Using VirusScan

McAfee

Document Release VS225

Table of Contents

Chapter 1 Introducing VirusScan

Thank you for purchasing VirusScan™, McAfee's powerful and advanced desktop anti-virus solution. VirusScan is designed to detect, remove and prevent computer viruses on IBM-PC or 100% compatible personal computers (PCs) that use DOS, Windows or OS/2. VirusScan will help you protect one of your most important assets – the information on your personal computer or local area network.

What is VirusScan?

VirusScan is actually two programs, **Scan** and **VShield**. Scan is used to detect and remove viruses, and to clean virus-infected files. VShield is a memory-resident program that continuously monitors and protects your system from viruses that might be introduced.

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 "Other Sources of Information" later in this chapter, and to Chapter 7, "Tips and Troubleshooting."

Overview

Installing and running VirusScan is not like using other software. Even if you are a "power user," *follow the tasks as outlined below*. Using another method to install and set up VirusScan may result in spreading viruses or even infecting the VirusScan files themselves. Refer to Chapter 2, "Installation and Setup" for more information.

- **Task 1: Validate VirusScan.** Before getting started, ensure that you have an authentic, unaltered and uninfected copy of VirusScan by using the Validate program. If you obtained a copy of VirusScan from any source other than the McAfee bulletin board or another McAfee service, run Validate on all the program files and compare the results with the information in the PACKING.LST file for the program you validated. If the validation results

match what is in the file, it is highly unlikely that the program has been modified.

NOTE: If the information in the PACKING.LST 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. For more information, refer to "McAfee Support" later in this chapter.

For details on validating the VirusScan program files, refer to "Validate VirusScan" in Chapter 2, "Installation and Setup."

- **Task 2: Install VirusScan.** VirusScan's installation procedure begins with a system scan to ensure that your system is not already infected with a virus.

NOTE: VirusScan may detect a virus at this point. **Do not panic.** Immediately refer to "If Install Detects a Virus" in Chapter 2, "Installation and Setup."

If no viruses are found in memory, VirusScan will be installed on your system, modifying your setup files if necessary. VShield will be activated to protect your system at start-up. The VirusScan installation procedure is customized to your operating system (DOS, Windows or OS/2). For more information, refer to Chapter 2, "Installation and Setup."

WARNING: Do not use any other method to install VirusScan, or you risk spreading a virus, or even infecting VirusScan itself.

- **Task 3: Create a clean start-up diskette.** McAfee recommends that you create a clean start-up diskette containing the Scan program for use in emergencies. Refer to "Creating a Clean Start-Up Diskette" in Chapter 2, "Installation and Setup."
- **Task 4: Back up your hard disk.** Some viruses may destroy disks or files they infect. To avoid losing valuable data, copy all the files on all of your hard disks onto fresh diskettes or a backup tape after successfully scanning your system. Use a commercial backup program or the one included with your operating system. Be sure to scan the backup program disk first to verify that the backup program itself is not infected. You should regularly back up important files after every successful scan. Refer to "Back Up Your Hard Disk" in Chapter 2, "Installation and Setup."
- **Task 5: Rescan new disks and software.** Although VShield will monitor your software for viruses, McAfee recommends that you scan your disks when introducing new programs, or using disks that may be infected. *Always* run VirusScan on a new diskette before executing, installing or copying its files. When installing or downloading software from a network server, bulletin board or on-line service, run VirusScan on the directory in which the files were placed before executing the files. For more information, refer to "Rescan New Disks and Software" in Chapter 2, "Installation and Setup."

- **Task 6: Updating VirusScan regularly.** New viruses and strains of existing viruses are being detected every day. McAfee's virus research team releases a new virus signature file update at least once every month. When you receive or download an update, verify that it is an unaltered and uninfected program file by running Validate. After ensuring that it is an authentic update, copy the VirusScan program files to your hard drive and your start-up diskette. Refer to "Updating VirusScan Regularly" in Chapter 2, "Installation and Setup."

How This Manual is Organized

This manual will help you get VirusScan running quickly and properly on DOS, Windows and OS/2 systems.

WARNING: Do not install VirusScan without following the tasks outlined above in "Overview" and in Chapter 2, "Installation and Setup," even if you consider yourself a "power user" or are familiar with other anti-virus products. Installing and VirusScan Reference is not like installing and using other software.

- Chapter 1, "Introducing VirusScan" (this chapter) introduces the VirusScan programs and provides information about McAfee.
- Chapter 2, "Installation and Setup," contains key information about installing and VirusScan Reference. Do not install VirusScan without following the procedures described in this chapter. Using another method to install VirusScan could spread a virus or even infect the VirusScan files themselves.
- Chapter 3, "VirusScan Reference," provides general information about VirusScan's three programs, WScan, Scan and VShield.
- Chapter 4, "WScan Technical Reference," is a detailed reference to the graphic interface version of Scan, including information such as system requirements, creating and saving scanning profiles and using cyclic redundancy check validation.
- Chapter 5, "Scan Technical Reference," is a detailed reference to the command line version of Scan, including a full list of command line options, saving and using a default configuration file and a description of error messages.
- Chapter 6, "VShield Technical Reference," is a detailed reference about VShield, a memory-resident program that continuously monitors and protects your system from viruses. This chapter includes information such as VShield's impact on system performance, notes for network administrators and using the companion program CheckVShield.
- Chapter 7, "Tips & Troubleshooting," explains how to get the most out of VirusScan and how to cope with some common problems.

- Appendix A, “Downloading McAfee Software,” provides information about using communications software to retrieve McAfee software, including VirusScan updates.
- Appendix B, “New VirusScan Features,” describes differences in command line options between this and previous versions of VirusScan.
- Appendix C, “Glossary,” lists frequently-used computer and virus terms.

About VirusScan

VirusScan is an advanced desktop anti-virus solution designed to protect your DOS, OS/2 or Windows system from viral infection. Employing McAfee’s patented Code Trace™ and Code Matrix™ virus scanning technologies, VirusScan consistently and accurately identifies both known viruses and new viruses, including file, multi-partite, stealth, mutating, polymorphic and encrypted types. VirusScan uses the following methods to detect these viruses:

- Known viruses are detected by searching the system for known characteristics (sequences of code) unique to each computer virus and reporting their presence if found. For viruses that encrypt or cipher their codes so that every infection is different, VirusScan uses detection algorithms that work by statistical analysis, heuristics and code disassembly.
- Strains of known viruses are detected by searching for “generic” or “family” virus strings that have been found repeatedly in different viruses. Since virus writers may use older code or programming techniques when writing new viruses, VirusScan can use these strings to detect viruses that have not yet been written.

What VirusScan Includes

The VirusScan product includes the following programs:

- **Scan**, which detects and removes viruses from your IBM-PC or 100% compatible personal computer that uses DOS, OS/2 or Windows system. There are two interfaces available for this product: a graphic interface, **WScan**; and a command-line interface, **Scan**. Refer to Chapter 3, “VirusScan Reference,” for general information about both programs. For more detailed information, refer to Chapter 4, “WScan Technical Reference,” and Chapter 5, “Scan Technical Reference.”

- **VShield** is a memory-resident program that continuously monitors and protects your system from viruses that might be introduced while you are working on your computer. VShield scans your system when you turn on or reset your computer, and scans programs when you launch them. It can also scan for viruses when you copy files or access a disk. Refer to “Using VShield” in Chapter 3, “VirusScan Reference,” for general information about using this product. For more detailed information about VShield, refer to Chapter 6, “VShield Technical Reference.”
- **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 “Validate VirusScan” in Chapter 2, “Installation and Setup,” for more information.

VirusScan also includes the following text files:

- **AGENTS.TXT**, a list of McAfee-authorized agents.
- **COMPUSER.TXT**, instructions on how to use the McAfee Virus Help Forum on CompuServe and how to get a free introductory membership.
- **PACKING.LST**, a description of all the files included in the VirusScan package.
- **README.1ST**, including version-specific validation information for all the program files included, as well as any new information.

License and Registration

The VirusScan software is provided under license from McAfee, Inc., a copy of which is provided with this manual. Please read it and comply with it. In addition, fill out and return the registration form in your VirusScan package.

McAfee Support

For help in using this product, or for more information about McAfee's VirusScan and other products, we invite you to contact McAfee Associates technical support. You can contact us:

McAfee, Inc.

2710 Walsh Avenue

Santa Clara, CA 95051-0963

U.S.A.

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
CompuServe	GO MCAFEE
Internet	support@mcafee.com
America Online	MCAFEE

Before You Call

NOTE: Before contacting McAfee, please ensure that you are running an authentic and unaltered version of the VirusScan program. VirusScan includes a program called Validate that will help you do this. Refer to "Validate VirusScan" in Chapter 2, "Installation and Setup."

For fast and accurate help, have the following information available when you contact McAfee:

- Product name and version number
- Type and brand of computer, hard disk and any peripherals

- DOS, Windows or OS/2 version
- Any TSRs or device drivers in use
- Printouts of your AUTOEXEC.BAT and CONFIG.SYS files
- A printout of the contents in memory, from the MEM command (provided in DOS 4.0 and later) or a similar utility
- A printout of the error and a step-by-step description of what led to this problem. Be as specific as possible. If you cannot be at your computer when you call, a printout of the screen will be helpful.

If you are overseas, you can contact a McAfee authorized agent. Agents are located in 50+ countries around the world and provide local sales and support for our software.

Internet Access

The latest evaluation versions of McAfee's anti-virus software are available by anonymous ftp (file transfer protocol) over the Internet from the **ftp.mcafee.com** site. If your domain resolver does not support names, use the IP address 192.187.128.3. Enter **anonymous** or **ftp** as your user ID and your own e-mail address as the password. Programs are located in the **pub/antivirus** directory. If you have questions, send e-mail to **support@mcafee.com.**

You can also find McAfee's anti-virus software at the SimTel Software Repository at **Oak.Oakland.EDU** in the **simtel/msdos/virus** directory and its associated mirror sites:

wuarchive.wustl.edu (US)

ftp.switch.ch (Switzerland)

ftp.funet.fi (Finland)

src.doc.ic.ac (UK)

archie.au (Australia)

NOTE: For more information, refer to Appendix A, "Downloading McAfee Software."

McAfee Products and Services

Founded in 1989, McAfee, Inc. is the leading provider of tools for productive computing for the DOS, OS/2 and Windows environments. Our anti-virus products are used by more than 16,000 corporations worldwide. Our utility products provide data security, automated version updating and system inspection and editing. McAfee is also the pioneer and leading provider of electronically distributed

software. All of McAfee's products can be purchased through dealers or downloaded from bulletin board systems and on-line services around the world.

McAfee does not stop at developing the world's best anti-virus and utility products. We back them with the industry's best service and technical support. Product support is provided by a full-time staff of virus researchers, programmers and support professionals, and delivered directly by McAfee or our network of more than 150 Authorized Agent offices in more than 50 countries worldwide.

Other Sources of Information

The McAfee BBS, CompuServe Virus Help Forum and America On-Line's MCAFEE group are excellent sources of information on virus protection. Batch files and utilities to help you use VirusScan software 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:

- 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**
- Internet **comp.virus** newsgroup
- America Online **MCAFEE**

Chapter 2 Installation and Setup

Even if you are a personal computer "power user" or are familiar with other anti-virus products, use the VirusScan installation procedure and follow the tasks outlined in this chapter. We are serious about this. Installing and running the VirusScan programs is not like using other software.

The procedures must be followed in order to avoid spreading a computer virus infection. Viruses spread when you start your computer (sometimes called booting) from an infected hard disk or diskette, or when you run an infected program. If your computer is infected, installing and running VirusScan on your hard disk may spread the infection, even to the VirusScan programs themselves. The tasks in this chapter will ensure that you have a clean environment to detect, eradicate and prevent viruses.

By following these procedures you will be creating a virus-free environment, much like a surgical team establishing a "sterile field" before performing surgery. Once it is established, they make sure that everything brought into the field has already been sterilized. In this procedure, you will create a clean anti-viral start-up diskette with which you can always re-establish the sterile field.

Your VirusScan diskette is write-protected to ensure that no virus can alter the programs and information stored there.

NOTE: Under no circumstances should you remove the write protection.

Overview

This chapter contains key information about installing VirusScan and creating a virus-free working environment. It is critical that you follow the installation and set up procedures outlined below. Using another method to install VirusScan could spread a virus, or even infect the VirusScan files themselves.

In this chapter, you will:

1. Validate any VirusScan files obtained from a source other than McAfee.
2. Install VirusScan, which encompasses:
    - Scanning your system.

- Modifying your setup files if needed.
- Activating VShield.

3. Make a clean start-up diskette.
4. Back up your hard disk.
5. Rescan when you use new applications or diskettes.
6. Update VirusScan regularly.

System Requirements

The VirusScan programs require an IBM-compatible personal computer and one of the following operating systems: DOS 3.1 or later, Windows 3.1 or later, or IBM OS/2 2.1 or later.

VShield is a terminate-and-stay-resident (TSR) program. VShield attempts to minimize the use of conventional memory by loading into expanded, extended or upper memory. For more information, refer to Chapter 6, “VShield Technical Reference.”

You will need a high-density 3.5” diskette drive to use the VirusScan install diskette in this package. Contact McAfee for other media, or download the software from the McAfee bulletin board system (BBS). Refer to “McAfee Support” later in this chapter. More information about electronically-distributed software is available in Appendix A, “Downloading McAfee Software.”

Validate VirusScan

This task explains how to validate your VirusScan program files to ensure that you are installing software which has not been tampered with.

If you obtained VirusScan or one of its program files 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. VirusScan includes the program, Validate, that will help you do this.

Use the following procedure to run Validate on the VirusScan program files:

1. Navigate to the directory to which you have downloaded or copied the files to. For example, if you have the files stored in C:\MCAFEE\VSCAN, type

   CD \MCAFEE\VSCAN

2. Type the command:

   `validate scan.exe`

   OS/2: Type the command **`os2val os2scan.exe`**

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

   NOTE: 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 "McAfee Support" in Chapter 1, "Introducing VirusScan."

Install VirusScan

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

NOTE: Do not use *any* other method to install VirusScan, or you risk spreading a virus.

About Installation

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

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

- **DOS.** Installs Scan and VShield in C:\MCAFEE\VIRUSCAN on your local drive. Modifies your AUTOEXEC.BAT so that VShield launches automatically when you start your computer.
- **Windows.** Installs Scan for Windows and VShield on your local drive, in C:\MCAFEE\VIRUSCAN. Modifies your AUTOEXEC.BAT file so that VShield launches automatically when you start your computer. Adds a Windows program group called MCAFEE, and places icons for Scan and VShield in it.
- **OS/2.** Installs the OS/2 version of Scan, and the DOS version of VShield, in C:\MCAFEE\VIRUSCAN on your local drive. Modifies your

AUTOEXEC.BAT file so that VShield launches in DOS or Win-OS/2 sessions when started.

During installation, if the Install program finds any previously installed VirusScan files, it will ask whether to update them. If at any time you wish to leave the Install program, press [ESC] and you will return to the DOS or OS/2 prompt.

NOTE: Be sure that no other anti-virus program is currently running before beginning the install, or the installation may fail.

Installation Steps

Follow the procedures as outlined below to install VirusScan on your system. Exit or unload any anti-virus programs before beginning the install process, or the installation may fail.

- **DOS Users.** If you are running an application program, exit from it to display the system prompt (C> or [C:\]).
- **Windows Users.** You can exit Windows to install VirusScan from the DOS system prompt (C> or [C:\]), or you can install VirusScan through Windows by quitting out of all applications and returning to the Program Manager.
- **OS/2 Users.** 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.

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

1. Insert the VirusScan program diskette in drive A.
2. Change to the A: drive by typing:

   ```
   a:
   ```

3. Start the Install program by typing:

   ```
   install
   ```

   Windows: Choose File | Run from Program Manager. In the Command Line field, type:

   ```
   a: install
   ```

   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 carefully.

4. If Scan continues with the installation after scanning, congratulations — most likely your system is currently virus-free. Follow the instructions on screen and, when finished, continue with “Creating a Clean Start-Up Diskette” later in this chapter.

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

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

STOP THE INSTALLATION. 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. *Go directly to* "If Install Detects a Virus" later in this chapter for details on how to remove the virus before you continue with the installation.

NOTE: 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 procedure. For more information, refer to "False Alarms" in Chapter 7, "Tips and Troubleshooting."

5. Assuming Install did not find a virus, you will now be prompted to choose a directory for the VirusScan programs. We recommend that you choose the default, C:\MCAFEE\VIRUSCAN.

   Install will copy the files and make any necessary modifications to your system start-up files so that VShield launches automatically when you start your computer.

6. You have successfully installed VirusScan. Turn off your computer, wait a few seconds and turn it on again. (This is called a "cold boot.")

7. After restarting, you will make a clean start-up diskette containing the Scan program for use in emergencies. Refer to "Creating a Clean Start-Up Diskette" later in this chapter for instructions. **Be sure to write-protect the new diskette.**

Continue with this chapter to see how you can use VirusScan to keep your computer virus-free. We recommend that you also read Chapter 3, "VirusScan Reference," for information about using WScan, Scan and VShield.

Back Up Your Hard Disk

NOTE: Ensure that your system is completely virus free before beginning this procedure. Perform this task immediately after you have completed a successful scan.

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 or 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.

Create a Clean Start-Up Diskette

NOTE: Ensure that your system is completely virus free before starting this procedure. Perform this task immediately after you have completed a successful scan.

DOS or Windows users should create a clean anti-viral start-up (boot) diskette that can be used to regain the “sterile field” should an infection occur. This is not necessary in OS/2, although it will be helpful to make backup copies of your OS/2 installation diskettes.

DOS or Windows

In DOS, start from the system prompt (C>). In Windows, you may open a DOS window, or duplicate these steps with the Windows File Manager.

1. Insert a blank or dispensable diskette in drive A. Make sure the diskette contains no important information, as this procedure will erase it.
2. Format it as a start-up diskette with the system files by typing:

   `format a: /s/v/u`

   Press [ENTER].

   NOTE: 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.

   When prompted for a volume label, enter **`virusfree01`**or another name of up to 11 characters.
3. Copy the Scan program files to the diskette, as shown in the following example:

   ```
   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:
   ```

   NOTE: If you changed the default directory during installation your path will be different.

4. 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 DOS programs that you think might be useful.

   NOTE: 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.

5. 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.
6. Label the diskette “Virus-Free Start-Up” and put it away in a secure place in case you need to reestablish a virus-free environment in the future. You may want to note the date and versions of DOS and VirusScan on the label.

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 CONFIG.SYS, STARTUP.CMD and AUTOEXEC.BAT files onto a clean start-up diskette. Write-protect the diskette, label it and put it away in a secure place.

Rescan New Disks and Software

Although VShield will monitor your software for viruses, it is recommended that you scan your disks when introducing new programs, or using disks that may be infected. New programs and files are generally introduced in two ways: by inserting a diskette and booting from it, and by installing new programs. It is also possible to download a virus via a modem.

You can use VShield with the /ANYACCESS option to scan diskettes automatically. For more information, refer to “/ANYACCESS” in Chapter 6, “VShield Technical Reference.” For instructions on running VirusScan, refer to Chapter 3, “VirusScan Reference.”

When You Insert an Unchecked Diskette

Every time you insert a new diskette in your drive, run Scan on it before executing, installing or copying its files. If you have several diskettes to scan, you can scan them consecutively using the /MANY option described in “Using Scan” in Chapter 3, “VirusScan Reference.” In fact, McAfee recommends that you do this now with all the diskettes you normally use, as well as diskettes received from friends, co-workers, salespeople and even your own diskettes if they have been in another workstation.

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 Scan on the directory in which the files were placed before you execute the files. For instructions on downloading and installing files, refer to Appendix A, “Downloading McAfee Software.”

Update VirusScan Regularly

Unfortunately, new viruses (and variants of old ones) appear and circulate often in the personal computer community. Fortunately, McAfee updates the VirusScan programs regularly — usually monthly, but sooner if many new viruses have appeared. Each new version can detect and remove as many as 60 to 100 new viruses or more, and can add new features. To find out what is new, review the README.1ST text file.

Download New Versions

You can download evaluation copies of new versions of McAfee products from the McAfee bulletin board. For more information, refer to “McAfee Support” in Chapter 1, “Introducing VirusScan.”

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

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

Validate VirusScan

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 that helps you do this. When you receive a new version of VirusScan, run Validate on all of the program files.

For example, to run Validate on Scan, start from the system prompt (C> or [C:\]):

1. Navigate to the directory to which you have downloaded the files. For example, if you have stored the files in C:\MCAFEE\DOWNLD\VIRUSCAN:

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

2. Type the command:

   ```
   validate scan.exe
   ```

   OS/2: Type the command **`os2val os2scan.exe`**

3. Compare the results with the information in the PACKING.LST, README.1ST or other text file for the program you validated. If the validation results match what is in the file, it is highly unlikely that the program has been modified.

Update VirusScan

Once you have validated the new version, copy it into your C:\MCAFEE\VIRUSCAN 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. Below is one way to do this; you may also use the Windows File Manager or the OS/ 2 environment.

Updating VirusScan on Your Hard Drive

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

1. Navigate to the directory to which you have retrieved the files, such as C:\MCAFEE\DOWNLD\VIRUSCAN:

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

2. Copy the contents of the directory to C:\MCAFEE\VIRUSCAN:

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

3. Turn off your computer, wait a few seconds and turn it on again (this is called a "cold boot") 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 "Make a Clean Start-Up Diskette" to create an updated start-up diskette. Indicate the date and VirusScan version on the new diskette. Store your older start-up diskette in a save place to serve as a back-up.

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 tab from its corner notch.
2. From the system prompt (C> or [C:\]), copy the Scan program files to the diskette.

   ```
   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:
   ```

   OS/2: Copy **OS2SCAN.EXE**instead of **SCAN.EXE.**
3. Remove the diskette from the drive and write-protect it again.

If Install Detects a Virus

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 following is displayed:

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

Stop the installation. **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. Follow the steps outlined below to use Scan to eliminate the virus and clean or delete any infected files before continuing with the installation.

NOTE: If you are at all unsure about how to proceed once you have found a virus, contact McAfee for assistance (refer to "McAfee Support" in Chapter 1).

Step 1. Restart From a Clean Environment

You must run Scan from a clean, virus-free environment. With DOS or Windows, restart from a clean diskette. With OS/2, simply close all DOS and Win-OS/2 sessions.

With DOS or Windows, the only way to ensure a clean environment is to turn your computer off to eliminate any viruses in memory, then restart from a virus-free diskette, preferably the original, write-protected DOS installation diskette that came with your computer. If you do not have one, get 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 one, you can create one following the procedure outlined in "Create a Clean Start-Up Diskette" earlier in this chapter, but only *after* you have successfully cleaned your system.)

1. Turn off your computer. (Do not just reset or reboot, which may leave some viruses intact in the computer's memory.)
2. Make sure your clean boot (start-up) diskette is write-protected.
   - 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.
3. Insert your start-up diskette in drive A.
4. 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.

OS/2: With OS/2, you can eliminate any viruses from memory by closing all DOS, Win-OS/ 2 and virtual DOS machine (VDM) sessions.

Step 2. Run Scan with the /CLEAN option

Start from the system prompt (probably A> or [A:\]). If you are running OS/2, open the Command Prompts folder in the OS/2 system folder and click the **OS/2 Full Screen** or **OS/2 Window** icon.

1. Make sure your clean boot (start-up) diskette is write-protected.
   - 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.
2. Insert the VirusScan program diskette in drive A.
3. Eliminate the first known virus by searching all files on all local drive(s) (including hard drives, compressed, CD-ROM and PCMCIA drives, but not diskettes) by typing:

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

   OS/2: Type **`os2scan /adl /clean /all`**

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

Scan keeps you informed of its progress and generally reports virus removed successfully.

1. If Scan reports that the virus was successfully removed, refer to Step 3, “If Viruses Were Removed.”
2. If Scan reports that the virus could not be safely removed, refer to Step 4, “If Viruses Were Not Removed.”

Step 3. If Viruses Were Removed

If Scan successfully removes all the viruses, restart your computer. Begin the installation procedure again as described in “Installing VirusScan” earlier in this chapter. Install will again scan your system and, assuming your system is now virus-free, will install VirusScan and activate VShield to protect your system from further infection.

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 “Rescan New Disks and Software” earlier in this chapter.

Step 4. If Viruses Were Not Removed

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

```
Virus cannot be removed from this file.
```

Make sure to take note of the filename, because you will need to restore it from back-ups. Run Scan again, this time using the /CLEAN and /DEL options to delete the remaining infected files, as described in Chapter 5, “Scan Technical Reference.” If you have any questions, contact McAfee (refer to “McAfee Support” in Chapter 1, “Introducing VirusScan.”).

After the virus-infected files are deleted, begin the installation procedure again as described in “Installing VirusScan” earlier in this chapter. Install will again scan your system and, assuming your system is now virus-free, will install VirusScan and activate VShield to protect your system from further infection.

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 “Rescan New Disks and Software” earlier in this chapter.

Chapter 3 VirusScan Reference

Chapter 2 provided information about installing VirusScan and creating a virus-free working environment. This chapter provides an overview of VirusScan's three programs, WScan, Scan and VShield.

Overview

This chapter contains general information about using VirusScan's virus detection and removal programs, Scan and WScan; and the memory-resident scanning program, VShield. For more detailed information about these programs, refer to Chapter 4, "WScan Technical Reference," Chapter 5, "Scan Technical Reference" and Chapter 6, "VShield Technical Reference."

Using WScan

VirusScan's WScan program provides most of the features of the Scan command line program but with a graphical user interface that runs under Windows 3.1 or later. If you are a DOS or OS/2 user you should use VirusScan's command line program, Scan. For more information, refer to "Using Scan" later in this chapter.

This section contains all the information most users of WScan will need. More detailed information is available in Chapter 4, "WScan Technical Reference."

NOTE: If a virus is resident in memory, the most secure way to clean your system is to turn off your computer, reboot from a clean start-up diskette and remove the virus using Scan as described in "Using Scan" later in this chapter. You should use WScan to clean infections only if:

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

Launching WScan

To start WScan, double-click the WScan icon in the McAfee Program Group. The WScan main window is displayed.

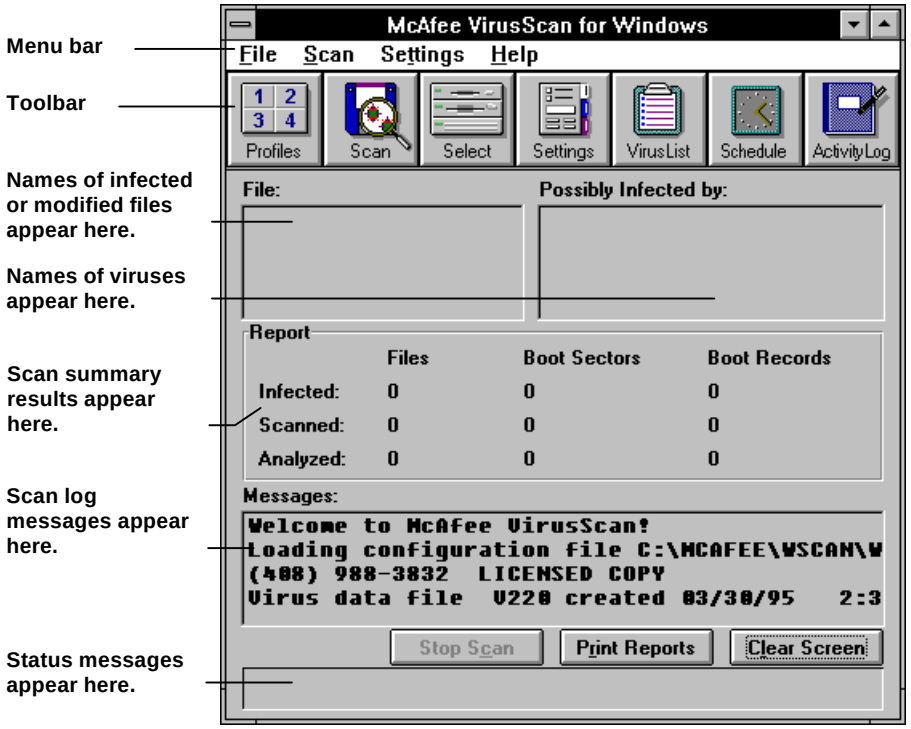


Figure 3-1. WScan main window.

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

NOTE: If WScan fails the self-check, or if it exits Windows, you should immediately *turn off your computer* and run the Scan command line program from a clean start-up diskette, as outlined in "Using Scan" later in this chapter. Do not use WScan to remove a virus in memory.

WScan does not check diskettes or fixed disks at start-up. To scan disks, refer to "Using WScan to Detect a Virus" later in this section. To clean infected disks, refer to "Using WScan to Remove a Virus" later in this section.

WScan Menu Bar

The WScan menu bar contains the following menus, all of which are described in detail in Chapter 4, “WScan Technical Reference.”

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

WScan Tool Bar

You can use the tool bar to quickly start a task without navigating the menu. The tool bar contains the following icons:

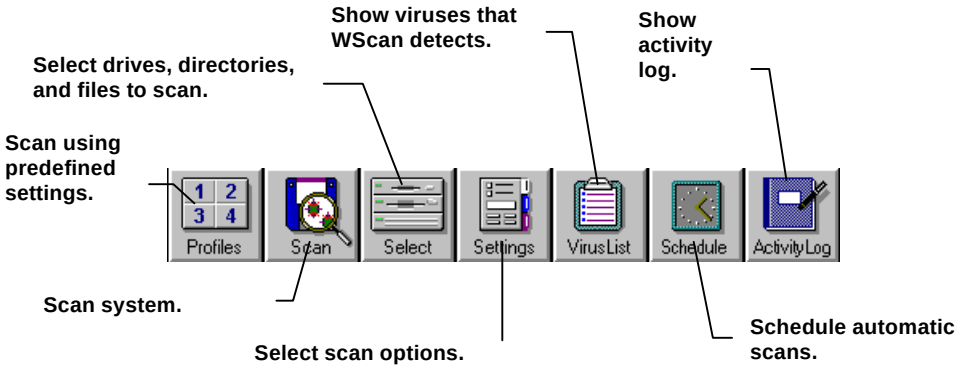


Figure 3-2. WScan tool bar.

Button	Description
	Choose this button to load a scanning configuration file (scanning profile). For more information about using profiles, refer to Chapter 4, “WScan Technical Reference.”
	Choose this button to begin scanning your system for viruses. For more information about scanning with WScan, refer to “Using WScan to Detect a Virus” later in this chapter.
	This button enables you to select the drives, directories and/or files you want to scan or clean. For more information, refer to “Using WScan to Detect a Virus” later in this chapter.

	Use this button to configure the WScan Notebook, where you can define scanning, reporting and validation options. For more information, refer to Chapter 4, “WScan Technical Reference.”
	Click here to display a list of the many viruses WScan can detect and remove. For more information, refer to “Displaying a List of Known Viruses” in Chapter 4, “WScan Technical Reference.”
	Use this button to schedule automatic scans. Refer to “Scheduling Scans” in Chapter 4, “WScan Technical Reference.”
	Choose this button to save an activity log of scanning dates and results. For more information, refer to “Using the Scan Activity Log in Chapter 4, “WScan Technical Reference.”

Exiting the Program

To exit WScan, choose File | Exit. If you have not saved changes to scan settings or options, a dialog box is displayed asking whether to save them. To save settings, choose Yes and follow the instructions in “Using Scan Settings Files” in Chapter 4, “WScan Technical Reference.” Otherwise, choose No.

Using WScan to Detect a Virus

Scan your system when you want to detect and identify viruses.

Use the following procedure to scan your system for viruses:

1. Select the items you want to scan by choosing File | Select Items to Scan or by clicking on the Select icon.

   The Select Items to Scan dialog box is displayed.

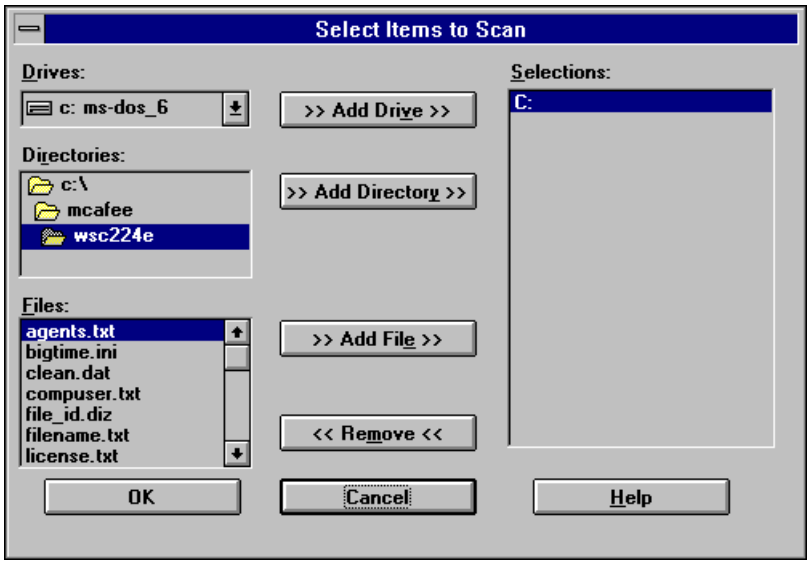


Figure 3-3. Selecting drives, directories and files to scan.

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 will appear in the Selections list.

Choose OK to return to the WScan Main Window.

2. Choose Scan | Start Scan or click the Scan icon.

   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 will only check executable files. To change the scanning settings, refer to Chapter 4, “WScan Technical Reference.”

- **Files analyzed** indicates how many files WScan has found on your system.

If WScan finds a virus in a file, boot sector or master boot record, refer to "Using WScan to Remove a Virus" later in this chapter for instructions on how to proceed.

Using WScan to Remove a Virus

Clean your system when you know or suspect that a virus infection has occurred. If a virus is resident in memory the most secure way to clean your system is to turn off your computer, reboot from a clean start-up diskette and remove the virus using Scan as described in "Using Scan" later in this chapter. You should use WScan to clean infections only if:

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

To use WScan to clean up infected files, the CLEAN.DAT file must be present in the subdirectory containing the WScan 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 contact McAfee (refer to "McAfee Support" in Chapter 1).

Use the following procedure to clean virus-infected files:

1. Select the items you want to scan by choosing File | Select Items to Scan or by clicking on the Select icon.

   The Select Items to Scan dialog box is displayed.

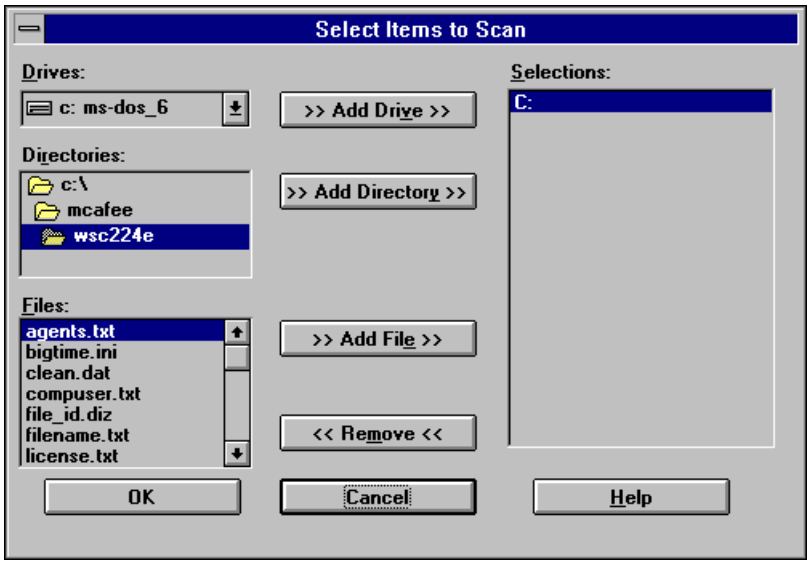


Figure 3-4. Selecting drives, directories and files to scan and clean.

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 will appear in the Selections list.

Note that all items that appear in the Selections list will be scanned. Remove an item you do not want to be included in the scan by selecting it and choosing Remove.

Choose OK to return to the WScan Main Window.

2. Configure WScan's cleaning options by choosing Settings | Actions or clicking on the Settings icon and clicking on the "Action" tab of the Notebook.

   The Actions property page is displayed.

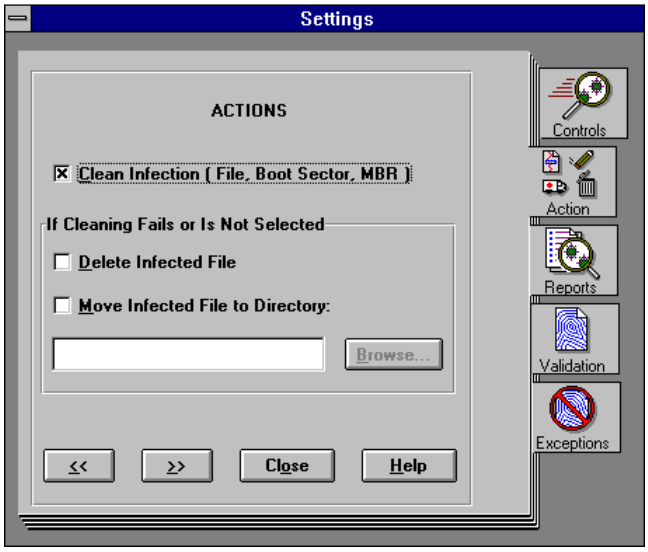


Figure 3-5. The Actions property page.

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

Choose OK to return to the WScan main window.

3. Choose Scan | Start Scan or click the Scan icon.

   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.

   If a virus is detected, WScan will attempt to restore the boot sector and any infected files. Between 10 and 20% of all viruses are not removable; they damage the infected file beyond repair. If WScan cannot safely remove the virus, a message is displayed indicating the name of the unrecoverable file.

NOTE: 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. 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) on the Actions property page of the Notebook. For more information, refer to “Selecting Scan Actions” in Chapter 4, “WScan Technical Reference.”

If you have any questions, contact McAfee (refer to “McAfee Support” in Chapter 1, “Introducing VirusScan.”).

False Alarms

Due to the nature of anti-virus software, there is a possibility that WScan 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 "Using WScan to Remove a Virus" earlier in this chapter. After you have performed these procedures, if you still feel that the virus alert was a "false alarm" please contact McAfee (refer to "McAfee Support" in Chapter 1). You can upload the file to our bulletin board system at (408) 988-4004, along with your name, address, daytime telephone number and electronic mail address (if any).

For more information, refer to "False Alarms" in Chapter 7, "Tips and Troubleshooting."

Using Scan

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

This section contains all the information most users of Scan will need. More detailed information is available in Chapter 5, "Scan Technical Reference."

NOTE: WScan is a graphic interface (Windows 3.1 or later) version of Scan. If you are a Windows user you can use WScan to perform the tasks outlined below. Refer to "Using WScan" earlier in this chapter for more information.

Launching Scan

Always start Scan from the system prompt (C> or [C:\]). If you are running Windows 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.

NOTE: 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:\MCAFEE\VIRUSCAN) in the command, or change to that directory.

Use the following syntax for Scan:

scan {drives} [options]

OS/2: Use **os2scan {drives} [options]**

- **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 back-slash (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. The following section, "Scan Command Line Options," lists some of the more commonly-used Scan command line options. A full listing and a more detailed explanation of each option is presented in "Scan Command Line Option Summary" in Chapter 5, "Scan Technical Reference."

Scan Command Line Options

/? or /HELP

Does not scan. Instead, displays a list of Scan command line options with a brief description of each. No scanning is performed when these options are specified. Use either of these options alone on the command line, for example:

scan /? /pause

This command will return a full listing of Scan's command line options, pausing when the screen is full. This listing is also available in Chapter 5, "Scan Technical Reference."

/ADL

Scans all local drives (including hard drives, compressed, CD-ROM and PCMCIA drives, but not diskettes) for viruses, in addition to those specified on the command line. In DOS, use /ADL to check all local drives. To scan both local and network drives, use /ADL and /ADN together in the same command line; for example:

scan /adl /adn

Scan will check all local drives and network drives for viruses.

/ADN

Scans all network drives for viruses, in addition to those specified on the command line. To scan both local and network drives, use /ADL and /ADN together in the same command line. Refer to /ADL for an example of using this command.

/ALL

Increases system security by performing a more thorough scan. Otherwise, Scan checks only standard executable files (with .COM, .EXE, .SYS, .BIN, .OVL and .DLL extensions), which are the files most likely to be infected by a virus. If /ALL is specified, Scan checks all files on the specified drive, which increases Scan's ability to detect viruses in overlay files but substantially increases the scanning time required.

For example:

```
scan a: /all /clean
```

The above command line will check all files on A: drive and will attempt to restore any infected files.

Use this option if you have found a virus or suspect one. (Note that the list of extensions for standard executables, above, has changed from previous releases of VirusScan.)

/CLEAN

Remove viruses from boot sector, master boot record and infected files.

Attempts to restore the boot sector, if infected and any infected files. Usually, between 10% and 20% of all viruses are not removable; they damage the file they infect beyond repair. If the infected file resides on a network drive, you must have rights to modify files on that drive to clean it. If it cannot restore a file, a message is displayed that identifies the unrecoverable file. To use /CLEAN, the CLEAN.DAT file must reside in the Scan directory. For more information, refer to "Cleaning Viruses" in Chapter 5, "Scan Technical Reference."

Consider the following command line:

```
scan c: /clean
```

Scan will search for viruses on C: drive and, if infected files or boot sectors are detected, will attempt to restore them.

The /CLEAN option can remove master boot record and boot sector viruses. If you use /CLEAN and /DEL in the same command line, Scan first attempts to disinfect an infected file, then deletes it only if it cannot be repaired. Similarly, if you use

/CLEAN and /MOVE in the same command line, Scan first attempts to clean an infected file, then moves it to the specified subdirectory if the file is unrecoverable.

If you are unfamiliar with viruses and virus methodology, you should get experienced help before you use DOS commands to remove a virus. This is especially true for "critical" viruses and master boot record or boot sector infections, because improper removal of these viruses can result in the loss of all data on the infected disks. For more information, refer to "McAfee Support" in Chapter 1, "Introducing VirusScan."

NOTE: When scanning a network drive using /CLEAN, you must have sufficient rights to update files on that drive.

/DEL

Overwrite and delete infected files.

Deletes and overwrites each infected file. Files erased by the /DEL option cannot be recovered (you should generate a report so that you can restore them from backups). Instead of using /DEL alone, we recommend using it in combination with the /CLEAN option to attempt to disinfect an infected file first, then delete it only if the file is unrecoverable. The /CLEAN option can remove master boot record and boot sector viruses, but the /DEL option cannot.

```
scan a: /clean /del /report c:\mcafee\infected.log
```

Scan will attempt to restore any infected files on A: drive, then delete any files which could not be cleaned. The results of scanning, including the names of any restored or deleted files, will be saved to the report file "INFECTED.LOG" in the directory C:\MCAFEE.

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

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

/FAST

Reduces scanning time by about 15%. Using the /FAST option, Scan examines a smaller portion of each file for viruses, although it examines more files overall. Using /FAST might miss some infections found in a more comprehensive (but slower) scan. For example:

```
scan c:\data /fast
```

This command will perform a "fast scan" on the directory DATA on C: drive.

Do not use this option if you have found a virus or suspect one.

/MANY

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

For example:

```
scan a: /many
```

Use this line command to scan floppy disks inserted into the A: drive.

/MOVE {directory}

Move infected files to the specified directory.

Moves all infected files found during a scan to the specified directory. If you use /MOVE in conjunction with /CLEAN, Scan attempts to restore an infected file first, then moves it to the specified directory only if the file cannot be restored. Consider the following example:

```
scan c: /clean /move d:\infected
```

Scan will attempt to restore any infected files, then move any files which could not be cleaned to the directory INFECTED on D: drive.

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

You can also use /MOVE to rename the extensions of infected files to prevent users from inadvertently running them. For more information, refer to “Scan Command Line Options” in Chapter 5, “Scan Technical Reference.”

/REPORT {filename}

Saves the output of Scan to filename in ASCII text file format. If *filename* exists, /REPORT erases and replaces it (or, if you also use /APPEND, adds the report information to the end of the existing file). You can include the destination drive and directory; for example, consider the line command

```
scan a: /report d:\vsreprt\all.txt
```

This will scan the floppy drive (A:) and create a report file called “ALL.TXT” on D:\VSREPRT. However, if the destination is a network drive, you must have rights to create and delete files on that drive. You can also use /RPTCOR, /RPTMOD and /RPTERR to add corrupted files, modified files and system errors to the report.

/RPTCOR

Used in conjunction with /REPORT, adds the names of corrupted files to the report file. A corrupted file is a file that a virus has damaged beyond repair, which typically occurs in 10% to 20% of all viral infections. For example, consider the line command

```
scan c: /report /append /rptcor c:\mcafee\report.txt
```

This will scan the hard drive (C:) and save the scanning results and the names of any corrupted files to a text file called “REPORT.TXT” in the MCAFEE subdirectory on C: drive. If “REPORT.TXT” already exists, the information will be appended (added) to the existing file.

NOTE: You can use /RPTCOR with /RPTMOD and /RPTERR on the same command line.

/RPTERR

Used in conjunction with /REPORT, adds system errors to the report file. System errors include problems reading or writing to a diskette or hard disk, file system or network problems, problems creating reports and other system-related problems. You can use /RPTERR with /RPTCOR and /RPTMOD on the same command line. Refer to /RPTCOR for an example of using this command.

/RPTMOD

Used in conjunction with /REPORT, adds the names of modified files to the report file. Scan identifies modified files when the validation/recovery codes do not match (using the /CF or /CV options). You can use /RPTMOD with /RPTCOR and /RPTERR on the same command line. Refer to /RPTCOR for an example of using this command.

/SUB

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; for example:

```
scan c:\games /sub
```

This line command will scan all the files in the directory GAMES and its associated subdirectories on the C: drive.

Do not use /SUB if you are scanning an entire drive, as Scan will automatically scan all directories and subdirectories on that drive.

Using Scan to Detect a Virus

Start from the system prompt (C> or [C:\]). If you are running Windows 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.

After typing each entry on the command line, press [ENTER]. If you include the /REPORT {filename} option, Scan saves a report of infected files and any system errors to the specified log file. The /ALL option will scan all files, not just standard executables.

1. Insert the VirusScan program diskette in drive A.
2. Scan your C drive for known viruses by typing:

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

   OS/2: Type **`a: os2scan c: /report c:\virus.log /all`**

   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:

   `a: scan c: d: /report c:\virus.log /all`

   OS/2: Type **`a: os2scan c: d: /report c:\virus.log /all`**

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

   `a: scan /adl /report c:\virus.log /all`

   OS/2: Type **`a: os2scan /adl /report c:\virus.log /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.

```
Virus data file V2.2.9507 created 07/13/95 14:14:43
No viruses found in memory.
Scanning C:
Summary report on C:
File(s)
        Analyzed:.......         1500
        Scanned:........          750
        Possibly Infected:.......   0
        Master Boot Record(s):..    1
        Possibly Infected:.......   0
        Boot Sector(s):.........    1
        Possibly Infected:.......   0
Time: 60.00 sec.
```

- **Analyzed** indicates how many 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 will only check executable files. To check all files, use the /ALL command line option. For more information about setting command line options, refer to Chapter 5, "Scan Technical Reference."
- **Possibly infected** indicates how many infected files Scan has found.

4. If Scan reports "No viruses found," congratulations — most likely your system is currently virus-free. Copy any important or critical files to fresh diskettes or tape back up so you will have current, clean files should a virus later infect your system and damage your work. Refer to "Back Up Your Hard Drive" in Chapter 2, "Installation and Setup."

   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 "Using Scan to Remove a Virus" in the next section.

5. After scanning your hard drive(s) and other drives, you should scan **all** the diskettes you use with the /MANY option. Insert a diskette into drive A: and type the following command:

   `scan a: /many /report c:\virus.log /all`

   OS/2: Type **`os2scan a: /many /report c:\virus.log /all`**

   Scan will check the diskette in drive A: and then prompt you to insert the next diskette with the message:

   ```
   Please replace the media and press any key to scan it.
   (ESC to exit)
   ```

   Insert the next diskette into A: and press any key to continue scanning. Continue until you have scanned all of your diskettes. When you are finished, press the ESC key.

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

   `a: scan a: /many`

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

If VirusScan finds a virus, refer immediately to “Using Scan to Remove a Virus” in the next section.

Using Scan to Remove a Virus

If you detect a virus, you can run Scan with the /CLEAN option to eradicate most known viruses from your disks. If you are at all unsure about how to proceed once you have found a virus, contact McAfee for assistance (refer to “McAfee Support” in Chapter 1, “Introducing VirusScan.”).

WARNING: Using DOS commands (i.e. FORMAT, FDISK, DEBUG) to remove a virus can result in the **loss of all data and use of the infected disks**. If you are unfamiliar with viruses and virus methodology, contact McAfee immediately for assistance before using DOS commands to remove a virus (refer to “McAfee Support” in Chapter 1, “Introducing VirusScan”). For more information, refer to “Using DOS Commands to Remove a Virus” in Chapter 7, “Tips and Troubleshooting.”

Scan has options to control and fine-tune the scope, validation and operation of its disinfection. For details, refer to Chapter 5, “Scan Technical Reference.”

Step 1. Restart From a Clean Environment

You must run Scan from a clean, virus-free environment. With DOS or Windows, restart from a clean diskette. With OS/2, simply close all DOS and Win-OS/2 sessions.

With DOS or Windows, the only way to ensure a clean environment is to turn your computer off to remove any viruses in memory, then restart from a virus-free diskette, preferably the original, write-protected DOS installation diskette that came with your computer. If you do not have one, get one from someone else who has the same version of DOS; do not use a diskette that might be infected. (Refer to “Making a Clean Start-Up Diskette” in Chapter 2, “Installation and Setup,” for instructions. Create this diskette *after* you clean your system.)

1. Turn off your computer. (Do not just reset or reboot, which may leave some viruses intact in the computer’s memory.)
2. Make sure your clean boot (start-up) diskette is write-protected.
   - 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.
3. Insert your start-up diskette in drive A.

4. Turn on your computer and wait until you see the system prompt (probably A>). Do not run any programs on your hard disk, or you may reactivate the virus.

OS/2: With OS/2, you can remove any viruses from memory by closing all DOS, Win-OS/ 2 and virtual DOS machine (VDM) sessions.

Step 2. Run Scan with the /CLEAN option

Start from the system prompt (probably A> or [A:\]). If you are running OS/2, open the Command Prompts folder in the OS/2 system folder and click the **OS/2 Full Screen** or **OS/2 Window** icon.

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

1. Insert the VirusScan program diskette in drive A.
2. Remove the first known virus on all local drive(s) (including hard drives, compressed, CD-ROM and PCMCIA drives, but not diskettes) by typing:

   `scan /adl /clean /all /report c:\infectd.txt`

   OS/2: Type **`os2scan /adl /clean /all /report c:\infectd.txt`**

   Scan keeps you informed of its progress and generally reports virus removed successfully. If the virus was successfully removed, refer to Section 3, "If Viruses Were Removed." If Scan reports that the virus could *not* be safely removed, refer to Section 4, "If Viruses Were Not Removed."
3. If the virus was detected on a diskette, switch to C: drive (by typing **`C:`** and pressing ENTER). Insert the diskette into drive A: and type:

   `scan a: /many /clean /all /report c:\infectd.txt`

   OS/2: Type **`os2scan a: /many /clean /all /report c:\infectd.txt`**

   Scan will check the diskette in drive A: and, if a virus is present, will remove the virus if possible. If Scan reports that the virus has been successfully removed, remove the diskette from the drive, insert the next diskette and press any key. If Scan reports that the virus could not be safely removed, remove the diskette from the drive, indicate that it is still infected by marking the label, insert the next diskette and press any key. After scanning all your diskettes, perform the procedure in Section 4, "If Viruses Were Not Removed," on any disks that could not be successfully cleaned.

   NOTE: The Scan program files should be on a drive that is not 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 (i.e. scan A: drive from C: drive or B: drive).

Step 3. If Viruses Were Removed

If Scan successfully removes all the viruses, restart your computer. Run Scan again to verify that your system is now virus-free. Be sure to examine and disinfect any diskettes you use as well, as diskettes are a common source of virus infection. Refer to "When to Rescan" in Chapter 2, "Installation and Setup."

Step 4. If Viruses Were Not Removed

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

```
Virus cannot be removed from this file.
```

Make sure to take note of the filename, 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, as described in "Scan Command Line Options" above and in Chapter 5, "Scan Technical Reference." If you have any questions, contact McAfee (refer to "McAfee Support" in Chapter 1).

False Alarms

Due to the nature of anti-virus software, there is a possibility that Scan 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 "Using Scan to Remove a Virus" earlier in this chapter. After you have performed these procedures, if you still feel that the virus alert was a "false alarm" please contact McAfee (refer to "McAfee Support" in Chapter 1). You can upload the file to our bulletin board system at (408) 988-4004, along with your name, address, daytime telephone number and electronic mail address (if any).

For more information, refer to "False Alarms" in Chapter 7, "Tips and Troubleshooting."

Using VShield

VirusScan's VShield program can help prevent viruses from infecting your system. It runs as a "terminate-and-stay-resident" (TSR) program, remaining in memory and scanning and intercepting programs as they are executed.

VShield checks programs, the master boot record, boot sector, system files and itself for virus signatures, the pattern of code unique to each virus. If VShield finds an infection, it prevents programs from running. It also prevents warm boots ([CTRL]+[ALT]+[DEL]) from infected disks.

This section contains all the information most users of VShield will need. More detailed information is available in Chapter 6, "VShield Technical Reference."

Launching VShield

The VirusScan installation program gives you the option of adding a line to your AUTOEXEC.BAT file which automatically activates VShield whenever you start or restart your computer. To activate VShield at any time:

- **DOS or Windows**. Restart your computer by pressing [CTRL]+[ALT]+[DEL], or by turning it off and then on again, or by any other reset method.
- **OS/2**. Restart all DOS and Win-OS/2 windows.

NOTE: If you have not changed the path statement in your AUTOEXEC.BAT file, you will need to include its location (usually C:\MCAFEE\VIRUSCAN) in the command, or change to that directory.

If you have difficulties running VShield, it may be due to conflicts with other TSR programs in your system, or with other programs that monitor disk access. Refer to "VShield Option Summary" in Chapter 6, "VShield Technical Reference," and to "Troubleshooting VShield" in Chapter 7, "Tips and Troubleshooting." Contact McAfee technical support if you need help (refer to "McAfee Support" in Chapter 1, "Introducing McAfee").

VShield minimizes the use of conventional memory by attempting to load into extended, expanded, upper memory or a combination thereof, before using conventional memory. For extreme memory limitations, you can use VShield's /SWAP option to reduce memory requirements to 8 Kb, although this decreases VShield's speed.

NOTE: The /SWAP option may not function in some Windows environments.

For details, refer to Chapter 6, "VShield Technical Reference."

Configuring VShield

VShield has options to control and fine-tune the scope, validation and operation of its virus prevention. At a minimum, consider specifying options to check diskettes (/ANYACCESS, /FILEACCESS or /BOOTACCESS). These options are not enabled by default; you must add them to the VShield command line. For details on these and other options, refer to Chapter 6, “VShield Technical Reference.”

When used in conjunction with some Scan options, VShield can help protect your system from new and unknown viruses. For details, refer to “Detecting New and Unknown Viruses” in Chapter 7, “Tips and Troubleshooting.”

Notes for using VShield in Windows and OS/2:

- In Windows, you can use the VShield icon to turn messages from VShield on and off. (VShield itself, however, remains active.) For details, refer to Chapter 5.
- In OS/2, VShield runs in DOS and Win-OS/2 sessions only, because viruses can operate only in those sessions.

VShield and Windows

The installation program can add a line to your AUTOEXEC.BAT file that automatically activates VShield whenever you start or restart your computer. In Windows, it also gives you a VShield icon that you can click to turn VShield messages on or off.

NOTE: You can change VShield 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. Refer to Chapter 6, “VShield Technical Reference,” for details.

VShield and OS/2

VShield 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 (refer to Appendix A, “Downloading McAfee Software”), 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 earlier in this section.

NOTE: We recommend using the command line option /FILEACCESS in OS/2. This option checks standard executable files whenever the file is accessed or executed, prevents the execution of infected programs and checks all files when accessed by a read or write operation.

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 “Using Scan to Remove a Virus” earlier in this chapter. After you have performed these procedures, if you still feel that the virus alert was a “false alarm” please contact McAfee (refer to “McAfee Support” in Chapter 1). You can upload the file to our bulletin board system at (408) 988-4004, along with your name, address, daytime telephone number and electronic mail address (if any).

For more information, refer to “False Alarms” in Chapter 7, “Tips and Troubleshooting.”

Chapter 4 WScan Technical Reference

Chapter 3 provided general information about WScan, Scan and VShield. This chapter contains more detailed information on VirusScan's graphic interface anti-virus program, WScan.

Overview

NOTE: This chapter contains detailed information about the graphic interface version of Scan, WScan. For a general overview of WScan and its features, refer to "Using WScan" in Chapter 3, "VirusScan Reference."

WScan provides most of the features of the Scan command line program through a graphical user interface. You can use a mouse or keyboard to choose WScan commands and options. It runs under Windows 3.1 or later and the program file is WSCAN.EXE.

This chapter describes how to use the graphical interface to scan and clean your system. To use the Scan program from the DOS prompt, refer to "Using Scan" in Chapter 3, "VirusScan Reference."

NOTE: If a virus is resident in memory, the most secure way to clean your system is to turn off your computer and start from a clean start-up diskette, as described in "Using Scan" in Chapter 3, "VirusScan Reference." Otherwise, you can securely use WScan to clean infections if:

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

System Requirements and Support

WScan requires Windows 3.1 or later. WScan works with the following networks:

- Novell NetWare
- 3Com 3/Share and 3/Open
- Artisoft LanTastic
- AT&T StarLAN
- Banyan VINES
- DEC Pathworks
- IBM LAN Server
- Microsoft LAN Manager
- any other IBMNET- or NETBIOS-compatible network operating system.

Contact McAfee or your local authorized agent, as described in “McAfee Support” in Chapter 1, “Introducing VirusScan,” if you do not see your network listed.

WScan is designed to check for pre-existing infections of known and unknown viruses on diskettes, hard drives, CD-ROM and compressed (SuperStor, Stacker, DoubleSpace and so on) disks on both stand-alone and networked personal computers, as well as network file servers. If you have a Novell NetWare/386 V3.11 or 4.0 file server, you may want to use the NetShield virus prevention software, a NetWare Loadable Module (NLM), in conjunction with WScan. For more information about NetShield, contact McAfee, as described in “McAfee Support” in Chapter 1, “Introducing VirusScan.”

Starting WScan

To start WScan, double-click the WScan icon in the Windows Program Manager. The WScan main window is displayed.

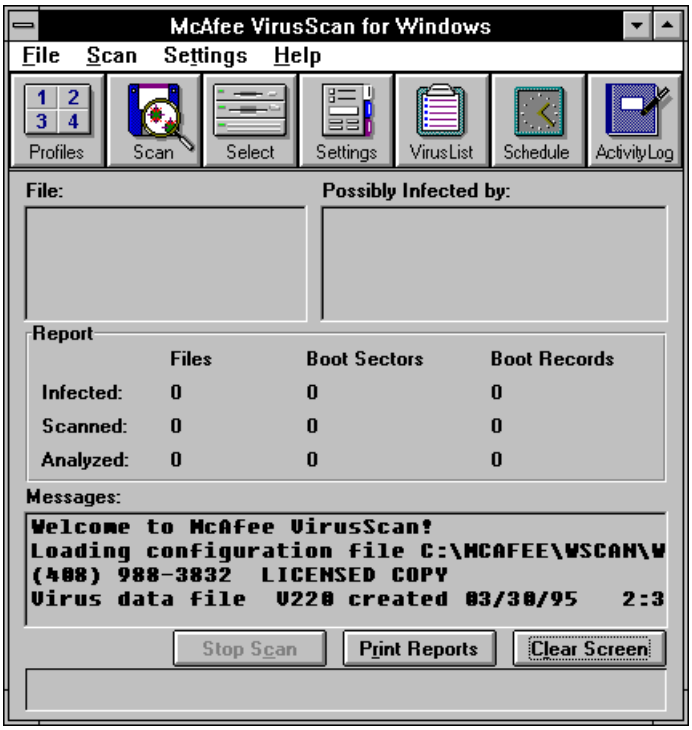


Figure 4-1. WScan main window.

As it loads, WScan performs a self-check of its program files to verify their integrity.

NOTE: If WScan fails the self-check, or if it exits Windows, then you should *turn off your computer*, then run the Scan command line program from a clean start-up diskette. Do not use WScan to remove a virus in memory. For instructions, refer to "Using Scan" in Chapter 3, "VirusScan Reference."

WScan does not check diskettes or fixed disks at start-up. To scan disks, refer to "Scanning Your System for Viruses" later in this chapter. To clean infected disks, refer to "Cleaning Your System" later in this chapter.

Using the Menu Bar

The WScan menu bar contains the following menus, all of which are described later in this chapter:

- **File** lets you load and save scan settings, select items to scan, choose profiles, print reports and exit the program.
- **Scan** lets you scan your system and schedule automatic future scans.
- **Settings** lets you select scan configuration options in the Notebook.
- **Help** lets you get on-line help for using WScan, display the virus list and obtain product support instructions.

Using the Tool Bar

You can use the tool bar to quickly start a task without navigating the menu. The tool bar contains the following icons (all described in this chapter), which you click to perform a task.

Figure 4-2. VirusScan tool bar.

- **Profiles** is described in “Loading and Using Profiles.”
- **Scan** is described in “Scanning Your System for Viruses.”
- **Select** is described in “Selecting Drives, Directories and Files to Scan.”
- **Settings** is described in “Selecting Scanning Options.”
- **Virus List** is described in “Displaying a List of Known Viruses.”
- **Schedule** is described in “Scheduling Scans.”
- **Activity Log** is described in “Using the Scan Activity Log.”

Exiting WScan

To exit WScan, choose File | Exit. If you have not saved changes to scan settings or options, a dialog box is displayed asking whether to save them. To save settings, choose Yes and follow the instructions in “Using Scan Settings Files” later in this chapter. Otherwise, choose No.

Scanning Your System for Viruses

Scan your system when you want to detect and identify viruses.

To scan, either select a profile, as described in “Loading and Using Profiles” later in this chapter, or follow these steps:

1. Select the items you want to scan and the scan settings you want to use by doing *one* of the following tasks:
   - Choose a settings file, as described in “Using Scan Settings Files” later in this chapter, or
   - Choose items and settings individually, as described in “Selecting Drives, Directories and Files to Scan” and “Selecting scanning options” later in this chapter. You must select at least one item to scan (by default, drive C is selected).
2. Choose Scan | Start Scan or click the Scan icon.

   WScan performs the check according to the settings and items 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 main WScan window.

   If WScan finds a virus in a file, boot sector, or master boot record, refer to “Cleaning Your System” later in this chapter for instructions on how to proceed.

Cleaning Your System

Clean your system when you know or suspect that a virus infection has occurred. If a virus is resident in memory, the most secure way to clean your system is to turn off your computer, reboot from a clean start-up diskette and use the command line program Scan, as described in "Using Scan" in Chapter 3, "VirusScan Reference." However, you can securely use WScan if:

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

To use WScan to clean up infected files, the CLEAN.DAT file must be present in the subdirectory containing the WScan 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 contact McAfee (refer to "McAfee Support" in Chapter 1, "Introducing VirusScan").

Use the following procedure to clean files which you suspect are infected:

1. Select the items you want to scan and the scan settings you want to use by doing one of the following tasks:

   - Choose a settings file, as described in "Using Scan Settings Files" later in this chapter, or
   - Choose items and settings individually, as described in "Selecting Drives, Directories and Files to Scan" and "Selecting scanning options" later in this chapter. You must select at least one item to scan (by default, drive C is selected) and you must select the Clean Infection (File, Boot Sector, MBR) check box on the Action page of the Notebook.

2. Choose Scan | Start Scan or click the Scan icon.

   WScan checks and cleans your system according to the settings and items 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 main window.

If WScan reports that an infected file is corrupted beyond repair, use the default reporting on the main screen to generate a report (as described in "Using Scan Settings Files" later in this chapter), or take note of the file name so that you know what to restore from backups. Consider cleaning your system again, this time selecting either Delete Infected File (to remove the file) or Move Infected File to Directory (to save it in a quarantine directory) on the Actions page of the Notebook. For more information, refer to "Selecting Scan Actions" later in this chapter.

Selecting Drives, Directories and Files to Scan

Before scanning or cleaning, you must select drives, directories or files to scan. You can scan local drives, including diskette drives, as well as network drives. You must select at least one item to scan. By default, drive C is selected. You can select up to 26 items in DOS and Windows.

To select items to scan, choose File | Select Items to Scan or click the Select icon. The Select dialog box is displayed.

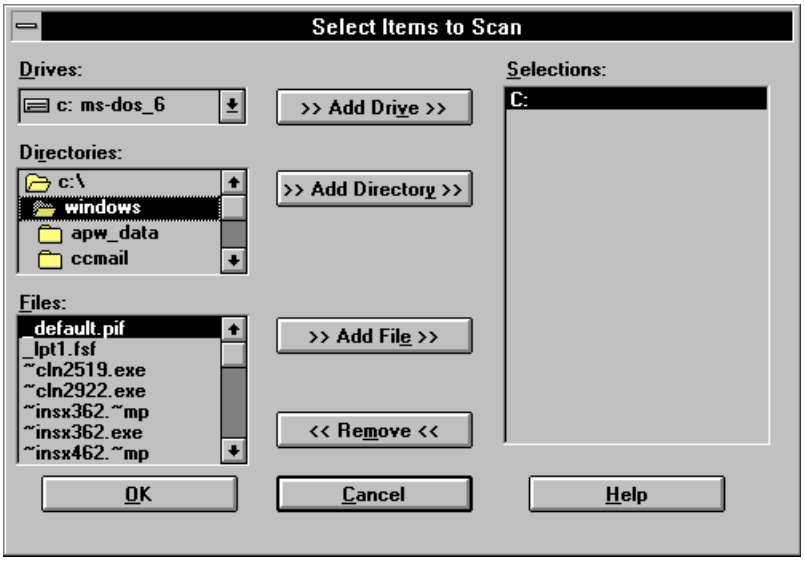


Figure 4-3. Selecting drives, directories and files to scan.

You can save your selections in a settings file, as described in “Using Scan Settings Files” later in this chapter. Otherwise, your selections are abandoned when you exit WScan and you must reselect them the next time you start WScan.

Adding Items to Scan

The Selections list contains the names of drives, directories and files to scan or clean.

- To add a drive to the Selections list, select it in 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 in the Directories list, then choose Add Directory. To scan subdirectories of a selected directory, you must select the Subdirectories check box on the Controls page of the Notebook, as described in “Controlling the scan scope” later in this chapter. If you select a drive, its subdirectories are scanned automatically, regardless of the Subdirectories setting.
- To add a file, select it in the Files list, then choose Add File.

The item you added appears in the Selections list.

Removing Items From the Selections List

All items that appear in the Selections list will be scanned. Remove an item you do not want to be included in the scan by selecting it and choosing Remove.

Selecting Items Using Drag and Drop

In Windows, you can 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.

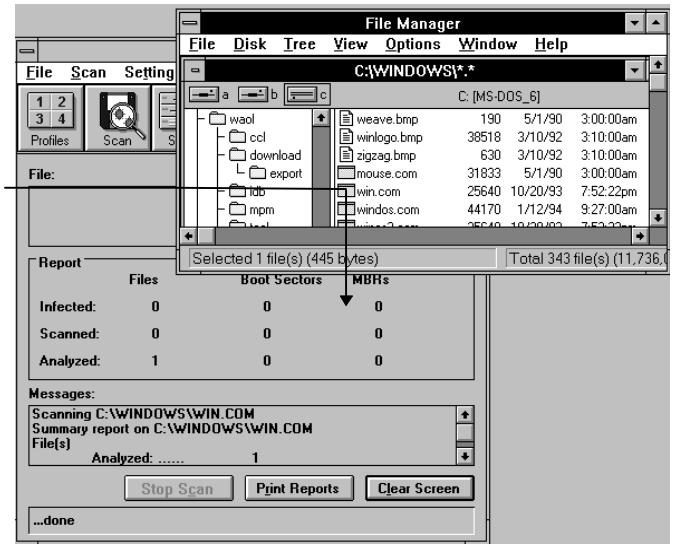


Figure 4-4. Selecting items using drag and drop.

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

NOTE: When the WScan window is minimized, files dragged to the icon will be assumed to be settings files. Refer to “Using Scan Settings File” later in this chapter.

Selecting Scanning Options

You can fine-tune the way WScan scans your system to increase system security, reduce scanning time and perform specific tasks. For example, you can delete infected files automatically or move them to a quarantine directory, generate a report of scanning results, use CRC integrity checking to detect unknown viruses and so on. You select these options in the WScan Notebook, which contains several property pages of scan options.

Using the Notebook

To display the Notebook, click the Settings icon or choose any option from the Settings menu.

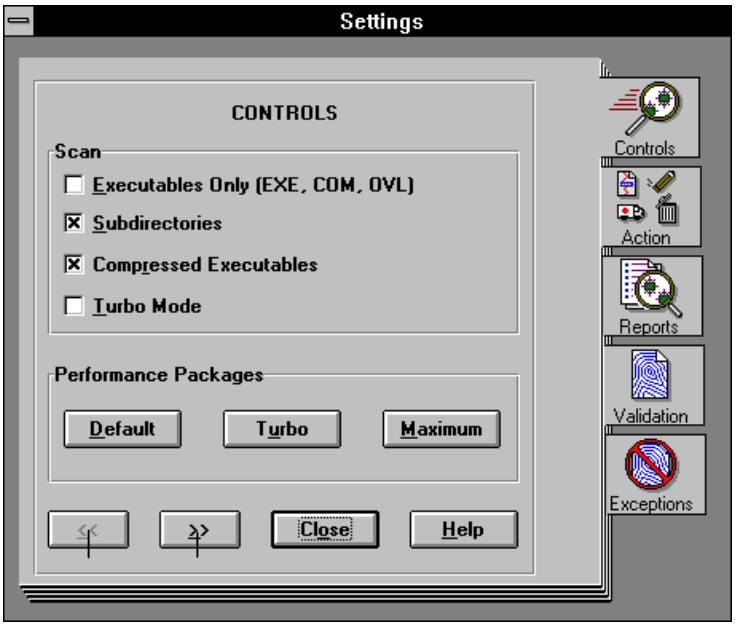
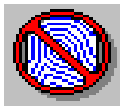


Figure 4-5. The WScan Notebook.

To display a property page, click its tab with the mouse, or choose the navigation arrow buttons to move to the previous page or the next page in the Notebook, or choose the property page name from the Settings menu.

The Notebook contains several property pages of scan options.

Icon	Property page	Scan options
	Controls	Scope of files to scan and speed/efficiency controls.
	Action	Actions to take when an infection is detected in a file, boot sector, or master boot record.
	Reports	Report files to generate from scan results.
	Validation	Validation codes used for program files.
	Exceptions	Files to exclude from validation.

You can save your selections in a settings file, as described in “Using Scan Settings Files” later in this chapter. Otherwise, your selections are abandoned when you exit WScan and options revert to their default settings the next time you start WScan.

Controlling the Scan Scope

The Controls property page of the Notebook lets you determine the scope of files to scan.

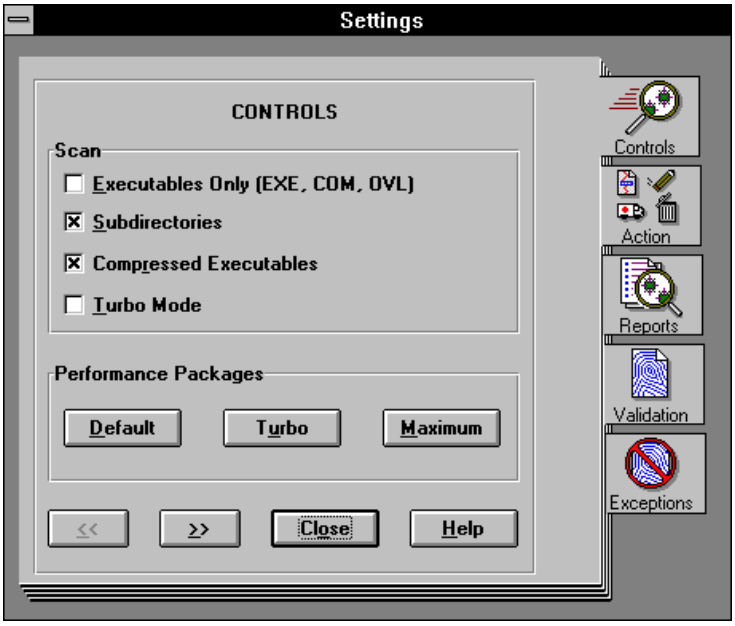


Figure 4-6. The Controls property page.

For details about how each selection affects scanning speed, refer to the corresponding command line option in Chapter 5, “Scan Technical Reference.”

- **Executables Only** reduces scan time when a full scan is not needed, by checking only executable files—those with a .COM, .EXE, .SYS, .BIN, .OVL and .DLL extension. These are the files most commonly infected by viruses. If this option is not selected, WScan checks all files on the selected drives and directories, which increases scan time. Do not use this option if you have found a virus or suspect one. When you run Scan from the command line, this is the default.
- **Subdirectories** tells WScan to check files in the subdirectories of selected directories (as described in “Selecting Drives, Directories and Files to Scan” earlier in this chapter). 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. The Scan command line equivalent is /SUB.

- **Compressed Executables** tells WScan to check inside executable, or self-decompressing, files that have been created using the 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 the validation options are used (refer to "Generating a Scan Report" later in this chapter). The Scan command line equivalent, if this option is not selected, is /NOCOMP.

NOTE: Scan does not check files with .ZIP or .ARJ extensions.

- **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. The Scan command line equivalent is /FAST.
- **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. The Scan command line equivalent is /ALL.

NOTE: Scan does not check files with .ZIP or .ARJ extensions.

- **Performance Packages** selects the following options automatically:

Option	Default	Turbo	Maximum
Executables Only	X	X	
Subdirectories		X	X
Compressed Executables	X		X
Turbo Mode		X	

Selecting Scan Actions

The Actions property page of the Notebook lets you determine what happens when files are scanned.

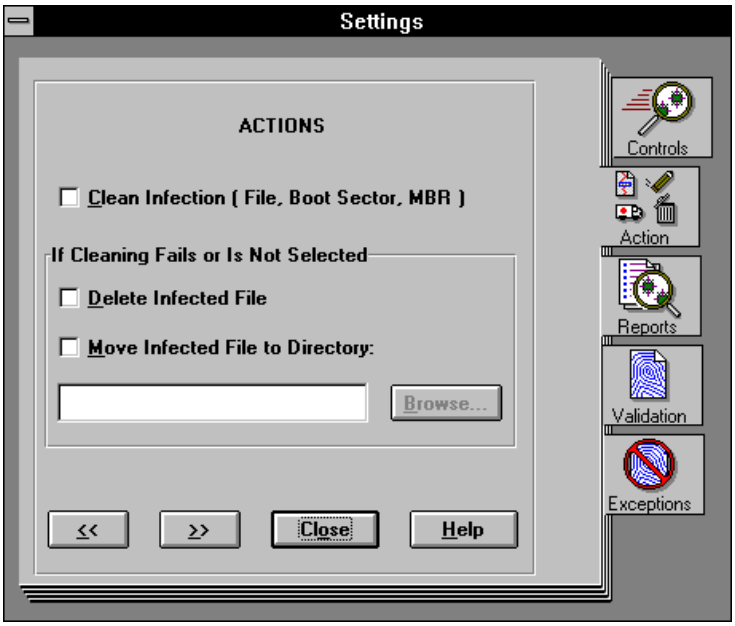


Figure 4-7. The Actions property page.

- **Clean Infection (File, Boot Sector, MBR)** tells WScan to restore the boot sector and any infected files. Between 10% and 20% of all viruses are not removable; they damage the infected file beyond repair. If the infected file resides on a network drive, you must have rights to change files on that drive. If WScan cannot restore a file, a message is displayed that identifies the name of the unrecoverable file. If Clean Infection (File, Boot Sector, MBR) is not selected, WScan merely reports the infection in the main WScan window. The Scan command line equivalent is /CLEAN.

  NOTE: To select this option, the CLEAN.DAT file must reside in the same directory as the WScan 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 contact McAfee (refer to “McAfee Support” in Chapter 1, “Introducing VirusScan”).

- **Delete Infected File** tells WScan to delete infected files automatically when found. Between 10% and 20% of all viruses are not removable; they damage the infected file beyond repair. Erased files cannot be recovered, so use the default reporting on the main screen to generate a report (refer to "Using Scan Settings Files" later in this chapter), or take note of the file name so that you know what to restore from backups. If the infected file resides on a network drive, you must be able to delete files on that drive. The Scan command line equivalent is /DEL.
- **Move Infected File to Directory** tells WScan to move virus infected files to a quarantine directory. You might want to do this to examine the files in greater detail, or to upload the files to the McAfee bulletin board (refer to "McAfee Support" in Chapter 1) for research. If selected, you must type the path of the quarantine directory, or choose Browse to select one from a list. The Scan command line equivalent is /MOVE.

  If you choose Browse, the Directory Selection dialog box is displayed.

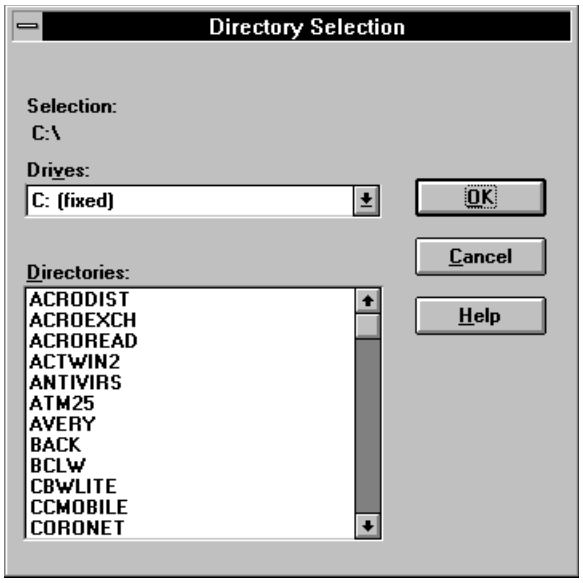


Figure 4-8. Selecting a directory.

When you select Delete Infected File or Move Infected File to Directory (you can select one or the other but not both in the same scan), McAfee recommends that you select Clean Infection (File, Boot Sector, MBR) as well so that WScan attempts to restore the virus first, then deletes or moves the file only if it cannot be recovered. In addition, Clean Infection (File, Boot Sector, MBR) can remove boot sector and master boot record (MBR) viruses, but Delete Infected File and Move Infected File to Directory alone cannot.

McAfee recommends that you get help to deal with a virus if you are unsure how to proceed. This is especially true for “critical” viruses and master boot record or boot sector infections, because improper removal can result in lost data or damaged disks. Refer to “McAfee Support” in Chapter 1, “Introducing VirusScan.”

Generating a Scan Report

The Reports page of the Notebook contains options to save scanning results to a report file that you can print for future reference. A report includes information about the items scanned, infections found, infections cleaned and optional details about corrupted files, modified files and system errors. To print the report, refer to “Printing a Report or Activity Log” later in this chapter.

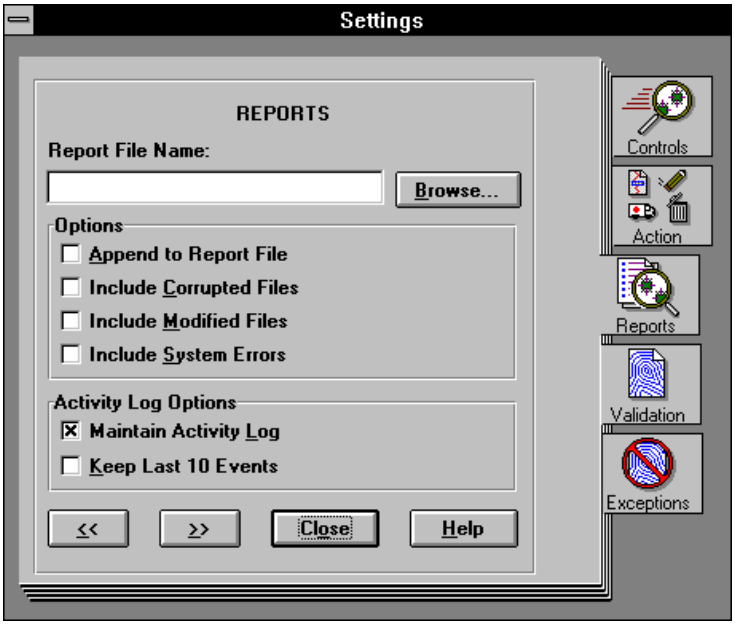


Figure 4-9. The Reports property page.

- **Report File Name** is the name of the report file you want to create or update. Type a file name, including 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. The Scan command line equivalent is /REPORT.

- **Append to Report File** tells WScan to add report information to the end of the specified report file. If this check box is not selected, WScan overwrites the specified report file, if it exists, with the new report. The Scan command line equivalent is /APPEND.
- **Include Corrupted Files** tells WScan to add information about corrupted files in the specified report file. Between 10% and 20% of all viral infections result in files that are corrupted beyond repair. The Scan command line equivalent is /RPTCOR.
- **Include Modified Files** tells WScan to add information about validated files that have been modified to the specified report file. The Scan command line equivalent is /RPTMOD.
- **Include System Errors** tells WScan to add information about errors that occurred while scanning to the report file, such as programs reading or writing to a diskette or hard disk, file system or network problems, and so on. The Scan command line equivalent is /RPTERR.
- **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 (by default, called SCAN.LOG in the current directory). For more information, refer to "Using the Scan Activity Log" later in this chapter. The Scan command line equivalent is /LOG.
- **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 on-line help.

Validating Program Files

The Validation page of the Notebook lets you use validation codes to determine whether validated files have been modified, which can indicate a possible viral infection and can detect new or unknown viruses. For more information, refer to Chapter 7, "Tips and Troubleshooting." You can exclude from validation self-modifying files that might generate false alarms, as described in "Excluding Files From Validation" later in this chapter.

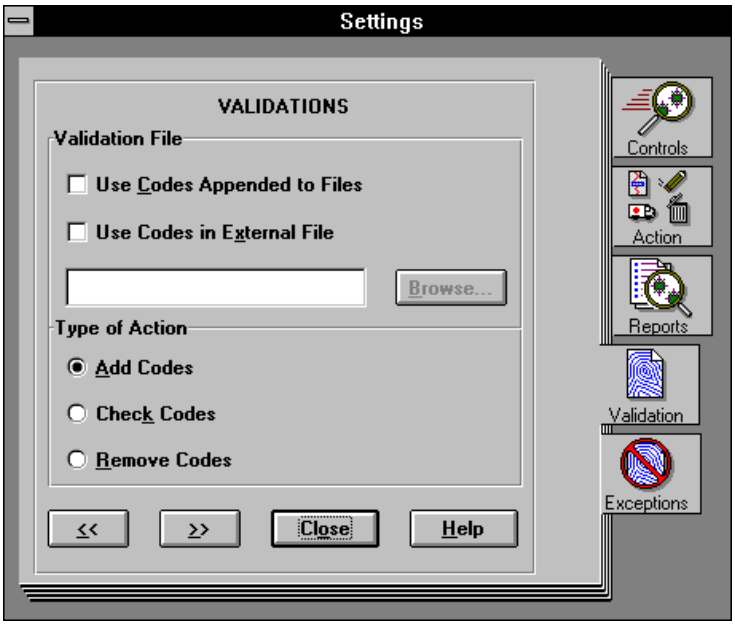


Figure 4-10. The Validations property page.

- **Use Codes Appended to Files** tells WScan to store validation/recovery codes in standard executable files (files with a .COM, .EXE, .SYS, .BIN, .OVL and .DLL extensions), 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.

  NOTE: This may cause errors in some files. Refer to "Excluding Files From Validation" later in this section for details.

- **Use Codes in External File** tells WScan to store validation/recovery codes in an external file you specify. If selected, you must type its 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 — the preferred method — validates files on a hard disk or diskette as well as system areas. If the file resides on a network disk, you must have sufficient rights to create and delete it.

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

- **Add Codes** tells WScan to add validation/recovery codes to the validation database file, if Use Codes in External File is selected, or to standard executable files, if Use Codes Appended to Files is selected. The Scan command line equivalents are /AF and /AV, respectively.

- **Check Codes** tells WScan to check validation/recovery codes that have previously been added to the validation database file, if Use Codes in External File is selected, or to standard executable files, if Use Codes Appended to Files is selected. If a validated file has been modified, WScan reports it. You can save this information in a report by selecting the Include Modified Files check box on the Reports page of the Notebook, as described in "Using Scan Settings Files" later in this chapter. The Scan command line equivalents are /CF and /CV, respectively.
- **Remove Codes** tells WScan to remove validation/recovery codes that have previously been added to the validation database file, if Use Codes in External File is selected, or to standard executable files, if Use Codes Appended to Files is selected. The Scan command line equivalents are /RF and /RV, respectively.

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

  You can also remove validation codes added with the /AF command line option by deleting the validation file. Scan your system to check for viruses, delete the validation file, then run Scan with the /AF command line option to create a new validation file with current information. Refer to "Updating Validation Codes" in Chapter 5, "Scan Technical Reference," for more information.

Excluding Files from Validation

The Validation Exceptions page of the Notebook contains a list of files to exclude from the validation checking options you select on the Validation page. For more information, refer to "Generating a Scan Report" earlier in this chapter. You can also create the exception file as an ASCII file using a text editor. For more information and a sample exception list file, refer to Chapter 5, "Scan Technical Reference." The Scan command line equivalent for excluding files is /EXCLUDE {*filename*}.

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 the validation.

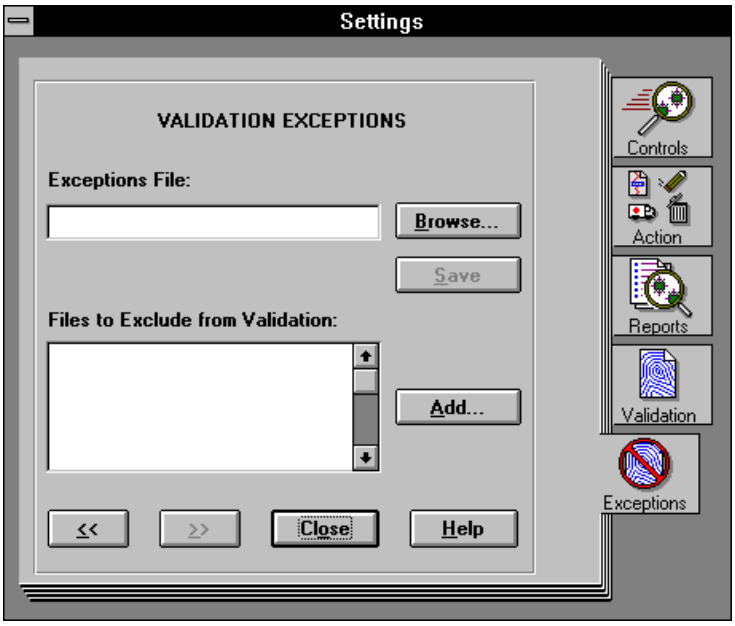


Figure 4-11. The Validation Exceptions property page.

- **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, then press [DEL].

Using Scan Settings Files

You can save the scan settings and the selected items in a settings (.INI) file. That way, you do not need to select scanning options and items individually every time you want to scan—you just load the settings file. You can save default scan settings in WSCAN.INI (WScan reads this file and uses these settings when it loads), or you can save them in a file with a different name. For details about the contents of a settings file, refer to the “WSCAN.INI” topic in on-line help.

NOTE: Selecting a profile overrides the saved scan settings for the duration of the profile scan. For details, refer to “Loading and Using Profiles” later in this chapter.

Saving Scan Settings

To save scan settings:

1. Choose File | Save Settings. The Save Settings dialog box is displayed.

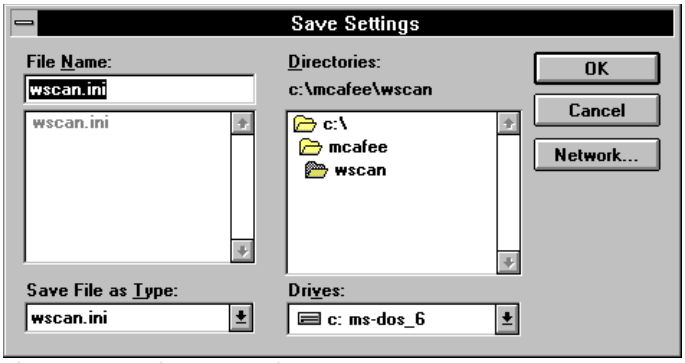


Figure 4-12. Saving scan settings.

2. Select a different file type, if needed.
3. Type a new name for the settings file you want to save.

Loading Scan Settings

To load a scan settings file:

1. Choose File | Load Settings. The Load Settings dialog box is displayed.

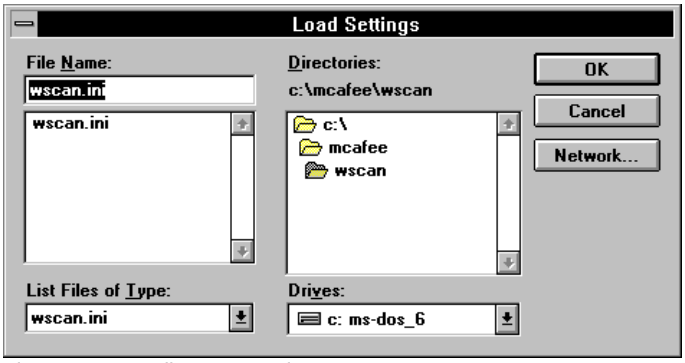


Figure 4-13. Loading scan settings.

2. Select a different file type, if needed.
3. Type or select the name of the settings file you want to use.

   The Scan command line equivalent is /LOAD.

Loading and Using Profiles

A *profile* is a simplified way to scan your system using scan options stored in a profile load file. Using profiles automates repetitive scanning tasks and makes it easier to scan your system.

NOTE: Before using profiles, they must be defined in the WSCAN.INI file. If no profiles are available, you (or your system administrator or information systems staff) must create them, then reload WScan. For instructions, refer to "Setting Up Profiles" later in this section.

To select a profile:

1. Choose File | Profiles or click the Profiles icon.

   The Run Profile dialog box is displayed.

Figure 4-14. Loading profiles.

2. Choose the profile you want.

   WScan loads the associated profile file, then scans your system using those settings.

Setting Up Profiles

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.

NOTE: Contact your system administrator or information services staff before attempting this procedure yourself. They might want to perform this procedure for you.

To set up or modify a profile, you need to use a text editor that can read and save WSCAN.INI as an ASCII text file. You also need to create the scan load file you want to use for each profile, as described in the discussion of the "/LOAD" option in Chapter 5, "Scan Technical Reference."

The Run Profile dialog box uses the following variables defined in the WSCAN.INI file.

Figure 4-15. Running a profile.

Here is an example of settings for the header variables in the WSCAN.INI file.

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

Here is an example of settings for one of the buttons in the WSCAN.INI file.

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

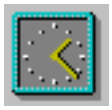
- **`[Profile1]`** begins the section for the first button (the next button is *Profile2*, and so on).
- **`Label`** is the short word or phrase that appears in the button.
- **`Description`** is the text that provides additional information about the profile and appears to the right of the button.
- **`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 on-line help.

Scheduling Scans



You can schedule WScan to automatically scan at a future date and time. Thereafter, WScan runs the scan at the scheduled time, **if the workstation is running and WScan is loaded**, even if you are using another application at the time. In this way, you can scan your system un-attended and ensure that scanning occurs on a regular basis. For each scheduled scan, you can specify when to scan, what to scan and which scan options to use. WScan saves the information for each scheduled scan in a separate .VSS file.

To schedule future scans, choose Scan | Schedule, or click the Schedule icon. The Schedule dialog box is displayed.

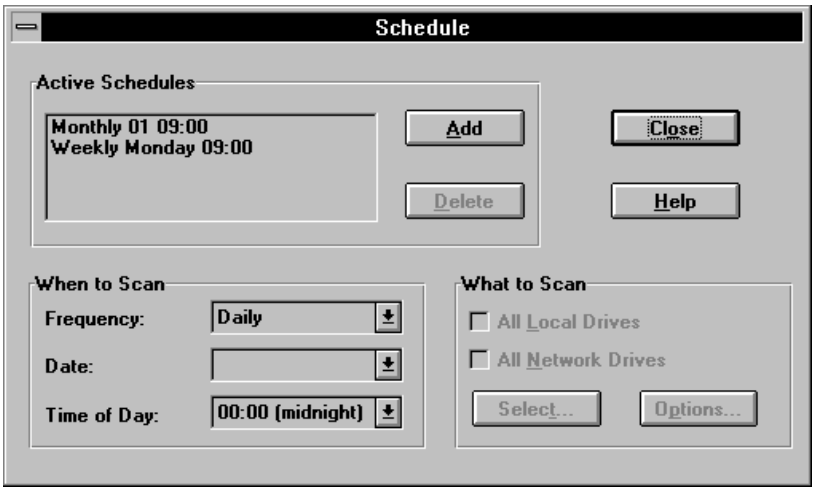


Figure 4-16. Scheduling scans.

- **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, choose Add, which creates a new .VSS file in the current directory. To remove a scheduled scan, select it in the Active Schedules list, then choose Delete, which deletes the associated .VSS file.
- **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).
- **All Local Drives** tells WScan to scan all local drives (including compressed, CD-ROM and PCMCIA drives) on the workstation during the automatic scan. The Scan command line equivalent is /ADL.
- **All Network Drives** tells WScan to scan all local drives on the workstation during the automatic scan. The Scan command line equivalent is /ADN.
- **Select** displays the Scanning Selection dialog box from which you can select drives, directories and files for the currently selected scheduled scan *only*. For more information, refer to “Selecting Drives, Directories and Files to Scan” earlier in this chapter. Selecting items from within the Scheduler dialog box *does not* change the items currently selected for scanning in the main application.

- **Options** displays the WScan Notebook from which you can select scanning options for the currently selected scheduled scan *only*. For more information, refer to “Selecting Scanning Options” earlier in this chapter. Selecting these options from within the Scheduler dialog box *does not* change the scanning options currently selected in the main application.

Using the Scan Activity Log

The *activity log* keeps track of the dates and times you scan your system, as well as associated messages regarding the items scanned and infections found. It provides an audit trail that you can use to verify regular scanning or, if you encounter an infection, to determine the last time the system was scanned for viruses and which items were found to be infected.

NOTE: To update the activity log with each scan, the Maintain Activity Log check box must be selected on the Reports page, as described in “Generating a Scan Report” earlier in this chapter.

Viewing the Activity Log

To view the activity log, choose Scan | Activity Log or click the Activity Log icon. The Activity Log dialog box is displayed.

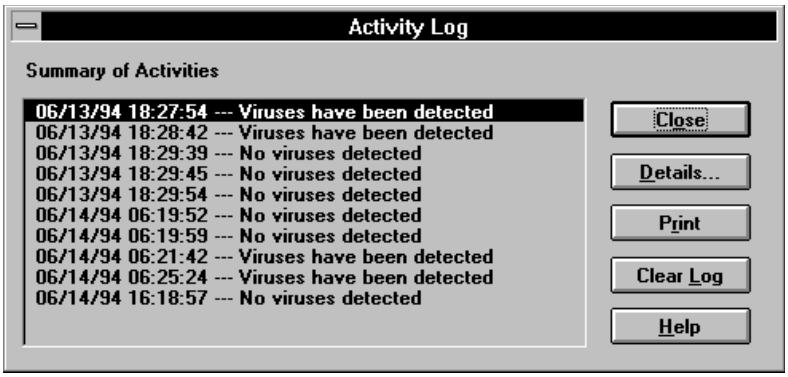


Figure 4-17. Viewing the Activity Log.

To see details about the items scanned and viruses found for an individual scan, select the entry in the **Summary of Activities** list, then choose **Details**. The Activity Log – Details dialog box is displayed.

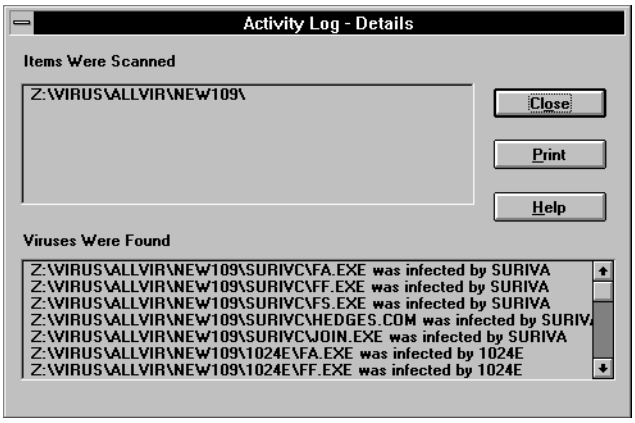


Figure 4-18. Viewing the Activity Log - Details.

To print the detail information, choose Print from the Activity Log – Details dialog box. To close this dialog box, choose Close.

To print the activity log, choose Print from the Activity Log dialog box. The Print dialog box appears, as described in “Printing a Report or Activity Log” later in this chapter. Select the options you want, then choose OK.

To clear the activity log, choose Clear Log from the Activity Log dialog box. A dialog box is displayed asking you to confirm deletion. Choose Yes to delete the activity log file.

Specifying a Different Log File Name

The default file name for the activity log is VSCAN.LOG. To specify a different log file name or path, use an ASCII text editor to change the LogFile variable in the [Maintain] section of the WSCAN.INI file, as shown in the following example.

```
[Maintain]
LogFile=c:\mcafee\logfile\myscan.log
```

Printing a Report or Activity Log

You can print the report you have created on the Reports page of the Notebook, as described in “Using Scan Settings Files” earlier in this chapter. You can also print the activity log, which is described in “Using the Scan Activity Log” earlier in this chapter.

- To print a report file, choose Print Report on the main window.

- To print the activity log, choose Print on the Activity Log dialog box.
- To print the virus list, choose Print in the Virus List dialog box.

1. The Print dialog box is displayed.

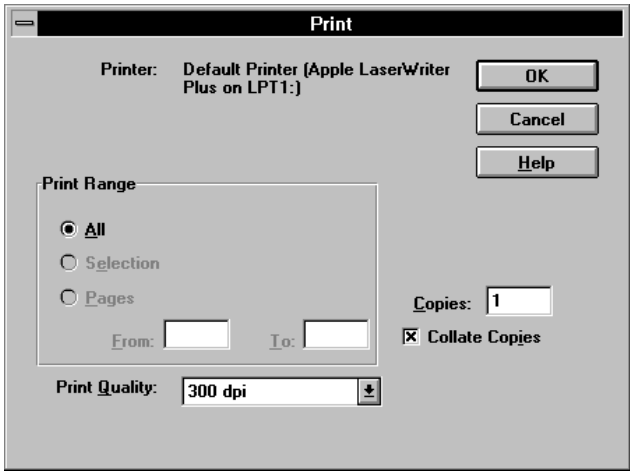


Figure 4-19. Printing the Activity Log.

Select print options and choose OK.

You can change the printer settings for specialized printing needs. To set up the printer:

1. Choose File | Print Setup or choose Setup on the Print dialog box.

The Print Setup dialog box is displayed.

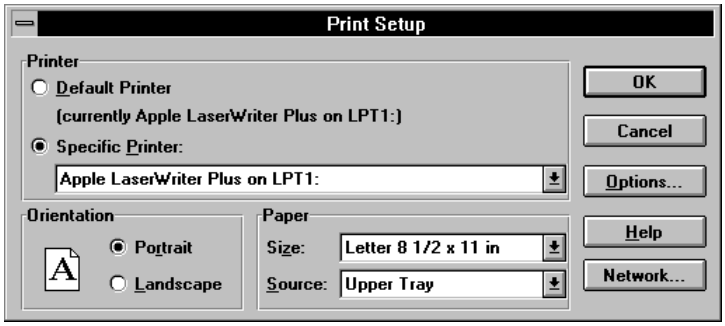


Figure 4-20. Print Setup dialog box.

Select print setup options and choose OK.

Displaying a List of Known Viruses

The virus list describes the many known viruses that WScan detects, identifies and disinfects. It tells you whether WScan can remove the virus and provides additional information about the virus and the types of files it infects. The virus list information is stored in the NAMES.DAT file. The Scan command line equivalent is /VIRLIST.

To display the virus list, choose Help | Virus List, or click the Virus List icon. The Virus List dialog box is displayed.

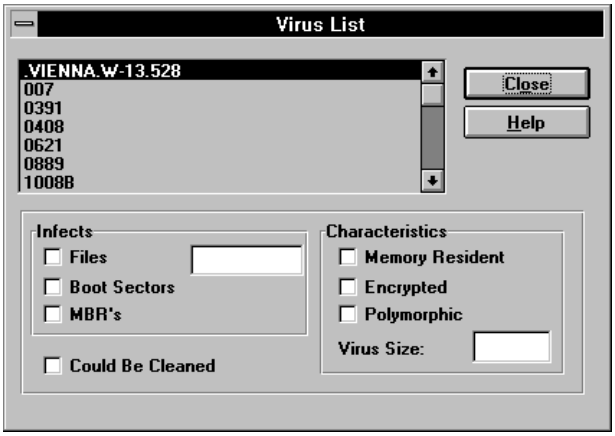


Figure 4-21. Viewing the VIrus List.

Scroll through the list using the scroll bars and select a virus to learn more about it. To scroll quickly, type the first letter of the virus you want to find.

- **Infects** describes what the selected virus infects:
  - **Files**, if selected, indicates that the virus infects files. If the virus targets files with specific extensions or files of a specific type, the extensions appear to the right of the check box.
  - **Boot Sectors**, if selected, indicates that the virus infects the boot sector.
  - **MBRs**, if selected, indicates that the virus infects the master boot record.
  - **Could Be Cleaned**, if selected, indicates that the virus is not destructive (overwriting) during infection. Some virus information may not be complete. In this case the “Could Be Cleaned” box is checked by default.
- **Features** describes behaviors of the selected virus:

- **Memory Resident**, if selected, indicates that the virus is a memory resident program that, like a (TSR) or a device driver, remains active in memory while the computer is running.
- **Encrypted**, if selected, indicates that the virus attempts to evade detection by self-encrypting.
- **Polymorphic**, if selected, indicates that the virus attempts to evade detection by changing its internal structure or its encryption techniques.
- **Virus Size** describes the amount, in bytes, that the virus increases the size of a file it infects. The default size for a MBR or boot sector infecting virus is 512.

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.

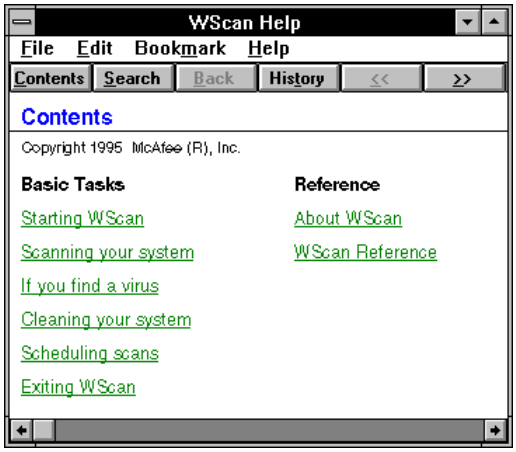


Figure 4-22. The Contents page of the on-line help.

- 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.

Chapter 5 Scan Technical Reference

Chapter 4 provided information about WScan, the graphic interface version of VirusScan. This chapter contains detailed information about VirusScan's command line anti-virus program, Scan.

Overview

NOTE: This chapter contains detailed information about the command line version of Scan. For a general overview of Scan and its features, refer to "Using Scan" in Chapter 3, "VirusScan Reference."

The Scan program detects, identifies and disinfects known DOS computer viruses. Scan checks memory as well as both the system and data areas of disks for virus infections. If Scan finds a known virus, in most cases it will eliminate the virus and fully restore infected programs or system areas to normal operation.

The command line options described here offer additional power and control over virus detection. They enable you to run Scan from batch or script files and are most useful in vulnerable environments and to network administrators and information services staff.

To obtain a list of all the viruses that Scan detects, run Scan with the /VIRLIST option.

In addition, Scan can also assign validation and recovery codes to files and use those codes to detect and treat infection by new and unknown viruses. If Scan has stored validation or recovery data for files, it may detect file changes and warn that infection by an unknown virus may have occurred. Scan can also use the recovery codes to remove new or unknown viruses and restore infected files.

This chapter describes how to use Scan from the DOS or OS/2 command prompt. For instructions on using WScan, refer to "Using WScan" in Chapter 3, "VirusScan Reference."

Scan runs on DOS, Windows and OS/2. The program files for command line versions are SCAN.EXE (DOS) and OS2SCAN.EXE (OS/2). This chapter describes them all.

NOTE: Because OS/2 operates in a protected mode environment, Scan for OS/2 does not check memory. To protect against viruses in OS/2 DOS and Win-OS/2 sessions, use the VShield (for DOS) virus prevention program.

System Requirements for Scan

Scan requires DOS 3.1 or later, Windows 3.1 or later, or IBM OS/2 Version 2.1 or later. Scan works with 3Com 3/Share and 3/Open, Artisoft LanTastic, AT&T StarLAN, Banyan VINES, DEC Pathworks, IBM LAN Server, Microsoft LAN Manager, Novell NetWare and any other IBMNET- or NETBIOS-compatible network operating systems. Contact McAfee or your local authorized agent if you do not see your network listed (refer to "McAfee Support" in Chapter 1).

Scan is designed to check for pre-existing infections of known and unknown viruses on diskettes, hard, CD-ROM and compressed (SuperStor, Stacker, DoubleSpace and so on) disks on both stand-alone and networked personal computers, as well as network file servers. If you have a Novell NetWare/386 V3.1X or 4.01 file server, you may want to use the NetShield™ virus prevention NetWare Loadable Module (NLM) in conjunction with Scan.

NOTE: To use Scan to clean (disinfect) virus-infected files, the CLEAN.DAT file must be present in the same subdirectory as Scan. 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 contact McAfee (refer to "McAfee Support" in Chapter 1).

Technical Overview

Known Virus Detection

Scan detects known viruses by searching the system for characteristics (sequences of code) unique to each computer virus and reporting their presence if found. For viruses that encrypt or cipher their code so that every infection is different, Scan uses detection algorithms that work by statistical analysis, heuristics and code disassembly.

New and Unknown Virus Detection

Scan can also check 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 Scan will report that the file may have become infected. Using Scan with the /CLEAN option and validation options (/AF, /AV, /CF, /CV, /RF and /RV) can use the validation and recovery data to restore infected files.

Note to Network Users

To use Scan on a network drive (or directory), you must be connected to that drive and have read access to it. Some command line options described in this chapter attempt to create, change and delete files. To use these options, you must have sufficient access rights. If you have questions about access rights, contact your network administrator.

Validating Scan

The Scan program in your VirusScan package is supplied on a write-protected diskette that should be secure from infection. We recommend that you update your copy of the VirusScan programs regularly. You can obtain an upgrade from several sources, as described in "Updating VirusScan Regularly" in Chapter 2, "Installation and Setup."

Before using a new version of Scan for the first time, verify that it has not been tampered with or infected by using the Validate program, as described in "Validate VirusScan" in Chapter 2, "Installation and Setup." If your new copy of Scan differs from the validation data in the on-line documentation file, it may have been damaged. Discard it and obtain a clean copy of Scan from a known source. Refer to "McAfee Support" in Chapter 1, or to Appendix A, "Downloading McAfee Software."

Scan performs an integrity test when run. This self-check allows Scan to determine if it has been modified. If Scan fails its integrity test, a warning message appears and Scan refuses to run and returns to the command line prompt. You must obtain an undamaged copy before continuing. Refer to "McAfee Support" in Chapter 1, "Introducing VirusScan."

NOTE: Scan may report a failed integrity check if you upgrade the VShield data files and attempt an immediate Scan. After upgrading VShield, turn off your computer and restart before attempting a scan. For more information, refer to "Upgrading VirusScan Regularly" in Chapter 2, "Installation and Setup."

Running Scan from the Command Line

Scan checks files and other areas of the system that can contain computer viruses. When a virus is found, Scan identifies the virus and the system area or file where it was found. By default, Scan examines only executable files (.EXE, .COM, .SYS, .BIN, .OVL and .DLL files). These are the files most likely to be infected with a virus. Use the /ALL option to scan all files on your system. Refer to "Scan Option Descriptions" later in this chapter for more information about the /ALL option.

NOTE: The list of extensions for standard executables has changed from previous versions of VirusScan. Refer to Appendix B for more information.

From DOS or OS/2, you can run Scan from the system prompt. (From OS/2, open the Command Prompts folder in the OS/2 system folder, then click the **OS/2 Full Screen** icon or the **OS/2 Window** icon to see the system prompt.)

Use the following syntax for Scan:

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

OS/2: Use `os2scan {drives} [options]`

- `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 back-slash (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`).

  NOTE: If you do not specify a drive to be scanned, Scan will search for a virus in memory, then return the message "No target for Scan was specified!"

- `[options]` indicates one or more of the Scan options as listed in the next section, "Scan Command Line Option Table."

Scan Command Line Option Table

DOS-OS/2 option	Description/Windows option
/? or /HELP	Display help screen (not available in Windows, use Help menu instead).
/ADL	Scan all local drives (including compressed, CD-ROM and PCMCIA drives, but not diskettes).
/ADN	Scan all network drives.

/AF {*filename*}	Store validation/recovery codes in *filename*.
/ALL	Scan all files, not just standard executables.
/APPEND	Append to, rather than overwrite, the file (used with /REPORT).
/AV	Add validation/recovery data to program files.
/BOOT	Scan boot sector and master boot record only.
/CF {*filename*}	Check validation/recovery codes in *filename*.
/CLEAN	Clean up infections in boot sector, master boot record and files when possible.
/CONTACTFILE {*filename*}	Display message stored in *filename* when a virus is found.
/CV	Check validation/recovery data in files.
/DEL	Overwrite and delete infected files.
/EXCLUDE {*filename*}	Exclude from scan any files listed in *filename* (with /AV).
/FAST	Speed up VirusScan's scanning; may detect fewer viruses.
/FREQUENCY {*hours*}	Set the time frequency with which to scan your system.
/HELP or /?	Display help screen (not available in Windows, use Help menu instead).
/LOAD {*filename*}	Use Scan settings stored in *filename*.
/LOCK	Halt the system when a file that is infected loads and attempts to execute.
/LOG	Save date and time VirusScan was last run in SCAN.LOG.
/MANY	Scan multiple diskettes.
/MEMEXCL {hhhh[-hhhh]}	Exclude memory area from scanning. (Default A000-FFFF, 0000=Scan all).
/MOVE {*directory*}	Move infected files to *directory*.
/NOBREAK	Disable CTRL-C / CTRL-BREAK during scans.
/NOCOMP	Skip checking compressed executables created with the LZEXE or PKLITE file compression programs.
/NODDA	No direct disk access.
/NOEMS	Do not use expanded memory (EMS) for data.
/NOEXPIRE	Disable data files expiration data notice.
/NOMEM	Skip memory checking (not applicable to OS/2).
/PAUSE	Enable screen pause.
/PLAD	Preserve last access dates on Novell drives.
/REPORT {*filename*}	Create report of infected files found during scan in *filename*.

/RF {*filename*}	Remove validation/recovery codes in *filename*.
/RPTALL	Add list of files scanned to the report file (used with /REPORT).
/RPTCOR	Add list of corrupted files to the report file (used with /REPORT).
/RPTERR	Add list of system errors to the report file (used with /REPORT).
/RPTMOD	Add list of modified files to the report file (used with /REPORT).
/RV	Remove validation/recovery data from files.
/SHOWLOG	Display information in SCAN.LOG.
/SUB	Scan subdirectories inside a directory.
/VIRLIST	Display list of viruses detected by VirusScan.

Scan Command Line Options

This section describes each Scan option in detail.

/? or /HELP

Display list of Scan options.

Does not scan. Instead, displays a list of Scan command line options with a brief description of each. No scanning is performed when these options are specified. Use either of these options alone on the command line.

/ADL

Scan all local drives (including compressed, CD-ROM and PCMCIA drives, but not diskettes).

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

/ADN

Scan all network drives.

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

/AF {*filename*}

Store validation/recovery codes in file.

Helps you detect and recover from new or unknown viruses. /AF logs validation and recovery data for executable files, the boot sector and master boot record on a hard disk or diskette, in the file you specify. The log file is about 95 bytes per file validated. You must specify a *filename*, which can include the target drive and directory (such as D:\VSVALID\VALCODES.VSC). If the target path is a network drive, you must have rights to create and delete files on that drive. If *filename* exists, Scan updates it. /AF adds about 300% more time to scanning.

To recover from a virus using the /AF information, use the /CF and /CLEAN options together in the same command line. Using any of the /AF, / CF or /RF options together in the same command line returns an error.

NOTE: /AF performs the same function as /AV, but stores its data in a separate file rather than changing the executable files themselves. For more information, refer to "Detecting New and Unknown Viruses" in Chapter 7, "Tips and Troubleshooting."

The /AV option does not store any information about the master boot record or boot sector of the drive being scanned.

/ALL

Check all files, not just standard executable files

Increases system security by performing a more thorough scan. Otherwise, Scan checks only standard executable files (with .COM, .EXE, .SYS, .BIN, .OVL and .DLL extensions), which are the files most likely to be infected by a virus. If /ALL is specified, Scan checks all files on the specified drive, which increases Scan's ability to detect viruses in overlay files but substantially increases the scanning time required. Use this option if you have found a virus or suspect one.

NOTE: The list of extensions for standard executables has changed from previous releases of VirusScan.

/APPEND

Append to the report file.

Used in conjunction with /REPORT, appends the report message text to the specified report file, if it exists. Otherwise, the /REPORT option overwrites the specified report file, if it exists.

/AV

Add validation/recovery data to files.

Helps you detect and recover from new or unknown viruses. /AV adds recovery and validation data to each standard executable file (.EXE, .COM, .SYS, .BIN, .OVL and .DLL), increasing the size of each file by 98 bytes. To update files on a shared network drive, you must have update access rights. The /AV option adds about 100% more time to scanning.

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

NOTE: The /AV option does not store any information about the master boot record or boot sector of the drive being scanned.

/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.

/CF {*filename*}

Check validation/recovery codes in file.

Helps you detect new or unknown viruses. Checks validation data stored by the /AF option in filename. If a file or system area has changed, Scan reports that a viral infection may have occurred. The /CF option adds about 250% more time to scanning. For more information, refer to “Detecting New and Unknown Viruses” in Chapter 7, “Tips and Troubleshooting.” You can use /CF and /CLEAN in the same command line to check validation/ recovery codes and remove any viruses found. Using any of the /AF, /CF or /RF options together in a command line returns an error.

NOTE: 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.

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.

/CLEAN

Remove viruses from boot sector, master boot record and infected files.

Attempts to restore the boot sector, if infected, and any infected files. Usually, between 10% and 20% of all viruses are not removable; they damage the file they infect beyond repair. If the infected file resides on a network drive, you must have rights to modify files on that drive to clean it. If it cannot restore a file, a message is displayed that identifies the unrecoverable file. To use /CLEAN, the CLEAN.DAT file must reside in the Scan directory. For more information, refer to "Cleaning Viruses" later in this chapter.

Use /CLEAN instead of /DEL when you want to restore infected files, not just delete or overwrite them. The /CLEAN option can remove master boot record and boot sector viruses, but the /DEL option cannot. If you use /CLEAN and /DEL in the same command line, Scan first attempts to disinfect an infected file, then deletes it only if it cannot be repaired. Similarly, if you use /CLEAN and /MOVE in the same command line, Scan first attempts to clean an infected file, then moves it to the specified subdirectory if the file is unrecoverable.

You can use /CLEAN and /CF or /CV in the same command line to check validation/recovery codes and remove any viruses found. We strongly recommend that you get experienced help in dealing with viruses if you are unfamiliar with anti-virus software and methods. This is especially true for "critical" viruses and master boot record or boot sector infections, because improper removal of these viruses can result in the loss of all data on the infected disks.

NOTE: When scanning a network drive using /CLEAN, you must have sufficient rights to update files on that drive.

/CONTACTFILE {*filename*}

Display a text message (saved in {filename} when a virus is detected.

/CONTACTFILE identifies a file that contains the message string to display when a virus is found. This option is especially useful in network environments, because you can easily maintain the message text in a central file rather on each workstation. Any character is valid except a backslash ("\"). Messages that begin with a slash ("/") or a hyphen ("-") should be placed in quotation marks.

/CV

Check validation/recovery data in files.

Helps you detect new or unknown viruses. Checks validation data added by the /AV option. If a file is modified, Scan reports that a viral infection may have occurred. The /CV option adds about 50% more time to scanning. You can use /CLEAN and /CV in the same command line to check validation/recovery codes and restore infected files. Using any of the /AV, /CV or /RV options together in the same command line returns an error.

For more information, refer to "Detecting New and Unknown Viruses" in Chapter 7, "Tips and Troubleshooting."

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

/DEL

Overwrite and delete infected files.

Deletes and overwrites each infected file. Files erased by the /DEL option cannot be recovered (you should generate a report so that you can restore them from backups). Instead of using /DEL alone, we recommend using it in combination with the /CLEAN option to attempt to disinfect an infected file first, then delete it only if the file is unrecoverable. The /CLEAN option can remove master boot record and boot sector viruses, but the /DEL option cannot.

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

This option has no effect if the Master Boot Record or Boot Sector is infected, since these are not actually files.

/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, refer to "Creating an Exception List File for the /EXCLUDE Option" in this chapter.

/FAST

Speed up Scan's scanning.

Reduces scanning time by about 15%. Using the /FAST option, Scan examines a smaller portion of each file for viruses, although it examines more files overall. Using /FAST might miss some infections found in a more comprehensive (but slower) scan. Do not use this option if you have found a virus or suspect one.

/FREQUENCY {*hours*}

Set the time frequency with which to scan your system.

In environments where the risk of viral infection is very low, use this option to prevent unnecessary or too-frequent scans. The lower the number of *hours* specified, the greater the scan frequency and the greater your protection against infection.

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 it, Scan stores the date and time that 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 of *hours*. If *hours* exceeds the elapsed time, Scan exits without scanning the system. Otherwise, Scan proceeds as usual to scan the system and, when finished, updates MCAFEE.FRC with the system date and time.

/HELP or /?

Display list of Scan options.

Does not scan. Instead, displays a list of Scan command line options with a brief description of each. No scanning is performed when these options are specified. Use either of these options alone on the command line.

/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 those settings from that file.

Use a text editor to create the file. You can put all 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. Use the /LOAD {filename} command line option to

perform a scan using the information saved in this file. For example, if you have created a configuration file called FLOPPY.CFG:

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

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

/LOCK

Halts the system to stop further infection if Scan finds a virus. /LOCK is appropriate 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.

/MANY

Scan multiple diskettes.

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

The Scan program files should be on a drive that is not 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 (i.e. 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.

The default for this command is A000-FFFF.

If you specify 0000, Scan not check memory during scans.

/MOVE {*directory*}

Move infected files to specified directory.

Moves all infected files found during a scan to the specified directory. If you use /MOVE in conjunction with /CLEAN, Scan attempts to restore an infected file first, then moves it to the specified directory 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 if the Master Boot Record or Boot Sector is infected, since these are not actually files.

You can also use the /MOVE {directory} [*.ext] command to rename the extensions of infected files to prevent users from inadvertently running them. The "*" and "." must be used, "ext" represents the three-letter extension you want the moved file to have. You may use the ? wildcard to preserve the original letters. For example,

```
SCAN /ADL /ALL /MOVE c:\mcafee\infected *.x??
```

Scan will move any infected files to the subdirectory "infected" in the directory "mcafee" on the C: drive. The first letter of any filename extensions moved will be changed to an "x", so if the file SYSTEM.INI is moved to the infected directory, the new filename will be SYSTEM.XNI.

For more information, refer to the README.1ST file.

/NOBREAK

Disable CTRL-C / CTRL-BREAK during Scan.

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.

/NOCOMP

Skip checking compressed executable files.

Reduces scanning time when a full scan is not needed. Otherwise, by default, Scan checks inside executable, or self-decompressing, files that have been created using the 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. If you use /NOCOMP, Scan does not check inside compressed files for viruses, although it can check for modifications to those files if they have been validated using validation/recovery codes.

NOTE: Scan does not check PKZIP files.

/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, Win95 and Windows for Workgroups with 32-bit disk access enabled.

/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

Disable 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 VirusScan Regularly” in Chapter 2, “Installation and Setup.”

/NOMEM

Skip memory checking.

Reduces scan time by omitting all memory checks for viruses. Use /NOMEM only when you are absolutely certain that your system is virus-free.

By default, Scan checks system memory for all critical known computer viruses that can inhabit memory. In addition to main memory from 0Kb to 640Kb, Scan checks system memory from 640Kb to 1088Kb that can be used by computer viruses on 286 and later systems. Memory above 1088Kb is not addressed directly by the processor and is not presently susceptible to viruses.

NOTE: /NOMEM is not applicable to OS/2 or WScan.

/PAUSE

Enable screen pause.

If you specify /PAUSE, the More? (H = Help) prompt appears when Scan fills up a screen with messages, such as when using the /SHOWLOG or /VIRLIST options. Otherwise, by default, Scan fills and scrolls a screen continuously without stopping, which allows Scan to run on PCs with many drives or that have severe infections without requiring you to attend. We recommend that you omit /PAUSE when keeping a record of Scan's messages using the report options (/ REPORT, /RPTCOR, /RPTMOD and /RPTERR).

/PLAD

Preserve last access dates (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 the result of scanning.

/REPORT {*filename*}

Create report of infected files and system errors.

Saves the output of Scan to filename in ASCII text file format. If *filename* exists, /REPORT erases and replaces it (or, if you use /APPEND, adds the report information to the end of the existing file). You can include the destination drive and directory (such as **`D:\VSREPRT\ALL.TXT`**), but if the destination is a network drive, you must have rights to create and delete files on that drive. You can also use /RPTALL, /RPTCOR, /RPTMOD and /RPTERR to add scanned files, corrupted files, modified files and system errors to the report.

For more information about report files, refer to "Configuring Reporting Options" later in this chapter.

/RF {*filename*}

Remove validation/recovery codes in file.

Removes recovery and validation data from *filename* created by the /AF option. If *filename* resides on a shared network drive, you must be able to delete files on that

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

The validation file can be deleted through DOS instead of using this option. Refer to "Updating Validation Codes" later in this chapter for more information.

/RPTALL

Add all scanned files to Scan report.

Used with /REPORT, adds the names of all files scanned to the report file.

/RPTCOR

Add corrupted files to Scan report.

Used in conjunction with /REPORT, adds the names of corrupted files to the report file. A corrupted file is a file that a virus has damaged beyond repair, which typically occurs in 10% to 20% of all viral infections. You can use /RPTCOR with /RPTMOD and /RPTERR on the same command line.

NOTE: 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 errors to Scan report.

Used in conjunction with /REPORT, adds system errors to the report file. System errors include problems reading or writing to a diskette or hard disk, file system or network problems, problems creating reports and other system-related problems. You can use /RPTERR with /RPTCOR and /RPTMOD on the same command line.

/RPTMOD

Add modified files to the Scan report.

Used in conjunction with /REPORT, adds the names of modified files to the report file. Scan identifies modified files when the validation/recovery codes do not match (using the /CF or /CV options). You can use /RPTMOD with /RPTCOR and /RPTERR on the same command line.

/RV

Remove validation/recovery from files.

Removes validation and recovery data from files validated with the /AV option, along with the SCAN.LOG file on the specified drive. To update files on a shared network drive, you must have access rights to update them. Using any of the /AV, /CV or /RV options together in the same command line returns an error.

/SHOWLOG

Update and display the contents of SCAN.LOG.

Stores the time and date Scan is being run by updating or creating a file called SCAN.LOG in the current directory and shows you the date and time of previous scans that have been recorded in the SCAN.LOG file using the /LOG switch. The SCAN.LOG file contains text and some special formatting. To pause when the screen fills with messages, specify the /PAUSE option.

/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. Do not use /SUB if you are scanning an entire drive.

/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, specify the /PAUSE option. Use /VIRLIST alone or with /PAUSE on the command line.

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

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

NOTE: VirusScan can detect many viruses. This file is over 50 pages in length.

Saving and Using Default Settings

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

Creating a Configuration File

Use the following procedure to create a configuration file:

1. Using a word processor or text editor such as Windows Write, create a new file.
2. Put all 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:\user /sub /report d:\virus.rpt /rpterr /append
   ```

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

   ```
   c:\user
   /sub
   /report
   d:\virus.rpt
   /rpterr
   /append
   ```

   In both examples, VirusScan will scan the directory “USER” and all its associated subdirectories on the C drive. A report file, called “VIRUS.RPT,” will be saved to the D drive. This report file will also include any errors encountered during the Scan. If “VIRUS.RPT” already exists, VirusScan will add the new information to the end of the existing file.
3. Save the file as “DEFAULT.CFG” in the same directory that Scan is stored in.

   The configuration file must be saved as an ASCII or DOS Text file. If you use a word processor to create it, be sure to save the file as ASCII or DOS Text.

Using the Configuration File

After creating the configuration file, Scan will default to the selected drive(s) and command line options specified in the DEFAULT.CFG file. For example:

1. Create the configuration file using the above procedure, ensure that it is saved in the same directory as Scan and that it is saved as an ASCII or DOS Text file.

2. At the system prompt, type

   scan

3. Scan will initiate a virus check using the drives and command line options specified in the file, DEFAULT.CFG. Using the above example, VirusScan will scan the directory "USER" and all its associated subdirectories on the C drive. A report file, called "VIRUS.RPT," will be saved to the D drive. This report file will also include any errors encountered during the Scan. If "VIRUS.RPT" already exists, VirusScan will add the new information to the end of the existing file.

Cleaning Viruses

Although /CLEAN removes many viruses and restores normal operation, viruses can be harmful and insidious and no anti-virus program can undo all their damage. Usually, between 10% and 20% of all viruses corrupt the files they infect, making them unrecoverable. If the file is infected with an uncommon virus that /CLEAN cannot remove, Scan notifies you and identifies the filename. Note this filename so that you know what to restore from a backup diskette or tape. If you use both the /CLEAN and the /DEL options, Scan will first attempt to repair an infected file and, if the file is damaged beyond repair, Scan will delete it. Deleted files are not recoverable except from backups.

WARNING: Do not attempt to remove a virus using DOS commands (i.e. FDISK, FORMAT, DEBUG). **Improper removal of viruses can result in the loss of all data and the use of infected disks.** If you are unfamiliar with viruses and virus methodology, you should get experienced help before using DOS commands to remove these viruses. For assistance, contact McAfee technical support or your local authorized agent (refer to "McAfee Support" in Chapter 1, "Introducing VirusScan"). For more information, refer to "Using DOS Commands to Remove a Virus" in Chapter 7, "Tips and Troubleshooting."

Basic Principles to Minimize Damage

These considerations lead to the three important principles:

1. **Before running Scan with the /CLEAN option, back up all of your programs and data.**

   Of course, this works best if you back up your files regularly, so that you can restore your files from a backup made before your system was infected. But even a backup from an infected system can be useful for restoring data, because

most viruses do not corrupt data. If a program no longer runs after being cleaned, replace it from the original diskettes or from a virus-free backup.

When disinfecting an infected system, it is important to start from a “sterile field,” as described in Chapter 2, “Installation and Setup.”

2. **Before running Scan with the /CLEAN option for DOS, restart your computer from a clean, write-protected diskette; before running it for OS/2, close all DOS and Win-OS/2 sessions.**

   Preferably, use the clean anti-virus start-up diskette you created in “Making a Clean Start-Up Diskette” in Chapter 2, “Installation and Setup.” And, because running any program can spread the infection:

3. **Do not run any programs, including Windows, before running Scan /CLEAN.**

   Run Scan /CLEAN from DOS instead of Windows. Exit completely from Windows. Do not run Scan /CLEAN from within a DOS window.

For more information, refer to Chapter 7, “Tips and Troubleshooting.”

Running Scan to Clean Up Infections

Before running Scan to clean up infections:

1. Clear the virus from system memory and prevent reinfection.

   With DOS or Windows, turn off your PC, then restart from a clean start-up diskette, preferably the anti-virus diskette you prepared in “Making a Clean Start-Up Diskette” in Chapter 2, “Installation and Setup.” If you do not have a clean start-up diskette, get one from someone else who has the same version of DOS; do not use a diskette that might be infected.

   With OS/2, close all DOS and Win-OS/2 sessions.

   With an OS/2 dual-boot system infected by a boot sector virus (like Form, or others identified by Scan), boot (start up) OS/2 first, delete the BOOT.DOS file from the \OS2 directory and then boot DOS to create a new, virus-free DOS boot sector file.

2. Run the Scan program to locate and identify the infections.
3. Back up the files on the infected disks (be sure not to overwrite any previous back-ups).
4. Repeat Step 1.
5. Run the Scan program with the /CLEAN option to remove infections.

Do not run any programs, including Windows, before running Scan /CLEAN. If you have Windows, run Scan /CLEAN from DOS.

When disinfecting a hard disk, *always* run Scan /CLEAN from a write-protected diskette to prevent infection of the Scan program. When disinfecting diskettes, make sure there is no active virus in memory before running Scan from your hard disk.

Successful and Unsuccessful Results

Scan /CLEAN reports the results of its attempt to remove the virus from each infected file. If a file has several infections, it will report on each.

If Viruses Were Not Removed

If Scan cannot remove a virus, a message similar to the following one is displayed:

```
Virus cannot be safely removed from this file.
```

Make sure to take note of the file name, because you will need to restore it from backups. If you have any questions about how to proceed, contact McAfee technical support or your local authorized agent (refer to “McAfee Support” in Chapter 1).

If Viruses Were Removed

If Scan /CLEAN has successfully removed all the viruses, turn your computer off again and restart from the system hard disk or diskette. Scan your hard disks again to make sure they are virus-free. If you suspect that your system was infected from a diskette, run Scan from your hard disk to examine and disinfect the diskettes you use.

Examples

These examples show different option settings.

OS/2: Remember to use **OS2SCAN** instead of **SCAN**.

- To scan all executable files on drive C:

  scan c:

- Scan all standard executable files on drive F, a network drive.

  scan f:

- Scan all executable files on drive A, a floppy drive. Scan will check the diskette in drive A, then prompt the user to insert additional disks to continue checking.

  ```
  scan a: /many
  ```

- Scan all local and network drives (including compressed, CD-ROM and PCMCIA drives, but not diskettes).

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

- Scan all files on drives F, G and H and delete any infected files found (we recommend using /CLEAN first to attempt to remove viruses before deleting files).

  ```
  scan f: g: h: /del /all
  ```

- Scan for viruses in all files and add validation codes to executable files on drives C, D and E.

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

- Scan for viruses on network drive M: and create a log file of infections, corruptions and errors in the file INFECTN.RPT on drive D. If D:/INFECTN.RPT already exists, Scan will append the new information to the existing report file.

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

- Scan all files in the directories USER\CRAIG, USER\CHRIS and USER\SCOTT, including their associated sub-directories, on drive E.

  ```
  scan e:\user\craig e:\user\chris e:\user\scott /sub /all
  ```

- Quickly scan drives C, D and E and report any executable files that have associated validation codes and have been modified.

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

- Scan a single file.

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

- Scan drives C and D and remove infections.

  ```
  scan c: d: /clean
  ```

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 ERRORLEVELs:

ERRORLEVEL	Description
0	No errors occurred and 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 occurred.
7	An error in accessing an international message file (MCAFEE.MSG).
8	A file required to run VirusScan, such as SCAN.DAT, is missing.
9	Incompatible or unrecognized option(s) or option argument(s) were specified in the command line.
10	A virus was found in memory.
11	An internal program error occurred.
12	An error occurred while attempting to remove a virus, such as no CLEAN.DAT file found, or Scan 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).
20	/FREQUENCY option in use.
21-99	Reserved.
100+	Operating system error; Scan adds 100 to the original error number.
102	CTRL+C or CTRL-BREAK was used to interrupt the Scan. (You can disable interrupts with the /NOBREAK command line option.)

Supplemental Notes

The following information will help you use Scan more effectively. For more information about using Scan and VirusScan, refer to Chapter 7, “Tips and Troubleshooting.”

Configuring Reporting Options

The /REPORT {filename} command line option can be used to create an ASCII text file, called {filename}, that we recommend you use to create an “audit trail” of scans and scanning results. If {filename} already exists, /REPORT erases and replaces it (or, if you use /APPEND, adds the report information to the end of the existing file). You can include the destination drive and directory (such as **`D:\VSREPRT\ALL.TXT`**), but if the destination is a network drive, you must have rights to create and delete files on that drive. Other options for /REPORT include /RPTALL, /RPTCOR, /RPTMOD and /RPTERR.

- **/RPTALL:** Add the names of all files scanned to the report file.
- **/RPTCOR:** Add the names of corrupted files (files that cannot be repaired with the /CLEAN option) to the report file. We recommend you use this setting if you are using the /DEL option so you can later replace deleted files with backups.
- **/RPTERR:** Add system errors to the report file. For more information, refer to “Error Levels” earlier in this chapter.
- **/RPTMOD:** Adds the names of modified files to the report file. Use this option when you are using the validation/recovery options (/CF or /CV).

You can use all these reporting options on the same command line. For example,

```
scan c: /report c:\infected.txt /append /rptall /rptcor
/rpterr /rptmod
```

The above example would scan the C: drive and save the report file as “INFECTED.TXT” on the C: drive. The report file would include the names of all files scanned, all corrupted files, all modified files and any system errors. If this file already exists, Scan will add the new information to the existing file.

Updating Validation Codes

If you install any new software or programs on your system, including a new version of DOS and are running Scan or VShield with the /CF (preferred) or /CV validation options, you need to install validation codes for the new files with Scan’s /AF (preferred) or /AV options.

The quickest way to update the validation codes is to remove all validation codes from the hard disk and then add them back. In other words, first run Scan with the /RF or /RV option, then run it again with the /AF or /AV option.

You can also remove validation codes added with the /AF command line option by deleting the validation file. Scan your system to check for viruses, delete the validation file, then run Scan with the /AF command line option to create a new validation file with current information.

Creating an Exception List File for the /EXCLUDE Option

If you set up validation codes using Scan's /AV or /AF options, subsequent scans using the /CV or /CF options will detect changes in executable files. This can generate 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; some of these files are listed below). Therefore, use the /EXCLUDE option in conjunction with /AV to identify such files and exclude them from the validation.

The exception list is an ASCII or DOS text file. If you use a word processor to create it, be sure to save the file as ASCII or DOS Text. Each line in the file contains the path and file name of one file that should not be validated. Here is an example:

```
c:\clipper\bin\clipper.exe
c:\123\123.com
c:\fox\foxprolx.exe
c:\dos\setver.exe
c:\pkware\pklite.exe
c:\pkware\pkzip.exe
c:\pkware\pkunzip.exe
c:\semware\q.exe
c:\swapvol.com
c:\wordstar\ws.exe
```

NOTE: Although the /AF option does not add code to any files other than the one specified, using /CF will report changes in self-modifying files as possible infections. Refer to the /RF option in "Scan Option Descriptions" earlier in this chapter for more information.

Chapter 6 VShield Technical Reference

Chapter 5 provided information about Scan, the command line version of VirusScan. This chapter contains detailed information about VirusScan's memory-resident program, VShield.

Overview

NOTE: This chapter contains detailed information about the memory-resident anti-virus program, VShield. For a general overview of Scan and its features, refer to "Using VShield" in Chapter 3, "VirusScan Reference."

VirusScan's VShield™ is a memory-resident program that helps to prevent virus infection. It complements the Scan virus detection program as part of your computer security plan. While Scan lets you check areas on disks for viruses, the VShield program checks these areas automatically as they load into your computer's memory. This ensures that you do not "catch" any new viruses while you are working on your computer.

VShield does this by remaining in memory and:

- Checking master boot records, boot sectors, system files and itself for viruses when you turn on or reset ([CTRL]+[ALT]+[DEL]) your machine.
- 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).

Follow the instructions in Chapter 2, "Installation and Setup," to install VShield. The installation program automatically modifies your AUTOEXEC.BAT file so that VShield loads into memory every time you turn on your computer. If you installed downloaded files according to the instructions in Appendix A, "Downloading McAfee Software," you updated AUTOEXEC.BAT manually.

If VShield finds a virus, you will hear three beeps and a message similar to the following is displayed:

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

If that happens, do not panic. Refer to “Using Scan” in Chapter 3, “VirusScan Reference,” to find out how to use the Scan program to get rid of the virus. If you need additional help, contact McAfee (refer to “McAfee Support” in Chapter 1).

NOTE: There is one way to infect your computer that VShield cannot prevent — only you can. Never accidentally start your computer from an unknown diskette. That’s how 80% of all viruses are passed! VShield checks diskettes if you warm boot, but cannot check them when you cold boot. Always make sure your diskette drives are empty before you turn your computer on.

VShield runs under DOS, Windows and OS/2 Virtual DOS Machine and WIN-OS/2 sessions. The program file is VSHIELD.EXE. The file called VSHLDWIN.EXE allows VShield to display messages from within Windows. The install program adds this program to your WIN.INI file automatically, or you update your WIN.INI file manually (if you installed downloaded software according to the instructions in Appendix A). If you need to conserve memory on your system, you can use VShieldCRC, a version of VShield that offers fewer protection options but requires less memory. The program file is VSHLDCRC.EXE.

A companion program called CheckVShield checks whether either VShield or VShieldCRC is loaded in memory. The program file is CHKVSHLD.EXE. CheckVShield is especially useful for network administrators who want to ensure that everyone who logs on to the network is running VShield. All of these related programs are included in your VirusScan diskettes and described in this chapter.

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. By default, VShield tries to conserve as much conventional memory as possible.

If you have only 640 Kb or less memory in your system, VShield requires minimal conventional memory. By using the /SWAP option, you can reduce its memory requirement to only 8 Kb of conventional memory, although this will decrease VShield’s speed and, possibly, its effectiveness.

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 or VShieldCRC use no conventional memory.

After VShield loads, a message is displayed that describes where VShield loaded into memory and how much memory it uses. You can control how VShield loads by

using the /NOUMB, /NOEMS and /NOXMS options, as described later in this chapter.

NOTE: VShield might require slightly more memory as the SCAN.DAT and NAMES.DAT files grow (through updates) to include more viruses. For more information about updating VirusScan, refer to "Updating VirusScan Regularly" in Chapter 2, "Installation and Setup."

VShield adds a small amount of time to program loads and reboots. Performance will vary, depending on your system. The /SWAP option adds more time, because VShield must reload from disk to check files. VShieldCRC adds an average of one second to each program load.

Once programs have been loaded, VShield does not degrade the performance of your system. Programs that load other files may run more slowly when you use the /FILEACCESS or /ANYACCESS options, because these options cause VShield to scan files whenever they are accessed, not just when they are executed.

Four Levels of Protection

You can think of VShield as providing four levels of protection. You can use VShield's options to customize it for the level of protection you need. Level II meets the protection needs of most systems.

- **Level I protection** is appropriate for users who have very little memory available on their systems. It provides only minimal protection.

  For Level I protection, first use Scan with the /AF or /AV option to add validation codes. Then, install VShieldCRC instead of VShield. VShieldCRC can inform you that a file has not been certified, a file has been modified, a file size has changed, or a file has not been added to the validation file. VShieldCRC will not prevent infection, nor will it tell you when you have a known virus. Use Scan instead to detect viruses, as described in "Using Scan" in Chapter 3, "VirusScan Reference." Refer to "Using VShieldCRC" later in this chapter for instructions.

- **Level II protection** is appropriate for most users. It will protect you from most viruses whether you have run Scan or not.

  For Level II protection, install VShield according to "Running VShield" later in this chapter. When loading, VShield checks memory automatically for viruses. Once resident in memory, VShield checks master boot records, boot sectors and program files (when executed) for virus signatures.

- **Level III protection** is appropriate for computers that are used by many people, as in an open-use computer lab, or onto which you frequently load files from

public sources. Level III protection checks for both validation codes and virus signatures, incorporating both Level I and Level II protection.

For Level III protection, first use Scan with the /AF {*filename*} option, then use VShield with the /CF {*filename*} option. The /AF option logs recovery and validation data for program files (but not the boot sector or the master boot record) to a file you specify. The /CF option tells VShield to check against that log. Refer to Chapter 5, "Scan Technical Reference," for instructions.

- **Level IV protection** is for environments where security is extremely important and new software is seldom introduced. It combines Level III protection with access control, specifying that only programs known to be safe can be run.

  For Level IV protection, run VShield with the /CERTIFY option. Refer to the "VShield Option Descriptions" later in this chapter for details about /CERTIFY.

NOTE: VShield has many optional features that you might use at any protection level. Refer to the table "VShield option summary" later in this chapter to see these options.

Running VShield

VShield checks programs, the master boot record, boot sector, system files and itself for virus signatures, the pattern of code unique to each virus. If VShield finds an infection, it prevents programs from running. It also prevents warm boots ([CTRL]+[ALT]+[DEL]) from infected disks.

You can use options to control and fine-tune the scope, validation parameters and operation of the VShield's checks. To use VShield with options, use the following syntax:

`vshield [options]`

`[options]` indicates one or more options described in the table in the next section.

NOTE: *Do not enter the square braces*, which indicate that what is within them is optional.

Because systems and environments differ, VShield gives you a choice of options. Consider the mixture of safety, performance and maintenance that meets your needs, then choose the combination of options that works best.

When you run VShield for the first time, VShield uses the virus information contained in SCAN.DAT and NAMES.DAT to creates a new file, VSHIELD.DAT, in the program directory. The VSHIELD.DAT file contains virus information in a format that is optimized for VShield operation. Thereafter, when you install an

updated version of SCAN.DAT, VShield updates VSHIELD.DAT automatically with any new virus information it finds in SCAN.DAT.

DOS

If you followed the installation instructions in Chapter 2 (or Appendix A for downloaded files), VShield begins working for you as soon as you install it, protecting the "sterile field" that the installation procedure creates. VShield is automatically added to your AUTOEXEC.BAT file, so it is activated every time you turn on your computer.

The install program places VShield at the beginning and end of AUTOEXEC.BAT. You should verify this by inspecting your AUTOEXEC.BAT file after you install VShield.

To do so, use a text editor to examine your AUTOEXEC.BAT and follow these steps. If you need help with this procedure, refer to your DOS documentation or contact McAfee (refer to "McAfee Support" in Chapter 1).

1. Check the placement of the VShield command line in the AUTOEXEC.BAT file.
   - VShield must be run before any menu programs, such as Windows, MS-DOS's DOSSHELL or Norton Commander, or it will not be loaded.
   - If AUTOEXEC.BAT loads any network drivers, keyboard drivers, disk caching programs, drive compression programs, or custom disk drivers, VShield must be run both before and after them. These kinds of programs disable VShield. The second time VShield is loaded, use only the /RECONNECT option, as described later in this chapter.
2. If necessary, move the line that loads VShield.
3. Add the VShield options of your choice to the command line.

NOTE: If you are not sure whether VShield is in the right place, contact McAfee (refer to "McAfee Support" in Chapter 1).

Windows

Using the install program in Chapter 2, "Installation and Setup" (or the instructions in Appendix A for downloaded files), the VShield command line is added to your AUTOEXEC.BAT file and your WIN.INI file is modified to include VSHLDWIN.EXE (which allows VShield to display messages under Windows). However, you may need to change your Windows configuration for VShield to run properly.

To do so, follow these steps. If you need help with this procedure, refer to your Windows documentation, or you can contact McAfee (refer to "McAfee Support" in Chapter 1).

1. Follow the instructions for DOS users in the previous section.
2. Start Windows.
3. In the Control Panel, configure Windows to run in 386 enhanced mode.
4. Load Windows. The VShield icon is displayed on your desktop.

If VShield finds or suspects a virus, a warning message is displayed. Choose OK to close the message dialog.

Double-clicking the VShield icon just displays a message confirming whether VShield is loaded.

OS/2

Because OS/2 is a protected environment, you need VShield only during Virtual DOS Machine (VDM) and WIN-OS2 sessions. When you install it, VShield is added to AUTOEXEC.BAT, so it is activated every time you start a VDM or WIN-OS/2 session.

If your start-up batch file is not AUTOEXEC.BAT, edit your start-up batch file to include VShield. We recommend you add the following line to your start-up batch file:

```
vshield /fileaccess
```

NOTE: Refer to "/FILEACCESS," an option we recommend using with OS/2, later in this chapter.

Special Instructions for Network Administrators

You have many options for setting up VShield on a network. The table "Configuring VShield to Your Network" later in this chapter lists options that apply in network environments. If you need assistance in choosing the best configuration for your network, contact McAfee (refer to "McAfee Support" in Chapter 1).

If you run VShield from a network drive, flag VSHIELD.EXE as EXECUTE ONLY, READ ONLY and SHAREABLE.

If you run VShield from clients' local drives (optimal):

- Edit all clients' AUTOEXEC.BAT files to load VShield, with the options that are appropriate for your environment, before any other drivers are loaded.

- Add VShield with the /RECONNECT option to the AUTOEXEC.BAT or the network login script, after the network drivers are loaded. Refer to /RECONNECT, later in this chapter, for more information.

Run CheckVShield from the login script. CheckVShield returns a DOS ERRORLEVEL that you can use in batch files to check and update VShield. For an example of using CheckVShield, refer to "Sample NetWare login script and .BAT file" later in this chapter.

VShield Option Table

DOS-OS/2 option	Description
/? or /HELP	Display a list of valid VShield command line options.
/ANYACCESS	Scan the boot sector whenever a diskette is accessed (read and write); scan executables; scan any newly created files.
/BOOTACCESS	Scan the boot sector for viruses whenever a diskette is accessed (including read and write).
/CERTIFY	Prevent files without validation codes from running.
/CF {*filename*}	Check for viruses using recovery and validation data stored by Scan /AF in the specified *filename*.
/CONTACT {*message*}	Display specified *message* when a virus is found.
/CONTACTFILE {*filename*}	Display message stored in *filename* when a virus is found.
/CV	Check validation codes added to files by Scan.
/EXCLUDE {*filename*}	Do not check files listed in *filename* for validation codes (/CV option).
/FILEACCESS	Scan executable files when they are accessed on a diskette, but do not check the boot sector.
/IGNORE {*drive(s)*}	Do not check programs loaded from the specified *drive(s)*.
/LOCK	Halt the system when a file that is infected loads and attempts to execute.
/NOEMS	Prevent VShield from loading into expanded memory (EMS).
/NOMEM	Do not check memory for viruses.
/NOREMOVE	Prevent VShield from being removed from memory with the /REMOVE switch.
/NOUMB	Prevent VShield from loading into upper memory blocks (UMB).
/NOWARMBOOT	Do not check the diskette boot sector for viruses during warm boot ([CTRL]+[ALT]+[DEL]).
/NOXMS	Prevent VShield from using extended memory (XMS) when it loads.
/ONLY {*drive(s)*}	Check programs loaded only from the specified *drive(s)*.

/POLY	Check for polymorphic viruses.
/RECONNECT	Restore VShield after certain drivers or TSRs have disabled it.
/REMOVE	Unload VShield from memory.
/SAVE	Save the command line options to the VSHIELD.INI file.
/SWAP [*pathname*]	Load VShield kernel (8Kb) only; swap the rest to*pathname*.
/XMSDATA	Loads VShield data files into XMS memory.

VShield Option Descriptions

/? or /HELP

Use this option to display a brief description of valid VShield command line options.

/ANYACCESS

Checks the diskette boot sector and all files for viruses whenever a diskette is accessed by a read or write operation, such as a DIR or COPY command and when a program on the 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 returns an error message.

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

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

/BOOTACCESS

Checks the boot sector of a diskette for viruses whenever a diskette is accessed by a read or write operation, such as the DIR or copy commands. By default, VShield checks programs when they execute, but does not check the boot sector of the

diskette for viruses. Using /BOOTACCESS with /ANYACCESS in the same command line returns an error message.

NOTES: 1) The /BOOTACCESS switch is not recommended for use with DOS and WIN-OS/2 sessions under OS/2 due to certain low-level operating system incompatibilities between OS/2 and DOS. Use the /FILEACCESS switch instead.

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

/CERTIFY

Prevents programs from running if they do not have Scan validation codes. Use it in high-security environments to prevent clients from running programs that have not been scanned. To use /CERTIFY, first run Scan with the /AF or /AV option, as described in Chapter 5, “Scan Technical Reference.” Then, use VShield with the /CERTIFY option and either the /CF or /CV option (either is required), such as:

```
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 create an exception list of files to exclude from validation. For instructions, refer to “Creating an Exception List for the /EXCLUDE Option” later in this chapter.

/CF {*filename*}

Checks validation data stored by Scan’s /AF {*filename*} option, where *filename* is the name of the validation data file created by Scan. If a file or system area has changed, VShield reports that a viral infection may have occurred. In this example:

```
vshield /cf c:\mcafee\valcodes.dat /noems
```

VShield looks in the VALCODES.DAT file for validation data. For instructions on using Scan /AF to add validation codes, refer to “Scan Option Descriptions,” in Chapter 5, “Scan Technical Reference,” and “Detecting New and Unknown Viruses” in Chapter 7, “Tips and Troubleshooting.’

/CONTACT {*message*}

Displays a custom message when a virus is found. This message is displayed in addition to all other VShield messages. Use /CONTACT to let network users know what to do if VShield finds a virus. 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 Dave at x3049!"
```

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*}

An alternative to the /CONTACT option, /CONTACTFILE identifies a file that contains the message string to display when a virus is found. This option is especially useful in network environments, because you can easily maintain the message text in a central file rather than changing the command line in the AUTOEXEC.BAT file on each workstation.

If your message is 50 characters or fewer, you can use /CONTACT instead. Using /CONTACT and /CONTACTFILE in the same command line returns an error message.

/CV

Checks validation codes added by Scan with the /AV option. If a file has changed, VShield reports that the file has been modified and a viral infection may have occurred. You can specify the /EXCLUDE option to exclude a list of files from validation checking. For instructions on using Scan to add validation codes, refer to "Scan Option Descriptions" in Chapter 5, "Scan Technical Reference," and "Detecting New and Unknown Viruses" in Chapter 7, "Tips and Troubleshooting."

/EXCLUDE {*filename*}

Excludes files listed in filename from validation when using /CV. For more information on excluding files from validation, refer to "Creating an Exception List for the /EXCLUDE Option" later in this chapter.

/FILEACCESS

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 or write operation. Using /ANYACCESS in the same command line with /FILEACCESS returns an error message.

NOTE: We recommend always using /FILEACCESS with OS/2.

For VShieldCRC, /FILEACCESS checks files only if they have been validated with the /AF or /AV options.

/IGNORE {*drives*}

Omits checking program loads from the specified drives, as shown in the following example:

```
vshield /ignore t: y: w:
```

Use /IGNORE or /ONLY to speed up VShield by excluding secure, virus-free network drives from virus checking. You can specify up to 26 drives. Refer to also /ONLY, described later in this section. Using /IGNORE and /ONLY in the same command line returns an error message.

/LOCK

Halts the system to stop further infection if VShield finds a virus. /LOCK is appropriate 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.

/NOEMS

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

/NOMEM

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.

/NOREMOVE

Prevents VShield from being removed from memory 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 remove VShield, but this option may prevent users from solving memory limitations or conflicts.

/NOUMB

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

/NOWARMBOOT

Omits checking the diskette boot sector during a warm boot ([CTRL]+[ALT]+[DEL]).

/NOXMS

Prevents VShield from using extended memory when it loads. This ensures that XMS is available exclusively to other programs. (Also refer to /XMSDATA later in this section.)

/ONLY {*drive(s)*}

Checks program loads only from the specified drive(s), ignoring all other drives, as shown in the following example:

```
vshield /only c: f: k:
```

Use /IGNORE or /ONLY to speed up VShield by excluding secure, virus-free network drives from virus checking. You can specify up to 26 drives. Also refer to /IGNORE earlier in this chapter. Using /ONLY and /IGNORE in the same command line returns an error message.

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

/POLY

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

NOTE: This option requires the VSHEML.EXE file to operate.

/RECONNECT

Restores VShield's links 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 VShield:

```
vshield /reconnect
```

NOTE: 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" displays on boot-up.

/REMOVE

Unloads VShield from memory. You may want to do this temporarily if you are running out of memory for programs. For best results, try using VShield with the /SWAP option first. Use /REMOVE only as a last resort.

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

/SAVE

Stores the VShield options you specify as the defaults in VSHIELD.INI. (If VSHIELD.INI does not exist, VShield 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 VShield's original defaults, use the /SAVE option alone:

```
vshield /save
```

NOTE: This command does not perform a scan or load.

/SWAP [*pathname*]

Installs a small (8Kb) kernel of VShield in memory that loads the rest of VShield from disk on demand. Specify a pathname 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, if the workstation disconnects from the network, the workstation will lock.

NOTE: Using /SWAP and /XMSDATA on the same line will return an error.

/XMSDATA

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 earlier in this section.)

NOTE: Using /SWAP and /XMSDATA on the same line will return an error.

Configuring VShield to Your Network

Because systems and environments differ, VShield gives you a choice of options. Consider the mixture of safety, performance and maintenance that meets your needs, then choose the combination of options that works best.

Requirement	Option	Comments
More complete protection, any environment	/ANYACCESS	Highest protection against infected diskettes; checks for viruses whenever a diskette is accessed.
	/FILEACCESS	Next highest protection against infected diskettes; checks for viruses whenever a standard file on a diskette is accessed.
	/BOOTACCESS	Of the three, lowest protection against infected diskettes; checks for viruses in the boot sector whenever a diskette is accessed.
	/POLY	Use to check for polymorphic viruses.
More complete protection, stable software environment	/CERTIFY	Use with /CF {*filename*} or /CV and an exception list.
	/CF {*filename*}	Use /CF or /CV. Of the two, /CF {*filename*} is recommended.
	/CV	Use /CF {*filename*} or /CV.

Network environments or multi-user	/CONTACT {*message*}	Use this (or /CONTACTFILE) to tell users what to do when virus is found.
	/CONTACTFILE {*filename*}	Use this (or /CONTACT) to tell users what to do when virus is found.
	/IGNORE {*drives*}	Use this (or /ONLY) to skip virus-free drives.
	/LOCK	Use with /CONTACT or /CONTACTFILE {*filename*}. *For high-risk environments.*
	/NOREMOVE	Prevents VShield from being removed from memory.
	/ONLY {*drives*}	Use this (or /IGNORE) to check only vulnerable drives.
	/RECONNECT	Required if drivers are loaded after VShield.
	/XMSDATA	Use when VShield is loaded from network login; VShield will continue running if the user disconnects from the network.
Faster performance, any environment	/NOMEM	Only use on a virus-free computer.
	/NOWARMBOOT	Omits checking the boot sector after a warm boot.
Manage memory, any environment	/NOEMS	Use when other programs need exclusive use of EMS memory.
	/NOUMB	Use when other programs need exclusive use of UMB memory.
	/NOXMS	Use when other programs need exclusive use of XMS memory.
	/REMOVE	May temporarily solve memory conflicts.
	/NOREMOVE	Use to ensure that VShield remains in memory.
	/SWAP	Use in environments with very limited memory.

Examples

The following examples show different option settings:

- To activate VShield (level II protection):

```
vshield
```

- To activate VShield (level II protection) for the quickest, most complete checking of all diskettes accessed in the system without sacrificing hard drive or network performance:

  ```
  vshield /anyaccess /only a: b: /xmsdata
  ```

- To activate VShield (level III protection), if you have previously run SCAN /AV:

  ```
  vshield /cv
  ```

- To activate VShield (level IV protection) and check a recovery and validation data file created when running Scan with the /AF option:

  ```
  vshield /certify /cf c:\valcodes.dat
  ```

- To activate VShield kernal in memory and swap from the directory in which VShield resides:

  ```
  vshield /swap
  ```

- To activate VShield (level III protection), ignore checking files in the EXCPTION.LST files and display a message if a virus is found:

  ```
  vshield /cv /exclude c:\excption.lst /contact "Call the PC Help Desk!"
  ```

- To re-enable VShield after it has been disconnected by network device drivers:

  ```
  vshield /reconnect
  ```

Error Levels

When VShield loads, it sets the DOS ERRORLEVEL. You can use the returned ERRORLEVEL in AUTOEXEC.BAT or other batch files to take different actions based on whether VShield has loaded in memory. Refer to your DOS manual for more information.

VShield returns these ERRORLEVELs:

ERRORLEVEL	Description
0	VShield successfully loaded in 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 (/CF or /CF checking) or three times if a virus is found.

Using VShieldCRC

For Level I protection on systems with limited memory, use VShieldCRC instead of VShield. VShieldCRC is a separate program that consumes little system overhead, but is not recommended for normal use because it provides only minimal protection. VShieldCRC can inform you that you have been infected with a virus, but it does not check for virus signatures nor does it prevent infection.

To use VShieldCRC, first use Scan with the /AF or /AV option. VShieldCRC checks the validation codes added by Scan. Refer to Chapter 5, "Scan Technical Reference," for instructions on using Scan.

To load VShieldCRC with options, use the following syntax:

```
vshldcrc [options]
```

[options] include the options listed in the table "VShieldCRC Option Summary" earlier in this chapter. For more information on all options except /LOGFILE, refer to "VShield Option Descriptions" earlier in this chapter.

Examples

The following examples show use of using VShield with CRC validation:

- To activate VShieldCRC (level I protection):

  ```
  vshldcrc
  ```

- To activate VShieldCRC and check validation data stored in VALCODES.DAT, a file that was created using Scan with the /AF option:

  ```
  vshldcrc /cf valcodes.dat
  ```

VShieldCRC Option Table

DOS option	Description
/? or /HELP	Display a list of valid VShieldCRC command line options.
/CERTIFY	Prevent files without validation codes from running.
/CF {*filename*}	Check for viruses using recovery and validation data stored by Scan /AF in the specified filename.
/CONTACT {*message*}	Display specified message when a virus is found.
/CONTACTFILE {*filename*}	Display message stored in specified filename when a virus is found.

/CV	Check validation codes added to files by Scan.
/EXCLUDE {*filename*}	Do not check files listed in filename for validation codes (used with /CV).
/FILEACCESS	Scan only validated executable files when they are accessed, but do not check the boot sector. Prevent infected programs from running.
/IGNORE {*drive(s)*}	Do not check programs loaded from specified drive(s).
/LOCK	Halt the system when a file that is not certified attempts to load and execute.
/LOGFILE {*filename*}	Write error information to filename.
/NOREMOVE	Prevent VShieldCRC from being removed from memory with a subsequent VShieldCRC command using /REMOVE.
/NOUMB	Prevent VShieldCRC from using upper memory blocks (UMB) when it loads.
/ONLY {*drive(s)*}	Check programs loaded only from the specified drive(s).
/REMOVE	Unload VShieldCRC from memory.

Using CheckVShield

CheckVShield allows network administrators to make sure that workstations are running VShield or VShieldCRC before users can log onto a network. Refer to "Sample NetWare Login Script and .BAT File" later in this chapter for a sample Novell NetWare login script using CheckVShield.

To load CheckVShield with options, use the following syntax:

`chkvshld [option(s)]`

`[option(s)]`include:

- **/?** and **/HELP** Display a list of valid CheckVShield command line 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 "*xxxxx*"** Tells CheckVShield to look for a specific version (2.00 or higher) of the VShield or VShieldCRC engine in memory. For example, /v "2.00" for VShield 2.00.

NOTE: This option does not consider .DAT file versions.

For example, to check for VShield or VShieldCRC in memory and suppress messages:

```
chkvshld /quiet
```

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 check. The ERRORLEVELs returned by CheckVShield are:

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

Creating an Exception List for the /EXCLUDE Option

VShield /CERTIFY permits a file to load only if:

- It has been validated by Scan, or
- It appears in the exception list file specified with the /EXCLUDE option, used in conjunction with /CV.

If you do not validate any files and do not use an exception list, /CERTIFY will disable all programs other than DOS internal commands.

The exception list file is an ASCII or DOS text file containing up to 1,024 characters. If you use a word processor to create it, be sure to save the file as ASCII or DOS Text. Each line in the file contains the path and filename of one file that should not be validated. Here is an example:

```
c:\clipper\bin\clipper.exe
c:\123\123.com
c:\fox\foxprolx.exe
c:\dos\setver.exe
c:\pkware\pklite.exe
```

```
c:\pkware\pkzip.exe
c:\pkware\pkunzip.exe
c:\semware\q.exe
c:\swapvol.com
c:\norton\ncache.exe
c:\wordstar\ws.exe
```

Sample NetWare Login Script and .BAT File

Here is a sample system login script for use by Novell NetWare system administrators. The login script gets the ERRORLEVEL from CheckVShield and displays messages on the user's screen. If VShield is not loaded correctly, there is an internal error with CheckVShield, either VShield or VShieldCRC is not installed, or an older version of VShield is present, the script exits users to a NOLOGIN.BAT file that logs them out.

```
#REM REPLACE "XXX" WITH CURRENT VERSION NUMBER
CHKVSHLD /V "VXXX"
   IF ERROR_LEVEL = "3" THEN
   FIRE PHASERS 5 TIMES
   WRITE "A CHKVSHLD internal error has occurred."
   WRITE "Please contact the Help Desk."
   #COMMAND /C NOLOGIN.BAT
   EXIT
   ELSE
   IF ERROR_LEVEL = "2" THEN
   FIRE PHASERS 5 TIMES
   WRITE "VShield has not been installed on your PC."
   WRITE "Access Denied. Please contact the Help Desk."
   #COMMAND /C NOLOGIN.BAT
   EXIT
   ELSE
   IF ERROR_LEVEL = "1" THEN
   FIRE PHASERS 5 TIMES
   WRITE "An old version of VShield has been installed."
   WRITE "Access to the network has been denied. Please"
   WRITE "contact the Help Desk to have a new version"
   WRITE "installed."
   #COMMAND /C NOLOGIN.BAT
   EXIT
   END
   END
END
```

Other uses for login scripts include: sending error messages to the network supervisor; updating the user's VSHIELD.EXE during login, and so on.

Here is a sample of the NOLOGIN.BAT file called by the login script:

```
ECHO OFF
REM Log the user off of the network
LOGOUT
```

Chapter 7 Tips and Troubleshooting

Chapter 6 provided information about VShield, the memory-resident component of VirusScan. This chapter provides information about getting the most out of VirusScan, how to detect unknown or new viruses and how to solve or avoid common problems.

Overview

The other chapters in this manual are meant to tell you clearly and concisely how to use the VirusScan software. Still, you may have questions or encounter confusing situations. This chapter contains two kinds of advice:

- Tips for getting the most out of VirusScan.
- Common problems and how to solve or avoid them.

If this information does not help resolve your question or problem, contact McAfee (refer to "McAfee Support" in Chapter 1).

Tips

Creating a Virus-Free Environment

- Be sure to follow the installation procedures as outlined in Chapter 2, "Installation and Setup."
- Configure your AUTOEXEC.BAT file to load VShield automatically at start-up (refer to "Using VShield" in Chapter 3, "VirusScan Reference").
- Scan **all** the diskettes you use by using Scan with the /MANY option (refer to "Using Scan" in Chapter 3, "VirusScan Reference). Never start your computer from an unknown diskette. Always make sure your disk drive(s) are empty before turning on or restarting your computer.
- Rescan whenever you introduce new programs onto your computer. Run VirusScan on a new diskette before executing, installing or copying its files onto

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

- Create a start-up diskette containing the Scan program by following the procedure outlined in Chapter 2, “Installation and Setup.” Make sure this disk is write-protected so that it cannot become infected.

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 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.

Updating VirusScan regularly is probably all you need to do to protect against new viruses. Refer to the instructions for obtaining new versions in “Updating VirusScan Regularly” in Chapter 2, “Installation and Setup.”

Use the Validation and Recovery Options

If your environment is highly vulnerable to viruses, or you require unusual security against them, you can use VirusScan’s validation and recovery options. Scan checks for new or unknown viruses by comparing files against previously recorded validation data. If a file has been modified, it no longer matches the validation data, and Scan 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 (/AF, /CF and /RF switches). This is the preferred method because it stores recovery data in a separate file.
- It can append a simple 98-byte validation code to .COM and .EXE files (/AV, /CV and /RV switches). This method applies to the files you specified only.

NOTE: Neither method stores data for the boot sector and master boot record.

Once the validation codes are stored, both Scan and VShield can use the /CV and /CF options to detect changes to the files. More importantly, if you have stored the recovery information with /AF, Scan can use it to restore infected files.

All of these options require continuing effort to store and maintain the codes. For example, if you install new programs or upgrade old ones, you should use the /RV or /RF options to remove all codes, then /AV or /AF to restore them.

If you want to use one of these methods, which should you use? We recommend the "F" options—/AF, /CF, and /RF—over the "V" options. /AF stores the validation and recovery information in a separate file, instead of modifying the program files themselves. This has the following advantages:

- You can store the recovery file off-line (on your clean anti-viral startup diskette, for example, or on a network drive or tape drive) and access it on demand to check for, and recover from, infection by unknown viruses. Use the procedure below to create a recovery diskette.
- This method keeps self-checking files (usually copy-protected programs) from reporting that they have been tampered with.

NOTE: If you use this method, you do not need an exception list. However, it is important that you run Scan with the /RF option on individual self-modifying files, such as Lotus 1-2-3, to remove the validation codes for those programs from the validation file.

The "V" options are primarily useful for companies that distribute software to their customers or employees, and want to incorporate an additional level of virus protection.

Developing a Security Program

VirusScan has been shown to be 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— not to mention theft or fire — can render a disk unrecoverable without a recent backup. Although outlining such a security program is beyond the scope of this manual, refer to "Other Sources of Information" in Chapter 1 for suggestions.

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

Interacting With Your Network

Many personal computers are interconnected through a local area network (LAN). VirusScan is highly compatible with most networks. Here are some ways of using the VirusScan software with your network:

Run Scan on Network Drives

Run from a workstation (PC) on the network, Scan checks network drives for viruses just as it does local drives. For convenience, the /ADN option scans all network drives to which the workstation is connected.

Use VShield and CheckVShield

By activating VShield as part of every workstation's AUTOEXEC.BAT file, you can prevent the workstations from introducing viruses into the network. Network administrators can ensure that VShield is active on each workstation by running CheckVShield as part of the network login script, before actual login.

Use NetShield

NetShield provides continuous virus protection on a NetWare server. NetWare network administrators can use it to check for both known and unknown viruses and to monitor all network activities. On other kinds of networks, you can use Scan to check network servers.

Using a Recovery Diskette

To store the recovery file on the clean startup diskette you created in "Making a Clean Start-Up Diskette" in Chapter 2, temporarily remove write-protection from the diskette and insert it in drive A. Run Scan on your hard disks with the /AF option. For example:

```
scan /adl /af a:\scancrc.crc
```

scans the local hard disk drives (including compressed, CD-ROM, and PCMCIA drives, but not diskettes) for known viruses and creates SCANCRC.CRC, a file containing recovery data and validation codes, on the diskette. After Scan finishes, write-protect the diskette.

To check for virus infection, turn your computer off, insert the write-protected recovery diskette in drive A and turn the power back on. The PC will now start from the diskette. At the DOS prompt, type:

```
scan /adl /cf a:\scancrc.crc
```

to compare the local hard disk drives against the recovery data stored on the diskette in the SCANCRC.CRC file.

If you detect an unknown virus, to disinfect your system, turn your PC off, insert the write-protected recovery diskette and turn the power back on. The PC will start from the diskette. At the DOS prompt, type:

```
scan /adl /cf a:\scancrc.crc /clean
```

to restore local hard disk drives (including CD-ROM and PCMCIA drives) with the recovery data stored in SCANCRC.CRC on the diskette.

If you install new software, or upgrade your DOS version, remember to up-date your recovery file. Refer to “Updating Validation Codes” in Chapter 5, “Scan Technical Reference.”

Reformatting Infected Diskettes with DOS 5.0 and Later

When reformatting infected diskettes using DOS 5.0 and later versions, be sure to add the /U switch to the FORMAT command. This tells DOS to perform an unconditional format of the diskette, without saving the original infected boot sector. This is necessary to erase certain infections and will prevent reinfection by unformatting the diskette.

Troubleshooting General Abnormalities

Failed Integrity Check

Scan performs an integrity test before running. This self-check allows Scan to determine if it has been modified. If Scan fails its integrity test, a warning message appears, and Scan refuses to run and returns to the command line prompt.

Scan may report a “false” failed integrity check if you upgrade VShield’s data files and perform an immediate Scan. After upgrading VirusScan, turn off your computer, wait a few seconds and turn it on again. Refer to “Upgrading VirusScan Regularly” in Chapter 2, “Installation and Setup.”

If you did not upgrade VirusScan files and receive a failed integrity check warning, your VirusScan program files may have been corrupted or damaged. Obtain an undamaged copy of VirusScan from a known source. Refer to “McAfee Support” in Chapter 1, “Introducing VirusScan.”

False Alarms

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 procedures as outlined in Chapter 3, "VirusScan Reference." That is, turn off your computer and reboot from a known clean start-up disk; run Scan again with the /ADL and /ALL switches from a write-protected diskette; and clean any infected files that Scan detects using the /CLEAN command. If you have any questions, contact McAfee immediately (refer to "McAfee Support" in Chapter 1, "Introducing VirusScan").

If, after following the procedures outlined above, you believe that VirusScan is falsely detecting a virus, refer to the list below of potential sources of false alarms:

- Set up your computer so that only one anti-virus program is running at a time. Remark out lines in the AUTOEXEC.BAT 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 certain all code from other anti-virus programs are cleared.

  NOTE: Your computer's BIOS may include an anti-virus feature. The only way to disable this feature is to remove it from your CMOS file.

  We make every attempt to prevent false alarms, but some viruses can only be detected in a very limited way. This is a reason two anti-virus programs can cause false alarms.

  If the virus warning is only on one file that has been used for years and is not on any other files, it may be a false alarm. Please contact McAfee or send the file to us for analysis.

- 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 the validation. For more information, refer to "Validating Program Files" in Chapter 4, "WScan Technical Reference," and to "Scan Option Descriptions" in Chapter 5, "Scan Technical Reference."

- Some older Hewlett-Packard and Zenith PCs modify the boot sector each time the system is booted. If you are using the /AF or /CF switches, Scan will report 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. To solve this problem, use the /AV and /CV switches instead (which do not check the system area for changes).

- OS/2 dual boot systems change the boot sector between DOS and OS/2 depending on which operating system is active. If you are using the /AF or /CF switches, Scan will report that the boot sector has been modified. To solve this problem, use the /AV and /CV switches instead (which do not check the system area for changes).
- If the virus is only found in memory and only when booted from the hard drive, it is most likely a false alarm. MEM should read 640K or 655,360 total conventional memory. Contact technical support if you are unsure (refer to "McAfee Support" in Chapter 1).
- Scan may incorrectly report viruses in the boot sector or master boot record of certain copy-protected diskettes. Contact technical support if you are unsure (refer to "McAfee Support" in Chapter 1).

Installation Failure

The installation may fail if you are running another anti-virus program during the install procedure. Be sure that all other anti-virus programs are unloaded from memory before beginning the install procedure. Refer to "Installation Steps" in Chapter 2, "Installation and Setup."

Network Problems

LanTastic will not let Scan see the boot sector. Remove LanTastic for a full Scan.

Slow Disk Access, Program Locks

Running VShield will slow your system slightly as described in Chapter 6, "VShield Technical Reference," especially if you use either the /ANYACCESS or /SWAP options. If you experience very slow disk access, or if programs lock or freeze while using Windows 3.1, you may be using a disk cache program that interferes with program operation, or you may need to increase the number of BUFFERS in your CONFIG.SYS file.

TSR Conflicts

Some "terminate-and-stay-resident" (TSR) software may conflict with VirusScan programs, especially VShield (which is itself a TSR). To check whether this is the

problem, “comment out” the other TSR files in your AUTOEXEC.BAT file and restart your system. If the errors disappear, the TSR conflict caused them.

Using DOS Commands to Remove a Virus

Before you use a DOS command (e.g. FORMAT.COM, FDISK.EXE, SYS.COM or DEBUG.EXE) to attempt to remove a virus, contact McAfee immediately for experienced help.

Using DOS commands to remove viruses or clean virus-infected files can result in the loss of all data and the use of infected disks. The common viruses Stoned and 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 program (.EXE) files or overlay files, and 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. If you are unfamiliar with viruses and virus methodology, you should get experienced help before using DOS commands to avoid losing data, programs or disks. For assistance, contact McAfee technical support or your local authorized agent. Refer to “McAfee Support” in Chapter 1, “Introducing VirusScan.”

Troubleshooting VShield

OS/2 Problems

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

Program Locks with /SWAP

When VShield is running with the /SWAP option, certain programs may lock up the computer. These programs may use memory without allocating it first (including older versions Lotus 1-2-3, pfs:Write and Professional Write, OfficeWrite and DisplayWrite4). Restart your computer and run VShield without the /SWAP option.

Unable to Remove VShield

If the /REMOVE option does not successfully remove VShield from memory, you have probably loaded other terminate-and-stay-resident (TSR) programs after VShield. VShield cannot be removed until the other TSRs are removed. If you need to unload VShield often, load it last.

VShield Already Connected

VShield's default command line (in your AUTOEXEC.BAT file) includes the /RECONNECT switch. If you receive the message "Error – VShield already connected" on start-up, edit your AUTOEXEC.BAT file to remove the /RECONNECT switch.

VShield Data File Has Been Damaged

Be sure to turn off your computer immediately after updating VShield's data files. Any file execution caused after updating these data files may trigger the error message "VShield Data File Has Been Damaged." You can solve this problem by turning off your computer, waiting a few seconds and turning it on again to restart VShield with the new data files.

For more information about updating VirusScan, refer to "Updating VirusScan Regularly" in Chapter 2, "Installation and Setup."

Appendix A Downloading McAfee Software

You can use your communications software to dial up the McAfee bulletin board system (BBS) and retrieve (download) evaluation versions of McAfee software by following these steps.

Dial Up

- The McAfee BBS phone number is (408) 988-4004.
- The BBS operates at up to 28,800 bps (baud). Set your communications parameters to 8 data bits, 1 stop bit, no parity, and your terminal emulation to ANSI or TTY.
- The BBS is Bell- and ITU- (formerly CCITT) compatible.

Log On

After receiving the CONNECT message from your modem:

Enter your name, geographic location, and password.

- To retrieve VirusScan programs, type `guest` for the first name and `user` for the last name.
- Or, if you want personal answers or feedback, create your own account by entering your first and last name and a password. Passwords should be 3–8 characters long and are case sensitive.

The Main Menu

Here are some of the important functions on the main menu:

F File transfer area (download McAfee updates)

M Message area (read and write messages in all sections and e-mail)

G Goodbye (hang up and leave the BBS)

NOTE: Only those logging in with their own names will see this menu. “Guest Users” can skip to the next section, “Downloading McAfee Programs.”

Downloading McAfee Programs

1. Select F from the Main Menu to go to the File transfer area. This is the area from which you can download McAfee programs.
2. Select 1 for the McAfee Antivirus Files. A sorted directory listing of files available for download will be displayed.
3. Type D for download, then type in the filename as found in the directory.
4. The BBS will prompt you to select a protocol. If possible, use an error-correcting protocol such as ZMODEM, YMODEM or XMODEM. (ZMODEM is recommended.)
5. The message “Awaiting start signal” is displayed. Tell your software to receive files. With PROCOMM for DOS or TELIX, press the [PAGE DOWN] key, with BITCOM, press the [F2] key. With Windows Terminal, select Transfers | Receive Binary File. For other communications programs, check your manual.
6. Your software will prompt you to select a protocol and file name to receive the file. Select the same protocol and name.

Unpacking Your Files

Once you have downloaded software, you need to unpack the downloaded files before you can use them for virus detection.

About Compressed Files

Compressed files take less disk space and require less time to transfer electronically. McAfee uses a shareware program, PKZIP (produced by PKWare of Brown Deer, WI, and *not* a McAfee product), to compress updated software. PKUNZIP (also from PKWare) is the utility used to decompress file previously compressed with PKZIP. Once a file is decompressed, it can be used normally.

NOTE: Since McAfee's products are zipped using PKZIP version 2.04g, you must also have version 2.04g. This is available on our BBS in area one (1) as PKZ204.EXE. This is a self-extracting zip file. Simply download the file and, at the DOS prompt, run it by typing PKZ204 and pressing ENTER. It self-extracts several files, including PKUNZIP.EXE.

How to Unpack

Once you have downloaded the McAfee products, quit to DOS, and change to the directory where you downloaded the software to. (If you used QMODEM, TELIX, PROCOMM or CROSSTALK it will be in that directory, or a subdirectory of it usually named DOWNLOAD). If you used Windows Terminal, this may be the Windows directory). Then, enter the following command:

PKUNZIP zipfile destination

zipfile is the name of the file you downloaded.

destination is the target directory to store the McAfee software.

For example,

PKUNZIP SCN216.ZIP C:\MCAFEE

unpacks the SCN216.ZIP file and stores it in the C:\MCAFEE directory. (If the C:\MCAFEE directory does not exist, create one using the MKDIR command.)

- If an older version of McAfee software already resides in that directory, you may get a message similar to the following example while decompressing:

  ```
  PKUNZIP: (W18) Warning! AGENTS.TXT already exists.
  Overwrite (y/n/a/r)?
  ```

  If this happens, type **A** for ALL and press ENTER. PKUNZIP will replace all files with the updated versions contained in the zip file.

- The last lines after all of the files are decompressed should be:

  ```
  Authentic files Verified!   # FZW807

  McAFEE Inc.
  ```

  If you do not see this message, you might have files that have been tampered with. Be sure that you obtained them from a valid source before using them.

- If you run VShield after updating, you might get the following message:

  ```
  WARNING: VSHIELD data file has been damaged.
  ```

  This occurs because VShield continually accesses its data file and it has detected a change. To correct this problem, turn off your computer, wait a few seconds and turn it on again. VShield will load with the new version.

Notes for Windows Users

If you downloaded WScan or VShield for the first time, you need to perform several additional configuration steps to complete your installation. You can skip this section if you are not running VirusScan under Windows.

Installing WScan

For WScan, you need to add the icon to your McAfee program group.

1. Create a McAfee program group, if one does not already exist. In the Windows Program Manager, choose File | New. In the New Program Object dialog box, select Program Group and choose OK. Enter a description (such as "McAfee") and a group filename (such as MCAFEE.GRP).

   - If a McAfee program group already exists, select it.

2. Create the WScan icon. In the Windows Program Manager, choose File | New. In the New Program Object dialog box, select Program Item and choose OK. Click Browse, locate the WSCAN.EXE file in the McAfee software directory, then double-click it. Choose OK to add the icon.

3. Double-click the icon to verify that it works.

NOTE: You do not need to make any changes to the WIN.INI file because WScan stores its startup settings in WSCAN.INI, in the same directory as WSCAN.EXE.

Installing VShield Under Windows

The VSHLDWIN.EXE program allows VShield to display warning messages in a Windows message dialog box. For VShield, you need to add the VShield icon to the McAfee program group and modify WIN.INI so that VSHLDWIN.EXE loads automatically when you start Windows.

1. Choose File | Run and Browse to the file VSHINST.EXE program and choose OK to launch this application. This program creates a McAfee program group (if one does not exist) and adds the icon for VSHLDWIN.EXE.

2. Edit your WIN.INI file using any ASCII text editor. Add the following line to the [windows] section of your WIN.INI file:

   ```
   run=VSHLDWIN.EXE
   ```

Restart Windows for your changes to take effect.

Updating Your AUTOEXEC.BAT File

Finally, you may need to edit the AUTOEXEC.BAT file to:

- Automatically load VShield. For more information, refer to “Starting VShield” in Chapter 3, “VirusScan Reference.”
- Add the McAfee software directory to your PATH statement.
- Restart your system for the changes to take effect.

Appendix B New VirusScan Features

Comparison of Scan versions 1.5 and 2.x

Version 1.5	**Version 2.x**	**Description/Windows option**
/? /H or /HELP	/? or /HELP	Display help screen.
/A	/ALL	Scan all files, including data files.
/AD{x}	/AD{*x*}	Scan all drives {L=Local, N=Network}. Leave blank for both drives.
/AF {*filename*}	/AF {*filename*}	Store validation/recovery codes in filename.
/AG {*filename*}	See /EXCLUDE	Add recovery/validation data to files except those listed in {filename}.
/AV {*filename*}	/AV	Add validation/recovery data to program files. Exclude those listed in {filename}; exclude those listed in /EXCLUDE option.
/BELL	default	Beep whenever a virus is found.
/BMP	default	Scan OS/2 Boot Manager partition only.
	/BOOT	Scan master boot record and boot sector only.
/CERTIFY		List files not having a validation code.
/CF {*filename*}	/CF {*filename*}	Check validation/recovery codes in {filename}
/CG		Check recovery/validation data in files.
/CHKHI	default	Check memory from 0Kb to 1,088Kb (not applicable to OS/2).
(CLEAN.EXE)	/CLEAN	Clean up infections in master boot records, boot sectors, and files when possible.
/CV	/CV	Check validation/recovery data in files.
/D	/DEL	Overwrite and delete infected files.
/DATE	/LOG	Save date and time VirusScan was last run. Save in SCAN.LOG file.
	/EXCLUDE {*filename*}	Exclude from scan any files specified in {filename}. Typically used in conjunction with the /AV option.

/EXT {*filename*}		Scan using external virus information from {filename}.
/FAST	/FAST	Speed up VirusScan's scanning; may detect fewer viruses.
	/FREQUENCY	Set the frequency for scanning. (Version 2.2)
/HISTORY {*filename*}	/APPEND	Append Scan report to {filename} (version 1.5). Append to, rather than overwrite, the report file (/REPORT, version 2.x)
/M	default	Scan memory for all viruses (not applicable to OS/2).
/MANY	/MANY	Scan multiple diskettes.
	/MOVE {*directory*}	Move infected files to {directory}.
/NLZ	/NOCOMP	Skip internal scan of LZEXE compressed files.
/NOBREAK	/NOBREAK	Disable CTRL-C and CTRL-BREAK during scan.
/NOEXPIRE		Do not display expiration notice.
/NOMEM	/NOMEM	Skip memory checking (not applicable to OS/2).
/NOPAUSE	/PAUSE	Disable screen pause (version 1.5 only). Enable screen pause (version 2.x only).
/NPKL	/NOCOMP	Skip internal scan of PKLITE compressed files.
	/PLAD	Preserve Last-Access date of scanned files on Novell drives.
/REPORT {*filename*}	/REPORT {*filename*}	Create report of infected files found during scan in [filename}.
/RF {*filename*}	/RF {*filename*}	Remove validation/recovery codes in {filename}.
/RG		Remove recovery/validation data from files.
	/RPTCOR	Add list of corrupted files to the report file (/REPORT).
	/RPTERR	Add list of system errors to the report file (/REPORT).
	/RPTMOD	Add list of modified files to the report file (/REPORT).
/RV	/RV	Remove validation/recovery data from files.
/SAVE	/SAVE	Save specified options as new defaults (not available in Windows).
/SHOWDATE	/SHOWLOG	Show date and time of last scan (version 1.5 only). Display information in SCAN.LOG (version 2.x only).

/SUB	/SUB	Scan subdirectories inside directory.
	/VIRLIST	Display list of viruses detected by VirusScan.
@filename	/LOAD {*filename*}	Use Scan settings stored in {filename}.

Comparison of VShield versions 1.5 and 2.x

Version 1.5	**Version 2.x**	**Description**
/? or /HELP	/? or /HELP	Display a list of valid VShield command line options.
/ACCESS		Check for viruses when files are opened and diskettes are accessed.
	/ANYACCESS	Scan the diskette boot sector for viruses whenever a diskette is accessed (including any read and write operations); scan .EXE, .COM, .DLL, .OVL, .BIN and .SYS files whenever the file is opened, read or updated; scan .EXE and .COM files upon execution; scan any newly created file, regardless of extension.
/BOOT	/BOOTACCESS	Scan the diskette boot sector for viruses whenever a diskette is accessed (including any read and write operations); **individual files on a diskette are not scanned when a diskette is accessed.**
/CERTIFY {*filename*}	/CERTIFY	Prevent files without validation codes from running. {filename} is an optional exception list (version 1.5 only).
/CF {*filename*}	/CF {*filename*}	Check for viruses using validation and recovery data stored by Scan /AF in the specified {filename}.
/CG		Check recovery and validation codes added to files by Scan.
/CHKHI	default	Check memory from 0-1088Kb when VShield loads.
/CONTACT {*message*}	/CONTACT {*message*}	Display {message} when a virus is found.
	/CONTACTFILE {*filename*}	Display the message stored in {filename} when a virus is found.
/CV	/CV	Check validation codes added to files by Scan.

	/EXCLUDE {*filename*}	Do not check files listed in {filename} for validation codes (/CV option).
/F {*pathname*}		Use with /SWAP for DOS 2.0 systems ONLY.
	/FILEACCESS	Scan .EXE, .COM, .DLL, .OVL, .BIN and .SYS files whenever the file is opened, read, or updated; scan .EXE and .COM files upon execution; the diskette boot sector is not checked when a diskette is accessed.
/IGNORE {*drive(s)* }	/IGNORE {*drive(s)* }	Do not check programs loaded from the specified {drive(s)}.
/LH	default	Load VShield into upper memory area.
/LOCK	/LOCK	Halt the system when a file that is infected or not certified loads and attempts to execute.
/M	default	Scan base memory for viruses when VShield loads.
/NB	/NOWARMBOOT	Disable boot sector check during install and reboot.
/NI6510		Fixes Racal Datacomm NI6510 conflict.
/NOBREAK		Prevent [CTRL]+[C] and [CTRL]+[BRK] from working during install.
/NOCONT		Prevent non-certified programs from running.
/NODISK		Turn off the boot sector check when VShield is loading.
/NOEMS	/NOEMS	Prevent VShield from using expanded memory (EMS) when it loads.
/NOFLOPPY	/IGNORE B:\ A:\	Turn off the boot sector check for diskettes.
/NOMEM	/NOMEM	Do not check memory for viruses upon running.
/NOREMOVE	/NOREMOVE	Prevent VShield from being removed from memory with the /REMOVE switch.
	/NOUMB	Prevent VShield from using upper memory blocks (UMB) when it loads.
	/NOXMS	Prevent VShield from using extended memory (XMS) when it loads.
/ONLY {*drive(s)* }	/ONLY {*drive(s)*}	Check programs loaded only from the specified {drive(s)}.

	/POLY	Check for polymorphic viruses.
/RECONNECT	/RECONNECT	Restore VShield after certain drivers or TSRs have disabled it.
/REMOVE	/REMOVE	Unload VShield from memory.
/SAVE	/SAVE	Save specified options as new defaults (version 1.5 only). Save the command line options to the VSHIELD.INI file (version 2.x only).
/SWAP [*pathname*]	/SWAP [*pathname*]	Load VShield kernel only (5Kb in version 1.5; 8Kb in version 2.x); swap the rest from {pathname}.

Comparison of VShield1 version 1.5 and VShieldCRC version 2.x

Version 1.5	**Version 2.x**	**Description**
	/? or /HELP	Display a list of valid VShieldCRC command line options.
	/CERTIFY	Prevent files without validation codes from running.
	/CF {*filename*}	Check for viruses using validation and recovery data stored by Scan /AF in the specified {filename}.
	/CONTACT {*message*}	Display {message} when a virus is found.
	/CONTACTFILE {*filename*}	Display message stored in specified {filename} when a virus is found.
	/CV	Check validation codes added to files by Scan.
	/EXCLUDE {*filename*}	Do not check files listed in {filename} for validation codes (used with /CV option).
	/FILEACCESS	Checks validated files whenever the file is accessed or executed. Whenever a validated .EXE, .COM, .DLL, .OVL, .BIN or .SYS file is opened, rea, or updated, Scan checks the accessed file. Whenever a validated .EXE or .COM file executes, Scan checks the file for viruses as it loads and prevents execution if the file is infected.
	/IGNORE {*drive(s)* }	Do not check programs loaded from specified {drive(s).
	/LOCK	Halt the system when a file that is not certified attempts to load and execute.

	/LOGFILE {*filename*}	Write error information to {filename}.
/NB		Disable boot sector checking during install and reboot.
	/NOREMOVE	Prevent VShieldCRC from being removed from memory with a subsequent VShieldCRC command using /REMOVE.
	/NOUMB	Prevent VShieldCRC from using upper memory blocks (UMB) when it loads.
	/ONLY {*drive(s)*}	Check programs loaded only from the specified {drive(s).}
/REMOVE	/REMOVE	Unload VShieldCRC from memory.

Appendix C Glossary

Entries

archived file

A file that has been archived using either LZEXE or PKLITE, file compression utilities.

boot

To start a computer. The first step is to load startup instructions from a disk's boot ROM or boot sector.

BIOS

A read-only memory chip that contains the coded instructions for the operating system to start the computer. 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 result in "false alarms," install failures and other problems.

boot sector

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

boot sector infections

Contamination of the boot sector by a virus. Particularly serious because information in the boot sector is loaded into memory first, before virus protection code can be executed. The only certain way to eliminate boot sector infections is to restart from a disk known to be uninfected, then clean up the infection.

clean startup diskette

A diskette known to be uninfected, that contains the coded instructions from which the computer can be started. Refer to Chapter 2 for instructions on preparing one.

cold boot

To start a computer from power-off state.

compressed file

A file (usually with a .ZIP extension) that has been compressed using the PKZIP file compression utility.

conventional memory

Up to 640Kb of main memory in which DOS executes programs.

corrupted file

A file that has been damaged. About 10% to 20% of viral infections involve viruses that damage files beyond repair.

detection

Scanning memory and disks for telltale marks or changes indicating that a virus might be present.

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 are immunized against viruses or contain self-modifying code. Scans /AV option uses the list to avoid adding codes to inappropriate files; VShield's /CERTIFY option can use it to allow certain unvalidated files to be run.

executable (file)

A file containing coded instructions to be executed by the computer. Executable files include programs and overlays.

expanded memory

Memory above the DOS 640Kb 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 640Kb limit of conventional memory. Often used for RAM disks and print spoolers.

false alarm

Detecting a virus 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.

memory

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

memory infection

Contamination of memory by a virus. The only certain way to eliminate memory infections is to **turn off your computer,** restart from a disk known to be uninfected and clean up the source of infection.

modified file

A file that has changed after validation/recovery codes have been added.

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. 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 Scan records about an executable file in order to recover if it is infected by a virus. See also *validation codes.*

self-modifying program

Software that deliberately changes its own program file, often to protect against viruses or illegal copying, and is therefore difficult to validate in conventional ways.

system errors

Errors that can prevent Scan from completing its job successfully. System error conditions include disk format errors (such as unformatted disks), media errors (bad sectors), file system errors (unreadable files), network errors (unable to log in), file

access errors (access permission denied), device access errors (printer out of paper) and report failures.

terminate-and-stay-resident (TSR)

A 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 640–1024Kb, just above the DOS 640Kb limit of conventional memory.

validate

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

validation codes

Information that Scan 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 in computer memory or on a disk, and spreads from one program to another. Viruses may damage data, cause the computer to crash, display messages or lie dormant.

warm boot

To restart (reset) a running computer, in DOS by pressing [CTRL]+[ALT]+[DEL].

write operation

Any operation in which information is recorded on a disk. Commands that perform write operations include those that save, move, and 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.

Index

W