Product Guide

VirusScan® Command Line

version 4.32.0

McAfee SECURITY

Issued November 2003 / VirusScan® Command-Line software version 4.32.0

DOCUMENT BUILD 008 -EN

Contents

Preface

This guide introduces McAfee® VirusScan® Command-Line software version 4.32.0, and provides the following information:

- Detailed instructions for installing the software.
- Descriptions of product features.
- Descriptions of all new features in this release of the software.
- Detailed instructions for configuring and deploying the software.
- Procedures for performing tasks.

Audience

This information is intended primarily for two audiences:

- Network administrators who are responsible for their company's anti-virus and security program.
- Users who are responsible for updating virus definition (DAT) files on their workstation, or configuring the software's detection options.

Conventions

This guide uses the following conventions:

Bold

All words from the user interface, including options, menus, buttons, and dialog box names.

Example

Type the **User name** and **Password** of the desired account.

`Courier`

The path of a folder or program; a web address (URL); text that represents something the user types exactly (for example, a command at the system prompt).

Examples

The default location for the program is:

```
C:\Program Files\Network Associates\VirusScan
```

Visit the Network Associates web site at:

```
http://www.networkassociates.com
```

Run this command on the client computer:

```
C:\SETUP.EXE
```

Italic

For emphasis or when introducing a new term; for names of product manuals and topics (headings) within the manuals.

Example

Refer to the *VirusScan Enterprise Product Guide* for more information.

<TERM>

Angle brackets enclose a generic term.

Example

In the console tree under **ePolicy Orchestrator**, right-click <SERVER>.

NOTE

Supplemental information; for example, an alternate method of executing the same command.

WARNING

Important advice to protect a user, computer system, enterprise, software installation, or data.

Getting information

Product Guide *	Product introduction and features, detailed instructions for configuring the software, information on deployment, recurring tasks, and operating procedures. *VirusScan Command-Line 4.32.0 Product Guide*
Help §	Product information in the Help system that is accessed from within the application. The Help system provides brief descriptions of the most common options.
Release Notes ‡	*ReadMe.* Product information, resolved issues, any known issues, and last-minute additions or changes to the product or its documentation.
Contacts ‡	Contact information for McAfee Security and Network Associates services and resources: technical support, customer service, AVERT (Anti-Virus Emergency Response Team), beta program, and training. This file also includes phone numbers, street addresses, web addresses, and fax numbers for Network Associates offices in the United States and around the world.

* An Adobe Acrobat .PDF file on the McAfee Security download site.

‡ Text files included with the software application.

§ Help accessed from the software application:

Contacting McAfee Security & Network Associates

Technical Support	
Home Page	http://www.networkassociates.com/us/support/
KnowledgeBase Search	https://knowledgemap.nai.com/phpclient/homepage.aspx
PrimeSupport Service Portal *	https://mysupport.nai.com
McAfee Security Beta Program	http://www.networkassociates.com/us/downloads/beta/
Security Headquarters — AVERT (Anti-Virus Emergency Response Team)	
Home Page	http://www.networkassociates.com/us/security/home.asp
Virus Information Library	http://vil.nai.com
Submit a Sample — AVERT WebImmune	https://www.webimmune.net/default.asp
AVERT DAT Notification Service	http://vil.nai.com/vil/join-DAT-list.asp
Download Site	
Home Page	http://www.networkassociates.com/us/downloads/
DAT File and Engine Updates	http://www.networkassociates.com/us/downloads/updates/
	ftp://ftp.nai.com/pub/antivirus/datfiles/4.x
Product Upgrades *	https://secure.nai.com/us/forms/downloads/upgrades/login.asp
Training	
McAfee Security University	http://www.networkassociates.com/us/services/education/mcafee/university.htm
Network Associates Customer Service	
E-mail	services_corporate_division@nai.com
Web	http://www.networkassociates.com/us/index.asp
US, Canada, and Latin America toll-free:	
Phone	**+1-888-VIRUS NO** or **+1-888-847-8766**
	Monday – Friday, 8 a.m. – 8 p.m., Central Time

For additional information on contacting Network Associates and McAfee Security— including toll-free numbers for other geographic areas — see the Contact file that accompanies this product release.

* Logon credentials required.

Introduction 1

The command-line scanner is a program that you can run from a command-line prompt. It provides an alternative to scanners that use a graphical user interface (GUI). Both types of scanner use the same virus-scanning engine.

The command-line scanner enables you to search for viruses in any drive, folder, or file in your computer "on demand" — in other words, at any time. The command-line scanner also features options that can alert you when they detect a virus or take a variety of automatic actions.

When kept up-to-date with the latest virus definition (DAT) files, the scanner is an important part of your network security. We recommend that you set up an anti-virus security policy for your network that incorporates as many protective measures as possible.

The scanner acts as an interface to the powerful virus-scanning engine — the engine common to all McAfee Security anti-virus products.

What's new in this release

This release introduces the following new features:

- *Scanning running processes*.
- Support for Microsoft Office 2003 XML documents.
- Improved support for .RAR formats.
- Updated support for latest .ZIP file formats.

Scanning running processes

Previous release	Feature was not supported.
Current release	A new option, `/WINMEM` scans inside running processes.
Benefits	Some potentially harmful code does not exist as files but rather as executable code in the memory space of an infected process. The potentially harmful software is now removed.
For more information	See the description of the new option, `/WINMEM`, in *Scanning processes in memory* on page 19.

Installing the Command-Line Software 2

To prevent the spread of viruses that might already be on your computer before you install the anti-virus software:

1. Review the system requirements below.
2. Ensure that your computer is virus-free.
3. Confirm that your date and time settings are accurate.

System requirements

- An IBM-compatible personal computer with an Intel 80386 processor or an equivalent, running MS-DOS version 6.22 or later.
- For best results, we recommend at least 4MB of memory and 4MB of free hard disk space.

Installing the software

If you suspect your computer is already infected, see *Removing Infections* on page 41 before you install the scanner software.

1. Create a directory for the software on your hard disk.
2. Depending on the source of your command-line program files, do one of the following:

   - **CD**
     Insert the CD into your CD-ROM drive, then copy the files from the CD to that directory.
   - **Disks**
     Insert the first disk into your A drive, change to the A drive, then copy the files from your disk drive to that directory.
   - **Files downloaded from a web site**
     Decompress the zipped files into that directory.

     NOTE
     We recommend that you use the `-d` option to extract command-line files and preserve their directory structure. Type `CD` to change to the directory to which you extracted the program files.

3 Add the directory you created to the PATH statement in your AUTOEXEC.BAT file.

4 Make a clean startup disk. See *Creating an emergency disk* on page 45 for more information.

To run the scanner from a Novell NetWare login script without running out of memory

Follow these steps immediately after installation.

1 Rename LOGIN.EXE to LOGIN1.EXE, then remove any references to the anti-virus software from the file.

2 Create a batch file named LOGIN.BAT.

3 At the first line of the batch file, add a call to the scanner, with the options you want to include.

4 Add a call to the file LOGIN1.EXE to the second line of the batch file.

These steps prevent LOGIN.EXE and SCAN.EXE from loading into memory at the same time. This allows the scanner to run before your computer tries to get access to the network. Your login script should then run without complications.

Validating your files

When you download or copy files from any outside source, your computer is at risk of virus infection — even if the risk is small. Downloading anti-virus software is no exception. It is important to verify that the software is authentic, unaltered, and not infected. Strict, extensive security measures ensure that the products you purchase and download from our web site and other electronic services are safe, reliable, and free from virus infections. However, anti-virus software attracts the attention of virus writers and Trojan-horse writers, and some find it amusing to post infected copies of commercial software, or use the same file names to camouflage their own work.

Download your files from the McAfee Security or Network Associates web site. If you download a file from any other source, it is important to verify that it is authentic, unaltered, and not infected. The software package includes a utility program called VALIDATE that you can use to ensure that your version of the software is authentic. When you receive a new version of this software, you can run VALIDATE on all of its program files and DAT files.

To ensure that you have exactly the same files as the original software, you need to compare the validation codes that VALIDATE.EXE generates against the packing list supplied with your copy of the software. The packing list is a text file that contains the validation codes that were generated from a cyclical redundancy check (CRC) when the software was packaged for delivery.

To validate your files:

1. Install the software as described in page 11.
2. In the Microsoft Windows taskbar, click **Start**, point to **Programs,** then choose **Command Prompt**.
3. In the window that appears, change your command prompt to point to the directory that contains the VirusScan files.
4. At the command prompt, type `VALIDATE *.*`

   The program examines all of the files in the program directory, then generates a file list that includes the following information:

   - The name of each file.
   - The size of each file, in bytes.
   - The creation date and time of each file.
   - Two validation codes in separate columns for each file.

   For example:

   ```
   NAMES DAT 242681  03-26-03 4:24a   35B2 4690
   ```

5. Print this output so that you can review it easily. Do one of the following:

   - If your printer is set to capture output from MS-DOS programs, type `VALIDATE *.* >PRN` at the command prompt. To learn how to set your printer, consult your Windows documentation.
   - Direct the output to a file, and print the file directly from any text editor, such as Microsoft Notepad. At the command prompt, type: `VALIDATE *.* > <filename>`

6. Print the packing list, so that you can review it easily. At the command prompt, type: `PACKING.LST >PRN`.
7. Compare the output from VALIDATE.EXE and PACKING.LST.

The sizes, creation dates and times, and validation codes for each file name must match *exactly*. If they do not, delete the file immediately. Do not open the file or examine it with any other utility; this may cause virus infection.

Checking your installation with VALIDATE.EXE does not guarantee that your copy is free from defects, copying errors, virus infections or tampering, but the program's security features make it extremely unlikely that anyone has tampered with files that have correct validation codes.

Testing your installation

After you install it, the anti-virus software is ready to scan your computer for infected files. You can verify that the software has installed correctly and that it can properly scan for viruses with a test. This was developed by the European Institute of Computer Anti-virus Research (EICAR), a coalition of anti-virus vendors, as a method for their customers to test any anti-virus software installation.

To test your installation:

1 Open a standard MS-DOS or Windows text editor, then type the following character string as *one line, with no spaces or line breaks:*

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

NOTE
The line shown above should appear as *one line* in your text editor window, so be sure to maximize your text editor window and delete any line breaks. Also, be sure to type the letter O, not the number 0, in the "X5O..." that begins the test message.

If you are reading this manual on your computer, you can copy the line directly from the Acrobat PDF file and paste it into Notepad. You can also copy this text string directly from the "Testing your installation" section of the README.TXT file, which is in your anti-virus program directory. If you copy the line from either of these sources, be sure to delete any carriage returns or spaces.

2 Save the file with the name EICAR.COM. The file size will be 68 or 70 bytes.

3 Start your anti-virus software and allow it to scan the directory that contains EICAR.COM. When the software examines this file, it reports `"Found EICAR test file NOT a virus."`

NOTE
This file is *not a virus* — it cannot spread or infect other files, or otherwise harm your computer. Delete the file when you have finished testing your installation to avoid alarming other users. Please note that products that operate through a graphical user interface do *not* return this same EICAR identification message.

Removing the software

1 Change your command prompt to point to the directory that contains the VirusScan files (as set up in Step 1 under *Installing the software* on page 11).

2 Delete all files in the directory.

Using the Command-Line Scanner 3

The command-line scanner is a program that you can run from a command prompt. To run a scan, type `scan` at the command prompt with the options you want. For a complete list of options, see page 23.

You should scan any file that is new to your computer, especially any newly downloaded or installed files. If your computers are susceptible to virus infection, you should scan as often as once a day.

The scanner operates with minimal use of system resources. The program also includes options for administrators that help to ensure that the scanner is being used most efficiently. For example, the `FREQUENCY` option sets a mandatory period between scans, which helps to minimize resources when the network is most busy.

What can you scan?

- **File types scanned by default.**

  These file types and many other common file types are scanned by default: .BIN, .COM, .DLL, .DOC, .DOT, .EXE, .HTM, .INI, .OVL, .RTF, .SYS, .VBS, .VXD, .XLA, .XLS, and .XLT.

- **Archived and compressed files recognized by the scanner.**

  You can scan compressed and archive file formats which include .ARC, .ARJ, .CAB, Diet, .GZIP, LZEXE, .LZH, PKLite, .RAR, .TAR, and .ZIP files.

  The scanner detects and reports any infections found in any compressed or archive file. The scanner can also clean files in .ZIP archive format. If you have access to Windows, you can clean certain infections from compressed files using VirusScan for Windows software.

  You can use the options `/UNZIP` and `/NOCOMP` to configure the scanner to handle compressed files. These and other scan options are described in the tables from page 26 to page 30.

What is heuristic analysis?

An anti-virus scanner uses two techniques to detect viruses — signature matching and heuristic analysis.

A *virus signature* is simply a binary pattern that is found in a virus-infected file. Using information in the DAT files, the scanner searches for those patterns. However, this approach cannot detect a new virus because its signature is not yet known, therefore the scanner use another technique — *heuristic analysis*.

Programs, documents or e-mail messages that carry a virus often have distinctive features. They might attempt unprompted modification of files, invoke mail clients, or use other means to replicate themselves. The scanner analyzes the program code to detect these kinds of computer instructions. The scanner also searches for "legitimate," non-virus-like behavior, such as prompting the user before taking action, and thereby avoids raising false alarms.

In an attempt to avoid detection, some viruses are encrypted. Each computer instruction is simply a binary number, but the computer does not use all the possible numbers. By searching for unexpected numbers inside a program file, the scanner can detect an encrypted virus.

By using these techniques, the scanner can detect both known viruses and many new viruses and variants.

Scanning NTFS streams

Some known methods of file infection add the virus body at the beginning or the end of a host file. However, a *stream* virus exploits the NTFS feature in Windows NT and Windows 2000 that allows multiple data streams. For example, a Windows 95 or Windows 98 FAT file has only one data stream — the program code or data itself. In NTFS, users can create any number of data streams within the file — independent executable program modules, as well as various service streams such as file access rights, encryption data, and processing time.

Unfortunately, some streams might contain viruses. The scanner can detect a stream virus in one of two ways; you can specify the full stream name, or you can include `/STREAMS` and specify either no stream name, or a part of a stream name using the wildcard characters `?` and `*`.

Currently no known viruses hide themselves in NTFS streams. One virus — W2K/Stream — uses streams to save a clean copy of its host. Stream viruses are a potential risk, but not a current risk.

The following table shows the effect of different commands on a stream called `file:stream` that contains a virus.

Table 3-1. Scanning streams

Command	Action
`SCAN /ALL /STREAMS FILE`	All streams were scanned. The virus is detected.
`SCAN /ALL FILE:STREAM`	The exact stream name was specified. The virus is detected.
`SCAN /ALL /STREAMS FILE:STREAM`	The exact stream name was specified. The virus is detected.
`SCAN /ALL FILE:STR*`	An exact stream name was *not* specified. The virus is not detected.
`SCAN /ALL /STREAMS FILE:STR*`	All streams beginning with “str” are scanned. The virus is detected.
`SCAN /ALL FILE`	No streams were named. The virus is not detected.

Using memory caches

When scanning a file for viruses and other potentially harmful software, the virus-scanning engine reads the file into computer memory in amounts determined by the operating system. Although changes are not normally necessary, you can improve the scanning speed by increasing the amount of memory that the engine uses. This can be controlled by the following options:

- `/OCRS`
- `/OCMAX`
- `/AFC`

Options `/OCRS` and `/OCMAX` are intended for use with offline or remote storage, such as Hierarchical Storage Management (HSM). The `/AFC` option can improve scanning performance in some cases.

OCRS

Typically the scanner reads only a few kilobytes of a file at a time, therefore a large number of reads might be required per file. The /OCRS option causes the engine to use a large internal "cache" for each file read instead. The size of reads for this cache is determined by a value in the range 0 through 4, as follows:

/OCRS=0 — 128KB

/OCRS=1 — 256KB

/OCRS=2 — 512KB

/OCRS=3 — 1MB

/OCRS=4 — 2MB

OCMAX

The /OCMAX option determines the maximum size of the internal cache for file reads. By default, the engine typically caches up to eight reads per file, and uses a cache of 128KB. So, if you set /OCRS=2 (for 256KB), the value for OCMAX defaults to 2MB. If you set the /OCRS=4, the value for OCMAX defaults to 16MB.

When setting the maximum size explicitly, you must specify the value of OCMAX as a number of Megabytes. For example, to specify a 2MB limit for the internal cache, use the following: /OCMAX=2.

AFC

When scanning files, the engine places the contents into computer memory (or *file cache*) before scanning them. This option allows you to vary the amount of cache that the scanner uses.

The cache is allocated "per file", so the engine uses a large amount of cache if there are many nested files. A larger cache size normally improves scanning speeds unless the computer has very low memory.

A range of cache sizes — 8MB to 512MB — is permitted. If you specify a value outside this range, the minimum or maximum value is assumed as appropriate. If you do not use this option, the scanner uses the default value of 12MB.

Scanning files in remote storage

Under some Microsoft Windows system, files that are not in frequent use can be stored in a remote storage system, such as the Hierarchical Storage Management (HSM) system. However, when the files are scanned using the /DOHSM option, those files become 'in use' again. To prevent this effect, you can include the /NORECALL option. In combination, these options request the stored file for scanning, but the file continues to reside in remote storage. The file is not transported back to local storage.

Scanning protected files

The scanner normally examines files such as other users' profiles and recycle bins for viruses. If you want to prevent this type of scanning in a Windows NT, Windows 2000 or Windows XP system, use the `/NOBKSEM` option.

Scanning processes in memory

Viruses such as CodeRed do not exist as files on disk but rather as executable code in the memory space of an infected process. To protect against this threat, you can include the `/WINMEM` option. The process is scanned in memory together with any files or DLLs associated with it.

NOTE
When using the /WINMEM option, specify at least one file for scanning too.

Examples

`SCAN EXAMPLE.EXE /WINMEM`	Scans the file `EXAMPLE.EXE` and all processes running on the computer.
`SCAN *.EXE /WINMEM`	Scans all processes running on the computer, and scans all files with a ".EXE" file name extension in the current directory.
`SCAN *.* /WINMEM`	Scans all processes running on the computer, and scan all files in the current directory.
`SCAN AA.EXE /WINMEM=1234`	Scans the specified process, 1234 and the file, AA.EXE in the current directory. The parameter is the process identifier or "PID". If the process is not running, the engine returns error code 21 and an error message.

Examples of on-demand scans

The examples in the following sections describe how to run typical on-demand scans. In the example on page 21, you can learn how to save the details of scans that you find useful as *scanning profiles*. Profiles provide an efficient means of handling multiple or repetitive scans, and you can also use profiles as templates for new scans as needed.

Example 1: Running a full scan

The first step in building a scan command is to determine which files or directories you want to examine. You can easily scan one file or folder at a time, but many scan options make targeting specific directories or drives easy. See page 26 for a list of these options. To run a full scan, you can use the `/ADN` option.

To run a full scan:

1. If you do not already have the VirusScan program directory listed in your path statement, change to the directory where you stored your VirusScan program files.
2. At the command prompt, type:

```
SCAN /ADN
```

The scanner scans all network drives and displays its results on-screen.

Example 2: Creating a report

The scanner can report its results in a log file you create and name. In this example, the scanner create its report in a log file called `WEEK40.TXT`, which appears in your current working directory.

To create a report:

1. If you do not already have the VirusScan program directory listed in your path statement, change to the directory where you stored your VirusScan program files.
2. At the command prompt, type:

```
SCAN /ADN /REPORT WEEK40.TXT
```

The scanner scans all network drives and generates a text file of the results. The contents of the report are identical to the text you see on-screen as the scanner is running.

Example 3: Saving the report to a file

To create a running report of the scanner's actions, use the `/APPEND` option to add any results of the scan to a file.

To create a running report:

1. If you do not already have the VirusScan program directory listed in your path statement, change to the directory where your VirusScan program files are stored.
2. At the command prompt, type:

```
SCAN /ADN /APPEND /REPORT WEEK40.TXT
```

The scanner scans all network drives, and appends the results of the scan to an existing file called `WEEK40.TXT`.

Example 4: Creating a scanning profile

Instead of typing all of the options for a scan at the command prompt each time you want to run the task, you can save the options in a text file as a *scanning profile*. You can then tell the scanner to load the options from that file.

To create a scanning profile:

1. Using any text editor, open a new file.
2. Add the options to configure your scan task in the same way that you type them at the command prompt. Save the file to the VirusScan program directory as `SAMPLE.TXT`.
3. To start a scan with these options, type:

```
SCAN /LOAD SAMPLE.TXT
```

Configuring a scan to run at startup

By using a scanning profile in the AUTOEXEC.BAT file, a computer can scan for viruses each time it starts.

To configure a virus scan at startup:

1. Change to the root directory by typing `C:`, then `CD \` at the command prompt.
2. To start the MS-DOS text editor, type:

```
EDIT AUTOEXEC.BAT
```

3 Locate the first line that has a reference to SCAN.EXE. Insert one space after the reference, then type:

```
/LOAD <filename>
```

where *<filename>* is the name of the scanning profile you want to run at startup. You can add a series of such files, each separated with a space, to load multiple scan profiles.

4 When you finish editing your AUTOEXEC.BAT file, save your changes, then quit your text editor.

5 Restart your computer to have the software run and load the command-line options you chose.

Creating a list of infected files

Although a summary report can be useful, you can also create a simple list that contains only the names of the infected files. You can create and control this list using the options, BADLIST, APPENDBAD, and CHECKLIST.

For example, the following command scans the directory DIR1 and all its subdirectories, and produces information on-screen:

```
SCAN C:\DIR1\*.* /SUB
```

To produce a simple list of infected files, you can add the BADLIST option:

```
SCAN C:\DIR1\*.* /SUB /BADLIST BAD1.TXT
```

The contents of BAD1.TXT might look like this list:

```
C:\DIR1\Games\hotGame.exe ... Found Acid.674 virus!
C:\DIR1\SCANTEST\vtest.com ... Found: EICAR test file NOT a virus.
```

You can add to the list of infected files by using the APPENDBAD option. For example, the following command scans the directory DIR2, and any infected files found here are added to the existing list:

```
SCAN C:\DIR2\*.* /SUB /BADLIST BAD1.TXT /APPENDBAD
```

Then, the contents of BAD1.TXT might look like this:

```
C:\DIR1\Games\hotGame.exe ... Found Acid.674 virus!
C:\DIR1\SCANTEST\vtest.com ... Found: EICAR test file NOT a virus.
C:\DIR2\prices.doc ... Found: virus or variant W97M/Concept!
C:\DIR2\Costs\may2003.doc ... Found the W97M/Ethan virus!
```

Using the CHECKLIST option, you can refer to that list, and scan the same files again later:

```
SCAN /CHECKLIST BAD1.TXT
```

Scanning options

The scanning options are organized into several functional groups:

- *General options*.
- *Target options* on page 26.
- *Response and notification options* on page 30.
- *Report options* on page 32.

The options are also listed alphabetically with brief descriptions on page 34.

General options

The following table lists the general scanning options.

Table 3-2. General options

General option	Limitations	Description
`/?`	None.	Display a list of command-line options, each with a brief description. You can add a list of scanning options to a report file. To do this, type at the command prompt: `SCAN /? /REPORT <filename>` The report is appended with the full set of options available for that scan task.
`/AFC=<size>`	.	Use a cache of specified size. Specify the size in megabytes. For example, to specify a 64MB cache, use /AFC=64. See page 18 for more information.
`/ANALYZE` `/ANALYSE`		Scan for possible new viruses in programs and macros. See *What is heuristic analysis?* on page 16 for details. For macro viruses only, use `/MANALYZE`. For program viruses only, use `/PANALYZE`.
`/APPENDBAD`	Use with `/BADLIST`.	Append names of infected files to an existing file, as specified by `/BADLIST`. See *Creating a list of infected files* on page 22 for details.
`/BADLIST <filename>`	None.	Create a list of infected files. See *Creating a list of infected files* on page 22 for details.
`/BEEP`	None.	Issue a tone when an infected file is found. By default, a tone is only issued when the scan ends.
`/BPRESTORE`	None.	Restore sectors from backup after cleaning.

Table 3-2. General options (*Continued*)

General option	Limitations	Description
/DRIVER	None.	Specify the location of the DAT files: scan.dat, names.dat, and clean.dat. If you do not specify this option in the command line, the program looks in the same directory from where it is executed. If the program cannot find these data files, it issues exit code 6.
/EXTLIST	None.	Display names of file extensions that are scanned by default.
/EXTRA <filename>	None.	Specify the location on any EXTRA.DAT file. An EXTRA.DAT is a small, supplemental virus-definition file that is released between regular DAT updates.
/FREQUENCY <hours>	None.	Do not scan before the specified number of hours after the previous scan. In environments where the risk of virus infection is very low, this option prevents unnecessary scans. Remember, frequent scanning provides greater protection against viruses.
/HELP	None.	Display a list of command-line options, each with a brief description. See "*/?*" on page 23 for more details.
/HTML <filename>	None.	Display the results in HTML format.
/LOAD <filename>	None.	Load scanning options from the named file, or scanning profile. You can call scanning profiles from any local directory. You can use this option to perform a scan you have already configured by loading custom settings already saved in an ASCII-formatted file.
/MANALYZE /MANALYSE		Scan for possible new viruses in macros. For program viruses only, use */PANALYZE*. For program and macro viruses, use */ANALYZE*.
/NOBKSEM	Windows NT, Windows 2000, and Windows XP only.	Prevent scanning of files that are normally protected. Such files can normally be accessed by the operating system's FILE_FLAG_BACKUP_SEMANTICS flag. See *Scanning protected files* on page 19 for details.
/NOEXPIRE	None.	Disable the "expiration date" message if the scanner's DAT files are out of date. For more details, see *Updating Your Anti-Virus Protection* on page 49.

Table 3-2. General options (*Continued*)

General option	Limitations	Description
/OCRS=<value>	None. Use with Microsoft Windows only.	Specify a value that represents the size of the internal cache size for each file read. The value may be specified as a digit that represents sizes between 128KB and 2MB. See *Using memory caches* on page 17 for details.
/OCMAX=<size>	None. Use with Microsoft Windows only.	Specify the maximum size of the internal cache for file reads. The size must be specified in megabytes. See *Using memory caches* on page 17 for details.
/PANALYZE /PANALYSE		Scan for possible new viruses in programs. For macro viruses only, use /MANALYZE. For program and macro viruses, use /ANALYZE.
/PROGRAM	None.	Scan for potentially harmful applications. Some widely available applications such as “password crackers” can be used maliciously or can pose a security threat.
/SILENT	None.	Do not display any information on-screen.
/STREAMS	NTFS only, run from within Windows NT.	Scan all streams within a file if it is in an NTFS partition on a Windows NT system. See *Scanning NTFS streams* on page 16 for more information.
/TIMEOUT <seconds>	None.	Set the maximum time to spend scanning any one file.

Target options

The following table lists scanning options that define the type of object or area to be scanned.

NOTE
To configure a scan, you must specify a target location for the scan, such as `C:\`, `A:\`, `/ADL`, `/ADN`.

Table 3-3. Target options

Target option	Limitations	Description
`/AD`	None.	Same as `/ALLDRIVES`.
`/ADL`	None.	Scan all local drives, including compressed and PC drives, in addition to any other drives specified on the command line. Do not scan disk drives.
`/ADN`	None.	Scan all network drives, in addition to any other drives specified on the command line.
`/ALL`	See note on page 29.	Scan all files regardless of extension. By default, only executable files are scanned. Using this option substantially increases the scanning time. Use it only if you find a virus or suspect you have one.
`/ALLDRIVES`	None.	Scan all drives. Scan all network drives and local drives, but not removable drives; these include disk drives, CD drives, and Zip drives. This is a combination of `/ADN` and `/ADL`.
`/ALLOLE`	None.	Treat all files as compound/OLE files regardless of file extension.
`/BOOT`	Do not use with `/NODDA`.	Scan boot sector and master boot record only.
`/CHECKLIST <filename>`	None.	Scan the files listed in the specified file. See *Creating a list of infected files* on page 22 for details.
`/DOHSM`	On Windows NT, 2000 and XP only.	Scan files that are offline. These are files that Hierarchical Storage Management (HSM) has archived because they have not been accessed for some time. See also `/NORECALL`.
`/EXCLUDE <filename>`	None.	Do not scan the files listed in the specified file. Use this option to exclude specific files from a scan. List the complete path to each file on its own line. You may use wildcards, `*` and `?`.
`/MAILBOX`	Use with `/MIME`	Scan plain-text mailboxes. These include Eudora, PINE, and Netscape. Most mailboxes will be in MIME format, and therefore the `/MIME` option is also required.

Table 3-3. Target options (*Continued*)

Target option	Limitations	Description
/MANY	None.	Scan multiple disks consecutively in a single drive. The program prompts you for each disk. You can use this option to check several disks quickly. If one disk is found to be infected, the scanning stops. You cannot use this option if you run the scanner from a boot disk and you have only one disk drive.
/MAXFILESIZE <size>	None.	Scan only files that are not larger than the specified number of megabytes.
/MIME	None.	Scan inside MIME files.
/NOBACKUP	None.	Do not prompt for backup of sectors before attempting to clean.
/NOBOOT	None.	Do not scan the boot sector.
/NOBREAK	None.	Disable CTRL-C and CTRL-BREAK during scans. Users cannot halt scans in progress if this option is set.
/NOCOMP	None.	Do not check compressed executables created with the LZEXE or PkLite file-compression programs. This reduces scanning time when a full scan is not needed. Otherwise, by default, the scanner checks inside executable, or self-decompressing files by decompressing each file in memory and checking for viruses.
/NOD	None.	Use with */CLEAN*. Do not scan all files regardless of extension. By default, /CLEAN scans and tries to clean viruses in *all* file types. When you include the /NOD option, the scanning and cleaning are limited to the susceptible file types only, as recognized by their file extensions.
/NODDA	Do not use with /BOOT.	Do not access disk directly. This prevents the scanner from accessing the boot record. This feature allows the scanner to run under Windows NT. You might need to use this option on some device-driven drives.
/NODOC	See note on page 29.	Do not scan document files. This includes Microsoft Office documents, OLE2, PowerPoint, CorelDraw, WordPerfect, RTF, Visio, Autodesk Autocad 2000, Adobe PDF 5, and Corel PhotoPaint 9 files.

Table 3-3. Target options (*Continued*)

Target option	Limitations	Description
/NODECRYPT	None.	Do not decrypt Microsoft Office compound documents that are password-protected. By default, macros inside password-protected compound documents are scanned by employing “password cracking” techniques. If, for reasons of security, you do not require these techniques, use this option. Password cracking does not render the file readable.
/NOJOKES	None.	Do not report any joke programs.
/NOMEM	None.	Do not scan memory for viruses. Use this option only when you are certain that your computer is virus-free.
/NORECALL	Use with /DOHSM	Do not move files from remote storage into local storage after scanning.
/NOSCRIPT	None.	Do not scan these types of file: HTML, JavaScript, Visual Basic, and Script Component Type Libraries. Stand-alone JavaScript and Visual Basic Script files will still be scanned.
/SECURE	None.	Scan inside all files including compressed files regardless of file extension, and use heuristic analysis. This is a combination of /ALL, /ANALYZE, and /UNZIP.
/SUB	None.	Scan any subdirectories inside a directory. By default, when you specify a directory to scan rather than a drive, the scanner examines only the files it contains, not its subdirectories. Use this option to scan all subdirectories within the specified directories. This option is not necessary if you specify an entire drive as a target.

Table 3-3. Target options (*Continued*)

Target option	Limitations	Description
/UNZIP	None.	Scan inside archive files, such as those saved in ZIP, LHA, PKarc, ARJ, WinACE, CAB, and CHM formats. If used with /CLEAN, this option attempts to clean non-compressed files inside ZIP files only. No other archive formats can be cleaned. The /CLEAN option does not delete or rename infected files within ZIP files. It does not rename the ZIP file itself. The program cannot cleaned infected files found within any other archive format; you must first extract them from the archive file.
/WINMEM /WINMEM=<PID>	Specify at least one file for scanning.	Scan inside running processes. Scan the specified process from its memory image. See page 19 for examples.

NOTE
The /ALL option overrides the /NODOC option, such that all files are scanned, but Microsoft Office files are not scanned for macros.

Response and notification options

The following table lists the response and notification options that you can use when a virus is detected.

Table 3-4. Response and notification options

Response and notification option	Limitations	Description
/CLEAN	None.	Clean viruses from *all* infected files and system areas. See *If the scanner detects a virus* on page 42 for more information.
/CONTACTFILE <filename>	None.	Display the contents of the specified file when a virus is found. This enables you to provide contact information and instructions to the user when a virus is encountered. We recommend using /LOCK with this option. This option is especially useful for networks, because you can maintain the message text in a central file, rather than on each workstation. Any character is valid in a contact message except a backslash (\). Messages beginning with a slash (/)or a hyphen (-) must be placed in quotation marks.
/DAM	None.	Delete all macros in a file if an infected macro is found. If you suspect you have an infection in your file, you can choose to remove all macros from the file to prevent any exposure to a virus. To pre-emptively delete all macros in a file, use this option with /FAM: SCAN <*filename*> /FAM /DAM If you use these two options together, all found macros are deleted, regardless of the presence of an infection.
/DEL	None.	Delete infected .COM and .EXE files. This option does *not* delete infected items within Microsoft Word documents or archives. If the scanner detects infected files within an archive, it does not delete the files within the archive, nor does it delete the archive itself. We recommend that you use the /CLEAN option to protect against viruses that infect file types other than .COM or .EXE. See *If the scanner detects a virus* on page 42 for more information.
/EVLOG	On Windows NT only.	Use NT Event Logging. Any detections are recorded in the Application Log of the Event Viewer.

Table 3-4. Response and notification options (*Continued*)

Response and notification option	Limitations	Description
/FAM	None.	Find all macros, not just macros suspected of being infected. The scanner treats any macro as a possible virus and reports that the file "contains one or more macros." However, the macros are *not* removed. If you suspect you have an infection in a file, you can remove all macros from the file by using the /FAM and /DAM options together. For example: SCAN <*filename*> /FAM /DAM
/LOCK	In MS-DOS systems only, not Windows NT.	Halt and lock the computer if a virus is found. This option is appropriate in vulnerable network environments, such as open-use computer laboratories. We recommend that you use this option with the /CONTACTFILE <filename> option to tell users what to do or whom to contact if the scanner locks their computer.
/MOVE <dir>	None.	Move all infected files found during a scan to the specified directory, preserving the drive letter and directory structure. This option has no effect if the Master Boot Record or boot sector is infected, because these are not files. See *If the scanner detects a virus* on page 42 for more information.
/NOBEEP	None.	Do not issue a tone when the scan ends. By default, a tone is issued at the end of a scan if an infection is found.
/NORENAME	None.	Do not rename an infected file that cannot be cleaned. For information about renaming, see Table 4-1 on page 42. See *If the scanner detects a virus* on page 42 for more information.
/PLAD	On NetWare volumes only.	Preserve the last-accessed time and date for files that are scanned. Some software (such as used for creating backups or archives) relies on a file's last-accessed time and date to work correctly. If you set this option, the engine resets that time and date to their original values after scanning the file.

Report options

By default, the results of a scan appear on-screen. The following table lists the options for displaying the results elsewhere. To capture a scanner report to a text file, use /REPORT with any additional options as needed. For examples of using reporting options, see page 20.

Table 3-5. Report options

Report option	Limitations	Description
/APPEND	None.	Append information to the specified report file instead of overwriting it. Use this option with /REPORT.
/LOUD	None	Display a progress summary during the scan. Note that this option can produce a large amount of information.
/PAUSE	Do not use with report options.	Enable a screen pause. When the screen is full of messages, the prompt "Press any key to continue" appears. Otherwise, by default, the screen fills and scrolls continuously without stopping. This allows the scanner to run without stopping on computers with multiple drives or that have severe infections. We recommend you do not use this option with the report options, REPORT, /RPTALL, /RPTCOR, and /RPTERR.
/REPORT <filename>	Do not use with /PAUSE.	Create a report of infected files and system errors, and save the data to the specified file in ASCII text file format. If that file already exists, /REPORT overwrites it. To avoid overwriting, use the /APPEND option with /REPORT. The scanner then adds report information to the end of the file, instead of overwriting it. You can also use /RPTALL, /RPTCOR and /RPTERR to add the names of scanned files, corrupted files, modified files, and system errors to the report. 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 may find it helpful to add a list of scanning options to the report files. To do this, type at the command prompt: SCAN /HELP /REPORT <*filename*> The results of your scanning report are appended with the full set of options available for that scan task. We recommend you do not use /PAUSE when using any report option.

Table 3-5. Report options (*Continued*)

Report option	Limitations	Description
/RPTALL	Use with /REPORT.	Include the names of all scanned files in the report file.
/RPTCOR	Use with /REPORT.	Include a list of corrupted files in the report file.
/RPTERR	Use with /REPORT.	Include system errors in the report file. System errors can include problems reading or writing to a disk or hard disk, file system or network problems, problems creating reports, and other system-related problems.
/VIRLIST	None.	Display the name of each virus that the scanner can detect. This option produces a long list, which is best viewed from a text file. To do this, type: SCAN /VIRLIST /REPORT <filename.txt> For full details about each virus, see the Virus Information Library (see *Contacting McAfee Security & Network Associates* on page 8).

Alphabetic list of options

For convenience, the options are repeated in this section alphabetically with a brief description. For full descriptions, see the previous sections.

Table 3-6. Alphabetic list of options

Option	Description	See ...
/?	Display a list of command-line options, each with a brief description.	page 23
/AD	Same as /ALLDRIVES.	page 26
/ADL	Scan all local drives, including compressed and PC drives, in addition to any other drives specified on the command line. Do not scan disk drives.	page 26
/ADN	Scan all network drives, in addition to any other drives specified on the command line.	page 26
/AFC=<size>	Use a cache of specified size.	page 23
/ALL	Scan all files regardless of extension.	page 26
/ALLDRIVES	Scan all drives. Scan all network drives and local drives, but not removable drives; these include disk drives, CD drives, and Zip drives.	page 26
/ALLOLE	Treat all files as compound/OLE files regardless of file extension.	page 26
/ANALYSE	Same as /ANALYZE.	page 23
/ANALYZE	Scan for possible new viruses in programs and macros.	page 23
/APPEND	Append information to the specified report file instead of overwriting it.	page 32
/APPENDBAD	Append names of infected files to an existing file, as specified by /BADLIST.	page 23
/BADLIST <filename>	Create a list of infected files.	page 23
/BEEP	Issue a tone when an infected file is found.	page 23
/BOOT	Scan boot sector and master boot record only.	page 26
/BPRESTORE	Restore sectors from backup after cleaning.	page 23
/CHECKLIST <filename>	Scan the files listed in the specified file.	page 26
/CLEAN	Clean viruses from all infected files and system areas.	page 30
/CONTACTFILE <filename>	Display the contents of the specified file when a virus is found.	page 30
/DAM	Delete all macros in a file if an infected macro is found.	page 30
/DEL	Delete infected .COM and .EXE files.	page 30
/DOHSM	Scan files that are offline.	page 26
/DRIVER	Specify the location of the DAT files: scan.dat, names.dat, and clean.dat.	page 24
/EVLOG	Use NT Event Logging.	page 30

Table 3-6. Alphabetic list of options (*Continued*)

Option	Description	See ...
/EXCLUDE <filename>	Do not scan the files listed in the specified file.	page 26
/EXTLIST	Display names of file extensions that are scanned by default.	page 24
/EXTRA <filename>	Specify the location on any EXTRA.DAT file.	page 24
/FAM	Find all macros, not just macros suspected of being infected.	page 31
/FREQUENCY <hours>	Do not scan before the specified number of hours after the previous scan.	page 24
/HELP	Display a list of command-line options, each with a brief description.	page 24
/HTML <filename>	Display the results in HTML format.	page 24
/LOAD <filename>	Load scanning options from the named file, or scanning profile.	page 24
/LOCK	Halt and lock the computer if a virus is found.	page 31
/LOUD	Display a progress summary during the scan.	page 32
/MAILBOX	Scan plain-text mailboxes.	page 26
/MANALYSE	Same as /MANALYZE.	page 24
/MANALYZE	Scan for possible new viruses in macros.	page 24
/MANY	Scan multiple disks consecutively in a single drive.	page 27
/MAXFILESIZE <size>	Scan only files that are not larger than the specified number of megabytes.	page 27
/MIME	Scan inside MIME files.	page 27
/MOVE <dir>	Move all infected files found during a scan to the specified directory, preserving the drive letter and directory structure.	page 31
/NOBACKUP	Do not prompt for backup of sectors before attempting to clean.	page 27
/NOBEEP	Do not issue a tone when the scan ends.	page 31
/NOBOOT	Do not scan the boot sector.	page 27
/NOBKSEM	Prevent scanning of files that are normally protected.	page 24
/NOBREAK	Disable Ctrl-C and Ctrl-Break during scans.	page 27
/NOCOMP	Do not check compressed executables created with the LZEXE or PkLite file-compression programs.	page 27
/NOD	Use with /CLEAN. Do not scan all files regardless of extension.	page 27
/NODDA	Do not access disk directly. This prevents the scanner from accessing the boot record.	page 27
/NODECRYPT	Do not decrypt Microsoft Office compound documents that are password-protected.	page 28
/NODOC	Do not scan document files.	page 27

Table 3-6. Alphabetic list of options (*Continued*)

Option	Description	See ...
/NOEXPIRE	Disable the “expiration date” message if the scanner’s DAT files are out of date.	page 24
/NOJOKES	Do not report any joke programs.	page 28
/NOMEM	Do not scan memory for viruses.	page 28
/NORENAME	Do not rename an infected file that cannot be cleaned.	page 31
/NOSCRIPT	Do not scan these types of file: HTML, JavaScript, Visual Basic, and Script Component Type Libraries.	page 28
/OCMAX=<size>	Specify the maximum size of the internal cache for file reads.	page 25
/OCRS=<value>	Specify a value that represents the size of the internal cache size for each file read.	page 25
/PANALYSE	Same as /PANALYZE.	page 25
/PANALYZE	Scan for possible new viruses in programs.	page 25
/PAUSE	Enable a screen pause.	page 32
/PLAD	Preserve the last-accessed time and date for files that are scanned.	page 31
/PROGRAM	Scan for potentially harmful applications.	page 25
/REPORT <filename>	Create a report of infected files and system errors, and save the data to the specified file in ASCII text file format.	page 32
/RPTALL	Include the names of all scanned files in the report file.	page 33
/RPTCOR	Include a list of corrupted files in the report file.	page 33
/RPTERR	Include system errors in the report file.	page 33
/SECURE	Scan inside all files including compressed files regardless of file extension, and use heuristic analysis.	page 28
/SILENT	Do not display any information on-screen.	page 25
/STREAMS	Scan all streams within a file if it is in an NTFS partition on a Windows NT system.	page 25
/SUB	Scan any subdirectories inside a directory.	page 28
/TIMEOUT <seconds>	Set the maximum time to spend scanning any one file.	page 25
/UNZIP	Scan inside archive files, such as those saved in ZIP, LHA, PKarc, ARJ, WinACE, CAB, and CHM formats.	page 29
/WINMEM	Scan inside running processes.	page 29
/VIRLIST	Display the name of each virus that the scanner can detect.	page 33

Scanning your disks

Disks pose a threat because many viruses infect computers when a computer 'boots' from an infected disk, or when users copy, run, or install programs or files that are infected. If you scan all new disks *before first use*, you can prevent new viruses entering any computer system.

Always scan all disks you use. Do not assume that disks received from friends, co-workers, and others are virus-free. Disks can also pose a threat even if they are not bootable. Therefore, we recommend that you check that your disk drives are empty before you turn on your computer. Then your computer will not pick up a boot-sector virus from an infected disk that was inadvertently left in a disk drive.

Preparing your computer

The scanner needs to run from your hard drive in order to scan disks inserted into the disk drive. This means that if you have the program running from disks, and you have only one disk drive on your computer, you must install and run the scanner from your hard drive in order to scan disks in the disk drive. See page 11 for installation instructions.

Scanning a disk

1. Using the `CD` command, change to the directory where the scanner was installed.
2. Type: `SCAN A: /MANY`
3. Insert the first disk to scan into the A drive, and press ENTER.

   The program scans the disk and displays the names of any infected files.

   NOTE
   If the scanner detects a virus on this disk, it runs the command-line option that you chose for dealing with the virus. See page 43 for details on removing viruses.
4. Remove the scanned disk from the A drive.
5. Insert the next disk and press ENTER.

Repeat Step 4 and Step 5 for all disks that you need to scan.

Error levels

When you run the on-demand scanner in the MS-DOS environment, an error level is set. You can use the `ERRORLEVEL` value in batch files to take actions based on the results of the scan. See your MS-DOS operating-system documentation for more information.

The on-demand scanner can return the following error levels:

Table 3-7. Error Levels

Error Level	Description
0	No errors occurred; no viruses were found.
2	Data file integrity check failed.
6	A general problem.
8	Scanner was unable to find a DAT file.
10	A virus was found in memory.
12	Cleaning failed. The scanner tried to clean a file, but has failed for some reason, and the file is still infected.
13	One or more viruses or hostile objects were found.
15	Self-check failed; the scanner may be infected or damaged.
19	The scanner succeeded in cleaning all infected files.
20	Scanning was prevented because of the `/FREQUENCY` option. See page 24 for more information.
21	Computer requires a reboot to clean the infection.
102	The user quit via `Esc-X`, `^C` or `Exit` button. This feature can be disabled with the `/NOBREAK` option.

Handling error messages

You can often correct the message, `Invalid switch or incorrect usage` by checking the form of the command in the alphabetic list on page 34.

Where an option has a parameter, insert only one space between them. For example, the following commands are intended to scan all directories on the C disk, and list any infected files in the file named `BADLIST.TXT`. The first two commands are valid, but the third command gives an error message because it has more than one space between the `BADLIST` option and its parameter, `BADLIST.TXT`.

```
SCAN C:\ /SUB /BADLIST BADLIST.TXT
SCAN C:\    /SUB     /BADLIST BADLIST.TXT

SCAN C:\ /SUB /BADLIST     BADLIST.TXT
```

Removing Infections 4

Although they are far from harmless, *most* viruses that infect your computer do not destroy data, play pranks, or render your computer unusable. Even the rare viruses that carry a destructive payload usually produce their nasty effects in response to a trigger event. In most cases, unless you know that a payload has activated, you have time to deal with the infection properly. However, this unwanted computer code can interfere with your computer's normal operation, consume system resources and have other undesirable effects, so take viruses seriously and remove them when you encounter them.

Unusual computer behavior, unexplained crashes, or other unpredictable events might not be caused by a virus. If you believe you have a virus on your computer because of occurrences such as these, a scan might not produce the results you expect, but it helps eliminate one potential cause of your computer problems.

To clean your computer

If you have a virus or you suspect that you have a virus, and you have not yet installed the on-demand scanner, follow these steps:

1 Turn off your computer.

> **WARNING**
> Do not reboot using the reset button or CTRL + ALT + DELETE. If you do, some viruses might remain intact or drop destructive payloads.

2 Place a clean startup disk into the disk drive. If you do not have this disk, see *Creating an emergency disk* on page 45.

3 Turn on your computer.

4 At the command prompt, type: `SCAN /ADL /ALL /CLEAN`.

5 **If viruses were removed:**

Shut down your computer and remove the disk. Begin the installation procedure described on page 11.

To find and remove the source of infection, scan your disks immediately after installation. For information, see *Scanning your disks* on page 37.

If viruses were not removed:

If the scanner cannot remove a virus, you see one of the following messages:

```
Virus could not be removed.

There is no remover currently available for the virus.
```

If the scanner finds a virus in a file and cannot remove it, you must delete the infected file and restore a copy from backups. If the virus is found in the Master Boot Record, refer to Security Headquarters — AVERT (Anti-Virus Emergency Response Team) for information about manually removing viruses. See page 8.

If the scanner detects a virus

Viruses attack computer systems by infecting files — usually executable program files or macros inside documents and templates. The scanner can safely remove most common viruses from infected files.

However, some viruses are designed to damage your files beyond repair. The scanner can move these irreparably damaged or corrupted files to a quarantine directory or delete them permanently to prevent further infection.

If the scanner cannot clean an infected file, it renames the file to prevent its use. When a file is renamed, only the file extension (typically three letters) is changed. The following table shows the methods of renaming.

Table 4-1. Renaming infected files

Original	Renamed	Description
Not V??	V??	File extensions that do not start with V are renamed with V as the initial letter of the file extension. For example, MYFILE.DOC becomes MYFILE.VOC.
V??	VIR	File extensions that start with *v* are renamed as .VIR. For example, MYFILE.VBs becomes MYFILE.VIR.
VIR, V01-V99		These files are recognized as already infected, and are not renamed again.
<blank>	VIR	Files with no extensions are given the extension, .VIR.

For example, if an infected file called BAD.COM is found, the scanner attempts to rename the file to BAD.VOM. However, if a file of that name already exists in the directory, the scanner attempts to rename the file to BAD.VIR, BAD.V01, or BAD.V02, and so on.

For file extensions with more than three letters, the name is usually not truncated. For example, NOTEPAD.CLASS becomes NOTEPAD.VLASS. However, an infected file called WATER.VAPOR becomes WATER.VIR.

Removing a virus found in a file

If the scanner detects a virus in a file, it displays the path names of infected files and takes the action specified in either the loaded scanning profile or command-line options. See *Using the Command-Line Scanner* on page 15 for information about creating scanning profiles. For example:

- If you selected `/MOVE`, the scanner automatically moves the infected files to the specified quarantine directory.
- If you selected `/CLEAN`, the scanner attempts to clean the file.
- If you selected `/DEL` and this is an .EXE or .COM file, the scanner deletes the infected file.
- If you selected `/NORENAME`, the scanner does not rename the infected file.

NOTE

Take care if you are using more than one of these options in combination. For example, if you specify `/MOVE` and `/CLEAN` together, the scanner creates a copy of an infected file in the specified quarantine directory before attempting to clean the file. If you want to keep an infected copy for investigation, this is useful, but if you intend only to remove any virus that might be present on the computer, it is more beneficial and more secure to use `/CLEAN` on its own. Generally speaking, simply specifying more command-line options does not necessarily increase the benefit of the scanning.

Running additional virus-cleaning tasks

These tasks include:

- *Cleaning macro viruses from password-protected files*.
- *Cleaning Windows NT hard disks*.

Cleaning macro viruses from password-protected files

The scanner respects users' passwords and usually leaves them intact. For example, in password-protected Microsoft Excel 95 files, the scanner removes macro viruses without disturbing users' passwords.

However, macro viruses that infect Microsoft Word files sometimes plant their own passwords. Depending on the capabilities of the virus, the scanner takes one of the following actions when trying to clean a password-protected file:

- **If the macro virus can plant its own password:**
  The scanner cleans the file, removes the planted password, and removes the virus.
- **If the macro virus cannot plant its own password**:
  The scanner notes the infection but does not remove the password.

Cleaning Windows NT hard disks

To clean the Master Boot Record (MBR) on a hard disk formatted with the Microsoft Windows NT file system (NTFS):

1. Start the computer that has the NTFS file system partition from a virus-free MS-DOS boot disk.
2. Run the scanner, using `SCAN /BOOT /CLEAN`. Be sure to run the scanner from a disk that you know is free from viruses.

This cleans the NTFS file system Master Boot Record, but the scanner cannot read the rest of the NTFS file system partition when you boot into a MS-DOS environment. To scan the rest of the NTFS file system partition, reboot into Windows NT, then run the scanner again.

Creating an emergency disk

In case your computer becomes infected, you need a clean startup, also called boot, or emergency disk. This section describes how to create that emergency disk. Any virus in your system might be transferred to your emergency disk and infect your computer again, so your computer *must* be virus-free to create it. If your computer is infected, go to another computer and scan it. If it is virus-free, create your boot disk at that computer.

This emergency disk is for scanning the boot sector and system files only; it is not intended for normal scanning.

> **NOTE**
> Because Windows NT cannot boot from a disk, you can format this boot disk from within a Windows NT environment.

To create a boot disk:

1. Exit from Windows or any applications to get the command prompt (`C:\>`).
2. Insert a blank, *unformatted* disk into the A drive.
3. Format the disk by typing the following command at the command prompt:

   ```
   FORMAT A: /S /U
   ```

   This overwrites any information already on the disk.
4. When you are prompted for a volume label, type an appropriate name for your startup disk.
5. Locate `HIMEM.SYS` on your hard drive.
   - **MS-DOS users:** By default, this file is in the `\DOS` directory.
   - **Windows users:** By default, this file is in the `\WINDOWS\COMMAND` directory.
6. Copy `HIMEM.SYS` to your A drive by typing the following at the command prompt:

   ```
   COPY HIMEM.SYS A:\
   ```

7 Create a file called CONFIG.SYS.

You can do this from within MS-DOS, or by using Notepad or any other text editor.

> **NOTE**
> A true text editor, such as Edit (in MS-DOS) or Notepad, saves characters to a file without additional formatting. However, most word-processing programs add extra information that can render a file unusable as a .TXT file. If you use a program such as Word or Wordpad to create text files, *save them in .TXT format.*

To create CONFIG.SYS at the command prompt:

a Type EDIT to start the MS-DOS editing program.

b Type the following lines:

```
DEVICE=HIMEM.SYS
DOS=HIGH
```

c Select **File, Save As** and type the name CONFIG.SYS.

d Click **OK** to save the file.

e Select **File, Exit** to close Edit and return to the command prompt.

To create CONFIG.SYS using Notepad or any other text editor:

a Launch the editing program, and open a new file.

b Complete Step b through Step e above.

8 Change to the scanner's program directory (as set up in Step 1 on page 11).

9 Copy the command-line version of the scanner software to the disk by typing the following commands at the command prompt:

```
COPY BOOTSCAN.EXE A:\

COPY EMSCAN.DAT A:\SCAN.DAT
COPY EMCLEAN.DAT A:\CLEAN.DAT
COPY EMNAMES.DAT A:\NAMES.DAT
COPY LICENSE.DAT A:\
COPY MESSAGES.DAT A:\
```

You have now copied, and renamed where necessary all the files that the scanner needs to scan the boot sector of an infected computer.

10 Copy any other MS-DOS utilities you might need to start your computer, to debug your system software, to manage any extended or expanded memory, or to do other tasks at startup. If you use a disk-compression utility, copy the drivers you need to decompress your files.

You have now copied all necessary programs for rebooting your computer onto this boot disk.

11 You might want to copy these additional useful command-line programs to a *second* disk:

NOTE
Do not copy the following programs to the clean boot disk you are making. Conventional disks do not have enough space to store both the scanner software and these programs.

DEBUG.*	LABEL.*
DISKCOPY.*	MEM.*
FDISK.*	SYS.*
FORMAT.*	XCOPY.*

If you use a disk-compression utility or a password-encryption utility, copy the drivers required to access your drives onto the clean boot disk. See the documentation for those utilities for more information about those drivers.

12 Label and write-protect these disks, and store them in a secure place.

Updating Your Anti-Virus Protection 5

Hundreds of new viruses are discovered every month. To offer you the best protection possible, we continually update the virus definition (DAT) files that the scanner uses to detect viruses. Although your software has technology that allows it to detect previously unknown strains of viruses or potentially harmful software, new virus types and other agents appear frequently.

The DAT files that came with your original copy of the anti-virus scanner might not be able to help the software detect a virus that was discovered months later. For maximum protection, we strongly recommend that you update your files regularly.

The command-line scanner uses the same virus definition files as our other anti-virus products that might be installed in your network, so you can be sure that with current DAT files in place, a command-line scanner offers the same protection as our other anti-virus software.

To update DAT files for the command-line software:

1. Download the DAT file, for example, dat-4320.zip, from the web site or FTP site. See *Contacting McAfee Security & Network Associates* on page 8 for the addresses.

   When you are selecting the latest DAT files, ignore any references to SuperDAT (a self-installing DAT file). You cannot use this type of file with the command-line scanner.

2. Create a temporary directory on your hard disk.

3. Copy the downloaded DAT file to the temporary directory.

4. Locate the directories on your hard drive where the command-line scanner is currently loaded (as set up in Step 1 on page 11).

5. The downloaded DAT file is in a compressed .ZIP format. Use a compression utility such as WinZip or PKZip to extract the files from the .ZIP file into that directory. Be sure to extract all the files. If using WinZip, select the **Use Folder Names** and the **All Files** options.

6. Allow the updated files to overwrite the existing DAT files.

   NOTE
   If other VirusScan products are loaded on your computer, or if you chose custom installation options, some DAT files might be located in more than one directory. If so, save these updated DAT files to each directory.

Index

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W