Avira Command Line Scanner

Manual

AVIRA

Table of contents

1. Product Description

We offer Avira Command Line Scanner so that you can use the Avira scanning technology at the command prompt, in order to scan your files directly, without browsing through a graphic user interface, and to apply your own configuration.

1.1 Features

With a single command line, you can:

- Set the area you want to scan: hard disks, network drives, archives, mailboxes, recursion level, etc.
- Detect extended threats, such as dialers, games, backdoors, etc.
- Take action on concerning files: repair, delete, move, etc.
- Set a quarantine folder.
- Specify a certain extension to be added to the concerning files.
- View statistics at the end of the scanning process.
- Customize the log and view or save it to the desired location.
- Apply your own configuration file to the scanning process.

1.2 System Requirements

- Operating system:
  - Windows: NT or newer.
  - Linux.
- RAM: 128 MB
- HDD: 30 MB

1.3 Licensing

You need an Avira license file in order to run the Command Line Scanner. The usual Avira license files are supported (Avira Professional Security, Avira Antivirus Premium, Avira Internet Security).

Note
The license file name must be *hbedv.key*.

2. Installation

You can simply download the archive from the Avira website and extract the product in a local directory of your choice. The Command Line Scanner supports commercial license files. All required files are included in our fusebundle package.

3. Command Line Options

The command syntax is:

```
scancl  [path to scan] [options]
```

Examples:

The following commands display the help message.

```
scancl -h
scancl -?
scancl --help
```

Scan drive `C:` and ask for the action to be taken for infected files.

```
scancl C: --defaultaction=ask
```

Scan the directory `D:\games\`; Extract and scan files in archives; Delete suspicious files, in case repairing fails.

```
scancl D:\games\ -z --defaultaction=repair,delete
```

Note
Usually, all options will be available on all operating systems. However, there might be OS-specific features, that will be available only for a certain OS and will not be displayed in others.

Note
The following list of parameters and return codes is also integrated in the program and can be displayed with the help command: `scancl -h`

3.1 Scan Options

	Options	Description
-a -x -e	--allfiles --smartextensions --extensionlist	Scan all files. Scan using smart extensions. Scan using the extensions list provided in VDF. **Note** These three options exclude each other. You can use only one at a time. Default is --smartextensions
	--allboot	Scan all boot records. Default option.
	--alldrives	Scan all drives (Windows only).
	--allhard	Scan all hard disks (Windows only).
	--allremote	Scan all network drives (Windows only).
	--archivemax ratio=<N>	Do not scan archive content which would exceed the given decompression factor limit (0 means unlimited, default: 250).
	--archivemax recursion=<N>	Do not scan archive content which would exceed the given nesting level (0 means unlimited, default: 10).
	--archivemaxsize=<N>	Do not scan archive content which would exceed the given extracted size. Options: 0- no restriction, default - 1GB, maximum 4GB.
	--boot=<str>	Scan the boot record of the given drive.
	--defaultaction=<str>	Set the action for infected files. See Actions on page 8. Default: ignore. You can use more than one action. For example: --defaultaction=repair,delete **Note** delete-archive (for ZIP, ARJ, RAR etc.) and delete will delete ONLY the mentioned type: archives OR regular files, respectively.
	--dmse	Set exit code to 101, if any macro is detected.
	--exclude=<str>	Exclude the given files or directories from scan.
	--fixallboot	Fix all boot records.
	--fixboot=<str>	Fix the boot record of the given drive.
	--heurlevel=<N>	Set heuristics level. Available levels: 0= off, 1=low, ..., 3=high. Default: 0.

	Options	Description
-i	--info	Display the list of known malware. When viewed on screen, you have to press **Enter** to proceed.
	--lang=<str>	Option not used currently. Reserved for future use.
	--noarchive	Do not scan inside archives. Default setting.
	--nolinks	Do not follow symbolic links. Default: follow symbolic links.
	--nombr	Do not scan master boot records. Default is --allboot (Windows only).
-n	--norecursion	Scan only the current level, without directory recursion. Not activated by default. The default setting is to scan subdirectories (See -s).
	--onefs	Scan only the root file system (not the mounted file systems). Default: Scan all file systems.
	--quarantine=<str>	Set the quarantine directory. Default: $(bindir)/quarantine
-s	--recursion	Scan recursively from the current level. Default option.
	--renameext=<str>	Change the extension of infected files. Example: to rename *file.com* as *file.mov* --renameext=mov
-z	--scaninarchive	Extract and scan files in archives. Not activated by default. This option does not enable scanning of mailboxes. In order to scan mailboxes, see -m.
-m	--scanmbox	Scan mailbox, too (might be time consuming): Outlook (PST), BSD, Mozilla, etc. Always with parameter -z. It is not possible to scan only mailboxes, because mailboxes are considered archives.
	--showall	Display detailed information during the scanning process. Default: show only infected or suspicious files.
-d	--subdirmaxlevel=N	Set a limit for the recursive folders (0 - no recursion, default - unlimited).

	Options	Description
	`--suspiciousaction=<str>`	Set the action for suspicious files. See Actions on page 8. Default: `ignore`. You can use more than one action. For example: `--suspiciousaction=repair,move` **Note** `delete-archive` (for ZIP, ARJ, RAR etc.) and `delete` will delete ONLY the mentioned type: archives OR regular files, respectively.
	`--withouttype=<type>`	Do not detect specified types of malware. See `--withtype` for the available values.
	`--withtype=<type>`	Detect other (non-virus, but unwanted) software, too: see Malware types on page 7. Available values: `--withtype:dial,joke,game,bdc,pck,spr,adspy,appl,phish,hiddenext,adware,pfs,all` The following types are detected by default: `dial,adspy,adware,bdc,hiddenext,phish` **Note** This option is overwritten every time, so you have to specify **all** the types you want to detect, each time you run `scancl`. No spaces allowed between types.
	`--workingdir=<str>`	Specify the installation directory.

Malware types

Detected malware (non-virus) types:

Parameter	Malware type
`adspy`	**Adware and Spyware:** Software that displays advertising pop-ups or software that sends user-specific data to third parties, without the users' consent.
`adware`	**Adware:** Software (or components of a software) that displays advertising.
`appl`	**Application:** An application that may pose a risk if used or an application that comes from a suspicious source.
`bdc`	**Backdoor Client:** This is the control software for backdoors and is generally harmless.

Parameter	Malware type
`dial`	**Dialer:** A Dial-Up program for connections that charge a fee. Its use might lead to huge costs for the user.
`game`	**Game:** A computer game. Normally, games cause no damage on the computer.
`hiddenext`	**Double Extension File:** Executable file, that hides its real file extension in a suspicious way. This camouflage method is often used by malware.
`joke`	**Joke:** A joke program is present as a file. Normally, jokes cause no damage on the computer; they just annoy the user.
`pck`	**Unusual Runtime Compression Tool:** The file has been compressed with an unusual runtime compression tool. Please make sure that this file comes from a trustworthy source.
`pfs`	**Fraudulent software:** Software that charges a fee, but contains no functions or installs suspicious components.
`phish`	**Phishing:** Fraudulent emails designed to convince the victim to reveal confidential information, such as user names, passwords or online banking data, on certain websites.
`spr`	**Programs that violate the private domain:** Software that may be able to compromise the security of your system, initiate unwanted program activities, damage your privacy or spy out your user behavior.
`all`	**All** malware types described above.

Actions

List of actions for concerning files:

Action	Behavior
`clean`	Repair the infected or suspicious files.
`move`	Move the infected or suspicious files to the quarantine.
`rename`	Change the extension of the infected or suspicious files.

Action	Behavior
`delete`	Delete infected or suspicious (regular) files.
`delete-archive`	Delete infected or suspicious archives of type: zip, arj, rar, etc.
`delete-mailbox`	Delete infected or suspicious mailbox files (mbox, Thunderbird, Mozilla, etc)
`disarm`	Make the locked file ineffective.
`ignore`	Take no action. (Default setting)

`ask`	Prompt the user to select an action:
	`1. Move`
	`2. Rename`
	`3. Delete file`
	`4. Ignore`
	and to specify if this action should apply to:
	`1. This file only`
	`2. All files infected with <virus>`
	`3. All infected files.`

Status

The status of a file can be:

Status	Behavior
`clean`	The file is not infected.
`infected`	The scanner detected an infection.
`suspicious`	The heuristic algorithm detected a possible infection.
`repaired`	The scanner removed the infection and repaired the file.
`moved`	The scanner moved the file to quarantine.
`renamed`	The scanner added a specific extension to the concerning file.
`deleted`	The scanner deleted the file.
`ignored`	The scanner took no action.

3.2 Output Options

	Options	Description
	`--colors`	Display results in color. Default: `--nocolors`.
`-c`	`--config=<filename>`	Specify a configuration file.
`/?` `-h`	`--help`	Display the help text. You have to press **Enter** to proceed.
	`--listtypes`	Display the list of malware types. See Malware types on page 7.
`-l`	`--log=<filename>`	Log to the specified file.
	`--logappend`	Append new log data to the existing file. Default: overwrite logfile.
	`--logformat=`	Set the format of the log messages: - `singleline`: only one-line messages for each alert, warning or error; - `regular`: all scanned files appear in the log. For each file 3 lines are logged. The first line contains the path with the filename; the second line contains the "date modified", the "time modified" file information and the filesize; for infected files, the third line contains the alert/ warning/ error. If the file is clean, an empty line is logged. Default: `--logformat=regular`
	`--nocolors`	Display monochrome results. It is the default option, but it can be used when the configuration file has colors enabled.
	`--nostats`	Display only summary results after scanning.
`-q`	`--quiet`	Scan in quiet mode.
	`--stats`	Display detailed statistics after scanning. Default.
	`--temp=<dir>`	Set the directory for temporary files. Default is `%TEMP%` or `$TEMP`.
	`--verboselog`	Scan in verbose mode, displaying all messages.
`-v`	`--version`	Display version information (VDF, engine, AVPack, license info).

3.3 Error Codes

Error code	Error description
0	Normal program termination, no detection, no error
1	Found concerning file or boot sector
2	A signature was found in memory
3	Suspicious file found
100	Avira has only displayed the help text
101	A macro was found in a document file
20?	Program aborted with one of the following error codes:
203	Invalid option
204	Invalid (nonexistent) directory given in the command line
205	The log file could not be created
210	Avira could not find a necessary library file
211	Program aborted, because the self-check failed
212	The virus definition files could not be read
213	An error occurred during initialization (engine and VDF versions incompatible)
214	No valid license found
215	ScanCL self-test failed
216	File access denied (no permissions)
217	Directory access denied (no permissions)

4. Default Options

- Malware types detected by default: `dial,adspy,adware,bdc,hiddenext,phish`.
- Scan using smart extensions.
- Do not scan in archives.
- Scan recursively.
- Heuristics: off.
- Scan all boot records.
- Scan all file systems.
- Follow symbolic links.
- Action for infected files: `ignore`.
- Action for suspicious files: `ignore`.

- Display monochrome messages.
- Display detailed statistics after scanning.
- Log to standard output device.
- Log in regular mode.
- Default quarantine: `$(bindir)/quarantine`
- Directory for temporary files: `%TEMP%` or `$TEMP`

5. Customized Scanning With a .conf File

To make the scanning process even easier, just specify a configuration file for *scancl* and it will make the job for you. Instead of typing the same long commands for each profile, you can save the options in *.conf* files and launch the Scanner with specific configurations:

```
scancl --config=<filename>
```

You can edit the configuration file *scancl.conf* included in the installation directory, or you can create a new .conf file altogether.

6. Updates

Avira Command Line Scanner cannot be installed as a standalone product, therefore it cannot be updated separately.

In order to use the latest engine and signature files, you must ensure that the executables of the Avira Command Line Scanner are copied in the installation directory of a fully installed and licensed commercial Avira product.

Examples: all Windows products, Avira MailGate, Avira WebGate.

Issued Q1-2012

AVIRA

live free.™

Avira Operations GmbH & Co. KG
Kaplaneiweg 1 | 88069 Tettnang
Germany

Telephone: +49 7542-500 0
Facsimile: +49 7542-500 3000
www.avira.com