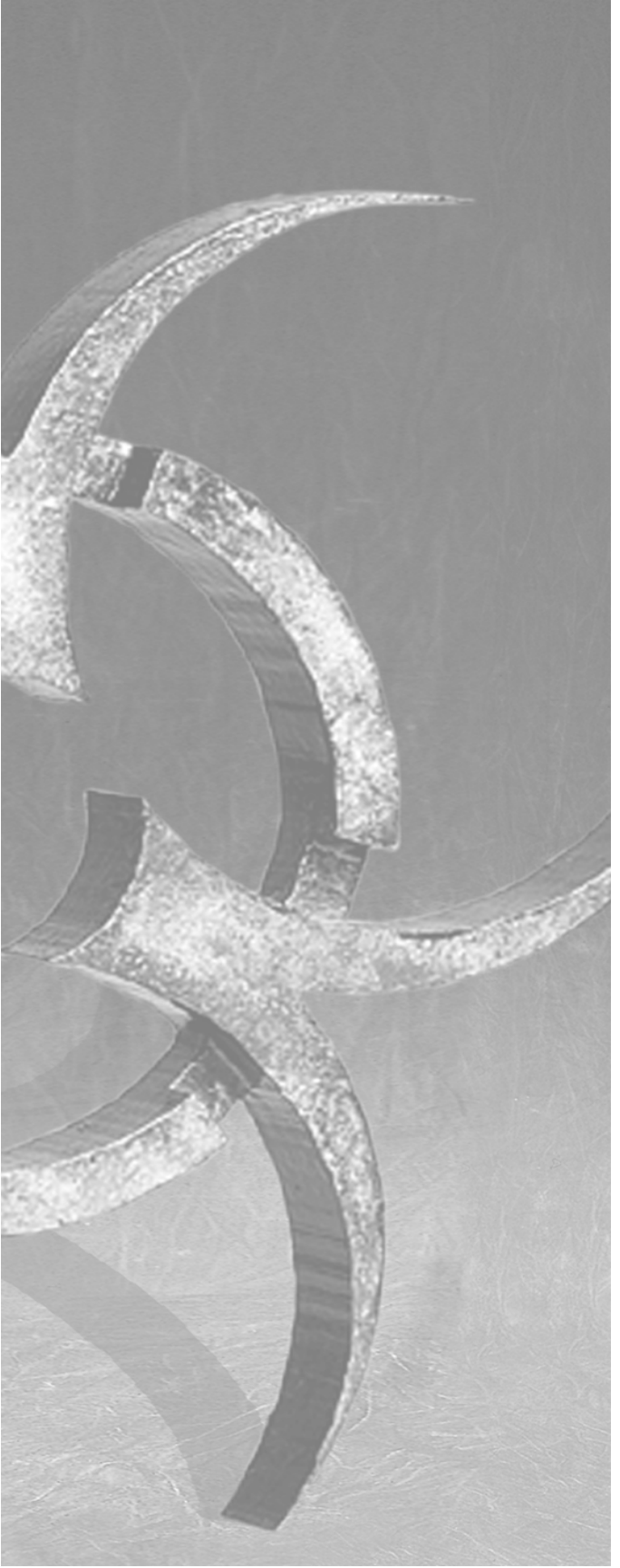

VirusScan Command Line Anti-Virus Software

Product Guide

Version 4.16.0

McAfee

A Network Associates Company

Table of Contents

Preface

Purpose

This Product Guide provides the following information: descriptions of all product features, instructions for configuring and deploying the software, and procedures for performing tasks. It also provides a roadmap for getting additional information or help.

Audience

This guide is designed for people with some responsibility for configuring and using the software on their own workstations.

Getting more information

HELP	Additional information about the product available in the Help system that is included in the application. To access Help topics, use the the /? parameter in the application.
README.TXT	Product information, system requirements, resolved issues, any known issues, and last-minute additions or changes to the product or this guide.
CONTACT.TXT	A list of phone numbers, street addresses, web addresses, and fax numbers for Network Associates offices in the United States and around the world. It also includes contact information for services and resources, including: • Technical Support • Customer Service • Download Support • AVERT Anti-Virus Research Site • McAfee Beta Site • On-Site Training • Network Associates Offices Worldwide • Resellers
LICENSE.TXT	The terms under which you may use the product. Read it carefully. If you install the product, you agree to the license terms.

Contacting McAfee and Network Associates

Technical Support	http://knowledge.nai.com
Product Documentation	tvd_documentation@nai.com
McAfee Beta Site	www.mcafeeb2b.com/beta/
AVERT Anti-Virus Research Site	www.mcafeeb2b.com/avert
Download Site	www.mcafeeb2b.com/naicommon/download/
.DAT File Updates	www.mcafeeb2b.com/naicommon/download/dats/find.asp
Product Upgrades	www.mcafeeb2b.com/naicommon/download/upgrade/login.asp Valid grant number required. Contact Network Associates Customer Service.
On-Site Training	www.mcafeeb2b.com/services/mcafee-training/default.asp
Finding a Reseller	www.mcafeeb2b.com/naicommon/partners/tsp-seek/intro.asp

Network Associates Customer Service

E-mail	services_corporate_division@nai.com
Web	www.nai.com www.mcafeeb2b.com

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 — including toll-free numbers for other geographic areas — see the CONTACT.TXT file that accompanied this product release.

Introduction 1

What is a command-line scanner?

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

The command-line scanner enables you to search for viruses in any drive, folder, or file in your computer "on demand" or, 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.

The scanner, kept current with updated virus definition (.DAT) files from McAfee AVERT labs, can serve as an important part of your network security. We strongly urge you to set up an anti-virus security policy for your network, incorporating as many protective measures as possible.

How does a command-line scanner work?

The scanner acts as an interface to the powerful anti-virus scanning engine—the engine common to all McAfee and Dr. Solomon's products.

To run a scan operation, type `scan` at the command line with the options you want. For a complete list of options, see "On-Demand Scanning" on page 17.

The Command-Line scanner consists of a set of programs for running targeted scan operations from the MS-DOS Prompt or Command Prompt windows, or from protected MS-DOS mode. The set includes:

- SCAN.EXE. This scanner runs only in 32-bit environments. This is the main command-line interface. When you run this file, it first checks its environment to see whether it can run by itself. If your computer is running in 16-bit or protected mode, SCAN.EXE transfers control to one of the other programs—SCANPM.EXE or SCAN86.EXE.
  - SCANPM.EXE. This runs in 32-bit environments. It provides you with a full set of scan options for 32-bit protected-mode DOS environments. It also includes support for extended memory and flexible memory allocations. SCAN.EXE transfers control here when its specialized capabilities can enable your scan operation to run more efficiently.

- SCAN86.EXE. This runs only in 16-bit environments. It includes a limited set of capabilities for 16-bit environments. SCAN.EXE transfers control here if your computer is running in 16-bit mode, but without special memory configurations.

Installing Command-Line Software 2

Before you begin

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

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

System requirements

- An IBM-compatible personal computer with an Intel 80386 processor, or an equivalent, running DOS version 5.0 or later. The SCAN86.EXE component requires a computer with only an Intel 8086 processor or equivalent.
- For best results, we recommend at least 4MB of memory and 4MB of free hard drive space. The SCAN86.EXE component requires only 500KB of memory.

Installing VirusScan software

If you suspect your system is already infected, see "If you suspect you have a virus" on page 43 before you install the scanner software.

To install VirusScan software

1. Create a directory for the software on your hard disk.
2. Depending on the source of your command-line program files, complete a, b, or c:
    a. If you are installing from a compact disc, insert the compact disc containing the files into your CD-ROM drive, then copy the files from the CD-ROM to the directory you created earlier.

b. If you are installing from diskettes:

- Insert the first diskette into your A drive.
- Change to the A drive, then copy the files from your diskette drive to the directory you created in Step 1.

c. If you are installing from files you downloaded from a web site, decompress the zipped files into the directory you created on your hard disk.

> **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 start-up disk. See "Creating an emergency diskette" on page 47 for more information.

To run the scanner from a 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 VirusScan software from the file.
2. Create a batch file named LOGIN.BAT.
3. Add a call to the scanner, with the options you want to include, to the first line of the batch file.
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, this places your computer 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. But 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.

You can protect yourself by ensuring that you do the following:

- Download your files only from the McAfee or Network Associates web site, bulletin board, or other approved electronic source such as AOL or CompuServe.
- Validate the files that you download. (The software package includes a validation program, VALIDATE.EXE.)

When you download a file from any other source, it is important to verify that it is authentic, unaltered, and not infected. To facilitate this, 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, 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 VirusScan software as described in "Installing VirusScan software" on page 11.
2. Click **Start** in the Windows taskbar, 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. If you chose the default installation options, the files are located in this path:

   C:\PROGRAM FILES\NETA\SCAN

4. Run VALIDATE.EXE by typing `VALIDATE *.*` at the command prompt.

   VALIDATE.EXE examines all of the files in your VirusScan program directory, then generates a file list that includes:

   - Each file name
   - Its size in bytes
   - Its creation date and time
   - Two validation codes in separate columns.

   NOTE: If instead you want to verify individual files, follow the command, `validate` with the name of the file at the command prompt. You can also specify a range of files, using the DOS wildcards `?` and `*`.

5. We recommend that you redirect the output from VALIDATE.EXE to your printer so that you can review it easily. Complete one of the following steps to do this:

   - If you have set your printer to capture output from MS-DOS programs, type `validate >prn` at the command prompt. To learn how to set your printer to print from MS-DOS programs, consult your Windows documentation.
   - Alternatively, you can direct the output to a file on your hard drive. You can then print that file directly from any text editor, such as Microsoft Notepad. To direct the output to a file, type `validate *.* > c:\<directory name>\<filename>` at the command prompt.

   To finish the validation, you need to compare your output from VALIDATE.EXE with the validation codes in your copy of the software. Complete the sequence below to generate the packing list.

To generate the packing list and complete your comparison:

1. To display the packing list, type `packing.lst` at the command prompt, then press `ENTER`.
2. Complete one of the following steps to print the contents of the packing list:

   - Type `type packing.lst >prn` at the command prompt to redirect the output from PACKING.LST to your printer.

- Alternatively, you can direct the output to a file on your hard drive. You can then print the file directly from any text editor, such as Microsoft Notepad. To direct the output to a file, type `validate *.* > c:\<directory name>\<filename>` at the command prompt.

3. Compare the output from VALIDATE.EXE to that from 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; doing so can risk virus infection.

Checking your VirusScan 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 VirusScan software is ready to scan your system for infected files. You can verify that it 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 DOS or Windows text editor, then type the following character string as *one line, with no spaces or carriage returns*:

   ```
   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 carriage returns. 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 VirusScan 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 VirusScan software and allow it to scan the directory that contains EICAR.COM. When the VirusScan software examines this file, it reports `"Found EICAR test file NOT a virus."`

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

Removing VirusScan software

Change to the VirusScan Command-Line program directory, then delete all VirusScan files from your hard disk.

On-Demand Scanning 3

What is on-demand scanning?

An on-demand scan operation is one that you initiate. You maintain full control over the scope of the scan operation, how the software notifies you or others if it finds a virus, and how you want it to handle any corrupted files.

You can set the scanner to run when you start up your computer and thereby provide regular protection. To learn how to configure a scan operation to run at system startup, see page 21.

When should you scan?

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

The on-demand 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 scanner's FREQUENCY option sets a mandatory period between scans, to help minimize resources when the network is most busy. A full list of options begins on page 24.

What can you scan?

File types scanned by default

These file types as well as 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, .TD0, .??_, and .ZIP files.

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

NOTES: You can use the switches /UNZIP and /NOCOMP to help configure how the scanner handles compressed files. These and other scan options are described in the tables from pages 27 to 31.

The scanner cannot scan compressed files in low-memory (16-bit) environments.

What is heuristic analysis?

An anti-virus scanner uses two techniques to detect viruses: signatures 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. This approach cannot detect a new virus because its signature is not yet known, therefore another technique, known as *heuristic analysis* is employed.

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 of self-propagation. 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 being detected, 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

Unlike previously known methods of file infection (adding the virus body at beginning, ending or any other part of a host file), a "Stream" virus exploits the NTFS file system (in Windows NT/2000) feature, which allows multiple data streams. For instance, a Windows 95/98 (FAT) file has only one data stream – the program code or data itself. Windows NT/2000 (NTFS) enables users to 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 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.

Examples

If `file:stream` contains a virus, these commands have the following effect.

Table 3-1. Scanning streams

Command	Action
`scan /all /streams file`	The virus is detected. All streams were scanned.
`scan /all file:stream`	The virus is detected. The exact stream name was specified.
`scan /all /streams file:stream`	The virus is detected. The exact stream name was specified.
`scan /all file:str*`	The virus is not detected. An exact stream name was *not* specified.
`scan /all /streams file:str*`	The virus is detected. All streams beginning with “str” are scanned.
`scan /all file`	The virus is not detected. No streams were named.

Understanding on-demand scan operations

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

Example 1: Determining scan targets

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 27 for a list of these options.

To start a scan operation from the command line:

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
   ```

3. Press ENTER on your keyboard to start the scan operation.

   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
   ```

3. Press ENTER on your keyboard to start the scan operation.

   The scanner scans all network drives and generates a text file of the results. The contents of the report are identical to what 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 operation to a file.

To add to a file:

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
   ```

3. Press ENTER on your keyboard to start the scan operation.

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

Example 4: Creating a scanning profile

Instead of typing all of the options for a scan operation at the command line 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 command-line options to configure your scan task in the same way that you type them at the command line. Save the file to the VirusScan program directory as SAMPLE.TXT.
3. To start a scan operation with these options, type the following line at the command prompt:

   ```
   scan /load sample.txt
   ```

Configuring a scan operation to run at system startup

To have your computer scan for viruses each time it starts, you can have the scanner start when you start your computer and load its command-line options from a scanning profile you created.

To configure a virus scan operation at system startup:

1. Change to the root directory by typing `cd c:\` at the command prompt.
2. Type the following:

   ```
   edit autoexec.bat
   ```

The DOS text editor starts.

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 system 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 the Acid.674 virus !!!

C:\DIR1\SCANTEST\virtest.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 the Acid.674 virus !!!

C:\DIR1\SCANTEST\virtest.com ... Found: EICAR test file NOT a virus.

C:\DIR2\prices.doc ... Found: virus or variant W97M/Concept !!!

C:\DIR2\Costs\may2000.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
```

On-demand scanning options

The scanning options are organized into several functional groups:

- "General options" on page 24
- "Target options" on page 27
- "Response and notification options" on page 31
- "Report options" on page 34

The options are also listed alphabetically (with briefer descriptions) on page 36.

General options

The following table lists the general scanning options.

General Command-Line 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.
/ANALYZE	Extended memory is required.	Scan using heuristics for both program viruses and macro viruses. You may type /ANALYSE instead. Note: Use /MANALYZE for macro viruses only; use /PANALYZE for program viruses only.
/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.
/BEEP	None.	Issue a tone when an infected file is found. By default, a tone is only issued when the whole scan operation ends.
/BPRESTORE	None.	Restore sectors from backup after cleaning.

General Command-Line Option	Limitations	Description
/EXTLIST	None.	Display names of file extensions that are scanned by default.
/EXTRA <*filename*>	None.	Specify an extra driver.
/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 24 for more details.
/HTML <*filename*>	None.	Display the results in HTML format.
/!IVN	None.	Display the internal version number.
/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 operation you have already configured by loading custom settings already saved in an ASCII-formatted file.
/MANALYZE	Extended memory is required.	Set the heuristic scanning features to find new macro viruses. You may type /MANALYSE instead. Note: Use /PANALYZE for program viruses only; use /ANALYZE for program and macro viruses.
/NOEXPIRE	None.	Disable the "expiration date" message if the scanner's data files are out of date. For more details, see "What are the .DAT files?" on page 51.
/PANALYZE	Extended memory is required.	Enable heuristics scanning for new program viruses. You may type /PANALYSE instead. Note: Use /MANALYZE for macro viruses only; use /ANALYZE for program and macro viruses.

General Command-Line Option	Limitations	Description
/PROGRAM	None.	Scan for malicious 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 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 18 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 an on-demand scan operation, you must specify a target location for the scan (such as C:\, A:\, /ADL, /ADN).

Target Command-Line Option	Limitations	Description
/AD	None.	Same as /ALLDRIVES.
/ADL	None.	Scan all local drives—including compressed and PC drives, but not diskette drives—in addition to any other drive specified on the command line.
/ADN	None.	Scan all network drives for viruses, in addition to any other drives specified on the command line.
/ALL	None.	Scan all files regardless of extension. Note: 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 diskette 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	Not with /NODDA.	Scan boot sector and master boot record only. Do not use this option with /NODDA.
/CHECKLIST <*filename*>	None.	Scan the files listed in the specified file. See page 22 for more details.
/DOHSM	On Windows NT only.	Scan files that are offline. Note: These are files that NT's Hierarchical Storage Management has archived because they have not been accessed for some time.
/EXCLUDE <*filename*>	None.	Do not scan the files listed in the specified file. Use this option to exclude specific files from a scan operation. List the complete path to each file on its own line. You may use wildcards, * and ?.

Target Command-Line Option	Limitations	Description
/MANY	None.	Scan multiple diskettes consecutively in a single drive. The program prompts you for each disk. You can use this option to check several diskettes quickly. You cannot use this option if you run the scanner from a boot disk and you have only one diskette drive.
/MAXFILESIZE <*nn.n*>	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 scan operations. Users can not halt scan operations in progress if this option is set.
/NOCOMP	Extended memory is required when decompressing files.	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 this option, the scan and cleaning is limited to the susceptible file types only, as recognized by their file extensions.
/NODDA	Do not use this option 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.

Target Command-Line Option	Limitations	Description
/NODOC	None.	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.
/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 jokes.
/NOMEM	None.	Do not scan memory for viruses. Use this option only when you are certain that your computer is virus-free.
/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.

Target Command-Line Option	Limitations	Description
/SUB	None.	Scan 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.
/UNZIP	Extended memory is required.	Scan inside archive files, including 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 are supported for cleaning. /CLEAN will not delete infected files within ZIPs nor will it rename infected files within ZIPs. /CLEAN will also not rename the ZIP file itself. If any files are identified within any other archive format that cannot be cleaned you must first extract them from the archive file.

Response and notification options

The following table lists the response and notification options after a virus has been detected.

Response and Notification Option	Limitations	Description

/ALERTPATH <*dir*>	This can only be used on networks where the servers are running the correct version of NetShield.	Designate a directory as a network path to a remote NetWare volume or Windows NT directory that is monitored by Centralized Alerting.
		The scanner sends an .ALR text file to the server when it detects an infected file.
		From this directory, NetShield will, through its Centralized Alerting feature broadcast or compile the alerts and reports according to its established configuration.
		Requirements:
		• These remote NetWare or Windows NT servers running NetShield for Windows NT v2.5.3 and later, or NetShield for NetWare v2.3.3 and later.
		• You must have write-access to the <*directory*> you specify.
		• <*directory*> must contain the NetShield-supplied CENTALRT.TXT file.
		Add these variables to your AUTOEXEC.BAT file to ensure that the .ALR file which is sent identifies the infected system and its user:
		`Set COMPUTERNAME=<name of computer>`
		`Set USERNAME=<user name>`

/CLEAN	None.	Clean viruses from *all* infected files and system areas.
/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. Note*:* Any character is valid in a contact message except a backslash (\). Messages beginning with a slash (/)or a hyphen (-) should be placed in quotation marks.

Response and Notification Option	Limitations	Description
/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 may choose to remove all macros from a data 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 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 switch to protect against viruses that infect file types other than .COM or .EXE.
/EVLOG	NT only.	Use NT Event Logging. Any detections are recorded in the Application Log of the Event Viewer.
/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 DOS systems only, not NT.	Halt and lock the system if a virus is found. This option is appropriate in vulnerable network environments, such as open-use computer labs. 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 system.

Response and Notification Option	Limitations	Description
/MOVE <*dir*>	None.	Move all infected files found during a scan operation to the specified directory, preserving the drive letter and directory structure. Note: This option has no effect if the Master Boot Record or boot sector is infected, because these are not files.
/NOBEEP	None.	Do not issue a tone when the scan operation ends. By default, a tone is issued at the end of a scan operation if an infection is found.
/NORENAME	None.	Do not rename an infected file that cannot be cleaned. For information about renaming, see page 45.
/PLAD	On NetWare volumes only.	Preserve the file's Last Access Date after scanning. Some software (such as used for creating backups or archives) relies on a file's Last Access Date to work correctly. If you set this option, the engine resets that date to its original value after scanning the file.

Report options

By default, the results of a scan operation 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 switches as needed. For examples of using reporting options, see page 20.

Report Command-Line Option	Limitations	Description
/ALERTPATH <*dir*>	None.	Designate the directory <*dir*> as a network path monitored by Centralized Alerting. See page 31 for a full description.
/APPEND	None.	*A*ppend information to the specified report file instead of overwriting it. Use this option with /REPORT <filename>.
/PAUSE	Not 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 PCs 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 Command-Line Option	Limitations	Description
/REPORT <*filename*>	Not 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.
/RPTALL	Specify with /REPORT.	Include the names of all scanned files in the report file.
/RPTCOR	Specify with /REPORT.	Include a list of corrupted files in the report file.
/RPTERR	Specify 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 Library on the web site, http://vil.nai.com.

Alphabetic list of options

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

Command-line option	Description
/?	Display a list of command-line options, each with a brief description.
/AD	Same as /ALLDRIVES.
/ADL	Scan all local drives—including compressed and PC drives, but not diskette drives—in addition to any other drive specified on the command line.
/ADN	Scan all network drives for viruses, in addition to any other drives specified on the command line.
/ALERTPATH <dir>	Designate a directory as a network path to a remote NetWare volume or Windows NT directory that is monitored by Centralized Alerting.
/ALL	Scan all files regardless of extension.
/ALLDRIVES	Scan all drives. Scan all network drives and local drives, but not removable drives; these include diskette drives, CD drives, and Zip drives.
/ALLOLE	Treat all files as compound/OLE files regardless of file extension.
/ANALYZE	Scan using heuristics for both program viruses and macro viruses.
/APPEND	Append information to the specified report file instead of overwriting it.
/APPENDBAD	Append names of infected files to an existing file, as specified by BADLIST.
/BADLIST <filename>	Create a list of infected files.
/BEEP	Issue a tone when an infected file is found.
/BOOT	Scan boot sector and master boot record only.
/BPRESTORE	Restore sectors from backup after cleaning.
/CHECKLIST <filename>	Scan the files listed in the specified file.
/CLEAN	Clean viruses from all infected files and system areas.
/CONTACTFILE <filename>	Display the contents of the specified file when a virus is found.

Command-line option	Description
/DAM	Delete all macros in a file if an infected macro is found.
/DEL	Delete infected .COM and .EXE files.
/DOHSM	Scan files that are offline.
/EVLOG	Use NT Event Logging.
/EXCLUDE <filename>	Do not scan the files listed in the specified file.
/EXTLIST	Display names of file extensions that are scanned by default.
/EXTRA <filename>	Specify an extra driver.
/FAM	Find all macros, not just macros suspected of being infected.
/FREQUENCY <hours>	Do not scan before the specified number of hours after the previous scan.
/HELP	Display a list of command-line options, each with a brief description.
/HTML <filename>	Display the results in HTML format.
/!IVN	Display the internal version number.
/LOAD <filename>	Load scanning options from the named file, or “scanning profile.”
/LOCK	Halt and lock the system if a virus is found.
/MANALYZE	Set the heuristic scanning features to find new macro viruses.
/MANY	Scan multiple diskettes consecutively in a single drive.
/MAXFILESIZE <nn.n>	Scan only files that are not larger than the specified number of megabytes.
/MIME	Scan inside MIME files.
/MOVE <dir>	Move all infected files found during a scan operation to the specified directory, preserving the drive letter and directory structure.
/NOBACKUP	Do not prompt for backup of sectors before attempting to clean.
/NOBEEP	Do not issue a tone when the scan operation ends.
/NOBOOT	Do not scan the boot sector.

Command-line option	Description
/NOBREAK	Disable CTRL-C and CTRL-BREAK during scan operations.
/NOCOMP	Do not check compressed executables created with the LZEXE or PkLite file-compression programs.
/NOD	Use with /CLEAN. Do not scan all files regardless of extension.
/NODDA	Do not access disk directly. This prevents the scanner from accessing the boot record.
/NODECRYPT	Do not decrypt Microsoft Office compound documents that are password-protected.
/NODOC	Do not scan document files.
/NOEXPIRE	Disable the “expiration date” message if the scanner’s data files are out of date.
/NOJOKES	Do not report any jokes.
/NOMEM	Do not scan memory for viruses.
/NORENAME	Do not rename an infected file that cannot be cleaned.
/NOSCRIPT	Do not scan these types of file: HTML, Javascript, Visual Basic and Script Component Type Libraries.
/PANALYZE	Enable heuristics scanning for new program viruses.
/PAUSE	Enable a screen pause.
/PLAD	Preserve the file’s Last Access Date after scanning.
/PROGRAM	Scan for malicious applications.
/REPORT <filename>	Create a report of infected files and system errors, and save the data to the specified file in ASCII text file format.
/RPTALL	Include the names of all scanned files in the report file.
/RPTCOR	Include a list of corrupted files in the report file.
/RPTERR	Include system errors in the report file.
/SECURE	Scan inside all files (including compressed files) regardless of file extension, and use heuristic analysis.

Command-line option	Description
/SILENT	Do not display any information on screen.
/STREAMS	Scan all streams within a file if it is in an NTFS partition on a Windows NT system.
/SUB	Scan subdirectories inside a directory.
/TIMEOUT <seconds>	Set the maximum time to spend scanning any one file.
/UNZIP	Scan inside archive files, including those saved in ZIP, LHA, PKarc, ARJ, WinACE, CAB and CHM formats.
/VIRLIST	Display the name of each virus that the scanner can detect.

Scanning your diskettes

Why diskettes pose a threat

Many viruses invade computers when systems boot from an infected disk, or when users copy, run, or install programs or files that are infected. If you scan all new diskettes (floppy disks) *before first use* you can prevent new viruses entering any computer system.

You should always scan all diskettes you use. Do not assume that disks received from friends, co-workers, and others are virus-free.

Though it may be hard to believe, diskettes pose a threat even if they are not bootable. To help address this threat, we recommend that you check that your disk drives are empty before you turn on your computer. Then your system will not pick up a boot-sector virus from an infected diskette that was inadvertently left in a disk drive.

Preparing your system

The scanner needs to run from your hard drive in order to scan diskettes inserted into the diskette drive. This means that if you have the program running from diskettes, and you have only one diskette drive on your computer, you must install and run the scanner from your hard drive in order to scan diskettes in the diskette drive. (See Chapter 2, "Installing Command-Line Software," for installation instructions.)

Scanning a diskette

To scan a diskette:

1. Using the `cd` command, change to the directory where the scanner was installed.
2. Type:
   ```
   scan a: /many
   ```
3. Insert the first diskette to scan into the A drive, and press `ENTER`.

   The disk is scanned and the names of any infected files are displayed.

   > **NOTE:** If the scanner detects a virus on this disk, it runs the command-line option you chose for dealing with the virus. See "Removing a virus found in a file" on page 45 for details on removing viruses.

4. Remove the scanned diskette from the A drive.

5. Insert the next diskette and press ENTER.

Repeat Steps 4- 5 for all diskettes that need to be scanned.

Error levels

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

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

ErrorLevel	Description
0	No errors occurred; no viruses were found.
2	Data file integrity check failed.
6	A general problem.
8	Can not find a data file.
10	A virus was found in memory.
12	Clean failed. The scanner tried to clean a file, but that cleaning 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	All clean. The scanner succeeded in cleaning all infected files.
20	Scanning was prevented because of the /FREQUENCY switch. See page 25.
21	Computer requires a reboot to clean the infection.
102	The user quit via ESC-X, ^C or Exit button. Note: This feature can be disabled with the /NOBREAK command-line option.

Handling error messages

You can often correct the message, *Invalid switch or incorrect usage* by checking the form of the command in the list in "Alphabetic list of options" on page 36.

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

If you suspect you have a virus

Firstly, don't panic! Although far from harmless, *most* viruses that infect your machine will 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 see evidence of a payload that has activated, you will 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 them seriously and remove them when you encounter them.

Secondly, keep in mind that odd computer behavior, unexplained system 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 virus scan operation might not produce the results you expect, but it helps eliminate one potential cause of your computer problems.

To clean your system:

If you have or suspect that you have a virus, and you haven't 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 start-up diskette into the diskette drive. If you do not have a clean start-up disk, see "Creating an emergency diskette" on page 47.
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 diskette. Begin the installation procedure described in Chapter 2, "Installing Command-Line Software."

   To find and eliminate the source of infection, scan your diskettes immediately after installation. For information, see "Scanning your diskettes" on page 40.

   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 it from backups. If the virus was found in the Master Boot Record, refer to documents on the McAfee web site about manually removing viruses.

If the scanner detects a virus

Viruses attack computer systems by infecting files—usually executable program files or Microsoft Word 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 files, called "corrupted" files to a quarantine directory or delete them permanently to prevent further infection of your system.

If the scanner cannot clean an infected file, it renames the file to prevents 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 recognised 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 it to bad.vir. However, if a file of that name already exists in the directory, the scanner attempts to rename it to 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 Chapter 3, page 17 for details on 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 a .EXE or .COM file, the scanner deletes the infected file.
- If you selected /NORENAME, the scanner does not rename the infected file.

Running additional virus-cleaning tasks

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

Cleaning Windows NT hard disks

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

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

   This will clean 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 DOS environment. To scan the rest of the NTFS file system partition, reboot into Windows NT, then run the scanner again.

Creating an emergency diskette

In case your system becomes infected, you need a clean start-up (also called boot, or emergency) diskette. This section describes how to create that emergency diskette. Any virus in your system might be transferred to your emergency diskette and infect your system again, so your system *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 diskette at that computer.

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

IMPORTANT: Because Windows NT cannot boot from a diskette, you can format this boot diskette 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* diskette into the A drive.
3. Format the diskette by typing the following command at the command prompt:

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

   This overwrites any information already on the diskette.
4. When the system prompts you for a volume label, enter an appropriate name for your start-up diskette.
5. Locate HIMEM.SYS on your hard drive.
   - **DOS users:** By default, this 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 DOS, or by using Notepad or any other text editor.

   IMPORTANT: 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 additional 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, *be certain to save them in .txt format.*

   - To create CONFIG.SYS at the command prompt:

     a. Type:

        ```
        Edit
        ```

        The DOS editing program starts.

     b. Type the following lines:

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

     c. Select **File, Save As ...** and enter 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 steps b. through e. above.

8. Change to the scanner's program directory. By default, this is C:\NETA\SCAN.

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 DOS utilities you may need to start your computer, to debug your system software, to manage any extended or expanded memory you have, or to do other tasks at startup. If you use a disk-compression utility, copy the drivers you need to uncompress your files.
11. You have now copied all necessary programs for rebooting your system onto this boot diskette.
12. You may want to copy these additional useful command-line programs to a *second* diskette:

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

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

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

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

Using Virus Definition Files 5

What are the .DAT files?

Hundreds of new viruses are discovered each month. The virus definition (.DAT) files that came with your original copy of the anti-virus scanner might not be able to help the software detect a virus discovered months later.

The files named CLEAN.DAT, NAMES.DAT, and SCAN.DAT provide virus information to the anti-virus scanner. These are the virus definition files we are referring to in this Guide.

To have the best virus protection possible, you must regularly download and install updates to these three virus definition files that the anti-virus scanner use. McAfee continually updates these files. Weekly updates of .DAT files are available to licensed users at the McAfee web site (www.nai.com) and other electronic services.

If 90 days have passed since you last updated the .DAT file, the scanner notifies you that an update is needed. (You can turn off this feature by using the /NOEXPIRE option. See page 25.) Please see "Updating .DAT files" on page 52 for instructions on updating the DATs.

❑ **NOTE:** 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 other McAfee anti-virus software.

Updating .DAT files

The 4000 series of .DAT files are compatible with McAfee anti-virus products that use scan engine versions 4.1.xx only. The .DAT files included with this release of the software do *not* work with any VirusScan product that uses a 3.x or v2.x scan engine.

You may only download updated .DAT files as stated by the maintenance terms outlined in the README file that accompanies the software, and as detailed in the software license agreement.

To update .DAT files for the Command Line software:

1. Download the data file (for example, DAT-4160.ZIP) from any of these sources:
   - McAfee web site, http://www.nai.com
   - McAfee ftp site, at ftp://ftp.nai.com/pub/antivirus/datfiles/4.x
   - McAfee downloads are also available in the anti-virus area of AOL and CompuServe.

   IMPORTANT: When you are selecting the latest DATs, you will find references to self-installing .DAT files. You cannot use installable .DAT files with the Command-Line scanner.
2. Create a temporary directory on your hard disk.
3. Copy the .DAT file ZIP archive you downloaded to that temporary directory.
4. Locate the directories on your hard drive where Virus Scan is currently loaded. Typically, the files are stored in C:\NETA\SCAN.
5. The updated .DAT file you just downloaded is in a compressed "ZIP" format. Unzip the file using any PKUNZIP-compatible decompression software. If you do not have the decompression software, you can download PKUNZIP (shareware) from any of the McAfee electronic sites.
6. You can unzip the files directly to the Virus Scan Command-Line program directory. Allow the updated files to overwrite the existing .DAT files.

- **NOTE:** If other Virus Scan products are loaded on your system, 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

Symbols

B

C

D

E

F

G

H

I

J

L

M

N

O

P

Q

R

S

T

V

W