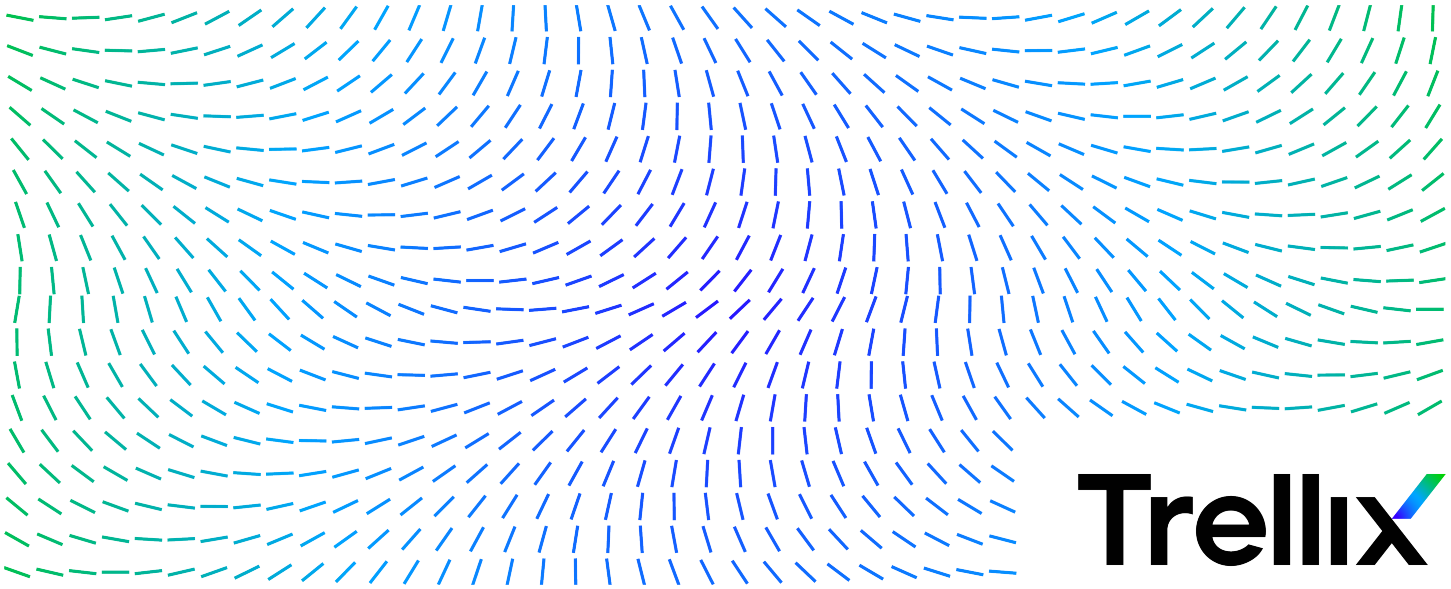
Revision A

Command Line Scanner

(Product Guide – Version 7.0.4)



Contents

Preface

About this guide

This information describes the guide's target audience, the typographical conventions and icons used in this guide, and how the guide is organized.

Audience

Trellix documentation is carefully researched and written for the target audience.

The information in this guide is intended primarily for:

- **Administrators** — People who implement and enforce the company's security program.
- **Users** — People who use the computer where the software is running and can access some or all of its features.

Conventions

This guide uses these typographical conventions and icons.

Italic	Title of a book, chapter, or topic; a new term; emphasis
Bold	Text that is emphasized
`Monospace`	Commands and other text that the user types; a code sample; a displayed message
Narrow Bold	Words from the product interface like options, menus, buttons, and dialog boxes
Hypertext blue	A link to a topic or to an external website
	**Note:** Extra information to emphasize a point, remind the reader of something, or provide an alternative method
	**Tip:** Best practice information
	**Caution:** Important advice to protect your computer system, software installation, network, business, or data
	**Warning:** Critical advice to prevent bodily harm when using a hardware product

What's in this guide

This guide is organized to help you find the information you need.

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

- Trellix Anti-Malware Scan Engine version 6700

Find product documentation

On the **ServicePortal**, you can find information about a released product, including product documentation, technical articles, and more.

Task

1. Go to the **ServicePortal** at https://www.trellix.com/en-us/support.html and click the **Knowledge Center** tab.
2. In the **Knowledge Base** pane under **Content Source**, click **Product Documentation**.
3. Select a product and version, then click **Search** to display a list of documents.

Introducing Command Line Scanner

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 the scanners use the same scanning engine. This section describes:

- Product features
- Getting product information
- Contact information

Product features

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

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. 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.

Getting product information

Unless otherwise noted, product documentation comes as Adobe Acrobat .PDF files, or from the Trellix download site.

- **Product Guide** — Introduction to the product and its features; detailed instructions for configuring the software; information on deployment, recurring tasks, and operating procedures.
- **Help** — Product information in the Help system that is accessed from within the application on its man pages.
- **Release Notes** — ReadMe. Product information, resolved issues, any known issues, and last-minute additions or changes to the product or its documentation.
- **License Agreement** — The Trellix 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 Trellix services and resources: technical support, customer service, Security Headquarters (Trellix Advanced Research Center), beta program, and training.

Contact information

Threat Center: Trellix Advanced Research Center	**Trellix Advanced Research Center Threat Library** https://www.trellix.com/en-us/advanced-research-center.html **Support Notification Service (SNS** https://www.trellix.com/en-us/contact-us/sns-preferences.html
Download Site	https://www.trellix.com/en-us/downloads.html **Product Upgrades** (Valid grant number required) **Security Updates** (DATs, engine) **HotFix and Patch Releases** • **For Security Vulnerabilities** (Available to the public) • **For Products** (ServicePortal account and valid grant number required) **Product Evaluation** **Trellix Beta Program**
Technical Support	https://www.trellix.com/en-us/support.html **KnowledgeBase Search** https://supportm.trellix.com/webcenter/portal/supportportal/pages_knowledgecenter **Trellix Technical Support ServicePortal** (Logon credentials required) https://supportm.trellix.com/
Customer Service	**Web** https://www.trellix.com/en-us/contact-us.html
Professional Services	**Enterprise:** https://www.trellix.com/en-us/index.html

Installing Command Line Scanner

We distribute the Command Line Scanner software in two ways — on a CD, and as an archived file that you can download from our website 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:

Microsoft operating systems

- Windows 7 32-bit and x64 Editions (with current and previous Service Pack)
- Windows 8.x 32-bit and x64 Editions (with current and previous Service Pack)
- Windows 10 32-bit and x64 Editions
- Windows Server 2008 32-bit and x64 Editions (with current and previous Service Pack)
- Windows Server 2012 x64 Editions (with current and previous Service Pack)
- Windows Server 2016 x64 Editions (with current and previous Service Pack)
- Windows Server 2019 x64 Editions
- Windows 11 32-bit and x64 Editions
- Windows Server 2022 x64 Editions

Disk space and memory

- At least 512 MB of free hard disk space
- At least an additional 512 MB of free hard disk space reserved for temporary files
- At least 512 MB of RAM for scanning operations (1024 MB recommended) for Windows platform
- At least 1024 MB of RAM for updating operations

Other recommendations

To take full advantage of the regular updates to DAT files from our website, 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, read *Chapter 4: Removing Infections* on before you install the scanner.

Task

1 Create a directory for the software on your hard disk. If you are using the command-line, you can 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 website:** Download the file to the directory that you created in Step 1, and decompress the zipped files into that directory.

Tip

Type `CD` to change to the directory to which you extracted the program files.

3 Add the directory you created in Step 1 to the PATH environment variable.

See also
Removing Infections on page 4

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. 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
```

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.

Note

The program performs a standard digital signing check of the engine binary prior to execution. If the computer is not connected to the internet, this check might fail unexpectedly and display a warning.

To test your installation:

Task

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*
```

Caution

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, ensure to type the letter O, not the number 0, in the “X5O...” that begins the test message.

Caution

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`.

Caution

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.

Troubleshooting when scanning

The following table lists the most common error messages returned if the scan program fails when scanning. The table also suggests a likely reason for the error and recommends possible solutions.

Table 2-1 Program messages

Program message	Remedy
Missing or invalid DAT files	Re-install the DAT files.
The program has been altered; please replace with a good copy	Re-install from the original media; the program might be infected.
Failed to initialize the AVENGINE	Increase the number of processes on the server in proportion to the size of the DAT file.

Removing the program

To remove the product from your system:

Task

1 Change your command prompt to point to the directory that contains the Command Line Scanner files.

2 Delete all files in the directory.

Caution

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.

Caution

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

See also

Installing the software on page 9

Using Command Line Scanner

Command Line Scanner is a program that you can run from a command prompt. If the scanner installation directory has been added to the PATH environment variable or is in the current directory, you can run a scan by typing SCAN at the command prompt with the options you want.

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.

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 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, .PDF, .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 Command Line Scanner for Windows software.

  You can use the options `/UNZIP` and `/NOCOMP` to configure the scanner to handle compressed files.

See also
Scanning options on page 21
Response and notification options on page 26

Scanning removable media

Removable media 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.

Task

1 Using the `CD` command, change to the directory where the scanner was installed.

2 Type: `SCAN D: /MANY`

Note

Use the drive letter assigned to your specific removable media.

3 Insert a disk into the D drive, and press `Enter`.

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

Note

If the scanner detects a virus on this disk, it runs the command-line option that you chose for dealing with the virus.

4 Remove the scanned disk from the D drive.

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

See also
Removing a virus found in a file on page 37

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. 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.

Table 3-1 Scanning streams *(continued)*

Command	Action
`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

To increase the scanning speed, the scanner uses local memory caches. The behaviour of these caches can be controlled by the following switches:

- `/MEMSIZE`
- `/AFC`
- `/HIDEMD5`

MEMSIZE

Each file less than a specific size is completely loaded into memory before scanning. Default maximum size is 1mb. This size can be adjusted using the /MEMSIZE switch that defines a maximum size in Kb.

For example, /MEMSIZE=2000 causes all files under 2mb to be loaded into memory for scanning.

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.

HIDEMD5

This option allows the display of MD5 checksum of infected files to be hidden, if required.

Scanning processes in memory

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

Note

When using the `/WINMEM` option, specify at least one file for scanning 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.
- **Response and notification options** — determine how the scanner responds to infected files.
- **Report options** — determine how the scanner displays the results of the scan.
- **General options** — for such things as user help.

Each group of options appears in its own table with a description of its function.

See also
Choosing the options on page 21
Scanning options on page 21
Response and notification options on page 26
Report options on page 27
General options on page 28

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 also
Scanning options on page 21

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 /VERSION
  ```
- 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 also
Preventing Infections on page 4

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:

Task

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

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

See also
Choosing the options on page 21
Command-line conventions on page 17

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
```

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 also
Scanning options on page 21

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:

Task

1. If you do not already have the Command Line Scanner installation directory included in your PATH environment variable, change the current directory to where you installed your Command Line Scanner 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`.

XML reports

You can generate an XML format report using the /XMLPATH switch. For example, run the following command from the install directory:

```
scan . /XMLPATH=report.xml /RPTALL
```

This will generate a file called **report.xml** with the following content.

```
<?xml version="1.0" encoding="utf-8"?>
<!-- Scan Results -->
<Scan>
<Preamble>
<Product_name value="Trellix Command Line Scanner for Win32" />
<Version value="6.0.4.564" />
<AV_Engine_version value="5600.1067" />
<Dat_set_version value="7057" />
</Preamble>
<Date_Time value="2013-May-09 13:38:16" />
<Options value=". /xmlpath=report.xml /rptall " />
<File name="D:\vcl\avvclean.dat" status="ok" />
<File name="D:\vcl\avvnames.dat" status="ok" />
<File name="D:\vcl\avvscan.dat" status="ok" />
<File name="D:\vcl\config.dat" status="ok" />
<File name="D:\vcl\mc5300up.001" status="ok" />
<File name="D:\vcl\mcscan32.dll" status="ok" />
<File name="D:\vcl\report.xml" status="ok" />
```

```
<File name="D:\vcl\runtime.dat" status="ok" />
<File name="D:\vcl\scan.exe" status="ok" />
<File name="D:\vcl\vcl604wpg.pdf" status="ok" />
<summary On-Path="D:\vcl" Total-files="14" Clean="10" Not-Scanned="4" Possibly-Infected="0" />
<Time value="00:00.01" />
</Scan>
```

See also
Schema for the XML reports on page 4

Choosing the options

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

- Scanning options.
- Response and notification options.
- Report options.
- General options.

In the descriptions, variables such as file names or path appear in chevrons (< >).

See also
Scanning options on page 21
Response and notification options on page 26
Report options on page 27
General options on page 28
Command-line conventions on page 17

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.

Caution

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.

Table 3-2 Scanning options *(continued)*

Option	Limitations	Description
/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.
/ALL	See note on page 26	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.
/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. 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.
/ASCII	None	Displays filenames as ASCII text.
/BADLIST <FILENAME>	None	Create a list of infected files.
/BOOT	Do not use with /NODDA	Scan boot sector and master boot record only.
/CHECKLIST <FILENAME>	None	Scan the files listed in the specified file.
/CORRUPT	None	Scan.ZIP files that have corrupt headers. The scanner uses the central directory information instead.
/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.
/DRIVER	None	Specify the location of the DAT files: AVVSCAN.DAT , AVVNAMES.DAT , and AVVCLEAN.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 specif ied in < *FILENAME*>. List the complete path to each directory or file on its own line. You may use wildcards, * and ?.
/EXTENSIONS	None	Scan defaults and user extension list.

Table 3-2 Scanning options *(continued)*

Option	Limitations	Description
/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
/FREQUENCY <HOURS>	None	Do not scan before the specified number of hours afte r 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.
/HIDEMD5		This option allows the display of MD5 checksum of infected files to be hidden, if required.
/JSONPATH <FILENAME>	None	Create JSON report.
/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.
/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.
/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.
/MAXFILESIZE <SIZE>	None	Examine only those files that are smaller than the sp ecified size. Specify the file size in megabytes. For example, /MAXFILESIZE 5 means scan only files that are smaller than 5mb.

Table 3-2 Scanning options *(continued)*

Option	Limitations	Description
/MEMSIZE	None	Manage local memory caches used by the scanner to increase the scanning speed.
/MIME	None	Scan MIME-encoded files. This type of file is not scanned by default.
/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.
/NOBOOT	None	Do not scan the boot sector.
/NOBREAK	None	Disable Ctrl-C and Ctrl-Break during scans. Users cannot halt scans in progress if this option is set.
/NOCOMP	None	Do not check compressed executables created with th e 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.
/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 th at 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 26	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.
/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.
/PANALYZE /PANALYSE		Use heuristic analysis to identify potential new progr am viruses. By default, the program scans only for known viruses. This option is a subset of /ANALYZE.

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 xe "security threat" security threat.
/QUITCONTAINER	None	Exit the container mid-decoding/reading phase.
/RECURSIVE		Examine any subdirectories in addition to the specified target directory.
/RPTOBJECTS		Reports the number of objects scanned at all levels in the summary.
/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.
/SHOWENCRYPTED		Display encrypted documents. This switch retains the 5800 reporting behavior while scanning encrypted MS Office and PDF documents (without this parameter, the 5900 engine by default reverts to 5700 reporting behavior). The reporting of encrypted files is performed by using this parameter as these files are not reported by default.
/STREAMS	NTFS only, run from within Windows NT and later versions	Scan all streams within a file if it is in an NTFS partiti on.
/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.
/THREADS <nThreads>	None	Scan multithreaded with specified number of threads.
/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 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.
/XMLPATH <FILENAME>	None	Create XML report.

See also
Preventing Infections on page 4
Scanning removable media on page 13
What can you scan? on page 13
Scanning files in remote storage on page 14
Scanning NTFS streams on page 14
Scanning protected files on page 15
AFC on page 15
Scanning processes in memory on page 16
Configuring scans on page 17
Creating a list of infected files on page 19
Response and notification options on page 26
Using heuristic analysis on page 19

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 option`	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.
`/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. 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.

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.
/NORENAME	None.	Do not rename an infected file that cannot be cleaned.
/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.

See also
Virus detection by the Scanner on page 36

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.

Table 3-4 Report options

Option	Limitations	Description
/APPEND	Use this option with /REPORT.	Add any results of the scan to a file.
/HTML <FILENAME>	None	Create a file containing the results in HTML format.
/JSONPATH <FILENAME>	None	Create JSON report.
/LOUD	None	Display a progress summary during the scan. Note that this option can produce a large amount of information.

Table 3-4 Report options *(continued)*

Option	Limitations	Description
/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 xe "scanning options, added to report ; reports : with scanning options" 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 xe "/PAUSE : not with /REPORT [PAUSE]" /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>
/XMLPATH <FILENAME>	None	Create XML report.

See also
Producing reports on page 20
Contact information on page 8

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 below 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 br ief 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.
/DECOMPRESS	None	Decompress DAT files after an update.
/EXTLIST	None	Display names of file extensions that are scanned by default.
/FDC	None	Stop on failed digital signing check.
/HELP	None.	See the /? option.
/NORECALL	Use with /DOHSM	Do not move files from remote storage into local storage after scanning.
/SILENT	None.	Do not display any information on-screen.

See also
Scanning files in remote storage on page 14

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
/?	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, in addition to any other drives specified on the command line. Do not scan removable media.
/ADN	Scan all network drives, in addition to any other drives specified on the command line.
/AFC=<SIZE>	Specify the size of the file cache.
/ALL	Scan all files regardless of extension.
/ALLDRIVES	Scan all drives. Scan all network drives and local drives, but not removable drives; these include disk drives, CD drives, and Zip drives.
/ALLOLE	Check every file for OLE objects.
/ANALYSE	Same as /ANALYZE.
/ANALYZE	Use heuristic analysis to find possible new viruses in "clean" files.
/APPEND	Add any results of the scan to a file.
/APPENDBAD	Append names of infected files to an existing file, as specified by /BADLIST.
/ASCII	Displays filenames as ASCII text.

Table 3-6 Alphabetic list of options *(continued)*

Option	Description
/BADLIST <FILENAME>	Create a list of infected files.
/BOOT	Scan boot sector and master boot record only.
/CHECKLIST <FILENAME>	Scan the files listed in the specified file.
/CLEAN	Automatically remove any infections.
/CONTACTFILE <FILENAME>	Display the contents of the specified file when a virus is found.
/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.
/DRIVER	Specify the location of the DAT files: AVVSCAN.DAT, AVVNAMES.DAT, and AVVCLEAN.DAT.
/EXCLUDE <FILENAME>	Exclude the directories or files from the scan as specified in <FILENAME>.
/EXTENSIONS	Scan defaults and user extension list.
/EXTLIST	Display names of file extensions that are scanned by default.
/EXTRA <FILENAME>	Specify the location on any EXTRA.DAT file.
/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	See the /? option.
/HIDEMD5	Allows the display of MD5 checksum of infected files to be hidden, if required.
/HTML <FILENAME>	Create a file containing the results in HTML format.
/JSONPATH <FILENAME>	Create JSON report.
/LOAD <FILENAME>	Load scanning options from the named file, or scanning profile.
/LOUD	Display a progress summary during the scan.
/MAILBOX	Scan plain-text mailboxes.
/MANALYSE	Same as /MANALYZE.
/MANALYZE	Use heuristics analysis to identify potential macro viruses.
/MANY	Scan multiple disks consecutively in a single drive.
/MAXFILESIZE <SIZE>	Examine only those files that are smaller than the specified size.
/MEMSIZE	Manage local memory caches used by the scanner to increase the scanning speed.
/MIME	Scan MIME-encoded files.
/MOVE <DIR>	Move any infected files to a quarantine location as specified.
/NOBKSEM	Prevent scanning of files that are normally protected.
/NOBOOT	Do not scan the boot sector.
/NOBREAK	Disable Ctrl-C and Ctrl-Break during scans.
/NOCOMP	Do not check compressed executables created with the LZEXE or PkLite file-compression programs.

Table 3-6 Alphabetic list of options *(continued)*

Option	Description
/NOD	Scan only the susceptible file types.
/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 DAT files are out of date.
/NOJOKES	Do not report any joke programs.
/NOMEM	Do not scan memory for viruses.
/NORECALL	Do not move files from remote storage into local storage after scanning.
/NORENAME	Do not rename an infected file that cannot be cleaned.
/NOSCRIPT	Do not scan files that contain HTML, JavaScript, Visual Basic, or Script Component Type Libraries.
/PANALYSE	Same as /PANALYZE.
/PANALYZE	Use heuristic analysis to identify potential new program viruses.
/PAUSE	Enable a screen pause.
/PLAD	Preserve the last-accessed time and date for files that are scanned.
/PROGRAM	Scan for potentially unwanted applications.
/QUITCONTAINER	Exit the container mid-decoding/reading phase.
/RECURSIVE	Examine any subdirectories in addition to the specified target directory.
/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.
/RPTOBJECTS	Reports the number of objects scanned at all levels in the summary.
/RPTERR	Include system errors in the report file.
/SECURE	Examine all files, decompress archive files, and use heuristic analysis.
/SHOWCOMP	Report any files that are packaged.
/SHOWENCRYPTED	Display encrypted documents.
/SILENT	Do not display any information on-screen.
/STREAMS	Scan all streams within a file if it is in an NTFS partition.
/SUB	Scan any subdirectories inside a directory.
/THREADS <nThreads>>	Scan multithreaded with specified number of threads.
/TIMEOUT <SECONDS>	Set the maximum time to scan any one file.
/UNZIP	Scan inside archive files, such as those saved in ZIP, LHA, PKarc, ARJ, WinACE, CAB, and CHM formats.
/VIRLIST	Display the name of each virus that the scanner can detect.

Table 3-6 Alphabetic list of options *(continued)*

Option	Description
/WINMEM	Scan inside running processes.
/XMLPATH <FILENAME>	Create XML report.

See also
Scanning files in remote storage on page 14

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.
21	Computer requires a reboot to clean the infection.

See also
Scanning options on page 21

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.

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
```

See also
Options in alphabetic order on page 29

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.

Cleaning 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:

Task

1. Isolate your infected computer from any network that it uses.
2. Download and unzip up-to-date anti-virus software and DAT files onto another computer and create a CD.
3. Create a directory for the software on the hard disk of the infected computer.
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 8 and Step 9 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 Trellix Advanced Research Center Home Page.

If the infections were removed:

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

To find and remove the possible source of infection, scan your diskettes immediately after installation.

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.

If the virus still cannot be removed, refer to the Trellix Advanced Research Center Home Page for information about manually removing infections.

See also
Contact information on page 8
Scanning removable media on page 13
Installing Command Line Scanner on page 3

Virus detection by the Scanner

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.

Caution

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.

See also
Cleaning macro viruses from password-protected files on page 37

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.

Preventing Infections

Command Line Scanner 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 Command Line Scanner software and other Trellix security software.
- Schedule scans — at system boot and/or at regular intervals.
- Make frequent backups of important files. Even if you have Command Line Scanner 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 Command Line Scanner 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 Command Line Scanner software in detecting these new variations. For example, the DAT files with your original copy of Command Line Scanner 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 also
Contact information on page 8

Updating your DAT files

DAT files are contained in a single compressed file that you can download from the internet.

Task

1. Navigate to this URL: https://update.nai.com/products/commonupdater/current/vscandat1000/dat/0000/
2. Look for a filename that is of the format **avvdat-nnnn.zip**, where nnnn is the DAT version number.

   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 Command Line Scanner.

Tasks

- *Using the new DAT files* on page 40

Using the new DAT files

Task

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. Use a suitable compression utility to extract the files from the .ZIP file into that directory. Ensure to extract all the files.
4. Allow the updated files to overwrite the existing DAT files.

Note

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.

Tip

After an update, run the following command once to decompress the newly downloaded DATs and accelerate the time for subsequent initializations `--SCAN /DECOMPRESS`.

Tip

This product is not suitable for on-access (single file) scanning.

Schema for the XML reports

The formal schema for the XML reports is as follows:

```
<?xml version="1.0" encoding="UTF-8"?>
<!--W3C Schema for the CLS 6.0 XML Report format-->
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema">
<xs:element name="Scan">
<xs:complexType>
<xs:sequence>
<xs:element ref="Preamble"/>
<xs:element ref="Date_Time"/>
<xs:element ref="Options"/>
<xs:group ref="FileSummary" maxOccurs="unbounded" minOccurs="0"/>
<xs:element ref="Time"/>
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name="Preamble">
<xs:complexType>
<xs:sequence>
<xs:element ref="Product_name"/>
<xs:element ref="Version"/>
<xs:element ref="License_info"/>
<xs:element ref="AV_Engine_version"/>
<xs:element ref="Dat_set_version"/>
<xs:element ref="Extra_Dat_Info" minOccurs="0"/>
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name="Date_Time">
<xs:complexType>
<xs:attribute name="value" type="xs:string" use="required"/>
</xs:complexType>
</xs:element>
<xs:element name="Options">
<xs:complexType>
<xs:attribute name="value" type="xs:string" use="required"/>
</xs:complexType>
</xs:element>
<xs:element name="Time">
<xs:complexType>
<xs:attribute name="value" type="xs:string" use="required"/>
</xs:complexType>
</xs:element>
<xs:group name="FileSummary">
<xs:sequence>
<xs:element ref="File" maxOccurs="unbounded" minOccurs="0"/>
<xs:element ref="Summary" maxOccurs="unbounded"/>
</xs:sequence>
</xs:group>
<xs:element name="File">
<xs:complexType>
<xs:attribute name="status" type="xs:string" use="required"/>
<xs:attribute name="name" type="xs:string" use="required"/>
<xs:attribute name="virus-name" type="xs:string" use="optional"/>
<xs:attribute name="detection-type" type="xs:string" use="optional"/>
</xs:complexType>
</xs:element>
<xs:element name="Summary">
<xs:complexType>
<xs:attribute name="Total-processes" type="xs:int" use="optional"/>
<xs:attribute name="On-Path" type="xs:string" use="optional"/>
<xs:attribute name="Total-files" type="xs:int" use="optional"/>
<xs:attribute name="Total-Objects" type="xs:int" use="optional"/>
<xs:attribute name="Possibly-Infected" type="xs:int" use="optional"/>
```

```
<xs:attribute name="Objects-Possibly-Infected" type="xs:int" use="optional"/>
<xs:attribute name="Not-Scanned" type="xs:int" use="optional"/>
<xs:attribute name="Clean" type="xs:int" use="optional"/>
<xs:attribute name="Possibly-Infected-MBR" type="xs:int" use="optional"/>
<xs:attribute name="Possibly-Infected-BootSector" type="xs:int" use="optional"/>
<xs:attribute name="Master-Boot-Records" type="xs:int" use="optional"/>
<xs:attribute name="Boot-Sectors" type="xs:int" use="optional"/>
<xs:attribute name="Cleaned" type="xs:int" use="optional"/>
<xs:attribute name="Moved" type="xs:int" use="optional"/>
<xs:attribute name="Deleted" type="xs:int" use="optional"/>
</xs:complexType>
</xs:element>
<xs:element name="Product_name">
<xs:complexType>
<xs:attribute name="value" type="xs:string" use="required"/>
</xs:complexType>
</xs:element>
<xs:element name="Version">
<xs:complexType>
<xs:attribute name="value" type="xs:string" use="required"/>
</xs:complexType>
</xs:element>
<xs:element name="License_info">
<xs:complexType>
<xs:attribute name="value" type="xs:string" use="required"/>
</xs:complexType>
</xs:element>
<xs:element name="AV_Engine_version">
<xs:complexType>
<xs:attribute name="value" type="xs:decimal" use="required"/>
</xs:complexType>
</xs:element>
<xs:element name="Dat_set_version">
<xs:complexType>
<xs:attribute name="value" type="xs:short" use="required"/>
</xs:complexType>
</xs:element>
<xs:element name="Extra_Dat_Info">
<xs:complexType>
<xs:attribute name="Path" type="xs:string" use="required"/>
<xs:attribute name="Additional_Viruses" type="xs:string" use="required"/>
</xs:complexType>
</xs:element>
</xs:schema>
```

The following table lists the Status attributes and the relevant description for each attribute.

Table A-1 Status attribute description

Status attributes	Description
ok	The object was scanned ok.
infected	Virus-name and detection-type will contain further detail.
corrupted	The object is corrupt. This message is usually issued for files within archives; for example, a corrupted .ZIP file.
error locked	The object could not be opened for reading or data could not be read from the object.
password-protected	The object is encrypted and the engine does not understand the encryption method. This value is usually issued for compressed files that are password-protected.
packaged	The object is packaged with a packer. The object is neither being reported as infected nor as being clean.
error bcs-file	The object is a Block, FIFO, or character special file. This is only used in UNIX systems.

Table A-1 Status attribute description *(continued)*

Status attributes	Description
error outofmemory	A memory allocation failed and the scan cannot continue.
error process not running	The specified process was not found. This for process objects only.
Scan Time Out	Scanning stopped due to /TIMEOUT option.
Unknown error	Unspecified internal error. This may be returned for errors that are not covered by other XML status strings.

Index

F

G

H

I

J

L

M

N

O

P

Q

R

S

T

U

V

W

0A00

Trellix