
Table of Contents

Chapter 1. About This Document..... 3

Who Should Read This Document	3
What You'll Find in This Book	4
Notation and Symbols.....	5
Terminology and Tips	7

Chapter 2. Getting Started 8

What Is VirusScan?	8
If You Suspect You Have a Virus	9
What Your VirusScan Package Includes	13
About Installation	14
Validating VirusScan Program Files	17
Installing VirusScan	19
Creating a Clean Start-Up Diskette	23
Backing Up Your Hard Drive.....	26
Scanning Your Diskettes	27
Updating the VirusScan Database.....	30
How to Contact Us	33
Other Sources of Information.....	35

Chapter 3. Setting Up VirusScan 36

Setting Up VirusScan in Windows	36
Setting Up VirusScan in DOS and OS/2.....	42
Setting Up On-Access Scanning (VShield).....	60

Setting Up Settings Files and Scanning Profiles 78

Chapter 4. Scanning..... 85

Overview 85

When Should I Scan for Viruses? 86

Scanning in Windows 88

Scanning in DOS and OS/2 97

Cleaning Your System 103

Validation and Recovery 113

Reporting, Logging, and Notification..... 121

**Appendix A. Creating a Secure
System Environment 129**

Keys to a Secure System Environment 129

Detecting New and Unknown Viruses 131

Understanding False Alarms 133

Using DOS Commands to Remove a Virus 135

Glossary 136

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, Windows/NT, OS/2, or NetWare. VirusScan helps you protect one of your most important assets—the information on your computer or local area network (LAN).




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

Installation and usage instructions and guidelines for protecting computers against viruses are all here. 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.

 If you believe that you already have a virus, please proceed to [“If You Suspect You Have a Virus”](#) on page 9.

What You'll Find in This Book

This user's guide contains information you need for installing and 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:

Getting the basics

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

Installing and using VirusScan

Chapter 2, "Getting Started." Instructs you on how to install and validate the VirusScan programs for optimal anti-virus protection for your personal computer or network.

Chapter 3, "Setting Up VirusScan." Explains how to run VirusScan, use the tool bar and menu bar in Windows, and the use command-line syntax for DOS and OS/2 users.

Chapter 4, "Scanning." Provides procedures for on-demand and on-access 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.

Appendix A, "Creating a Secure System Environment." Provides recommendations for creating and maintaining a virus-free working 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 is designed to eliminate 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 **screen text**. Placeholders for items such as file names or command parameters are in {curly brackets}. Optional placeholders are placed in [square brackets].

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

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.



This note contains important information for all users.



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 DOS and OS/2, as well as entering commands using the VirusScan graphical user interface in Windows.

In DOS and OS/2, this means you enter the command at the DOS or OS/2 prompt. In Windows, you make selections using your mouse and keyboard.

Selecting elements

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



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.

What Is VirusScan?

VirusScan is McAfee's powerful and advanced desktop anti-virus solution. It detects, removes, and prevents computer viruses on IBM-PC or 100 percent IBM-compatible machines running DOS, Windows 3.x, Windows 95, Windows/NT, or OS/2. VirusScan helps protect one of your most important assets — the information on your personal computer or local area network.

You can use VirusScan to detect and remove viruses, and to clean, move, or delete virus-infected files. VirusScan continuously monitors and protects your system against viruses.

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 A, "Creating a Secure System Environment."](#)

If You Suspect You Have a Virus

If you believe that your system has been infected by a virus, follow these steps to scan your system and remove any viruses encountered.

Step

Action


1. Restart from a clean environment.
 - In DOS or OS/2, exit any applications and turn off 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.
 - In Windows/NT, choose Shut Down from File Manager, or press CTRL+ALT+DEL and choose Shut Down. Turn off your computer when Windows informs you it is safe to do so.
2. Get a write-protected DOS or OS/2 start-up diskette into drive A:, preferably the original DOS or OS/2 installation diskette that came with your computer. You can also use a Windows 95 emergency recovery diskette.

✍ If you do not have a write-protected DOS start-up diskette, borrow one from someone else who has the same version of DOS; do not use a diskette that might be infected. (If you do not have a virus-free start-up diskette, you can create one using the procedure outlined in “[Creating a Clean Start-Up Diskette](#)” on page 23, but perform this task only after you have successfully completed these steps to clean your system.)
3. Make sure this diskette is write-protected.
 - For a 3.5” diskette, make sure that the square hole is open.
 - For a 5.25” diskette, make sure that the corner notch is covered with a write-protect tab. Always use the write-protect stickers provided with the diskette, not tape.



Make sure your diskette is write-protected.

4. Insert the diskette into drive A:.
5. Turn on your computer and wait until you see the system prompt (probably A>). If you restarted using your original DOS installation diskette, exit from DOS Setup. Do not run any programs on your hard disk, or you may reactivate the virus. Turn on your computer and wait until you see the DOS prompt (A> or [A:\]). If you restarted using the DOS installation diskette or another diskette, exit from Setup to display the DOS prompt.
6. Remove the start-up diskette and insert the write-protected VirusScan program diskette into drive A:. This diskette is labeled Emergency Recovery Diskette. It is the last diskette in the VirusScan package.

 *If you downloaded VirusScan for DOS from the McAfee BBS, unzip the file containing SCAN.EXE and run it. For more information about downloading evaluation copies of software from the McAfee BBS, see ["How to Contact Us" on page 33](#).*

7. Insert the write-protected VirusScan program diskette into drive A.
8. Do one of the following:
 - In DOS and Windows environments, enter the following command to eliminate the first known virus by searching all files on all local drive(s) (including hard drives, compressed, CD-ROM, and PCM-CIA drives, but not diskettes):

```
scan /adl /clean /all
```

or

- In OS/2, enter the following command to eliminate the first known virus:

```
os2scan /adl /clean /all
```

Response: VirusScan keeps you informed of its progress and generally reports that the virus has been removed successfully.

Action: If Scan reports that the virus was removed successfully, refer to [“If viruses were removed.”](#) If Scan reports that the virus could not be removed successfully, refer to [“If viruses were not removed.”](#)



Windows/
NT

✍ If you are a Windows/NT user with an NTFS (New Technologies File System) partition, you will not be able to see the NTFS partition from DOS. This procedure will eliminate any virus that may be on the master boot record (MBR) or boot sector of the hard drive. After completing this procedure, perform a scan through WScan for Windows/NT to eliminate any viruses that have infected files on the NTFS by following the procedure outlined in [“Removing a virus in Windows 3.x and Windows/NT”](#) on page 107.

If viruses were removed

If Scan successfully removes all the viruses, shut down your computer and remove the VirusScan program diskette. You may now begin the installation procedure as described in [“Installing VirusScan”](#) on page 19. After completing the installation procedures, you should scan all the diskettes you use to find and eliminate the source of the infection. Proceed to [“Scanning Your Diskettes”](#) on page 27.

If viruses were not removed

If Scan cannot remove a virus, it will tell you:

Virus could not be removed.

Make sure to take note of the file name, because you will need to restore it from backups. Run Scan again, this time using the **/CLEAN** and **/DEL** options to delete the remaining infected files. For more information about using **/DEL**, refer to [“Cleaning Your System”](#) on page 103.

After the virus-infected files are deleted, begin the installation procedure as described in [“Installing VirusScan”](#) on page 19. Install scans your system and, assuming your system is now virus-free, installs VirusScan and activates on-access scanning (VShield) to protect your system from further infection.

You should now scan all the diskettes you use to find and eliminate the source of the infection. Proceed to the next step, [“Scan and disinfect your diskettes”](#) on page 12.

Scan and disinfect your diskettes

One common source of virus infection is diskettes. Once you have finished installing VirusScan on your hard disk, use Scan again to examine and disinfect all the diskettes you use, as described in [“Scanning Your Diskettes” on page 27](#).

What Your VirusScan Package Includes

The VirusScan package includes the following programs:

- Scan, which detects and removes viruses from your IBM-PC or 100% compatible personal computer that uses the DOS, OS/2, or Windows operating system. There are two interfaces available for this product: a graphical interface, Scan95 (for Windows 95) and WScan (for Windows 3.x and Windows NT); and a command-line interface, Scan (for DOS and OS/2). For more information about Scan, Scan95, and WScan, refer to [“Setting Up VirusScan” on page 36](#).
- VShield continuously monitors and protects your system from viruses that might be introduced while you are working on your computer. VShield can scan your system when you turn on or reset your computer, and can scan programs when you launch them. It can also scan for viruses when you copy files or access a disk. For more information about VShield, refer to [“Setting Up On-Access Scanning \(VShield\)” on page 60](#).
- Validate helps you maintain VirusScan's ability to detect and remove viruses. Whenever you download or obtain VirusScan updates, you should run Validate on the program files to ensure that they are unaltered and uninfected. Refer to [“Validating VirusScan Program Files” on page 17](#) for more information.

About Installation

Be sure to use the installation and setup procedures outlined in this chapter to install VirusScan. Even if you are a “power user,” or are familiar with other anti-virus products, it is very important to install the product as documented in this manual. Be sure to follow these instructions closely since installing or using the product incorrectly may cause further virus infections in your personal computer or network. Or worse, it could lead to virus infections in the VirusScan program files. By following the procedures in this chapter, you’ll create a virus-free environment in which you can prevent virus infections before they occur.

This virus-free environment is similar to the “sterile field” a surgical team establishes before performing surgery. Once the sterile field is established, the surgical team makes sure that anything brought into the field is also sterilized. Use the procedures in this chapter to create a sterile field for your computer or network, including the procedure on how to establish the sterile field by creating a clean start-up diskette.

Your VirusScan diskette is write-protected to ensure that no virus can alter the programs and information stored on it. We strongly recommend that you do *not* remove the write-protection.

Your main steps

This chapter contains key information about installing VirusScan and creating a virus-free environment. Follow the installation procedures outlined below to ensure that you do not spread existing viruses throughout your computer, your network, or to the VirusScan program files.


During the installation process, VirusScan checks your system for viruses. If VirusScan reports that a virus has been discovered during the installation process, immediately stop the installation process. Then refer to [“What to do if a virus is detected during installation” on page 22](#) for instructions on how to remove the virus. Afterwards, begin the installation process again from step 1 below (restart from a clean environment).

Here are your main steps for implementing VirusScan virus protection on your system:

- | Step | Action |
|------|--|
| 1. | Shut down your computer and restart from a clean environment using a DOS or OS/2 start-up diskette. Follow the procedures outlined in “If You Suspect You Have a Virus” on page 9 for instructions on how to do this. |
| 2. | Follow the instructions under “Validating VirusScan Program Files” on page 17 if you received the product from an online service. |
| 3. | Complete the procedures below to install VirusScan (see “Installing VirusScan” on page 19 for more information): <ul style="list-style-type: none">▪ Scan your system.▪ Modify your setup files, if necessary.▪ Activate on-access scanning (VShield). |
| 4. | Create a start-up diskette as described in “Creating a Clean Start-Up Diskette” on page 23 . |
| 5. | Complete the steps under “Backing Up Your Hard Drive” on page 26 . |
| 6. | Check your diskettes for viruses, as described in “Scanning Your Diskettes” on page 27 . |
| 7. | Follow the procedures under “Updating the VirusScan Database” on page 30 . |

System requirements

The VirusScan programs require an IBM-compatible personal computer and one of the following operating systems: DOS 3.3 or later, Windows 3.x, Windows 95, Windows/NT, or IBM OS/2 2.1 or later.

 *If you have a Novell NetWare/386 V3.x or 4.x file server, you may want to use the NetShield virus prevention software, a NetWare Loadable Module (NLM), in conjunction with VirusScan. For more information about NetShield, refer to [“How to Contact Us”](#) on page 33.*

You will need a high-density 3.5” diskette drive to use the VirusScan installation diskette in this package. Contact McAfee for other media, or download the software from the McAfee bulletin board system (BBS). Refer to [“Updating the VirusScan Database”](#) on page 30.

You will also need a blank 3.5” diskette in order to create a clean start-up diskette.

Validating VirusScan Program Files

This section explains how to validate your VirusScan program files to ensure that you are installing the original version of the program files. If you received the VirusScan product from an online service, it is important to verify that the files are authentic, unaltered, and uninfected. VirusScan includes the program `Validate`, which you can use to be sure you're working with the original product files.

Use the following procedure to validate the VirusScan program files:

1. Exit from any applications and display a DOS system prompt (`C>` or `C:\`).
 - In Windows 3.x, choose **File/Exit** to return to DOS.
 - In Windows 95, choose **MS-DOS Prompt** from the Start Menu.
 - In Windows/NT, open a Windows 32-Bit Application Console window.
 - In OS/2, open the Command Prompts folder and click on the OS/2 Full Screen or OS/2 Window icon.
2. Navigate to the directory to which you have downloaded or copied the VirusScan program files to. For example, if you have the files stored in `C:\MCAFEE\VIRUSCAN`, enter the following command:

```
CD C:\MCAFEE\VIRUSCAN
```

3. Validate the program files. For example, to validate `Scan`:

In DOS or Windows, type:

```
validate scan.exe
```

In OS/2, type:


```
os2val os2scan.exe
```

4. Compare the results with the information provided in the PACKING.LST file or other text file for the program you have validated. If the validation results match what is in the file, it is highly unlikely that the program has been modified.

If the information in the text file does *not* match the results of the Validate program, or if you are at all unsure about the authenticity of any VirusScan file, contact McAfee for assistance. Refer to [“How to Contact Us”](#) on page 33.

Installing VirusScan

This section explains how to check your system and install the VirusScan software in the DOS, Windows, or OS/2 environment.

 *Do not use any other method to install VirusScan or you risk spreading a virus within your system.*


About installation

The VirusScan installation program performs certain tasks automatically: it scans your system, installs VirusScan, modifies your setup files (if needed), and activates on-access scanning (VShield). These tasks are described in detail later in this chapter.

VirusScan also automatically customizes its installation procedure to match your system configuration as follows:



- Installs Scan and VShield in C:\MCAFFEE\VIRUSCAN on your local drive. Modifies your AUTOEXEC.BAT so that VShield launches automatically when you start your computer.

 *During installation, if the Installer finds any previously installed VirusScan files, it will ask whether to update them.*



Windows 95

- Installs Scan95 and VShield95 on your local drive, in C:\Program Files\McAfee. Adds a Windows 95 program group called McAfee VirusScan95. Modifies your AUTOEXEC.BAT so that VShield95 is launched automatically when you launch Windows 95.



Windows 3.x

- Installs WScan for Windows, Scan for DOS, and VShield on your local drive, in C:\MCAFFEE\VIRUSCAN. Modifies your AUTOEXEC.BAT file so that VShield is launched automatically when you start your computer. Modifies your WIN.INI to load VSHLDWIN.EXE. Adds a Windows program group called MCAFFEE that includes icons for starting Scan and VShield.

Windows/
NT

- Installs WScanNT on your local drive, in C:\MCAFFEE\NTSCAN.



- Installs the OS/2 version of Scan and the DOS version of VShield in C:\MCAFFEE\VIRUSCAN on your local drive. Modifies your AUTOEXEC.BAT file so that VShield launches when a DOS or Win-OS/2 session is started.

✍ During installation, if the Installer finds any previously installed VirusScan files, it will ask whether to update them.

- If at any time you wish to leave the installation program, press ESC and you will return to the DOS or OS/2 prompt, or to Windows.

Installation procedure

Before you begin, review the following prerequisites:



- In native DOS, exit all programs to display the system prompt (C> or [C:\]).
- In Windows 3.x, close all applications and use the Windows Run option to start the installation program.

Windows
3.x, 95, NT

- In Windows 95, close all applications and choose Run from the Start menu.
- In Windows/NT, close all applications and choose Run to start the installation program.



- Close all DOS and Win-OS/2 sessions, open the Command Prompts folder and click the OS/2 Full Screen or OS/2 Window icon.

To ensure that the installation process is completed successfully, be sure that no other anti-virus program is currently running before you start the installation program.

Step

Action

1. Insert the VirusScan program diskette in drive A.

2. Enter the following command to start the Installer.

In Windows 3.x, Windows/NT, and Windows 95, type

```
x: \SETUP.EXE
```

In DOS and OS/2, type

```
x: INSTALL
```


where *x* is the floppy drive that contains the VirusScan diskette, or the location where you decompressed the program files after you downloaded the product from an online service.

Response: Your system is scanned to determine if a virus is present. It may take several minutes for the program to check for viruses in memory and then on the system and user portions of your drives. Scan keeps you informed of its progress. Read the information carefully.

3. Do one of the following:
 - If Scan continues with the installation after scanning, continue with Step 4 below.or
 - If Scan finds one or more viruses, a message similar to the following is displayed:

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

Action: Exit the Installer. Do not panic, even if the virus has infected many files. However, do not run any other programs, especially if the virus is found in memory. Go directly to [“What to do if a virus is detected during installation” on page 22](#) for details on how to remove the virus before you continue with the installation.

 *VirusScan may report a “false alarm” if another anti-virus program is currently running. Ensure that all other anti-virus programs have been unloaded from memory before beginning the installation.*

4. Choose a directory for the VirusScan programs. We recommend that you choose the default.

Response: The program files are copied to the directory you specified, and your system start-up files are updated so that on-access scanning (VShield) is run automatically when the computer is started.

Action: You have successfully installed VirusScan. Shut down your computer, wait a few seconds and turn it on again. Then continue with the installation and setup procedures outlined in this chapter. For a list of the tasks you need to perform to protect your system, see [“Your main steps” on page 14](#).

What to do if a virus is detected during installation

VirusScan’s installation procedure begins with a scan of your computer’s memory and all local drives (including hard drives, compressed, CD-ROM and PCMCIA drives, but not diskettes). If a virus is detected, a message similar to the one shown below is displayed:

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

Follow the steps outlined in [“If You Suspect You Have a Virus” on page 9](#) to eliminate the virus and clean or delete any infected files before you continue with the installation process.

After removing the virus, turn your computer off, remove the VirusScan program diskette, and restart your computer. Begin the installation procedure again as described in [“Installing VirusScan” on page 19](#). Install will again scan your system and, assuming your system is now virus-free, will install VirusScan and activate on-access scanning (VShield) to protect your system from further infection.

You should now scan all the diskettes you use to find and eliminate the source of the infection. Once you have finished installing VirusScan on your hard disk, use VirusScan again to examine and disinfect all the diskettes you use, as described in [“Scanning Your Diskettes” on page 27](#).

Creating a Clean Start-Up Diskette

Ensure that your system is completely virus-free before beginning this procedure. Perform this task only after successfully installing VirusScan.

We recommend that you create a clean start-up (boot) diskette that can be used to regain the “sterile field” should an infection occur.

In the OS/2 environment

A circular icon containing the text "OS/2".


In OS/2, it is helpful to create a clean copy of important files. Copy the VirusScan OS/2 program and data files and your AUTOEXEC.BAT, CONFIG.SYS, STARTUP.CMD, and \OS2\DLL\NLS.DLL files onto a clean start-up diskette. Write-protect the diskette, label it, and put it away in a secure place.

In the DOS and Windows environments

- | Step | Action |
|------|--|
| 1. | Exit from any applications and display a DOS system prompt (C> or C:\). <ul style="list-style-type: none">■ In Windows 3.x, choose File/Exit to return to DOS, or you can duplicate these steps from the File Manager.■ In Windows 95, choose MS-DOS Prompt from the Start Menu, or you can duplicate these steps from Windows Explorer.■ In Windows/NT, open a Windows 32-Bit Application Console window.■ In OS/2, open the Command Prompts folder and click on the OS/2 Full Screen or OS/2 Window icon. |
| 2. | Insert a blank or dispensable 1.2 MB diskette in drive A. This procedure will erase the diskette. |

3. Format it as a start-up diskette with the system files by typing:


```
format a: /s /u
```

 *The /U command switch should not be used if you are using a version of DOS before DOS 5.0. The /U option in recent DOS versions ensures that the system portions of the diskette are overwritten. If you use this procedure through a DOS window in Windows 95, the disk will be formatted in DOS version 7.0.*

When prompted for a volume label, enter virusfree01 or another name of up to 11 characters.

4. Copy the VirusScan program files to the diskette, as shown in the following example (for DOS users):


```
copy c:\mcafee\viruscan\scan.exe a:
copy c:\mcafee\viruscan\scan.dat a:
copy c:\mcafee\viruscan\clean.dat a:
copy c:\mcafee\viruscan\names.dat a:
```

 *If you changed the default directory during installation your path will be different. VirusScan95 uses the default directory C:\Program Files\McAfee. Windows/NT uses the default directory C:\MCAFFEE\INTSCAN.*

5. You might also want to copy useful DOS programs to the diskette, as shown in the following example:

```
copy c:\dos\chkdsk.* a:
copy c:\dos\debug.* a:
copy c:\dos\diskcopy.* a:
copy c:\dos\fdisk.* a:
copy c:\dos\format.* a:
copy c:\dos\label.* a:
copy c:\dos\mem.* a:
copy c:\dos\sys.* a:
copy c:\dos\unerase.* a:
copy c:\dos\xcopy.* a:
```

In the same way, copy other programs that you think might be useful.

 *If you use a disk compression utility, be sure to copy the drivers required to access the compressed disks onto the clean start-up diskette.*

6. Remove the diskette from the drive and write-protect it so that it cannot become infected.
 - For a 3.5" diskette, slide its corner tab so that the square hole is open.
 - For a 5.25" diskette, cover its corner notch with a write-protect tab. Be sure to use the write-protect stickers provided with your diskettes, not tape.
7. Label the diskette "Virus-Free Start-Up" and put it away in a secure place in case you need to re-establish a virus-free environment in the future. You may want to note the date and versions of DOS and VirusScan on the label.

Backing Up Your Hard Drive


Ensure that your system is completely virus-free before beginning this procedure. Perform this task only after successfully installing VirusScan.

Some viruses may leave certain disks or files unusable even after being "cleaned." To avoid losing valuable data, back up your system regularly so you can restore your work should a virus destroy or damage important files. You should regularly scan your hard drive(s) and, if no viruses are detected, back up your files to fresh diskettes or backup tapes. You can use a commercial backup program (such as the one included with your operating system), but be sure to scan the backup program disk first to make sure that the backup program itself is not infected. Do not run the backup program if it is infected; instead, reload it from your original installation diskettes.

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 60.*

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 “Scanning” on page 85 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: Scan95 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 Scan95 detects a virus on this diskette, refer to “[Removing a virus in Windows 95](#)” on page 105 to clean the diskette.*

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

Scanning your diskettes in Windows 3.x and Windows/NT

Step	Action
1.	Launch VirusScan by double-clicking the WScan 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 WScan 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.  <i>If WScan detects a virus on this diskette, refer to “Removing a virus in Windows 3.x and Windows/NT” on page 107 to clean the diskette.</i>

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 one 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 Scan detects a virus on this diskette, refer to “Cleaning in DOS and OS/2” on page 110 to clean the diskette.*

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


Updating the VirusScan Database

New viruses (and variants of old ones) are constantly appearing and circulating throughout the personal computer community. McAfee updates the VirusScan programs regularly—usually monthly, but sooner if many new viruses have appeared. Each new version may detect and remove as many as 60 to 100 new viruses, or may add new features to the VirusScan product. To find out what's new, read the WHATSNEW.TXT text file you received with this product.

Download new versions

You can download evaluation copies of new versions of McAfee products from the McAfee bulletin board. For more information, refer to the README text file.

New versions of McAfee software are stored in compressed form to reduce transmission time.

 *Always download and decompress the files in a separate directory from your current files. That way, if you do discover a problem with the new files, you still have the previously installed files.*

Validate the VirusScan program files

When you download a program file from any source other than the McAfee bulletin board or other McAfee service, it is important to verify that it is authentic, unaltered, and uninfected. McAfee anti-virus software includes a program called Validate to ensure that your version of VirusScan is authentic. When you receive a new version of VirusScan, run Validate on all of the program files.

Refer to [“Validating VirusScan Program Files” on page 17](#) for information on using Validate.

Copy the updated VirusScan program files

Once you have validated the new version, copy it into the VirusScan installation directory. In addition, you need to create a new start-up diskette or copy the Scan program files onto your existing clean start-up diskette. To do so, you can follow the procedure below.

Updating VirusScan on your hard drive

Start from the system prompt (C> or [C:\]).

1. Navigate to the directory you copied the downloaded files to, such as C:\MCAFEE\DOWNLD\VIRUSCAN:

```
cd \mcafee\downld\viruscan
```

2. Copy the contents of this directory to the directory you installed the VirusScan products to. For example:

```
copy *.* c:\mcafee\viruscan
```

3. Shut down your computer, wait a few seconds, and turn it on again before performing any scans. VirusScan may report a “failed integrity check” if you attempt a scan immediately after an update.

Updating your start-up diskette

Follow the procedure outlined in [“Creating a Clean Start-Up Diskette” on page 23](#) to create a new start-up diskette. Indicate the date, VirusScan version, and DOS version on the new diskette. Store your older start-up diskette in a safe place to serve as a backup.

If you want to upgrade your existing start-up diskette instead of creating a new one, use the following procedure:

1. Temporarily remove write-protection from your clean start-up diskette and insert it in drive A.
 - For a 3.5” diskette, slide its corner tab so that the square hole is closed.
 - For a 5.25” diskette, remove the write-protect tab from its corner notch.

2. Do one of the following:

- In the DOS or Windows environments, copy the Scan program files to the diskette. For example, in DOS:

```
copy c:\mcafee\viruscan\scan.exe a:  
copy c:\mcafee\viruscan\scan.dat a:  
copy c:\mcafee\viruscan\clean.dat a:  
copy c:\mcafee\viruscan\names.dat a:
```

or

- In OS/2,

```
copy c:\mcafee\viruscan\os2scan.exe a:  
copy c:\mcafee\viruscan\scan.dat a:  
copy c:\mcafee\viruscan\clean.dat a:  
copy c:\mcafee\viruscan\names.dat a:
```

3. Remove the diskette from the drive and write-protect it again.

- For a 3.5" diskette, slide its corner tab so that the square hole is open.
- For a 5.25" diskette, cover its corner notch with a write-protect tab. Be sure to use the write-protect stickers provided with your diskettes, not tape.

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
U.S.A.

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 Support.

Phone	(408) 988-3832
FAX	(408) 970-9727
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
McAfee FAX-on-Demand system	(408) 988-3034
CompuServe	GO MCAFEE
Internet	support@mcafee.com
America On-line	keyword MCAFEE
Microsoft Network (MSN)	GO MCAFEE
World Wide Web	http://www.mcafee.com

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
- Operating system 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.

Other Sources of Information

The McAfee BBS, CompuServe Virus Help Forum, and America On-Line's MCAFEE group are excellent sources of information on viruses and virus protection. Batch files and utilities to help you use VirusScan are often available, along with helpful advice.

Independent publishers, colleges, training centers, and vendors also offer information and training about virus protection and computer security.

We especially recommend the following books for learning about computer viruses:

- Ferbrache, David. *A Pathology of Computer Viruses*. London: Springer-Verlag, 1992. (ISBN 0-387-19610-2)
- Hoffman, Lance J. *Rogue Programs: Viruses, Worms, and Trojan Horses*. Van Nostrand Reinhold, 1990. (ISBN 0-442-00454-0)
- Jacobson, Robert V. *The PC Virus Control Handbook, 2nd Ed.* San Francisco: Miller Freeman Publications, 1990. (ISBN 0-87930-194-0)
- Jacobson, Robert V. *Using McAfee Associates Software for Safe Computing*. New York: International Security Technology, 1992. (ISBN 0-9627374-1-0)

In addition, the following sources can provide useful information about viruses:

- National Computer Security Association (NCSA), 10 South Courthouse Avenue, Carlisle, PA 17013
- CompuServe **VIRUSFORUM** or **GO MCAFEE**
- Internet **comp.virus** newsgroup
- America Online **MCAFEE**

Setting Up VirusScan

This chapter contains general information about setting up and using VirusScan's primary functions, virus detection and virus removal. It also includes information about the memory-resident scanning program, VShield.

Setting Up VirusScan in Windows

Windows 95 users use Scan95, the scanning and cleaning component of VirusScan95. Windows/NT and Windows 3.x users can use WScan, the virus detection and removal program which can be set up and used through the Windows interface. Both Scan95 and WScan provide most of the features of the Scan command line program but with a graphical user interface that runs under Windows.

If you are a DOS or OS/2 user, you should use VirusScan's command line program. For more information, refer to ["Setting Up VirusScan in DOS and OS/2" on page 42](#).

Scan95 for Windows 95

Launching Scan95 for Windows 95

There are four easy methods to start VirusScan95: 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/Scan95**, 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 Scan95 program.
- From your desktop, create a Scan95 shortcut. For information about creating shortcuts with Windows 95, refer to your Windows 95 manual or on-line help.
- To launch Scan95 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.

The Scan95 interface

The main Scan95 window automatically appears whenever you scan for viruses. While navigating through the Scan95 window, you will notice that several of the buttons/items appear on many windows:

- *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 78](#). For more information about the activity log, refer to [“Reporting, Logging, and Notification” on page 121](#). 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 Scan95 to its default settings.
- *Where & What.* This property page is used to define the scope of a scan. For more information about scanning, refer to [“Scanning” on page 85](#).
- *Actions.* This property page is used to define Scan95’s response if a virus is detected. Refer to [“Scanning” on page 85](#) for more information.

- *Reports*. This property page is used to determine Scan95's notification, reporting, and logging options. For more information, refer to "[Reporting, Logging, and Notification](#)" on page 121.

Exiting the program

To exit VirusScan95, choose **File/Close**, double-click on the VirusScan95 icon in the upper left corner of the window, or click on the X button in the upper right corner of the window.

Getting help

VirusScan95 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**.

WScan for Windows 3.x and Windows NT

Launching WScan in Windows 3.x and Windows NT

To start WScan, double-click the WScan icon in the McAfee Program Group, or use File Manager to navigate to the VirusScan directory and double-click on WSCAN.EXE.

As WScan is loaded, a self-check of the program files is performed to verify their integrity.

If WScan fails the self-check, or if it exits Windows, you should immediately shut down your computer and follow the procedures for using Scan from a clean start-up diskette, as outlined in [“Cleaning in DOS and OS/2” on page 110](#).

WScan does not check diskettes or fixed disks at start-up. To scan disks, refer to [“Scanning in Windows” on page 88](#).








The WScan interface

The WScan interface consists of the menu bar, the tool bar, and the Notebook.

- The WScan 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 WScan 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 81 .
	Choose this button to begin scanning your system for viruses. For more information about scanning with WScan, refer to “Scanning in Windows” on page 88 .
	This button enables you to select the drives, directories, and/or files you want to scan or clean. For more information about scanning with WScan, refer to “Scanning” on page 85 .
	Use this button to configure the WScan Notebook, where you can define scanning, reporting, and validation options. For more information about scanning with WScan, refer to “Scanning” on page 85 .
	Click here to display a list of the many viruses WScan can detect and remove.
	Use this button to schedule automatic scans. For more information about scheduling scans, refer to “Scheduling scans” on page 94 .
	Choose this button to save an activity log of scanning dates and results. For more information, refer to “Reporting, Logging, and Notification” on page 121 .

Exiting the program

To exit WScan, choose **File/Exit**. If you have not saved changes to scan settings or options, a dialog box asks whether to save them. To save settings, choose Yes. (For information about using saved scanning settings, refer to [“Using settings files in Windows” on page 78](#).) Otherwise, choose No. You will be returned to Windows.

Getting help

WScan 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/Contents**. 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.
- To get help on using the on-line help system, choose **Help/Help on Help**, or press F1 while in the Help window.

Setting Up VirusScan in DOS and OS/2

VirusScan's Scan program examines your PC and disks for viruses in DOS and OS/2. The first time you run Scan, do so from the original, write-protected diskette so that the programs themselves cannot be infected.




Windows
3.x, 95, NT

If you're running Windows, refer to ["Setting Up VirusScan in Windows" on page 36](#) for the procedures for using VirusScan.

Launching Scan

Always start Scan from the system prompt (C> or [C:\]). If you're running OS/2, be sure to 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 have not changed the path statement in your AUTOEXEC.BAT file (or, for OS/2 users, the PATH and LIBPATH statements in your CONFIG.SYS file), you will need to include its location (usually C:\MCAFFEE\VIRUSCAN) in the command, or change to that directory.*

In DOS, use the following syntax for Scan:

```
scan {drives} [options]
```

In OS/2, use the following syntax:

```
os2scan {drives} [options]
```

Where:

Scan (or os2scan) launches the application.

{drives} indicates one or more drives to be scanned. You must specify at least one drive to be scanned. If you specify a drive with just the drive letter and a colon (e.g., scan c:), all its subdirectories will be scanned. If you specify only a backslash (e.g., scan \), only the root directory of the active drive will be scanned. You can also scan a specific directory (e.g., scan c:\mcafee).

[options] indicates one or more of the Scan options.

Scan command line options

There are many options that can be added to the command line to configure the scope of the scan. Refer to the following list of command line options.

 To display this listing on screen, run Scan with the `/?` option.

Scanning options reference table

This table lists all the Scan options in alphabetical order. Detailed information about each option is available in the next sections: “General scanning options,” “Reporting, logging, and notification options,” “Target drive, file, and scanning options,” and “Validation/recovery options.”

Option	Type	Description
<code>/?</code> or <code>/HELP</code>	General	Display help screen.
<code>/ADL</code>	Target	Scan all local drives (including CD-ROM, compressed, and PCMCIA drives, but not diskettes).
<code>/ADN</code>	Target	Scan all network drives.
<code>/AF {filename}</code>	Validation/recovery	Store validation/recovery codes in {filename}.
<code>/ALL</code>	Target	Scan all files, not just standard executable extensions or MS-Word extensions.
<code>/APPEND</code>	Reporting	Append to, rather than overwrite, the report file.
<code>/AV</code>	Validation/recovery	Add validation/recovery data to program files.
<code>/BOOT</code>	Target	Scan boot sector and master boot record only.
<code>/CF {filename}</code>	Validation/recovery	Check validation/recovery codes stored in {filename} by <code>/AF</code> .

Option	Type	Description
/CLEAN	General	Clean up infections in boot sector, master boot record, and files if possible.
/CONTACTFILE {filename}	Reporting	Display message stored in {filename} if a virus is detected.
/CV	Validation/recovery	Check validation/recovery data stored in files by /AV.
/DEL	General	Overwrite and delete infected files.
/EXCLUDE {filename}	Validation/recovery	Exclude from scan any files listed in {filename}. (Used with /AV.)
/FAST	Target	Speed up VirusScan's scanning; may detect fewer viruses.
/FORCE	General	Use generic remover to clean a master boot record or boot sector virus.
/FREQUENCY {hours} or {daily}	General	Set the time frequency with which to scan your system.
/HELP or /?	General	Display help screen.
/LOAD {filename}	General	Use Scan settings stored in {filename}.
/LOCK	Reporting	Halt system if a virus is found.
/LOG	Reporting	Save the date and time VirusScan was last run in SCAN.LOG.
/MANY	Target	Scan multiple diskettes.
/MEMEXCL {hhhh[-hhhh]}	Target	Exclude memory area from scanning.
/MOVE {directory} or {*.ext}	General	Move infected files to {directory}, or rename infected file's extension with {ext}.
/NOBREAK	Reporting	Disable CTRL+C / CTRL+BREAK during scans.

Option	Type	Description
/NOCOMP	Target	Skip checking compressed executables created with LZEXE or PKLITE file compression programs.
/NODDA	Target	No direct disk access.
/NODOC	Target	Skip checking for macro viruses in files with .DOC or .DOT extensions.
/NOEMS	General	Do not use expanded memory (EMS) for data.
/NOEXPIRE	General	Disable data files expiration date notice.
/NOMEM	Target	Disable memory checking (not applicable to Scan for OS/2).
/PAUSE	General	Enable screen pause.
/PLAD	General	Preserve last access date on Novell drives.
/REPORT {filename}	Reporting	Create report of infected files found during scan in {filename}.
/RF {filename}	Validation/recovery	Remove validation/recovery codes in {filename}.
/RPTALL	Reporting	Add list of files scanned to the report file.
/RPTCOR	Reporting	Add list of possibly corrupted files to the report file.
/RPTERR	Reporting	Add list of system errors to the report file.
/RPTMOD	Reporting	Add list of modified files to the report file.
/RV	Validation/recovery	Remove validation/recovery data from files.
/SHOWLOG	Reporting	Display information in SCAN.LOG.

Option	Type	Description
/SUB	Target	Scan subdirectories inside a directory.
/VIRLIST	General	Display list of viruses detected by Scan.

General scanning options

- `/?` or `/HELP`. Display list of Scan options.

Does not scan; displays the list of Scan command line options with a brief description of each. Use either option alone on the command line.


- `/CLEAN`. Remove viruses from boot sector, master boot record, and/or infected files.

Attempts to restore the boot sector, if infected, and any infected files. If the infected file is on a network drive, you must have rights to modify files on that drive. To use `/CLEAN`, the `CLEAN.DAT` file must reside in the Scan directory.


 For more information, refer to *“On-access scanning in Windows 3.x” on page 95.*

- `/DEL`. Overwrite and delete infected files.


Deletes and overwrites each infected file. Files erased by the `/DEL` option cannot be recovered. This option has no effect on Master Boot Record or boot sector viruses.

 Create a report using the `/REPORT` and `/RPTALL` options so you know which files have been deleted. Restore these deleted files from backups or the original diskettes.

Instead of using /DEL alone, McAfee recommends using it in combination with the /CLEAN option, so Scan will first attempt to disinfect the damaged file, deleting it only in cases where the file is damaged beyond repair.


 *Using /MOVE and /DEL in the same command line returns an error message.*

When scanning a network drive using /DEL, you must have delete access to that drive.

 *For more information, refer to “Cleaning in DOS and OS/2” on page 110.*

- /FORCE. Use generic remover to clean a master boot record or boot sector virus.

If /CLEAN cannot remove a virus from the master boot record or boot sector, consider running /CLEAN again with the /FORCE option. VirusScan will again attempt to remove the virus, using a generic remover which will work against most infections. However, using this option could result in the loss of all data or use of the infected drive(s). Before using this switch, make sure you have a recent back up of the infected drive(s). For more information, refer to “Backing Up Your Hard Drive” on page 26.

 *Using /FORCE without /CLEAN returns an error.*

- /FREQUENCY {hours} or {daily}. Limits scanning to prevent too-frequent scans.

In environments where the risk of viral infection is very low, use this option to prevent unnecessary or too-frequent scans. You can limit the scans to once per day by specifying ‘daily’ as the parameter, allowing only one scan per 24-hour period (between 12:00:01 am to 11:59:59 pm), or specify a number to limit scans for the specified number of hours. The lower the number of hours specified, the greater the scan frequency. For example, refer to the following command line:

```
scan c: /frequency 2
```

In the above example, you are instructing Scan to examine the C:\ for viruses, then prevent all subsequent scans for two hours.

The first time this option is used on a workstation, Scan creates a hidden file named MCAFEE.FRC in the root directory of drive C. In this file, Scan stores the date and time the system was scanned. Thereafter, whenever this option is used, Scan checks this file and compares the time elapsed from the last scan with the specified number in {hours}. If {hours} exceeds the elapsed time, Scan exits without performing a scan. Otherwise, Scan proceeds as usual to examine the system and, when finished, updates MCAFEE.FRC with the system date and time.

- /LOAD {filename}. Use Scan settings stored in {filename}.

By default, Scan loads its internal default settings plus any options specified on the command line. You can store all custom settings in a separate ASCII text file, then use /LOAD to load these settings from that file.

Use any text editor to create the file. Put each option on the same command line or on separate lines, separated by hard carriage return and line feed. Use with 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:


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

The above command line will initiate a scan using its internal default settings plus any options specified in FLOPPY.CFG.

 For more information, refer to [“Setting Up Settings Files and Scanning Profiles” on page 78](#).

- /MOVE {directory} or {*.ext}. Move infected files to specified directory, or rename infected file with new three-letter extension.

Moves all infected files found during a scan to the specified directory, or renames the infected file with the three-letter extension specified in {*.ext}. If you use /MOVE in conjunction with /CLEAN, Scan attempts to restore an infected file first, then moves or renames it only if the file cannot be restored. Using /MOVE and /DEL in the same command line returns an error message. This option has no effect on Master Boot Record or boot sector viruses, since they are not actually files.


 Create a report using the /REPORT, /RPTALL and /RPTCOR options so you know which files have been moved or renamed. Restore these files from backups.

When scanning a network drive using /MOVE, you must have sufficient rights to access to that drive.

If you wish to use the renaming feature of the /MOVE option, you must specify the new extension. You may use the /? wildcard to preserve the original character. For example:

```
scan /move *.v??
```

This command renames any infected files by keeping the original eight-letter prefix and changing the first character of the three-letter extension to a "v". If the file TEST.EXE was found to be infected, for example, it would be renamed to TEST.VXE, a non-executable file extension. In this way you can prevent users from inadvertently running infected files.

 For more information, refer to ["Cleaning in DOS and OS/2" on page 110](#).

- /NOEMS. Do not use expanded memory (EMS).

Prevents Scan from using expanded memory (LIM EMS 3.2), ensuring that EMS is available exclusively to other programs.

- /NOEXPIRE. Do not display data files expiration date and notice.

Scan will disable the "expiration date" message if the VirusScan data files are out of date.

 For information about updating VirusScan data files, refer to ["Updating the VirusScan Database" on page 30](#).

- /PAUSE. Enable screen pause.


By using /PAUSE, Scan will prompt you to press any key when the screen fills up with messages, such as using the /SHOWLOG or /VIRLIST options. Do not use /PAUSE if you are not attending your PC during scans.

- /PLAD. Preserve last access date (*on NetWare drives only*).

Prevents changing the last access date attribute for files stored on a network drive in a Novell network. Normally, NetWare updates the last access date when Scan 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 a result of the scanning.

- /VIRLIST. Display the contents of SCAN.DAT.

Shows you the name and a brief description of the viruses that VirusScan detects. To pause when the screen fills with messages, use the /PAUSE option. Use /VIRLIST alone or with /PAUSE on a command line (do not specify a target for the scan or any other options).

 *VirusScan can detect over 6,000 viruses. This file is over 100 pages in length!*

You can save the list of virus names and descriptions to a file by redirecting the output of the command. For example, in DOS:

```
scan /virlist > filename.txt
```

This command saves the SCAN.DAT information to a file, filename.txt.

Reporting, logging, and notification options


You can use the reporting and logging options to create an audit trail of scanning dates, times, and results. The notification options can be used to alert users or administrators that a virus has been detected. For more information, refer to [“Reporting, Logging, and Notification” on page 121](#).

- /APPEND. Append to report file.

Used with /REPORT to add new information to an existing report file with the same file name. If /APPEND is not specified, VirusScan overwrites the existing report file if the file names are the same.

- /CONTACTFILE {filename}. Display a text message (saved in {filename}) when a virus is detected.

Use /CONTACTFILE to notify users that a virus has been detected. The message can be created in any text editor, but the file should be saved in text-only format. This message will be displayed when a virus is discovered.

 *This file should not exceed 250 KB.*

- /LOCK. Halts the system to stop further infection if Scan 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.*

- /LOG. Save date and time of last scan.

Stores the time and date Scan is being run by updating or creating a file called SCAN.LOG in the current directory.

- /NOBREAK. Disable CTRL+C/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.

- /REPORT {filename}. Create a report of infected files and system errors.

Saves the output of Scan to {filename} in ASCII text file format. If the specified file name already exists, Scan overwrites the file with the new information. (Use /APPEND to add the new information to the existing file.) You can use /RPTALL, /RPTCOR, /RPTERR, and /RPTMOD on the same command line.


For more information, refer to [“Reporting and logging in DOS and OS/2” on page 125](#).

- `/RPTALL`. Add all scanned files to Scan report.

Adds the names of all files scanned to the report file created with `/REPORT`.

- `/RPTCOR`. Add list of possibly corrupted files to Scan report.

Adds the names of files which may have been corrupted (damaged beyond repair) by the virus to the report file created with `/REPORT`.

 *There may be false readings in some files that require an overlay or another executable to run properly (i.e., a file that is not executable on its own).*

- `/RPTERR`. Add all errors to Scan report.

Adds system errors to the report file created with `/REPORT`. System errors include read/write problems, network access errors, etc.

- `/RPTMOD`. Add all modified files to Scan report.

Adds the names of all modified files detected during the scan to the report file created with `/REPORT`. Modified files are determined by using the `/CF` or `/CV` options (refer to [“Validation/recovery options” on page 55](#)).

- `/SHOWLOG`. Update and display the contents of `SCAN.LOG`.

Updates or creates the file `SCAN.LOG` in the current directory with the date and time of the current scan, then displays the date and time of previous scans that have been recorded in the `SCAN.LOG` file using the `/LOG` switch. Use the `/PAUSE` option to pause the screen when it is full.

Target drive, file, and scanning options

- `/ADL`. Scan all local drives.

Scan all local drives for viruses, including compressed, CD-ROM, hard drives, and PCMCIA drives, but not diskette drives. To scan both local and network drives, use /ADL and /ADN together on the same command line.

- /ADN. Scan all network drives.

Scans all network drives for viruses, in addition to any drives specified on the command line. To scan both local and network drives, use /ADL and /ADN together on the same command line.

- /ALL. Check all files, not just VirusScan's pre-defined list of file types.

By default, Scan checks only standard executable files (with .COM, .EXE, .SYS, .BIN, .OVL, and .DLL extensions) and Microsoft Word document files (with .DOC or .DOT extensions), which are the files most likely to be infected by a virus. In addition, Scan checks the files to ensure that those with executable extensions are executable programs and that files with MS-Word extensions are MS-Word documents.

If /ALL is specified, Scan checks all executable and Word document files on the specified drive without regard to the file extensions. This increases Scan's ability to detect viruses in overlay files but substantially increases the scanning time required. Use this option in high-risk environments or if you suspect you have a virus. Scan will not check files which are not executable or MS-Word documents, however.

- /BOOT. Scan boot sector and master boot record only.

Scans the boot sector and master boot record on the specified drive(s), but not files or directories on those drives.

- /FAST. Speed up scanning time.

This option instructs Scan to examine a smaller portion of each file for viruses. This allows Scan to examine more files overall, but still reduces scanning time by approximately 15 percent. Using /FAST may miss some infections that would be found in a more comprehensive scan (such as with /ALL). Do not use this option if you suspect your system is infected.

- /MANY. Scan multiple diskettes.

Use this option to scan multiple diskettes consecutively in a single drive. Scan will prompt you for each diskette. Once you have established a virus-free system environment, use this option to quickly check all the diskettes you use.

The Scan program files should not be on a drive that is going to be removed. For example, an error may result if you use the command line:

```
a: scan a: /many
```

Perform the scan from a drive that is not to be removed (e.g., scan A: drive from C: drive or B: drive).

- /MEMEXCL {hhhh[-hhhh]}. Exclude memory area from scanning.

This command line option has been added to prevent Scan from checking areas in upper memory which might contain memory-mapped hardware. If you specify a range in {hhhh[-hhhh]}, the range specified will be excluded.

- /NOCOMP. Skip checking inside compressed executable files.

Reduces scanning time by excluding executable (or self-decompressing) files that have been created using LZEXE or PKLITE file compression programs. Scan decompresses each file in memory and checks for virus signatures, which takes time but results in a more thorough scan. This option prevents Scan from checking compressed files for viruses, although they will be checked for modifications if they have been validated using validation/recovery codes (refer to [“Validation/recovery options” on page 55](#)).

- /NODDA. No direct drive access.

Prevents VirusScan from accessing the boot record. This feature has been added to allow Scan to run under Windows NT.

- /NODOC. Skip checking for macro viruses in MS-Word documents.


Reduces scanning time by omitting MS-Word documents from scans. Use this option only if you have installed other protection against MS-Word macro viruses, or if you do not use MS-Word.

- /NOMEM. Skip memory checking.

 *This option is not applicable to Scan for OS/2.*

Reduces scanning time by omitting all memory checks for viruses. Use this option only when you are absolutely certain your system is virus-free.

By default, Scan checks system memory for all critical known computer viruses that can inhabit memory. Memory above 1088 KB is not addressed directly by the processor and is not believed to be susceptible to computer viruses.

 *Use /MEMEXCL 0000 to scan the upper memory block (640 KB to 1,024 KB) for viruses.*

- /SUB. Scan subdirectories.


By default, when you specify a directory to scan rather than a drive, Scan will examine only the files it contains, not its subdirectories. Use /SUB to scan all subdirectories inside any directories you have specified. This option is ignored if you are scanning an entire drive.

Validation/recovery options

These options are used to detect and recover from new or unknown viruses. For more information about validation/recovery codes, refer to [“Validation and Recovery” on page 113](#).

- /AF {filename}. Store validation/recovery codes in {filename}.

/AF logs validation and recovery data for scanned files, the boot sector and master boot record on a hard disk or diskette in the file specified. The log file is about 89 bytes per file validated. The {filename} must be specified and can include the target drive and directory (e.g., C:\VS_VALID\VAL-CODES.VSC). If the target path is a network drive, you must have rights to create and delete files on that drive. If {filename} already exists, Scan updates it. /AF adds about 300 percent more time to scanning.


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

To recover from a virus using the /AF information, use the /CF and /CLEAN options together in the same command line.

/AF is similar to the /AV option except it stores its data in a separate file rather than changing the scanned files themselves (see /AV below).

- /AV. Add validation/recovery codes to file.

/AV adds validation and recovery data to each file scanned, increasing the size of each file by 98 bytes. If the target file is on a network drive, you must have update access rights to that drive. /AV adds about 100 percent more time to scanning.

 *Using any of the /AV, /CV, or /RV options together in the same command line returns an error.*

To recover from a virus using the /AV information, use the /CV and /CLEAN options together in the same command line. To exclude self-modifying or self-checking files that might cause false alarms, use /EXCLUDE.

/AV is similar to the /AF option except it stores its data in the file itself rather than a separate data file (see /AF above). Also, the /AV option does not store any information about the master boot record or boot sector of the drive being scanned.

- /CF {filename}. Check validation/recovery codes in {filename}.


Checks validation data stored by the /AF option in the specified file. If a file or system area has changed, Scan reports that a viral infection may have occurred. The /CF option adds about 250 percent more time to scanning.

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

Use /CF and /CLEAN together on the same command line to remove any viruses and repair any virus-infected files using the information saved in the specified {filename}.

- /CV. Check validation/recovery codes in files.

Checks validation data stored by the /AV option. If a file has changed, Scan reports that a viral infection may have occurred. The /CV option adds about 50 percent more time to scanning.

 *Using any of the /AV, /CV, or /RV options together in the same command line returns an error.*

Use /CV and /CLEAN together on the same command line to remove any viruses and repair any virus-infected files using the information saved in the file.

 *The /CV option does not check the system areas for changes.*


- /EXCLUDE {filename}. Scan using exception list file.


Allows you to exclude files from /AF validation and /CF checking. Self-modifying or self-checking files can cause a false alarm during a scan.

To create {filename}, use a text editor or word processor to create an ASCII or DOS Text file containing up to 1,024 characters. Each line in this file should be the path and filename of a file or directory that should not be validated.

- /RF {filename}. Remove validation/recovery codes in {filename}.

/RF deletes validation and recovery data for executable files, the boot sector and master boot record on a hard disk or diskette from the file specified. The {filename} must be specified and can include the target drive and directory (e.g., C:\VS_VALID\VALCODES.VSC), but if the target path is a network drive, you must have rights to create and delete files on that drive.

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

 *You can also delete the validation file through DOS.*

- /RV. Remove validation/recovery codes from files.

/RV deletes validation and recovery data from files validated with the /AV option. If you are attempting to remove validation codes from files on a network drive, you must have rights to create and delete files on that drive.

 Using any of the /AV, /CV, or /RV options together in the same command line returns an error.

Scan error levels

After Scan has finished running, it sets the ERRORLEVEL. You can use the ERRORLEVEL in batch files to take different actions based on the results of the scan. Refer to your DOS operating system documentation for more information. Scan returns 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.

ERRORLEVEL	DESCRIPTION
10	A virus was found in memory.
11	An internal program error occurred.
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 (see "General scanning options" on page 46).
21-99	Reserved.
100+	Operating system error; Scan 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.)

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, VShield95 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.



Never boot from an unchecked diskette.

There is one way to infect your computer that VirusScan cannot prevent—only you can. Never start your computer from an unknown or unscanned diskette. That's how 80 percent of all viruses are passed! On-access scanning (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.



Windows/
NT


On-access scanning (VShield) is not applicable to the Windows/NT operating system.

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 ["Scanning" on page 85](#). Then upload any files which 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 33](#).

Setting up on-access scanning in Windows 95

 For more information about VShield95, refer to “On-access scanning in Windows 95” on page 90.



Windows 95

When you double-click on the VShield95 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 VShield95 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 from the pull-down list box from the following options: 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 "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. Refer to "Backing Up Your Hard Drive" on page 26." on page 100. For information about using on-access scanning in Windows 3.x, refer to "On-access scanning in Windows 3.x" on page 95.*

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 how much memory VShield loads by using the /NOUMB, /NOEMS, and /NOXMS options.*

Launching on-access scanning in DOS, Windows 3.x, or 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:\MCAFFEE\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.*

VShield option table

These options are available in VShield for DOS, Windows 3.x, and OS/2.

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 Scan /AF in {filename}.
/CONTACT {message}	Notification	Display specified message when a virus is found.

Option	Type	Description
/CONTACTFILE {filename}	Notification	Display message stored in {filename} if a virus is detected.
/CV	Validation/recovery	Check validation/recovery data stored in files by Scan /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.
/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.

Option	Type	Description
/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.

General VShield options

- `/?` or `/HELP`. Display list of on-access scanning (VShield) options.

Use this option to display the on-access scanning command line options.


- `/NOREMOVE`. Disable `/REMOVE` switch.

Prevents on-access scanning from being disabled with the `/REMOVE` option in a subsequent VShield command. When you load VShield with the `/NOREMOVE` option, subsequent loads with the `/REMOVE` option will have no effect. Your network will be more secure if users cannot disable on-access scanning, but this option may prevent users from solving memory limitations or conflicts.

- `/RECONNECT`. Re-enable on-access scanning if it has been disabled by another TSR.


Restores VShield's link to DOS after another program has disabled it, such as a network driver, keyboard driver, custom disk driver, drive compression program, or disk caching program. These types of programs replace the normal DOS system interrupts so that VShield no longer recognizes program loads. After the lines in your `AUTOEXEC.BAT` file (or network login script) that load these programs, add this command line to restore on-access scanning:

```
vshield /reconnect
```

 This line is added to your `AUTOEXEC.BAT` file during installation. Edit your `AUTOEXEC.BAT` file to remove this switch if the message "Error - VShield already connected" is displayed at start-up.

- `/REMOVE`. Disables on-access scanning.

Unloads VShield from memory. You may want to do this temporarily if you are running out of memory for programs or are experiencing conflicts with other TSR programs. For best results, try the `/SWAP` option first.

 */REMOVE will not work if other memory-resident programs were loaded after VShield, or if VShield was loaded previously with the /NOREMOVE option.*


- `/SAVE`. Save the command line options to the `VSHIELD.INI` file.

Stores the on-access scanning options you specify as the defaults in `VSHIELD.INI`. (If `VSHIELD.INI` does not exist, VirusScan will create it.) In the following example, `/SAVE` saves the `/CONTACTFILE N:\MSGFILE` as the default setting:

```
vshield /contactfile n:\msgfile /save
```

To remove custom options and return to the original defaults, use the `/SAVE` option alone:

```
vshield /save
```

 *This command does not perform a scan or activate on-access scanning.*

Memory options

Use these options to reduce VShield's memory size.

- `/NOEMS`. Do not use expanded memory (EMS).

Prevents VShield from using expanded memory (LIM EMS 3.2) when it loads. This ensures that EMS is available exclusively to other programs.

- `/NOUMB`. Do not use upper memory block (UMB).

Prevents VShield from loading into the upper memory block (UMB, 640 KB to 1024 KB). This ensures that the UMB is available exclusively to other programs.

- `/NOXMS`. Do not use extended memory (XMS).


Prevents VShield from loading into extended memory (XMS). This ensures that XMS is available exclusively to other programs.

 */XMSDATA will load VShield's data files (only) into extended memory.*

- `/SWAP [pathname]`. Load VShield kernel (8 KB) only; swap the rest to [pathname].

Installs a small (8 KB) kernel of VShield in memory that loads the rest of VShield from disk on demand. Specify a path only if you want VShield to swap to a path other than the directory where VShield resides.

Use `/SWAP` only if you have very little memory available, but require a high assurance of safety. `/SWAP` will slow down your system and may cause conflicts with programs that fail to allocate memory properly. If you do not have enough memory to load VShield without swapping, consider using `VShieldCRC` instead. We do not recommend storing the swap file on a network path because, should the workstation disconnect from the network, the workstation will lock.

 *Using `/SWAP` and `/XMSDATA` on the same line will return an error.*

- `/XMSDATA`. Loads VShield data files into XMS memory.

Loads data files into extended memory. In a network environment, `/XMSDATA` will lower utilization and allow VShield to continue running if the user disconnects from the network. (Also refer to `/NOXMS`.)

 *Using `/XMSDATA` and `/SWAP` on the same line returns an error.*

Notification options

The notification options can be used to alert network users and/or administrators that a virus has been detected.

- `/CONTACT {message}`. Display a text message when a virus is detected.

The message is displayed in addition to all other on-access scanning messages. Use /CONTACT to let network users know what to do if a virus is detected. The message can be up to 50 characters long and can contain any character except a backslash “\”. Messages that start with a hyphen “-” or slash “/” should be placed in quotation marks. For example:

```
vshield /contact "VIRUS DETECTED! Call Jeff at  
x3030!"
```

If your message is longer than 50 characters or you want to store the message text in a file, use /CONTACTFILE instead.

 *Using /CONTACT and /CONTACTFILE in the same command line returns an error message.*


- /CONTACTFILE {filename}. Display a text message (saved in {filename}) when a virus is detected.

Use /CONTACTFILE to notify users that a virus has been detected. The message can be created in any text editor, but the file should be saved in text-only format. This message will be displayed when a virus is discovered.

 *Using /CONTACTFILE and /CONTACT in the same command line returns an error message.*

- /LOCK. Halts the system to stop further infection if a virus is detected.

This option is useful in highly vulnerable network environments, such as open-use computer labs.

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

Target options

Use these options to configure on-access scanning options.

OS/2


The /ANYACCESS and /BOOTACCESS options are not recommended for use with DOS and WIN-OS/2 sessions under OS/2 due to certain low-level operating system incompatibilities between DOS and OS/2. Use the /FILEACCESS switch instead.

- /ANYACCESS. Scan the boot sector whenever a diskette is accessed (read/write); scan executables; scan any newly created files.

Checks the diskette boot sector and all files for viruses whenever a diskette is accessed by a read/write operation, such as a DIR or COPY command, or when a program on a diskette is opened, read, updated, or executed.

/ANYACCESS prevents execution if a program file is infected. It also checks any new files created, such as with a copy command, regardless of the file's extension.

This is the highest level of protection against viruses that infect boot sectors. Using /ANYACCESS with either /BOOTACCESS or /FILEACCESS in the same command line will return an error message.

 Use VSHIELD /ANYACCESS /ONLY A: B: for the highest protection against viruses on diskettes without slowing hard drive or network connections.

- /BOOTACCESS. Scan the boot sector for viruses whenever a diskette is accessed (including read/write operations).

Checks the boot sector of a diskette for viruses whenever a diskette is accessed by a read/write operation, such as a DIR or COPY command. By default, on-access scanning checks programs when they execute, but does not check the boot sector of the diskette for viruses.

Using /BOOTACCESS with either /ANYACCESS or /FILEACCESS on the same command line will return an error message.



Windows
3.x

✍ This option does not work from within Windows File Manager. For virus-checking within Windows, use the /FILEACCESS or /ANYACCESS switch instead.

- /FILEACCESS. Scan executable files when they are accessed on a diskette, but do not check the boot sector.

Checks standard executable files whenever the file is accessed or executed and prevents execution of infected programs. Checks all files when accessed by a read/write operation. Using /FILEACCESS on the same command line as /ANYACCESS or /BOOTACCESS returns an error message. With VShieldCRC, /FILEACCESS checks files only if they have been validated with the /AV or /AF options.

✍ We recommend that you always use the /FILEACCESS switch with OS/2.

- /IGNORE {drive(s)}. Do not check programs loaded from the specified {drive(s)}.

Use this command to speed up on-access scanning by excluding drives which you know to be virus-free from scans. You can specify up to 26 drives with this command. Using /IGNORE and /ONLY in the same command line will return an error message.

- /NOMEM. Skip memory checking.

Skips the memory check for viruses when VShield loads. Using /NOMEM improves performance slightly but use it only if you are absolutely sure that your system is virus-free.


- /NOWARMBOOT. Do not check the diskette boot sector for viruses during warm boot.

Omits checking the diskette boot sector during warm boots (system resets, such as CTRL+ALT+DEL).

- /ONLY {drive(s)}. Check only programs loaded from the specified {drive(s)}.

Checks program loads only from the specified drive(s), ignoring all other drives. Use /ONLY to speed up on-access scanning by excluding secure drives from virus checking. You can specify up to 26 drives with this command.

Using /ONLY and /IGNORE on the same command line returns an error.

 Use VShield /ANYACCESS /ONLY A: B: for the highest protection against viruses on diskettes without slowing hard drive or network connections.

- /POLY. Check for polymorphic viruses.

Check for polymorphic viruses (viruses which attempt to evade detection by changing their internal structure or encryption techniques). VShield does not normally check for polymorphic viruses. Using /POLY on the same command line as /ANYACCESS, /FILEACCESS, or /SWAP returns an error.

 This option requires the VSHEML.EXE file to operate.

Validation/recovery options

These options are used to in conjunction with Scan's validation/recovery options to check for infection from a new or unknown virus. For more information about validation/recovery codes, refer to ["Validation and Recovery" on page 113](#).

- /CERTIFY. Prevent programs from running if they do not have validation/recovery codes.

Use this option in high-security environments to prevent users from running programs that have not been scanned. To use /CERTIFY, first use Scan's /AF or /AV option, as described in ["Validation/recovery options" on page 55](#). Then use VShield again with the /CERTIFY option and either /CF or /CV, as in the following example:

```
vshield /certify /cf c:\mcafee\recvalch.sav
```

Some programs, such as Lotus 1-2-3, contain self-modifying code and do not work correctly with validation codes attached. You may want to create an exception list of files to exclude from validation with the /EXCLUDE option.

- /CF {filename}. Check validation/recovery codes stored by Scan /AF in {filename}.

Checks validation data stored by Scan's /AF option in the specified file. If a file or system area has changed, on-access scanning reports that a viral infection may have occurred.

- /CV. Check validation/recovery codes stored by Scan /AV.

Checks validation data stored by Scan's /AV option. If a file has changed, on-access scanning reports that a viral infection may have occurred.

- /EXCLUDE {filename}. Exclude {filename} from validation code check.

Excludes files listed in file name from validation when using /CV. For more information on excluding files from validation, refer to ["Validation and Recovery" on page 113](#).

VShield error levels

When on-access scanning (VShield) is activated, it sets the DOS ERROR-LEVEL. 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.

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” on page 113.](#)) 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, refer to [“Setting up on-access scanning in DOS, Windows 3.x, or OS/2” on page 64.](#)

Option	Type	Description
/? or /HELP	General	Display a list of valid command line options.
/CERTIFY	Validation/recovery	Prevent files without validation codes from running.
/CF {filename}	Validation/recovery	Check validation/recovery codes stored by Scan /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 Scan /AV.
/EXCLUDE {filename}	Validation/recovery	Do not check files listed in {filename} for validation codes (/CV option).

Option	Type	Description
/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.
/IGNORE {drive(s)}	Target	Do not check programs loaded from the specified drive(s).
/LOCK	Notification	Halt the system when a file that is infected loads and attempts to execute.
/LOGFILE {filename}	General	Write error information to {filename}.
/NOREMOVE	General	Prevent VShieldCRC from being removed from memory with the / REMOVE switch.
/NOUMB	Memory	Do not use upper memory blocks (UMB).
/ONLY {drive(s)}	Target	Check only programs loaded from the specified drive(s).
/REMOVE	General	Unload VShieldCRC from memory.

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 "xxx"` tells CheckVShield to look for a specific version (2.00 or higher) of VShield or VShieldCRC in memory. For example, `/v "2.00"` instructs CheckVShield to look for VShield or VShieldCRC version 2.00 or higher.

 This option does not consider .DAT file versions.

CheckVShield error levels

When CheckVShield runs, it sets the DOS ERRORLEVEL. Use the ERRORLEVEL in batch files to take different actions based on the results of CheckVShield's ERRORLEVEL.

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

Setting Up Settings Files and Scanning Profiles

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 Scan95 (for Windows 95 users) or WScan (for Windows 3.x or Windows/NT) will use them as the default settings.

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

- | Step | Action |
|------|---|
| 1. | Configure Scan95 or WScan to the scanning settings that you will most often use.

<i>✎ Refer to "Scanning in Windows" on page 88 for information about configuring Scan95's or WScan's scanning settings.</i> |
| 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. Scan 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, Scan 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 Scan is stored in.

Response: After you create the configuration file, Scan 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 Scan95's or WScan's scanning profiles feature to create quick-access "buttons" to launch a particular scanning configuration in Windows 3.x and Windows/NT, 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: Scan95 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 and Windows/NT

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 WScan 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 and Windows/NT, 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 [Profilen] 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 WScan 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 WScan, 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 pre-selected 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: WScan 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 Scan 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 79](#).

 *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
```

Overview

This chapter explains how to scan your PC, network, and/or diskettes for viruses, and how to clean your system if a virus infection has occurred. This chapter also includes information about configuring VirusScan's infected file action, notification, and reporting options.

If you are using Windows 95, you will use Scan95, the scanning and cleaning component of VirusScan95, to perform these tasks. If you are using Windows/NT or Windows 3.x, you can perform these tasks through VirusScan's Windows interface program, WScan. If you are a DOS or OS/2 user you should use VirusScan's command line program, Scan. This chapter contains information about using VirusScan in all of these environments.

When Should I Scan for Viruses?

By scanning your PC and local drives, activating VShield, and scanning the diskettes you normally use for viruses (refer to “[Getting Started](#)” on page 8), you have created a virus-free environment. Much like the “sterile field” analogy discussed before, this virus-free environment can only be maintained if you are sure that any new programs, diskettes, or files introduced into your system are virus-free as well.

Viruses are generally introduced by booting from an infected diskette or by installing, copying, or running infected programs obtained from a diskette or downloaded via modem. We recommend that you rescan your system whenever you introduce new programs or use an unchecked diskette, whether the diskette was received from friends, co-workers, salespeople, or even one of your own diskettes if it has been used on another PC.

In addition, you should scan your system on a regular basis to ensure that your system is operating in a virus-free environment.

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 a network server, bulletin board, or on-line service, run VirusScan on the directory in which the files were placed before you execute the files.


Scan when you obtain a VirusScan update

VirusScan has the ability to detect unknown viruses, even new viruses that have never been encountered before. You can obtain even more protection against the next generation of viruses by downloading VirusScan updates from the McAfee BBS (408-988-4004). Our team of virus researchers are constantly developing new techniques to recognize and remove new viruses and variants of old viruses. Updates to your VirusScan data files are available through McAfee on a monthly basis, or more frequently if many new viruses have been detected. Whenever you obtain a VirusScan update, rescan your system and your diskettes immediately in case you have been infected by a previously unknown virus.

 For more information about downloading VirusScan updates from McAfee, refer to [“Updating the VirusScan Database” on page 30](#).

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.

 WScan for Windows 3.x and Windows/NT include scheduled scanning features which allows you to set up automatic scanning. For more information, refer to [“Scheduling scans” on page 94](#). Windows 95 users can schedule regular scans using the Microsoft PlusPack scheduling agent. For more information, refer to your Windows 95 PlusPack manual.



Windows
3.x, NT, 95

Scanning in Windows

VirusScan's WScan is used by Windows 3.x, Windows 95, and Windows/NT users. If you're using DOS or OS/2, refer to the next section, "[On-access scanning in Windows 3.x.](#)"

On-demand scanning in Windows 95



Windows 95

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. | <p>Enter the path of the drive, folder, or individual file you want Scan95 to scan, or choose Browse to navigate to the location. Your selection will appear in the 'Scan in' text box.</p> <ul style="list-style-type: none">■ 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 Scan95 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. <p><i>✎ Click on the Program Files button to edit the type of executable and MS-Word document files that Scan95 will examine. The default settings are: .386, .BIN, .COM, .DLL, .DO?, .DRV, .EXE, .FON, .OVL, .SYS, and .VXD.</i></p> <ul style="list-style-type: none">■ Select 'Compressed files' if you want files compressed with PKLITE or LZEXE to be scanned. |
| 3. | Click the Scan Now icon button. |

Response: Scan95 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 Scan95 main window.

- **Files infected:** Indicates how many infected files Scan95 has found.
- **Files scanned:** Indicates how many files Scan95 has scanned for viruses. If you are using the default scanning settings, Scan95 will only check executable files. To change the scanning settings, return to Step 2.
- **Files analyzed:** Indicates how many executable or MS-Word files Scan95 has found on your system.

4. Do one of the following:

- If Scan95 reports that no files are infected, congratulations—most likely your system is currently virus-free. Go to Step 5.

 *VirusScan95'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 30.*

or

- If Scan95 does detect a virus, do not panic, even if the virus has infected many files.
 - If Scan95 finds a virus in a file, refer to "Removing a virus in Windows 95" on page 105 for instructions on how to proceed.
 - If Scan95 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 in DOS and OS/2" on page 110.

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. Refer to [“Backing Up Your Hard Drive” on page 26](#).

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 (VShield95) finds an infection, it prevents programs from running. It also prevents warm boots (CTRL+ALT+DEL) from infected disks.



Never start your computer from an unknown diskette.


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! VShield95 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.

Using on-access scanning in Windows 95



Windows 95

VShield95 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 VShield95 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.

VShield95 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 61](#).

On-demand scanning in Windows 3.x and Windows/NT



Windows
3.x, NT

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


Step

Action

1. 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 WScan main window. To scan a single directory or file, drag it from the right window in the File Manager to the WScan window.*

- Choose OK to return to the WScan Main Window.
2. Choose **Scan/Start Scan** or click the Scan icon.

Response: WScan 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 WScan main window.

- **Files infected:** Indicates how many infected files WScan has found.
 - **Files scanned:** Indicates how many files WScan has scanned for viruses. If you are using the default scanning settings, WScan 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 93](#).
 - **Files analyzed:** Indicates how many executable type or MS-Word document files WScan has found on your system.
3. Do one of the following:
- If WScan reports that no files are infected, congratulations — most likely your system is currently virus-free. Go to Step 4.
 -  *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 30](#).*
 - If WScan does detect a virus, do not panic, even if the virus has infected many files.
 - If WScan finds a virus in a file, refer to [“Cleaning in Windows” on page 104](#) for instructions on how to proceed.
 - If WScan 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 in DOS and OS/2” on page 110](#).
4. 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. Refer to [“Backing Up Your Hard Drive” on page 26](#).

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, WScan 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, WScan 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 WScan to check inside executable or self-decompressing files that have been created using LZEXE or PKLITE file compression programs. If selected, WScan 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, WScan 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/NT and Windows 3.x” on page 113](#)).
- **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. Scan will check all subdirectories, all files (not just standard executables), and all compressed executables.

Scheduling scans

You can schedule WScan for Windows 3.x and Windows/NT to automatically scan at a specific date and time. WScan will scan drives, directories, and/or files you have selected, providing that the PC is running and WScan is loaded. 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 WScan, 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 WScan’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 WScan 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 WScan Notebook, from which you can select scanning options for the currently selected scheduled scan.
 - ✍ *Selecting items from within the Scheduler dialog box or the WScan Notebook does not change the items currently selected for scanning in the main application.*

On-access scanning in Windows 3.x



Windows/
NT: On-
access
scanning is
not applica-
ble to the
Windows/
NT environ-
ment.

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 64.

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.


Do not panic. Follow the instructions outlined in [“Cleaning Your System” on page 103](#) to use VirusScan to remove the virus and repair any virus-damaged files.

Running on-access scanning in Windows 3.x

The installation program can add a line to your AUTOEXEC.BAT file that automatically activates on-access scanning whenever you start or restart your computer. It also gives you a VShield icon that you can click to turn messages on or off (on-access scanning remains active if you turn the messages off).

Scanning in DOS and OS/2


VirusScan's Scan and VShield are used by DOS or OS/2 users, or Windows 3.x users who quit Windows to return to DOS. Windows 95 should use Scan95 and VShield95, and Windows/NT and Windows 3.x users who wish to remain in Windows should use WScan and VShield. Refer to the previous section, "Scanning in Windows."

 *Windows/NT and Windows 95 users can use the Scan command line program by booting from a DOS diskette, such as the clean anti-viral start-up diskette created in "Creating a Clean Start-Up Diskette" on page 23.*

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.  <i>The default directory is C:\MCAFEЕ\VIRUSCAN.</i>
2.	Scan your C drive for known viruses by entering the following command. In the DOS or Windows environments, type: <code>scan c: /all</code> In OS/2, type: <code>os2scan c: /all</code>

where:

Scan (or os2scan)	runs the application.
C:	specifies the hard drive (C:\) as the target of the scan.
/ALL	this option instructs Scan 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 Scan program to check for viruses in memory, then on the system and user portions of your drives. Scan keeps you informed of its progress. Read the information on the screen carefully. On the next page is a sample of what Scan 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 Scan has found on your system.
- **Scanned** indicates how many files Scan has scanned for viruses. If you are using the default scanning settings, Scan 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 Scan has found.

4. Do one of the following:
 - If Scan 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 30.
 - If Scan 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 in DOS and OS/2” on page 110.
5. To see the full list of Scan command line options, refer to “Scan command line options” on page 43.

✍ To display this listing 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. Refer to “Backing Up Your Hard Drive” on page 26.

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 64.

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.
```

Do not panic. Follow the instructions outlined in [“Cleaning Your System” on page 103](#) to use VirusScan to remove the virus and repair any virus-damaged files.

Running on-access scanning in DOS



The installation program can add a line to your AUTOEXEC.BAT file that automatically activates on-access scanning whenever you start or restart your computer.


You can change the on-access scanning options from the DOS command line by removing VShield from memory and rerunning it, by editing the VSHIELD command in your AUTOEXEC.BAT file, or by editing the default configuration file. See [“Setting up on-access scanning in DOS, Windows 3.x, or OS/2” on page 64](#) for more information.

Running on-access scanning in OS/2



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 OS/2 sessions, only under DOS and Win-OS/2 sessions inside of OS/2.

The VirusScan installation program, or the installation instructions for downloaded files, puts the VShield command in your AUTOEXEC.BAT file, where it will run automatically when you start a DOS or Win-OS/2 session. You can also run it from the DOS command line, as described in [“Setting up on-access scanning in DOS, Windows 3.x, or OS/2”](#) on page 64.

 *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.*

Using VShieldCRC in DOS and OS/2

VShieldCRC in DOS 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”](#) on page 113.) Then type:

```
vshldcrc [options]
```

where:

vshldcrc runs the application.

[options] any of the options defined in [“Setting up VShieldCRC in DOS, Windows 3.x, or OS/2”](#) on page 75.

Cleaning Your System

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 you created in Chapter 2, “Getting Started,” and clean your system using the command-line program Scan.

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 re-infection of your system.

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 Your System” on page 103. 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 33.

Cleaning in Windows

If you are a Windows 95, Windows/NT, or Windows 3.x user, you can remove viruses 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 Scan. Refer to [“Cleaning in DOS and OS/2” on page 110](#). Do not use Scan95 or WScan if a virus was detected in memory.

You should use Scan95 or WScan to clean infections only if:

- You are *absolutely sure* your operating system is virus-free (Scan95 or WScan reported no viruses found in memory), and
- You are *absolutely sure* that no operating system or VirusScan files are infected and spreading the infection when running.



Do not use Scan95 or WScan to clean a virus in memory.

Do not use Scan95 or WScan to remove a virus in memory.

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 file from the McAfee BBS at (408) 988-4004. For more information about McAfee, refer to [“How to Contact Us” on page 33](#).


If the virus was detected in memory, the master boot record, the boot sector, a VirusScan file, or an operating system file, you will use Scan 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. <ul style="list-style-type: none">▪ 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.▪ in Windows/NT, choose Shut Down from File Manager, or press CTRL+ALT+DEL and choose Shut Down. 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 (refer to “ Creating a Clean Start-Up Diskette ” on page 23). |
| 3. | Follow the procedures outlined in “ Cleaning in DOS and OS/2 ” on page 110 to remove the virus using Scan. |

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, Scan95 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 Scan95 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 61.

To remove a virus in Windows 95 using Scan95, begin by following the procedures outlined in “[On-demand scanning in Windows 95](#)” on page 88.


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 Scan95'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, Scan95 will offer you the following choices:

- Choose Continue if you want Scan95 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" on page 113) so you know which files have been deleted.*



3. Select 'Clean Infected File' so Scan95 will repair any virus-damaged files.
 - Scan95 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 Scan95 main window.
 - If a virus is detected, Scan95 attempts to restore the boot sector and any infected files. Scan95 can repair files damaged by many viruses, but some viruses damage the infected file beyond repair. If Scan95 cannot safely remove the virus, a message is displayed indicating the name of the unrecoverable file.
 -  *If Scan95 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" on page 27](#) to scan and clean your diskettes.


Removing a virus in Windows 3.x and Windows/NT

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

Step	Action
1.	Follow the procedures outlined in "On-demand scanning in Windows 3.x and Windows/NT" on page 91 .
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 WScan'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" on page 113) 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 33.*
 - Select the Clean Infection (File, Boot Sector, MBR) check box on the Action page of the Notebook.
 - Click OK to return to the WScan main window.

4. Choose **Scan/Start Scan** or click the Scan icon.
 - WScan 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 WScan main window.
 - If a virus is detected, WScan attempts to restore the boot sector and any infected files. WScan can safely remove many viruses from infected files, but some viruses will damage the infected file beyond repair. If WScan cannot safely remove the virus, a message is displayed indicating the name of the unrecoverable file.
 -  *If WScan 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 27 to scan and clean your diskettes.

Cleaning in DOS and OS/2

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

Windows users should use Scan if a virus is resident in memory, the master boot record (MBR), or the boot sector. Do not use WScan or Scan95 to remove a virus in memory.


To use Scan to clean up infected files, the CLEAN.DAT file must be present in the subdirectory containing the Scan 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 infected files from the McAfee BBS at (408) 988-4004. For more information about McAfee, refer to [“How to Contact Us” on page 33](#).

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/NT or Windows 95, shut down your computer and reboot from the DOS start-up diskette you created in [“What to do if a virus is detected during installation” on page 22](#).

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:\MCAFFEE\VIRUSCAN.*

If the virus was found in memory, reboot from the clean, write-protected start-up diskette you created in [Chapter 2, “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 Scan 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, Scan informs you that the virus has been removed successfully.

or

- If one or more infected files cannot be repaired, Scan 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 Scan 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 Scan to examine and disinfect all the disks you use, following the procedures outlined in "Scanning Your Diskettes" on page 27.*

4. If the virus-infected file is corrupted beyond repair, you need to delete the file and restore it from backup. Then run Scan 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.

Validation and Recovery

VirusScan's validation and recovery options are powerful tools used to detect and disinfect new or unknown 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 Scan95 for Windows 95.*

Validation and recovery in Windows/NT and 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 WScan 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, WScan 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 WScan 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 off your anti-virus 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/recovery options” on page 55](#).

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, Scan 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 Scan 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 VirusScan was installed to.

<i>The default directory is C:\MCAFEE\VIRUSCAN.</i> |
| 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:\VALCODES.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, Scan 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.

 <i>The default directory is C:\MCAFEE\VIRUSCAN.</i> |
| 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 in DOS and OS/2” on page 110) 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:\MCAFFEE\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 “Validation/recovery options” on page 55.

 /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 VirusScan was installed to.  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: <code>scan /adl /av</code> In OS/2, type <code>os2scan /adl /av</code> 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 Scan reports a virus has been detected, perform another scan using the /CV and /CLEAN options (refer to “[Cleaning in DOS and OS/2](#)” on [page 110](#)) 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.  <i>The default directory is C:\MCAFEE\VIRUSCAN.</i>
2.	Delete the validation and recovery codes by typing: <pre>scan /adl /rv</pre> In OS/2, type: <pre>os2scan /adl /rv</pre>

Reporting, Logging, and Notification

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, Scan95 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.*

 *VirusScan95 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 and Windows NT


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

Step	Action
1.	<p>Display the Reports page of the WScan Notebook by choosing Settings/Reports from the menu bar or by clicking on the Settings icon and choosing the Reports tab:</p> <ul style="list-style-type: none">▪ 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. <i> WScan for Windows NT supports long file names.</i>▪ Append to Report File instructs WScan 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, WScan 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. <i> For more information about validation checking, refer to “Validation and recovery in Windows/NT and Windows 3.x” on page 113.</i>▪ 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 WScan 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 Windows 3.x and Windows/NT” on page 124.](#)

- **Keep Last *n* Events** tells WScan 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 Windows 3.x and Windows/NT

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

Step	Action
1.	Display the Reports page of the WScan 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), WScan maintains an activity log of scanning dates, times, and results.
3.	Do either of the following: <ul style="list-style-type: none">▪ 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.*

 *VirusScan for Windows NT supports long file names.*


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 Scan to save the scanning results to a file, VIRUS.LOG, which is saved to the root directory.

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

- /APPEND instructs Scan to write the new information at the end of the specified report file, if the file already exists. If this option is **not** specified, Scan 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](#)” on page 113.

- /LOG tells Scan 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 Scan” on page 127.](#)

Using the Scan Activity Log in Scan

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

Step	Action						
1.	<p>Scan your C drive for known viruses and create a Scan Activity Log by typing:</p> <pre>scan a: /log</pre> <p>In OS/2, type:</p> <pre>os2scan a: /log</pre> <p>where:</p> <table><tbody><tr><td>Scan (or os2scan)</td><td>runs the application.</td></tr><tr><td>a:</td><td>specifies the target of the scan, in this case the diskette drive (A:\).</td></tr><tr><td>/log</td><td>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, Scan updates the file with the new information.</td></tr></tbody></table>	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, Scan updates the file with the new information.
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, Scan updates the file with the new information.						
2.	<p>To view the activity log, use the /SHOWLOG option instead of /LOG.</p> <pre>scan /adl /showlog /pause</pre> <p>In OS/2, type:</p> <pre>os2scan /adl /showlog /pause</pre>						


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 Scan is /LOCK. This option halts the system to stop further infection if Scan 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.*

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” on page 8](#). 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” on page 8](#).
- 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 27](#)).
 - 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 [“Creating a Clean Start-Up Diskette” on page 23](#).
 - ✍ *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.

✍ Refer to [“Backing Up Your Hard Drive” on page 26](#).

Although outlining a full security program is beyond the scope of this manual, refer to [“Other Sources of Information” on page 35](#).

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 VirusScan regularly
- Store and check validation and recovery information about your files.

Update VirusScan regularly

Most likely, McAfee will see new viruses long before you do. We update the VirusScan programs and data files often: usually monthly, but more often if many new viruses have appeared. Each new version may detect and eradicate as many as 60 to 100 new viruses or more, and may fix bugs that have been reported in earlier versions.

Updating VirusScan regularly is probably all you need to do to protect against new viruses. For more information about updating VirusScan, refer to the README text file.

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 [“Validation and Recovery” on page 113](#).

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 new software or upgrade existing software, you will have to delete the old codes and replace them with up-to-date validation/recovery information.

 *You will have to do this if you install a new operating system as well.*

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 [“Cleaning Your System” on page 103](#).

After following the procedures outlined above, if you still believe that VirusScan is false alarming (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 [“Validation and Recovery” on page 113](#).

- 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.

Using DOS Commands to Remove a Virus

Using DOS commands to delete, move, or repair virus-infected files can result in the loss of all data and the use of infected disks. The common virus Monkey, for example, can destroy the master boot record and all data on the disk if removed improperly with DOS commands. Other viruses will damage or overwrite executable files or overlay files, and any attempts to remove these viruses with DOS commands can damage or destroy the files.

It is very dangerous to attempt to remove any virus, or to clean a virus-infected file, with DOS commands. Follow the procedures outlined in [“Scanning” on page 85](#) to detect and remove viruses from your system.

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 startup 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.

clean start-up diskette

A write-protected diskette known to be uninfected that contains the coded instructions from which the computer can be started. Using a clean start-up diskette is the only sure way to eliminate a boot sector virus.

 Refer to “Creating a Clean Start-Up Diskette” on page 27 for instructions.

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).

A

Activity log
 defined 121

Author note
 defined 6

AUTOEXEC.BAT
 defined 42

B

Back up your hard drive
 how to 26

BBS
 defined 86

Books
 defined 35

C

Cleaning your system
 DOS 110
 OS/2 110
 Windows 3.x 107
 Windows 95 105
 Windows/NT 107

D

Diskette
 Scan your diskettes
 27

Documentation

 intro. 4

DOS

 Cleaning your system
 110

 Command line
 options 43

 Logging 125

 Notification 128

 Reporting 125

 Scanning 97

 Validation/recovery
 options 115

 VShield 64

DOS commands 135

Downloading 86

F

False alarms
 defined 103

H

Hard drive

 Backing up 26

 Updating VirusScan
 on 31

I

If Install detects a virus
 what to do 22

If you suspect you have a
virus
 what to do 9

Installation

 Back up your hard
 drive 26

 Creating a start-up
 diskette 23

 If Install detects a
 virus **22**

 Scan your diskettes
 27

 System require-
 ments 15

 Validate VirusScan
 17

Internet

 defined 86

K

Key notation
 defined 6

-
- L**
 - Logging
 - Scan 125
 - Scan95 121
 - WScan 123

 - M**
 - Manual organization
 - defined 4
 - McAfee
 - BBS 33
 - Internet addresses 33
 - support 33
 - Mouse
 - defined 7

 - N**
 - Networks
 - Supported 15
 - Notation and symbols
 - defined 5
 - Notes
 - DOS, defined 6
 - OS/2, defined 6
 - text, defined 6
 - Windows, defined 6
 - Notification
 - Scan 128
 - Scan95 122

 - O**
 - On-access scanning
 - see* VShield

 - OS/2
 - Cleaning your system 110
 - Command line options 43
 - Logging 125
 - Notification 128
 - Reporting 125
 - Scanning 97
 - Validation/recovery options 115
 - Other sources of information
 - defined 35

 - R**
 - Reporting
 - Scan 125
 - Scan95 121
 - WScan 123
 - Reporting, logging, and notification
 - defined 121

 - S**
 - Scan
 - Cleaning in DOS 110
 - Cleaning in OS/2 110
 - Cleaning your system 110
 - Command line options 43
 - Logging 125
 - Notification 128
 - Reporting 125
 - Scanning in 97
 - Validation/recovery options 115
 - Scan activity log
 - how to 121, 124
 - Scan your diskettes
 - how to 27
 - Scan95
 - Cleaning your system 105
 - Logging 121
 - Notification 122
 - Reporting 121
 - Scanning 88
 - Scanning
 - Diskettes 27
 - DOS 97
 - On-access *see* VShield
 - VShield
 - OS/2 **97**
 - Scheduling scans 87, 94
 - When to scan 86
 - Windows 3.x 91
 - Windows 95 **88**
 - Windows/NT 91
 - Scanning in Windows
 - how to 88
 - Scanning profiles
 - defined 78
 - Scheduling scans
 - how to 87, 94
 - Settings files
 - how to 78, 79**
 - Start-up diskette
 - Updating VirusScan on 31
 - Sterile field
 - defined 14, 23, 86, 129
 - System requirements
 - defined 15
-

T

Technical Support
contacting 33

Terminology and tips
defined 7

Training
scheduling 34

U

Update VirusScan regu-
larly
how to 30, 87, 131

V

Validate
how to 13, 17

Validation/recovery
options
DOS 115
OS/2 115

Virus

Cleaning 103
Creating a secure
system environment
129
Defined 141
Detected in memory
103
DOS commands 135
False alarms 103
Files corrupted by
107
If Install detects a
virus 22
If you suspect you
have a virus 9
New and unknown
30, 131

Other sources of
information 35

Removing 103

Scanning 85

VirusScan

Cleaning in DOS 110

Cleaning in OS/2 110

Cleaning in Windows
104, 105, 107

DOS 42

Installation 14

Introducing 8

OS/2 42

Reference 129

Scan command line
options 43

Scanning in DOS 97

Scanning in OS/2 97

Scanning in Windows
88

Scanning in Windows
3.x 91

Scanning in Win-
dows/NT 91

Scheduling scans 87

Updating 30, 87, 131

Validate 13, 17

Validation/recovery
options 113

VShield 13, 60, 64

VShield95 61, 90

Windows 36

Windows 3.x 39

Windows 95 36

Windows/NT 39

VShield

AUTOEXEC.BAT 65

False alarms 60

VShield95 61, 90

Windows/NT 60

W

WHATSNEW.TXT
defined 30

Windows

Cleaning in 104

Scanning in 88

Scanning profiles 81

Settings files 78

Windows 3.x 39, 64,
91, 107

Windows 95 36, 61,
88, 90, 105

Windows/NT 39, 91,
107

Windows 3.x

Cleaning your system
107

Reporting and log-
ging 123

Validation and recov-
ery 113

Windows 95

Cleaning your system
105

Notification 122

Reporting and log-
ging 121

Windows/NT

Cleaning your system

107

Reporting and log-

ging 123

Validation and recov-

ery 113

VShield 60

Write-protection

defined 14

WScan

Cleaning your system

107

Logging 123

Reporting 123