-checking programs, such as Lotus 1-2-3.

If you do use the latter method (storing validation/recovery information within the executable files themselves), you will need to create an exceptions list for self-checking programs. For more information, refer to "Using Validate for Virus Detection and Recovery" on page 67.

Once the validation codes are stored, you can instruct VirusScan to use the recorded information to check the files for changes. You can also use the recovery information to repair these files should they become damaged by a viral infection.

Validation checking is only effective if you maintain these codes. Whenever you install or upgrade software (including the operating system), you need to delete the old validation codes and replace them with up-to-date information.

Understanding False Alarms

A false alarm is a report of a virus in a file or in memory, even if a virus does not exist. False alarms are more likely if you are using more than one brand of virus protection software, especially if the virus is reported in memory rather than on the boot disk.

When you run more than one anti-virus program, you risk strange results and false alarms. For example, some anti-virus programs store their “virus signature strings” unprotected in memory. Running VirusScan may “detect” them falsely as a virus. Your system’s BIOS, use of validation codes, and other factors may also produce false alarms.

Always assume that any virus found by VirusScan is a real and dangerous virus, and follow the tasks outlined in “Removing Viruses” on page 49.

After following the procedures outlined above, if you still 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:

- 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, such as VSafe. Turn off your computer, wait a few seconds, and turn it on again to make sure that all code from other anti-virus programs are cleared from memory.

- Some BIOS chips include an anti-virus feature which 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. For more information, refer to “Using Validate for Virus Detection and Recovery” on page 67.

- Some older Hewlett-Packard and Zenith PCs modify the boot sector each time the system is booted. OS/2 dual boot systems change the boot sector between DOS and OS/2 depending on which operating system is active. 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.

Removing a Virus

If a virus is detected in your system, follow the procedure for removing a virus found in Chapter 4, “Advanced Functions,” immediately. Using this procedure right away eliminates the possibility of further damage to your computer data.

C

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. Whether it is our complimentary 90-day introductory technical support program or the optional 1-year personal online maintenance and support program, McAfee wants to ensure that all our customers receive the level of support they require.

In addition, we offer a variety of technical assistance plans designed to meet the needs of business customers, including training, consulting, and enterprise support, as well as 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 (.DATs), and 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 products are entitled to free online virus updates (new .DAT files) for the life of the product, one free online product upgrade (product version revision) with the newest features and virus protection (if applicable), and the free support services listed below during the first 90 days of software ownership.

- Technical support phone assistance during regular business hours, 6:00A.M.– 5:00P.M. PST, Monday through Friday, from our professionally trained support representatives at (408) 988-3832.
- 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.

To receive your free one-time online upgrade please contact our Sales Support 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.

Subscription maintenance and support program (free)

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

- Technical support phone assistance during regular business hours, 6:00A.M.–5:00P.M. PST, 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 protection (if applicable). If you upgrade your operating system, you can also upgrade your McAfee product to the new platform (for example, from Windows 3.1 to Windows 95).

- 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.

Optional support plans

Option 1—one-year personal online maintenance and support program

$149 U.S.

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 protections 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 maintenance and support programs

$149 U.S.

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 CDs (depending on the product) and a quarterly update newsletter. With this option, you can update your product to include the latest features and virus updates without having to download files 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 sales support department at (408) 988-3832.

✍ *McAfee reserves the right to change part or all components of its customer services 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.

✍ *McAfee reserves the right to change part of all of its Professional Services Program at any time without notice.*

Training

$190 U.S./hour or $1,200 daily, as well as packaged rates

McAfee's expertise and experience is available to your personnel, allowing an organization to take full advantage of 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

$190 U.S./hour or $1,200 daily, as well as packaged rates

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
- Installation and configuration

- Windows 95 configuration
- 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

$7,500 U.S. for a 4-day network management program or $5,500 for a 3-day anti-virus 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

$10,000 U.S. for a one-year subscription

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. CST Monday–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).

Each 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 enterprise support features

$5,000 U.S per feature

7 X 24 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.

Remote support

This feature provides customers with data connection support using McAfee's NetRemote product. This support option provides services such as remote network administration and management, network troubleshooting, and optimization.

D

Anti-Virus Hints

VirusScan finds and cleans most known (and some unknown) viruses. But part of the responsibility for virus protection is yours. To best ensure complete protection, you need the following:

- A clean start-up diskette (boot diskette)
- The most recent VirusScan data files

Making a Clean Start-up Diskette

In case your system becomes infected, you must have a clean (virus free) start-up (boot) diskette in order to restore your system's sterile field. 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, use the steps below to create a boot diskette.*

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

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 an earlier version of DOS, do not type the* **`/u.`** *If you are unsure of which version you are using, type* **`ver`** *at the* **`C:\>`** *prompt for version information.*

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 \mcafee\viruscan
   ```

5. Copy the DOS version of VirusScan to the diskette by typing the following commands at the **`C:\mcafee\viruscan`** prompt:

```
copy scan.exe a:

copy scan.dat a:

copy clean.dat a:

copy names.dat
```

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

   ```
   cd/
   ```

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

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

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

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

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

Important: Label and write protect this diskette. Store it in a secure place.See "Write Protecting a Diskette" on page 112 for more information.

Write Protecting a Diskette

Floppy diskettes are a convenient, portable device 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 diskette.

If your system does become infected with a virus, the write protection feature keeps your clean diskettes from also becoming infected, preventing reinfection after your system is cleaned.

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

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.

3.5" floppy diskettes

Step	Action
1.	Position the diskette face down with the metal slide facing you.

Examine the small rectangular hole on the upper left side. There should be a square, plastic tab that you can slide back and forth across the hole.

2. To write protect the diskette, slide the plastic tab upward toward the edge of the diskette so that the whole is completely covered.

Updating Data File for VirusScan

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 the older data files. That is, the data file that came with your copy of VirusScan might not be able to help VirusScan detect a virus that was discovered five 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 release about every four to six weeks.

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

How to apply the data file

Step	Action
1.	Download the data file (for example, DAT-9602.ZIP) from one of McAfee's electronic services. On most services, it is located in the anti-virus area.
2.	The file is in a compressed format. Decompress the file using any PKUNZIP-compatible decompressing software. If you don't have the decompressing software, you can download PKUNZIP (shareware) from the McAfee electronic sites. The file is: PKZ204G.EXE.

3. Find the directories on your hard drive where the software is currently loaded.

   Typically, the files are kept in C:\MCAFEE\VIRUSCAN. This varies depending on the version of the software you have and on whether or not a different directory was specified during installation.

   ✍ *There might be part of the software in more than one directory. If so, place the updated files in each directory.*

4. Copy the new files into these directory or directories, overwriting the old data files.

5. Reboot your computer so that changes take place immediately.

How to Clean Your System With VirusScan

If you detect a virus, you must run VirusScan from a clean, virus-free environment. Follow these steps:

Step	Action
1.	Turn off your computer. Do not reboot using the reset button or CTRL+ALT+DELETE; if you do so, some viruses might remain intact.
2.	Make sure that your clean startup diskette is write protected, and insert it into the A: drive. See “Write Protecting a Diskette” on page 112 for more information.
3.	Turn on your computer and wait for the system prompt. Because you are booting the computer with a diskette in drive A:, you will get an **A:\>** prompt.
4.	Remove the clean start-up diskette from drive A:.
5.	Insert the original VirusScan diskette into the A: drive. If you are running VirusScan for Windows, you might need to use diskette #2 of 2, or depending on your version of VirusScan, you might have a diskette labeled “Emergency Disk.”
6.	Eliminate the virus(es) on your hard drive(s) by typing the following command at the **A:\>** prompt: `scan c: /clean /all`
7.	After the virus has been removed, restart your computer. This time do not put the startup diskette in drive A:.
8.	If VirusScan was not previously installed, install it now.

Glossary

The following list defines some terms you might encounter while using VirusScan to guard your computer against boot sector viruses and other types of viruses.

BIOS

A read-only memory chip that contains the coded instructions for using hardware like 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 an anti-virus feature which 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.

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 very 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.

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.

conventional memory

Up to 640 KB 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 1 MB 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 1 MB limit of conventional memory. Often used for RAM disks and print spoolers.

false alarm

Reporting a viral infection when none is present.

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 640 KB 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) 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.

terminate-and-stay-resident (TSR)

A DOS program, like VShield, that remains active in memory while you run other programs.

turbo

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

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 640-1024 KB, just above the DOS 640 KB 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 the computer 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 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

H

I

K

L

M

N

O

P

R

S

T

U

V

W