Product Guide

VirusScan® Command Line

version 5.10.0

McAfee®
System Protection

Industry-leading intrusion prevention solutions

McAfee®

Contents

1 Introducing VirusScan® Command Line

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 scanning engine. This section describes:

- Product features
- What's new in this release
- Using this guide
- Getting product information
- Contact information

Product features

When installed on your Microsoft Windows system, VirusScan® Command Line becomes an effective solution against viruses, Trojan-horse programs, and other types of potentially unwanted software.

The command-line scanner enables you to search for viruses in any directory 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 the scanner detects a virus or that enable the scanner to 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 a security policy for your network that incorporates as many protective measures as possible. The scanner acts as an interface to the powerful scanning engine — the engine common to all our security products.

What's new in this release

This release of VirusScan® Command Line includes the following new features or enhancements:

- More protection: Automatic identification and removal of viruses delivering the next generation of best-of-breed anti-virus scanning engines. It offers improved protection against existing, new and potential threats and increases the depth and breadth of the protection we provide.
- It's faster than before: We've listened to our customers who asked for a faster Engine and it delivers superior performance to current McAfee Anti-Virus products on all supported platforms.
- 100% drop-in compatibility with existing McAfee Anti-Virus products and DAT files. It's easy to upgrade; just replace your existing Engine with the new version and you're protected. No worrying about compatibility.

Using this guide

This guide provides information on installing, configuring and using your product. For system requirements, refer to the Release Notes. The following topics are included:

- *Introducing VirusScan® Command Line* on page 5.
  An overview of the product, including a description of new or changed features; an overview of this guide; McAfee contact information.
- *Installing VirusScan® Command Line* on page 10.
- *Using the Command-Line Scanner* on page 16.
  The command options organized as functions and in alphabetic order.
- *Removing Infections* on page 39.
- *Preventing Infections* on page 43.

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 workstations, or configuring the software's detection options.

Conventions

This guide uses the following conventions:

Bold Condensed	All words from the interface, including options, menus, buttons, and dialog box names. **Example:** Type the **User** name and **Password** of the appropriate account.

`Courier`	The path of a folder or program; 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\McAfee\EPO\3.5.0`
	Run this command on the client computer:
	`scan --help`

Italic	For emphasis or when introducing a new term; for names of product documentation and topics (headings) within the material. **Example:** Refer to the *VirusScan Enterprise Product Guide* for more information.
Blue	A web address (URL) and/or a live link. **Example:** Visit the McAfee web site at: `http://www.mcafee.com`
<TERM>	Angle brackets enclose a generic term. **Example:** In the console tree, right-click <SERVER>.
	**Note:** Supplemental information; for example, another method of executing the same command.
	**Tip:** Suggestions for best practices and recommendations from McAfee for threat prevention, performance and efficiency.
	**Caution:** Important advice to protect your computer system, enterprise, software installation, or data.
	**Warning:** Important advice to protect a user from bodily harm when using a hardware product.

Getting product information

Unless otherwise noted, product documentation comes as Adobe Acrobat .PDF files, available on the product CD or from the McAfee download site.

Product Guide — Product introduction and features, detailed instructions for installing and configuring the software, information on deployment, recurring tasks, and operating procedures.

Help — Brief descriptions of the most common options, accessed from the software application.

Release Notes — *ReadMe.* Product information, resolved issues, any known issues, and last-minute additions or changes to the product or its documentation. *A text file is included with the software application and on the product CD.*

License Agreement — The McAfee License Agreement booklet that includes all of the license types you can purchase for your product. The License Agreement presents general terms and conditions for use of the licensed product.

Contacts — Contact information for McAfee services and resources: technical support, customer service, Security Headquarters (AVERT), beta program, and training. *A text file is included with the software application and on the product CD.*

Contact information

Security Headquarters: AVERT

Home Page
http://www.mcafeesecurity.com/us/security/home.asp

Virus Information Library
http://vil.mcafeesecurity.com

AVERT WebImmune, Submitting a Sample *(Logon credentials required)*
https://www.webimmune.net/default.asp

AVERT DAT Notification Service
http://vil.mcafeesecurity.com/vil/join-DAT-list.asp

Download Site

Home Page
http://www.mcafeesecurity.com/us/downloads/

Anti-Virus DAT File and Engine Updates
http://www.mcafeesecurity.com/us/downloads/updates/default.asp
ftp://ftp.mcafee.com/pub/antivirus/datfiles/4.x

Anti-Spam Rules File and Engine Updates
ftp://ftp.mcafee.com/spamdefs/1.x/

Product Upgrades *(Logon credentials required)*
https://secure.nai.com/us/forms/downloads/upgrades/login.asp

HotFix and Patch Releases for Security Vulnerabilities *(Available to the public)*
http://www.mcafeesecurity.com/us/downloads/updates/hotfixes.asp

HotFix and Patch Releases for Products *(ServicePortal account and McAfee Technical Support grant number required)*
https://mysupport.nai.com/products/products.asp

Product End-of-Life Support
http://www.mcafeesecurity.com/us/products/mcafee/end_of_life.htm

Software and Hardware Technical Support

Home Page
http://www.mcafeesecurity.com/us/support/technical_support

KnowledgeBase Search
http://knowledgemap.nai.com/

McAfee Technical Support ServicePortal *(Logon credentials required)*
https://mysupport.mcafeesecurity.com

McAfee Security Alerting Service (MSAS)
http://mysupport.nai.com/supportinfo/psvans_info.asp

Customer Service

E-mail
https://secure.nai.com/us/forms/support/request_form.asp

Web
http://www.mcafeesecurity.com/us/support/default.asp

Phone — US, Canada, and Latin America toll-free:
+1-888-VIRUS NO or **+1-888-847-8766** Monday – Friday, 8 a.m. – 8 p.m., Central Time

For information on contacting McAfee worldwide offices:
http://www.mcafeesecurity.com/us/contact/home.htm

McAfee Beta Program

http://www.mcafeesecurity.com/us/downloads/beta/mcafeebetahome.htm

Training: McAfee University

http://www.mcafeesecurity.com/us/services/education/mcafee/university.htm

2 Installing VirusScan® Command Line

We distribute the VirusScan® Command Line software in two ways — on a CD, and as an archived file that you can download from our web site or from other electronic services.

Review the *Installation requirements* to verify that the software will run on your system, then follow the installation steps.

Installation requirements

To install and run the software, you need the following:

- An IBM-compatible personal computer with a Pentium or equivalent processor.
- 10 MB of free hard disk space for a full installation.
- For Microsoft Windows 98 systems, a minimum of 64 MB RAM is required, 128 MB IS recommended.
- For Microsoft Windows NT and later systems, a minimum of 128 MB RAM is required, 256 MB IS recommended.
- The 64-bit version requires an AMD64 processor, running a 64-bit Microsoft Windows operating system.
- A CD drive, if you are not downloading the software from a web site.

Other recommendations

To take full advantage of the regular updates to DAT files from our web site, you need an Internet connection, either through your local area network, or via a high-speed modem and an Internet Service Provider.

Installing the software

If you suspect your computer is already infected, see *Removing Infections* on page 39 before you install the scanner software.

1 Create a directory for the software on your hard disk. If you are using DOS, you may use `MKDIR`.

2 Depending on the source of your command-line program files, do one of the following:

- **CD**
  Insert the CD into your CD drive, then copy the files from the CD to the directory that you created in Step 1.
- **Files downloaded from a web site**
  Download the file to the directory that you created in Step 1, and decompress the zipped files into that directory.

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 If you are using DOS, add the directory you created in Step 1 to the `PATH` statement in your `AUTOEXEC.BAT` file.

To run the scanner before a workstation logs on to a Novell NetWare server

To enable the scanner to run on a personal computer before it can logon to a Novell NetWare server, use the following steps immediately after installation

1 Rename `LOGIN.EXE` (in the `SYS:\LOGIN` folder on the NetWare server) to `LOGIN1.EXE`, then remove any references to the scanning software from the file.

2 Create a batch file named `LOGIN.BAT`. See also *Sample batch file* on page 12.

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

```
SCAN /ADL /SECURE /NOBREAK
```

4 Add a call to the file `LOGIN1.EXE` to a subsequent line of the batch file. For example:

```
lOGIN1.EXE %1 %2 %3
```

The previous 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.

Sample batch file

The following code is provided only as a suggestion, for you to use and modify to suit your own purposes. It has not been thoroughly tested. This sample batch file assumes that SCAN and the DAT files are in the current directory. It enables the login to the Netware server only if the scan finds no viruses on the workstation. All local drives are scanned, and the user cannot press CTRL BREAK to quit the scan.

```
@ECHO OFF

SCAN /ADL /SECURE /NOBREAK

  IF ERRORLEVEL 102 GOTO ERR102
  IF ERRORLEVEL 21 GOTO ERR21
  IF ERRORLEVEL 20 GOTO ERR20
  IF ERRORLEVEL 19 GOTO ERR19
  IF ERRORLEVEL 15 GOTO ERR15
  IF ERRORLEVEL 13 GOTO ERR13
  IF ERRORLEVEL 10 GOTO ERR10
  IF ERRORLEVEL 8 GOTO ERR8
  IF ERRORLEVEL 6 GOTO ERR6
  IF ERRORLEVEL 2 GOTO ERR2
  IF ERRORLEVEL 0 GOTO ERR0

:ERR102
  ECHO User exited.
  GOTO EXIT

:ERR21
  ECHO Clean on reboot. Please restart this PC to complete cleaning.
  GOTO EXIT

:ERR20
  ECHO Frequency error (Don't scan N hours after the previous scan).
  GOTO EXIT

:ERR19
  ECHO All cleaned.
  GOTO EXIT

:ERR15
  ECHO Self-integrity check failed
  GOTO EXIT

:ERR13
  ECHO Virus found!
  GOTO EXIT

:ERR10
  ECHO A virus was found in memory!
  GOTO EXIT

:ERR8
  ECHO DAT file not found.
  GOTO EXIT

:ERR6
  ECHO There has been a problem [not a virus] with scan.
  GOTO EXIT

:ERR2
  ECHO DAT file integrity check failed.
  GOTO EXIT

:ERR0
  ECHO Scan completed successfully. No viruses found.
  LOGIN1.EXE %1 %2 %3

:EXIT
```

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 our scanning 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, scanning 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 the software package from our 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.EXE 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.EXE 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 task bar, choose a Command Prompt.

3 In the window that appears, change directory to the directory that contains the VirusScan® Command Line files. (In DOS, you can use the CD command.)

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:

```
AVVSCAN DAT 242681  03-26-04 4:40a   35B2 4690 AVVSCAN.DAT
```

5 Print this output so that you can review it easily. 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 file, PACKING.LST directly from any text editor, such as Microsoft Notepad.

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 it is installed, the program is ready to scan your computer for infected files. You can run a test to determine that the program is installed correctly and can properly scan for viruses. The test was developed by the European Institute of Computer Anti-virus Research (EICAR), a coalition of anti-virus vendors, as a method of testing 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*
```

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 scanner's 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 scanning 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.`

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 program

To remove the product from your system:

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

2 Delete all files in the directory.

Removing the software leaves your computer unprotected against virus attack. Remove the product only when you are sure that you can upgrade quickly to a new version.

If you are an administrator, ensure that your users cannot accidentally remove their VirusScan® Command Line software.

3 Using the Command-Line Scanner

The command-line scanner is a program that you can run from a command prompt. If the scanner has been added to PATH or is in the current directory, you can run a scan by typing SCAN at the command prompt with the options you want. For a complete list of options, see page 26.

You should scan any file that is new to your computer, especially any newly downloaded or installed files. If your computers are susceptible to infection, you should scan as often as once a day. The scanner operates with minimal use of system resources.

The following features offer optimum protection for your computer and network:

- On-demand scanning options let you start a scan immediately or schedule automatic scans.
- Advanced heuristic analysis detects previously unknown macro viruses and program viruses.
- Updates to virus definition files and upgrades to program components ensure that the program has the most current scanning technology to deal with threats as they emerge.

Later sections in this guide describe each of these features in detail.

The command-line scanner also includes options for administrators that help to ensure that the scanner is being used most efficiently. For example, the /FREQUENCY option (on page 28) 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.**

  The following file types and many other common file types that are susceptible to infection 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 scanning options are described in the tables from page 26 to page 31.

- **Any potentially unwanted software, cookies and registry entries**.

  The scanner detects and reports these items, enabling you to remove them if necessary.

Scanning diskettes

Diskettes 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.

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

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

   

   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 41 for details on removing viruses.

4. Remove the scanned disk from the A drive.

Repeat Step 3 and Step 4 for all disks that you need to scan.

Scanning files in remote storage

Under some Microsoft Windows systems, 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 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 multiple data streams feature in Windows NT and more recent Windows operating systems. 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 `*`.

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.

Scanning protected files

The scanner normally scans files such as other users’ profiles and recycle bins. To prevent this type of scanning in Windows NT or later systems, use `/NOBKSEM`.

Using memory caches

When scanning a file for viruses and other potentially unwanted software, the scanner 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 scanner 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 scanner to use a larger 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 changes the maximum size of the internal cache for file reads. By default, the scanner typically caches up to *eight* reads per file and uses a cache read size of 128KB — and therefore a maximum cache size of 1M, which is 128KB x 8).

When setting the maximum size explicitly, you must specify the value of /OCMAX as a number of Megabytes. See the following examples for /OCRS and /OCMAX.

- Use 512KB read size. This *implies* a maximum cache size (OCMAX) of 4MB (8 x 512KB).

```
SCAN C:\ /OCRS=2
```

- Use 1MB read size. This *implies* a maximum cache size (OCMAX) of 8MB (8 x 1MB).

```
SCAN C:\ /OCRS=3
```

- Use a 1MB read size, but limit the cache size to 4MB.

```
SCAN C:\ /OCRS=3 /OCMAX=4
```

- Use a 2MB read size, but limit the cache size to 8MB.

```
SCAN C:\ /OCRS=4 /OCMAX=8
```

AFC

When scanning files, the scanner 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 scanner 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 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.

When using the `/WINMEM` option, specify at least one file for scanning as well.

Examples

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

Running an on-demand scan

You can scan any file or directory on your file system from the command line by adding options to the basic command. When executed without options, the program simply displays a brief summary of its options. When executed with only a directory name specified, the program scans every file in that directory only, and issues a message if any infected files are found. The options fall into the following main groups:

- **Scanning options —** determine how and where the scanner looks for infected files. See page 26.

- **Response and notification options —** determine how the scanner responds to infected files. See page 31.
- **Report options** — determine how the scanner displays the results of the scan. See page 33.
- **General options —** for such things as user help. See page 34.

Each group of options appears in its own table with a description of its function. See *Choosing the options* on page 26 for details.

Command-line conventions

Use the following conventions to add options to the command line:

- Separate each option with spaces.
- Do not use any option more than once on the command line.
- Follow the syntax correctly.
- To start the program, at the command prompt, type:

  ```
  SCAN
  ```

  (This example assumes that the scanner is available in your search path.)
- To have the program examine a specific file or list of files, add the target directories or files to the command line after `SCAN`. You can limit your scan by excluding certain files from scans with the `/EXCLUDE` option. See page 27 for details.

General hints and tips

The following examples assume that the scanner is available in your search path.

- To display a list of all the options, each with a short description of their features, type the command:

  ```
  SCAN /HELP
  ```
- To display a list of all the viruses that the program detects, type the command:

  ```
  SCAN /VIRLIST
  ```
- To display information about the version of the program, type the command:

  ```
  SCAN /HELP
  ```
- To run a full scan on all drives, type the command:

  ```
  SCAN /AD
  ```
- To run a full scan on the network drives, type the command:

  ```
  SCAN /ADN
  ```

To ensure maximum protection from virus attack, you must regularly update your DAT files. See *Preventing Infections* on page 43 for details.

Configuring scans

Instead of running each scan with all its options directly from the command line, you can keep the options in a separate text file, known as a *task file*. In the file, you can specify the actions that the scanner must take when a virus is detected. This allows you to run complete scans with ease, and at any time; you need only specify the files or directories that you want to scan.

To configure a scan:

1. Choose the command options that you want to use.

   See *Choosing the options* on page 26 for a description of available options.

2. Type the command options into a text editor just as you might on the command line.

3. Save the text as a file.

4. Type the following at the command prompt:

   ```
   SCAN /LOAD <FILENAME> <TARGET>
   ```

   Here, <*FILENAME*> is the name of the text file you created in steps Step 2 and Step 3, and <*TARGET*> is the file or directory you want to scan.

   If the scanner detects no virus infections, it displays no output.

To learn how to specify the options, see *Command-line conventions* on page 21.

The following examples show how you can configure scans using task files. The examples assume the scanner is available in the search path.

Example 1

To scan files in the `C:\WINDOWS` directory according to the settings you stored in the task file `C:\TASKS\CONFIG1.TXT`, type the command:

```
SCAN /LOAD C:\TASKS\CONFIG1.TXT C:\WINDOWS
```

The contents of the file `C:\TASKS\CONFIG1.TXT` are:

```
/MOVE C:\VIRUSES /NOCOMP /MAXFILESIZE 4
```

They instruct the scanner to move any infected files to `C:\VIRUSES`, to ignore compressed executables created with LZEXE or PkLite, and to examine only files smaller than 4MB.

As an alternative, you can arrange the contents of the task file as single lines:

```
/MOVE C:\VIRUSES
/NOCOMP
/MAXFILESIZE 4
```

Example 2

To scan only files smaller than 4MB and to ignore compressed executables created with LZEXE or PkLite in three separate directories, type the command:

```
SCAN /LOAD C:\TASKS\CONFIG2.TXT  /CHECKLIST C:\CHECKS\CHECK1.TXT
```

The contents of the task file `C:\TASKS\CONFIG2.TXT` are:

```
/NOCOMP
/MAXFILESIZE 4
```

The contents of the checklist file `C:\CHECKS\CHECK1.TXT` are:

```
C:\WINDOWS
C:\BIN
C:\PERL
```

Scheduling scans

You can schedule scans to run automatically.

To configure a virus scan for Windows NT and later versions:

To run a scan each time the computer starts, use the `Start Menu\Programs\Startup` folder in the `C:\WINNT\Profiles` folder.

To schedule a scan at other times, use the Schedule service and `at` commands.

See the Windows Help on your computer for more information.

To configure a virus scan at startup on DOS:

By running a scanning task from the `AUTOEXEC.BAT` file, a computer can scan for viruses each time it starts.

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 task file you want to run at startup. You can add a series of such files, each separated with a space, to load multiple tasks.

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\MAY2005.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
```

Using heuristic analysis

A 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 uses 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. Options that use heuristic analysis include `/ANALYZE`, `/MANALYZE`, and `/PANALYZE`. See Table 3-2, *Scanning options* on page 26.

Producing reports

The scanner can report its results in a log file that you create and name. In this example, the scanner creates 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.
3. To create a running report of the scanner's actions, use the `/APPEND` option to add any results of the scan to a file. At the command prompt, type:

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

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

Choosing the options

The following sections describe the options that you can use to target your scans:

- *Scanning options*.
- *Response and notification options* on page 31.
- *Report options* on page 33.
- *General options* on page 34.

The options are also listed alphabetically with brief descriptions on page 35.

In the descriptions, variables such as file names or path appear in chevrons (< >). To learn how to add these to the command line, see *Command-line conventions* on page 21.

Scanning options

Scanning options describe how and where each scan looks for infected files. You can use a combination of these options to customize the scan to suit your needs.

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

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

Table 3-2 Scanning options

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 removable media.
`/ADN`	None.	Scan all network drives, in addition to any other drives specified on the command line.
`/AFC=<SIZE>`		Specify the size of the file cache. By default, the cache size is 12MB. A larger cache size can improve scanning performance in some cases, unless the computer has low memory. The range of sizes allowed is 8MB to 512MB. Specify the size in megabytes. For example, to specify a 64MB cache, use `/AFC=64`. See also *AFC* on page 19.
`/ALL`	See note on page 30.	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.	Check every file for OLE objects.

Table 3-2 Scanning options (continued)

Option	Limitations	Description
/ANALYZE /ANALYSE		Use heuristic analysis to find possible new viruses in "clean" files. This step occurs after the program has checked the file for other viruses and potentially unwanted software. See *Using heuristic analysis* on page 25 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 also *Creating a list of infected files* on page 24.
/BADLIST <*FILENAME*>	None.	Create a list of infected files. See also *Creating a list of infected files* on page 24.
/BOOT	Do not use with /NODDA.	Scan boot sector and master boot record only.
/BPRESTORE	None.	Restore sectors from backup after cleaning.
/CHECKLIST <*FILENAME*>	None.	Scan the files listed in the specified file. See also *Creating a list of infected files* on page 24.
/DOHSM	On Windows NT and later versions 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 and *Scanning files in remote storage* on page 18.
/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 it cannot find these data files, it issues exit code 6.
/EXCLUDE <*FILENAME*>	None.	Exclude the directories or files from the scan as specified in <*FILENAME*>. List the complete path to each directory or file on its own line. You may use wildcards, * and ?.
/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. If you do not use this option in the command line, the program looks in the same directory from where it was executed. If it cannot find this file, the program issues exit code 6.
/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 a file is infected, you can remove all macros from the file using the /FAM and /DAM options together, although this should be used with caution. For example: SCAN <*FILENAME*> /FAM /DAM

Table 3-2 Scanning options (continued)

Option	Limitations	Description
/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.
/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. See also *Configuring scans* on page 22 and *Scheduling scans* on page 23.
/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. This option detects, but does not rename or clean mail items. The item must be extracted and cleaned separately.
/MANALYZE /MANALYSE		Use heuristics analysis to identify potential macro viruses. (In Microsoft Word, you can automate a task by using a *macro* - a group of Word commands that run as a single command.) This option is a subset of /ANALYZE. See *Using heuristic analysis* on page 25 for more information.
/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. This option is applicable to floppy disks and LS120 media diskettes only. See also *Scanning diskettes* on page 17.
/MAXFILESIZE <*SIZE*>	None.	Examine only those files that are smaller than the specified size. Specify the file size in megabytes. For example, /MAXFILESIZE 5 means scan only files that are smaller than 5MB.
/MIME	None.	Scan MIME-encoded files. This type of file is not scanned by default.
/NOBACKUP	None.	Do not prompt for backup of sectors before attempting to clean.
/NOBKSEM	Windows NT and later versions 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 18 for details.
/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.

Table 3-2 Scanning options (continued)

Option	Limitations	Description
/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	Use with */CLEAN*.	Scan only the susceptible file types. 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. See *File types scanned by default.* on page 17.
/NODDA	Do not use with /BOOT.	Do not access disk directly. This prevents the scanner from accessing the boot record. You might need to use this option on some device- driven drives.
/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.
/NODOC	See note on page 30.	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.
/NOEXPIRE	None.	Disable the "expiration date" message if the scanner's DAT files are out of date. For more details, see *Preventing Infections* on page 43.
/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.
/NOSCRIPT	None.	Do not scan files that contain HTML, JavaScript, Visual Basic, or Script Component Type Libraries. This type of file is normally scanned by default. Stand-alone JavaScript and Visual Basic Script files will still be scanned.
/OCMAX=<*SIZE*>	Use with Microsoft Windows only.	Specify the maximum size of the internal cache for file reads. The size must be specified in megabytes. See also *Using memory caches* on page 19.
/OCRS=<*VALUE*>	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 also *Using memory caches* on page 19.
/PANALYZE /PANALYSE		Use heuristic analysis to identify potential new program viruses. By default, the program scans only for known viruses. This option is a subset of /ANALYZE. See also *Using heuristic analysis* on page 25.

Table 3-2 Scanning options (continued)

Option	Limitations	Description
/PROGRAM	None.	Scan for potentially unwanted applications. Some widely available applications such as "password crackers" can be used maliciously or can pose a security threat.
/SECURE	None.	Examine all files, decompress archive files, and use heuristic analysis. This option activates the /ANALYZE, and /UNZIP options.
/SHOWCOMP	None.	Report any files that are packaged.
/STREAMS	NTFS only, run from within Windows NT and later versions.	Scan all streams within a file if it is in an NTFS partition. See also *Scanning NTFS streams* on page 18.
/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.
/TIMEOUT *<SECONDS>*	None.	Set the maximum time to scan any one file.
/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 clean infected files found within any other archive format; you must first extract them manually 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 also *Scanning processes in memory* on page 20.

Response and notification options

The response and notification options determine how the scanner responds to an infection. You can use a combination of these options to customize the scan. None of the options in the following table occur automatically. To activate each option, specify it in the command line.

Table 3-3 Response and notification options

Option	Limitations	Description
/CLEAN	None.	Automatically remove any infections. By default, the program states only that infections were found but does not try to clean the infected files. If the program cannot clean the file, it displays a warning message. If you use this option, repeat the scan to ensure that there are no more infections. See *If the scanner detects a virus* on page 41 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, although this should be used with caution. 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 41 for more information.
/EVLOG	On Windows NT and later versions.	Use Event Logging. Any detections are recorded in the Application Log of the Event Viewer.
/LOCK	In MS-DOS systems only, not Windows NT or later.	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.

Table 3-3 Response and notification options (continued)

Option	Limitations	Description
/MOVE *<DIR>*	None.	Move any infected files to a quarantine location as specified. When the program moves an infected file, it replicates the full directory path for the infected file inside the quarantine directory, so that you can determine the original location of the infected file. 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 41 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 41. See *If the scanner detects a virus* on page 41 for more 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 that you do not use this option with the report options, /REPORT, /RPTALL, /RPTCOR, and /RPTERR.
/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 scanner 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, see *Producing reports* on page 25.

Table 3-4 Report options

Option	Limitations	Description
/APPEND	Use this option with /REPORT.	Append information to the specified report file instead of overwriting it.
/HTML *<FILENAME>*	None.	Create a file containing the results in HTML format.
/LOUD	None	Display a progress summary during the scan. Note that this option can produce a large amount of information.
/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 more information 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 /APPEND /REPORT *<FILENAME>* We recommend you do not use /PAUSE when using any report option.
/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 *Contact information* on page 9).

General options

General options provide help or give extra information about the scan. You may use a combination of these options to customize the scan. None of the options in Table 3-5 occur automatically. To activate each option, specify it as part of the command line.

Table 3-5 General options

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 task.
/BEEP	None.	Issue a tone when an infected file is found. By default, a tone is only issued when the scan ends.
/EXTLIST	None.	Display names of file extensions that are scanned by default.
/HELP	None.	See the /? option.
/NORECALL	Use with /DOHSM	Do not move files from remote storage into local storage after scanning. See also *Scanning files in remote storage* on page 18.
/SILENT	None.	Do not display any information on-screen.

Options in alphabetic order

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 34
/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 removable media.	page 26
/ADN	Scan all network drives, in addition to any other drives specified on the command line.	page 26
/AFC=<SIZE>	Specify the size of the file cache.	page 26
/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	Check every file for OLE objects.	page 26
/ANALYSE	Same as /ANALYZE.	page 27
/ANALYZE	Use heuristic analysis to find possible new viruses in "clean" files.	page 27
/APPEND	Append information to the specified report file instead of overwriting it.	page 33
/APPENDBAD	Append names of infected files to an existing file, as specified by /BADLIST.	page 27
/BADLIST <FILENAME>	Create a list of infected files.	page 27
/BEEP	Issue a tone when an infected file is found.	page 34
/BOOT	Scan boot sector and master boot record only.	page 27
/BPRESTORE	Restore sectors from backup after cleaning.	page 27
/CHECKLIST <FILENAME>	Scan the files listed in the specified file.	page 27
/CLEAN	Automatically remove any infections.	page 31
/CONTACTFILE <FILENAME>	Display the contents of the specified file when a virus is found.	page 31
/DAM	Delete all macros in a file if an infected macro is found.	page 31
/DEL	Delete infected .COM and .EXE files.	page 31
/DOHSM	Scan files that are offline.	page 27
/DRIVER	Specify the location of the DAT files: SCAN.DAT, NAMES.DAT, and CLEAN.DAT.	page 27
/EVLOG	Use Event Logging.	page 31
/EXCLUDE <FILENAME>	Exclude the directories or files from the scan as specified in <FILENAME>.	page 27
/EXTLIST	Display names of file extensions that are scanned by default.	page 34
/EXTRA <FILENAME>	Specify the location on any EXTRA.DAT file.	page 27
/FAM	Find all macros, not just macros suspected of being infected.	page 27
/FREQUENCY <HOURS>	Do not scan before the specified number of hours after the previous scan.	page 28
/HELP	See the /? option.	page 34
/HTML <FILENAME>	Create a file containing the results in HTML format.	page 33

Table 3-6 Alphabetic list of options (continued)

Option	Description	See ...
/LOAD <FILENAME>	Load scanning options from the named file, or scanning profile.	page 28
/LOCK	Halt and lock the computer if a virus is found.	page 31
/LOUD	Display a progress summary during the scan.	page 33
/MAILBOX	Scan plain-text mailboxes.	page 28
/MANALYSE	Same as /MANALYZE.	page 28
/MANALYZE	Use heuristics analysis to identify potential macro viruses.	page 28
/MANY	Scan multiple disks consecutively in a single drive.	page 28
/MAXFILESIZE <SIZE>	Examine only those files that are smaller than the specified size.	page 28
/MIME	Scan MIME-encoded files.	page 28
/MOVE <DIR>	Move any infected files to a quarantine location as specified.	page 32
/NOBACKUP	Do not prompt for backup of sectors before attempting to clean.	page 28
/NOBEEP	Do not issue a tone when the scan ends.	page 32
/NOBKSEM	Prevent scanning of files that are normally protected.	page 28
/NOBOOT	Do not scan the boot sector.	page 28
/NOBREAK	Disable Ctrl-C and Ctrl-Break during scans.	page 28
/NOCOMP	Do not check compressed executables created with the LZEXE or PkLite file-compression programs.	page 29
/NOD	Scan only the susceptible file types.	page 29
/NODDA	Do not access disk directly. This prevents the scanner from accessing the boot record.	page 29
/NODECRYPT	Do not decrypt Microsoft Office compound documents that are password-protected.	page 29
/NODOC	Do not scan document files.	page 29
/NOEXPIRE	Disable the "expiration date" message if the scanner's DAT files are out of date.	page 29
/NOJOKES	Do not report any joke programs.	page 29
/NOMEM	Do not scan memory for viruses.	page 29
/NORECALL	Do not move files from remote storage into local storage after scanning. See also Scanning files in remote storage on page 18.	page 34
/NORENAME	Do not rename an infected file that cannot be cleaned.	page 32
/NOSCRIPT	Do not scan files that contain HTML, JavaScript, Visual Basic, or Script Component Type Libraries.	page 29
/OCMAX=<SIZE>	Specify the maximum size of the internal cache for file reads.	page 29
/OCRS=<VALUE>	Specify a value that represents the size of the internal cache size for each file read.	page 29
/PANALYSE	Same as /PANALYZE.	page 29
/PANALYZE	Use heuristic analysis to identify potential new program viruses.	page 29
/PAUSE	Enable a screen pause.	page 32
/PLAD	Preserve the last-accessed time and date for files that are scanned.	page 32
/PROGRAM	Scan for potentially unwanted applications.	page 30
/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 33
/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

Table 3-6 Alphabetic list of options (continued)

Option	Description	See ...
/SECURE	Examine all files, decompress archive files, and use heuristic analysis.	page 30
/SHOWCOMP	Report any files that are packaged.	page 30
/SILENT	Do not display any information on-screen.	page 34
/STREAMS	Scan all streams within a file if it is in an NTFS partition.	page 30
/SUB	Scan any subdirectories inside a directory.	page 30
/TIMEOUT <SECONDS>	Set the maximum time to scan any one file.	page 30
/UNZIP	Scan inside archive files, such as those saved in ZIP, LHA, PKarc, ARJ, WinACE, CAB, and CHM formats.	page 30
/WINMEM	Scan inside running processes.	page 30
/VIRLIST	Display the name of each virus that the scanner can detect.	page 33

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	The scanner found no viruses or other potentially unwanted software, and returned no errors.
2	Integrity check on DAT file failed.
6	A general problem occurred.
8	The scanner was unable to find a DAT file.
10	A virus was found in memory.
12	The scanner tried to clean a file, the attempt failed, and the file is still infected.
13	The scanner found one or more viruses or hostile objects — such as a Trojan-horse program, joke program, or test file.
15	The scanner's 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 28 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 *Options in alphabetic order* on page 35.

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
```

4 Removing Infections

Although they are not 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 your computer has a virus or you suspect it has, and you have not yet installed the on-demand scanner, follow these steps:

1. Ensure that your computer has up-to-date software and DAT files. Use either a recently purchased CD, or download and unzip the software onto a CD that you created on another computer.
2. Isolate your infected computer from any network that it uses.
3. Create a directory for the software on your hard disk.
4. Insert the CD into your CD drive, then copy the files from the CD to the directory that you created in Step 3.
5. Add the directory to the `PATH` statement in your `AUTOEXEC.BAT` file or use the **System Properties** window.
6. At the command prompt, type the following to thoroughly scan the computer:

   ```
   SCAN /ADL /ALL /CLEAN /WINMEM /PROGRAM
   ```

7. Shut down your computer and boot it into Safe Mode.
8. Scan your disks again immediately after the boot. At the command prompt, type:

   ```
   SCAN /ADL /ALL /CLEAN /WINMEM /PROGRAM
   ```

   This step is necessary because some infections can affect other files but this will not be apparent until the computer has booted.

9 If necessary, repeat Step 7 and Step 8 to ensure that all effects of the original infection are removed.

10 If you cannot remove all effects of the original infection, refer to the Virus Information Library for more information about manually removing an infection. For any further assistance, refer to the AVERT Home Page. See the addresses in *Contact information* on page 9.

If the infections were removed:

Shut down your computer and remove the CD. Reconnect to the network, and begin the installation procedure described on page 10.

To find and remove the possible source of infection, scan your diskettes immediately after installation. For information, see *Scanning diskettes* on page 17.

If infections were not removed:

If the scanner cannot remove an infection, you see one of the following messages:

```
Virus could not be removed.

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

In this case, refer to the Virus Information Library. See *Contact information* on page 9 for more information about manually removing an infection.

If the virus still cannot be removed, refer to the AVERT Home Page for information about manually removing infections. See *Contact information* on page 9.

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. 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 you specified. 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.

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 some password-protected Microsoft Excel 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.

5 Preventing Infections

VirusScan® Command Line is an effective tool for preventing infections, and it is most effective when combined with regular backups, meaningful password protection, user training, and awareness of threats from viruses and other potentially unwanted software.

To create a secure system environment and minimize the chance of infection, we recommend that you do the following:

- Install VirusScan® Command Line software and other McAfee security software.
- Schedule scans — at system boot and/or at regular intervals.
- Make frequent backups of important files. Even if you have VirusScan® Command Line software to prevent attacks from viruses, damage from fire, theft, or vandalism can render your data unrecoverable without a recent backup.

Detecting new and unidentified viruses

To offer the best protection possible, we continually update the definition (DAT) files that the VirusScan® Command Line software uses to detect potentially unwanted software. For maximum protection, you should regularly retrieve these files.

We offer free online DAT file updates for the life of your product, but cannot guarantee that they will be compatible with previous versions. By updating your software to the latest version of the product and updating regularly to the latest DAT files, you ensure complete protection for the term of your software subscription or maintenance plan.

Why do I need new DAT files?

Hundreds of new viruses and other potentially unwanted objects appear each month. Often, older DAT files cannot assist the VirusScan® Command Line software in detecting these new variations. For example, the DAT files with your original copy of VirusScan® Command Line might not detect a virus that was discovered after you bought the product.

If you suspect you have found a new virus, use WebImmune. See *Contact information* on page 9 for the address.

Updating your DAT files

The DAT files are contained in a single compressed file. Download the new file from either of the following sources:

- **FTP server.** Open a connection to the ftp site. See *Download Site* under *Contact information* on page 9 for the address.

  Use `anonymous` as your user name and your e-mail address as your password to gain access. Look for a compressed file in the directory `pub/antivirus/datfiles/5.x`. The file has the format *dat-nnnn.zip*, where *nnnn* is the DAT version number. For example: `dat-5001.zip`.

- **Web Site.** Start your browser, then go to the **Downloads** area for the latest file.

The number given to the file changes on a regular basis. A higher number indicates a later version of the DAT files. When you are selecting the latest version of DAT file, ignore any reference to SuperDAT (a self-installing DAT file). You cannot use this type of file with the command-line scanner.

To use the new DAT files:

1. Create a download directory.
2. Change to the download directory, and download the new compressed file from the source you have chosen. The downloaded DAT file is in a compressed .ZIP format.
3. Locate the directory on your hard drive where the command-line scanner is currently loaded (as set up in Step 1 on page 11).
4. 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.
5. Allow the updated files to overwrite the existing DAT files.

If other SupportingProductName software 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