Release Notes for F-Secure Anti-Virus Command-Line Scanner

This document contains detailed information about the command-line scanner of F-Secure Anti-Virus products. Please also see the product's release notes about known problems.

Technical Support

Web:	http://www.f-secure.com/support/
Your local contact:	http://www.f-secure.com/f-secure/contact_information.html
F-Secure contact:	support@f-secure.com

Sales

Web:	http://www.F-Secure.com/products/
Your local contact:	http://www.f-secure.com/f-secure/contact_information.html
F-Secure contact:	sales@f-secure.com

F-Secure USA	**F-Secure Europe**
F-Secure Inc.	F-Secure Corporation
100 Century Center Court, Suite 700	PL 24
San Jose, CA 95112, USA	FIN-00181, Helsinki, Finland
tel (888) 432-8233	tel +358 9 2520 0700
fax (408) 350-2339	fax +358 9 2520 5001
http://www.f-secure.com/	http://www.europe.f-secure.com/

Please do not call F-Secure directly if you have a local F-Secure Business Partner in your area. For an up-to-date listing of F-Secure Business Partners world-wide, see http://www. f-secure.com/partners/.

F-SECURE® LICENSE TERMS

F-Secure license terms are included in the software. You must read and accept them before you can install and use the software.

Overview

F-Secure Anti-Virus Command-Line Scanner is part of F-Secure Anti-Virus products. This tool is included in both the workstation and server products. It makes it easy to access the virus scanner through the command prompt. The functionality includes:

- On-demand scanning. The user can start a virus scan task from the command prompt, and stop it by pressing Control+C.
- Scheduling. The command-line scanner can be invoked through the AT command or the Control Panel/Scheduled Tasks applet easily.
- Remote execution. Scan tasks can be invoked on remote computers using standard system tools. This is especially valuable on file servers.
- Automation. The command-line scanner supports silent execution, shell scripts, exit codes, and redirection of output to text files to make it easy to automate running of F-Secure Anti-Virus in a virus detection test, for example. The tool can handle very large virus collections and the text format used in the scan report is easy to process further. Additionally, there's no user interface overhead to slow down scan tasks. Multiple instances of the command-line scanner can be run simultaneously on the same system.
- Testing. Quality engineers' team can use the command-line scanner to automate torture tests. The tool makes it possible to use just one of the supported scan engines, which lets the tester isolate a specific engine for close examination. The tool supports scanning files in multiple separate paths with single invocation.
- Support for security policies. The exclusion and extension lists can be controlled remotely through F-Secure Policy Manager. The on-demand scan statistics are written to the F-Secure Anti-Virus policy file at the end of each scan. If the computer is managed using F-Secure Policy Manager, virus alerts and scan reports are sent through F-Secure Management Agent to the F-Secure Policy Manager Console. Scan results are also logged in the standard log file.

Architecture

F-Secure Anti-Virus is based on a service-based architecture supporting real-time scanning, where a service process scans all the files for viruses as they're accessed. This makes the product very transparent but has the disadvantage that it is hard to invoke the scanner on demand programmatically or manually.

F-Secure Anti-Virus Command-Line Scanner doesn't include an embedded virus scan engine at all. Instead, it uses the instance of the scanning service already running in the system to invoke the virus scanner to perform the actual scans. This architecture has the following benefits:

- Performance. Since the command-line scanner doesn't contain the actual virus scanner, it doesn't need to load or initialize lots of code, which makes it fast to run it from another program repeatedly. No virus signature database information needs to be kept in the utility's memory either.
- Easy updates. The command-line scanner doesn't require updates at all. The automatic update mechanism of F-Secure Anti-Virus is used instead to maintain the virus scan engines and virus signature databases.

The supported platforms are:

- Windows 2000 SP4
- Windows XP
- Windows Server 2003
- Windows Vista
- Windows Server 2008
- Windows 7

Installation

F-Secure Anti-Virus Command-Line Scanner is installed as a part of F-Secure Anti-Virus. No additional installation steps are necessary.

Command-Line Format

General

The command-line format is:

```
FSAV [options] [targets]
```

Options are identified by the starting character "/". Any argument not starting with this character is considered a scanning target. The target arguments may include a mixed list of regular (d:\dir\file.ext) and UNC (\\server\resource\dir\file.ext) pathnames. For example:

```
FSAV suspect.exe
FSAV /disinf c:\temp\*.*
FSAV /report=virusreport.txt c: d: e: f: x: y: z:
FSAV \\server1\stuff \\server2\morestuff
FSAV /archive w:\webfiles f:\ftpfiles
```

The command-line can include multiple targets. The target defaults to '*.*' if none is defined. Target names that contain spaces or other special characters must be enclosed in double quotes.

Subdirectories are always included in the scanning. For example, "fsav c:\temp*.doc" will scan c:\temp and all its subdirectories, searching for viruses in all .doc files.

If the path includes a specific filename extension then it will be used to override the current extension list. For example, giving "c:*.doc" on the command line will set the extension list to "doc". If no extension is given in the target, the value given with the /EXT option is used instead. If the /EXT option is not given on the command-line, the included extensions value from the security policy is used as the default.

The exclusions defined in the security policy are honored and files on the exclusion list will not be scanned.

The scanner will skip all special files (pipes, devices etc.).

Boot sectors are included in scanning if the drive letter of a local hard disk is specified in a target path, unless this has been overridden using the /NOBOOT option. For example, "fsav *.*" only scans files on the hard disk, while "fsav c:*.*" scans both files and boot sectors on the hard disk.

The command-line options are:

```
/ALL         Do a "dumb" scan of all files.
/APPEND      Append to existing report file.
/ARCHIVE     Scan inside .ZIP, .ARJ and .LZH files.
/BEEP        Beep when a virus is found.
/DELETE      Delete infected files.
/DISINF      Disinfect whenever possible.
/EXT=        List of file extensions to be used in the scan
/HARD        Scan the hard disk(s).
/HELP        Display this list.
/LIST        List all files checked.
/NOBOOT      Do not scan boot sectors.
/NOBREAK     Do not abort scan if Ctr+C is pressed.
/POLICY      Read scanning parameters from the policy.
/QUAR        Quarantine infected files.
/RENAME      Rename infected COM/EXE files.
/REPORT=     Send the output to a file.
/ROOTKIT     Scan system for rootkits.
/SCANNER=    Use only single scanner ("AVP", "Libra" or "Orion").
/SILENT      No output.
/SPYWARE     Scan the specified path for spyware
/SYSTEM      Scan the computer for active malware
/USEACCOUNT Always use the command-line scanner's account for scanning.
/VERSION     Show scanner version information.
```

The command line options are case insensitive (e.g. /ALL, /all, /All etc are considered identical).

Target (path) scanning, system scanning and spyware scanning

Note: the /SPYWARE option has changed in command-line scanner version 7.50 build 13500, and a new option /SYSTEM has been added. If you have previously used scripts to run the command-line scanner using the /SPYWARE option then the scripts must be changed to accommodate the new behavior. See below for more information.

The /SYSTEM option requests a scan of the system for active malware. This scan is faster than the full scan of hard drives, because it only searches the locations that are likely to contain active malware. This type of scan also searches the system registry for entry points to active software.

The /SYSTEM option allows scans without specifying the target path parameter at all.

System scanning always looks for both viruses and spyware in the system.

The target path scan can either scan for viruses only, or for both viruses and spyware. The /SPAWARE option determines if the target path is scanned for spyware also.

For spyware, the /DISINF and /RENAME actions do not apply: it is only possible to quarantine (/QUAR) or remove (/DELETE) spyware. However, if the /DISINF option is given on command line then detected spyware will be quarantined. This will allow scanning tasks to be run that disinfect found viruses and quarantine found spyware.

Some examples of target path, system and spyware scanning options are shown below.

1. Scan the directory c:\samples for viruses and spyware:
   ```
   fsav.exe c:\samples /spyware
   ```
2. Scan the directories c:\test1 and c:\test2 for viruses and spyware, disinfecting the found viruses and quarantining the found spyware:
   ```
   fsav.exe c:\test1 c:\test2 /spyware /disinf
   ```
3. Scan the system for active (installed) spyware, quarantining the found spyware:
   ```
   fsav.exe /system /quar
   ```
4. Scan the system for active (installed) spyware, plus scan the whole c: drive for viruses and spyware:
   ```
   fsav.exe c:\ /system /spyware
   ```

Rootkit scanning

Rootkit scanning (scanning of hidden files using the /ROOTKIT option) is only available under a privileged account. Log on to the computer under an account with administration privileges on that computer to use the /ROOTKIT option.

Rootkit scanning also works under the Local System account, making it possible for scheduled scanning tasks to scan hidden files.

Scanning options read from policy

If the /POLICY option is used then various scanning parameters will be read from the product's policy (settings). The following policy settings are used:

- Action on infected items (such as disinfect, quarantine) etc. The action setting is taken from the product's manual scanning settings.
- Spyware scanning settings. Spyware is scanned for unless it has been disabled in the policy. Note that this setting is enabled by default and cannot be disabled from the product's user interface. However, if the product is managed using F-Secure Policy Manager then spyware scanning can be disabled under F-Secure Anti-Spyware/Anti-Spyware Scanner/Manual Scanning options. The action (report only, quarantine or

remove) on detected spyware will also be taken from manual scanning settings of the product with the /POLICY option.

- Rootkit scanning settings. Files hidden by rootkits will be scanned unless rootkit scanning has been disabled in the policy. This setting is also enabled by default and cannot be disabled from the product's user interface, but it can be disabled if the product is managed using F-Secure Policy Manager. In this case, rootkit scanning will not be done if it has been disabled under F-Secure Anti-Virus/Settings for Manual Scanning/Rootkit Scanning options.

For example, assuming that the product is being used with its default configuration, the following command will scan the whole c: drive for both viruses and spyware, and will also scan files hidden by rootkits:

```
fsav.exe c:\ /policy
```

The above noted behavior has the following implication: because scheduled scanning tasks (either as enabled from the product's user interface, or as defined using the Scheduled Tasks items with Policy Manager) are also executed with the /POLICY option, these scanning tasks will also have spyware and rootkit scanning enabled (unless explicitly disabled from Policy Manager).

The /POLICY option will also cause the scanning report to be created automatically in Anti-Virus directory.

User account used for scanning

The FSAV.EXE process only acts as the command and reporting interface: files are not opened and scanned by this process, but by the product's scanning service. FSAV.EXE process normally passes information about the user account under which it is executed to the scanning service so that the service could scan the user's files as if it was done by FSAV.EXE itself. In some cases however, the account information is not passed and the scanning service scans the files under the Local System account. Normally this is not a problem, because the "scheduled scanning" feature of the product configures FSAV.EXE to be run under the Local System account anyway.

Sometimes it may be needed to run FSAV.EXE under a particular account, e.g. by defining a scheduled task to run FSAV.EXE under some account. This cannot be done from the product's user interface, but the Windows "Scheduled Tasks" applet can be used to define the scheduled task with a particular account. In order to make sure that the scanning service always uses the account under which FSAV.EXE is executed in this scenario, add the /USEACCOUNT option (alternatively, /USRACCOUNT and /USERACCOUNT are also accepted) to the command line. This option is available in FSAV.EXE versions 9.20 and later.

Reporting

Screen output

All normal output such as start-up texts and other informative messages are sent to the standard output channel (stdout).

Sample report when no viruses were found:

```
C:\Program Files\F-Secure\Anti-Virus>fsav c:\test\clean
F-Secure Anti-Virus Command Line Scanner, version 7.20.13032
Scans files for viruses
Copyright c 2001-2007, F-Secure Corporation

Results of virus scanning:

Scanned
Files:               1
Not scanned:         0

Boot Sectors
Scanned:             2
Infected:            0

Time: 00:01

No viruses found
```

Sample report when a virus was found:

```
C:\Program Files\F-Secure\Anti-Virus>fsav c:\test\virus
F-Secure Anti-Virus Command Line Scanner, version 7.20.13032
Scans files for viruses
Copyright c 2001-2007, F-Secure Corporation

Results of virus scanning:
C:\TEST\VIRUS\EICAR.COM Infection: EICAR_Test_File

Scanned
Files:               1
Not scanned:         0

Result
Viruses:             1

Boot Sectors
Scanned:             2
Infected:            0

Time: 00:00
```

Report file

Contents of the report file when a virus was found (note that the report file contains more details than screen output):

```
F-Secure Anti-Virus Command Line Scanner, version 7.20.13032
Scans files for viruses
Copyright © 2001-2007, F-Secure Corporation

23 January 2007 10:38:47

Command line: c:\test\virus /REPORT=REPORT.TXT

Workstation name: clone111-r2-a
```

```
Scanning options:
Target: c:\test\virus
Scan defined files: COM EXE SYS OV? BIN SCR DLL SHS HTM HTML HTT VBS JS INF
VXD DO? XL? RTF CPL WIZ HTA PP? PWZ P?T MSO PIF . ACM ASP AX CNV CSC DRV INI
MDB MPD MPP MPT OBD OBT OCX PCI TLB TSP WBK WBT WPC WSH VWP WML BOO HLP TD0
TT6 MSG ASD JSE VBE WSC CHM EML PRC SHB LNK WSF {* PDF ZL? XML AVB BAT CEO
CMD LSP MAP MHT MIF PHP POT WMF NWS TAR TGZ
Action:
 Viruses: Report only
Scan inside archives: off

Scanning Engines:
F-Secure AVP: 7.00.171, 2007-01-22
F-Secure Libra: 2.04.01, 2007-01-19
F-Secure Orion: 1.02.37, 2007-01-22
F-Secure Draco: 1.00.35, 2007-01-17

Results of virus scanning:
C:\TEST\VIRUS\EICAR.COM Infection: EICAR_Test_File

Scanned
Files:                1

Result
Viruses:              1
Spyware:              0
Suspected:            0
Riskware:             0

Actions
Disinfected:          0
Deleted:              0
Renamed:              0
Quarantined:          0

Boot Sectors
Scanned:              2
Infected:             0
Suspected:            0
Disinfected:          0

Time: 00:00
```

Return codes

The command-line scanner supports the following return codes. When an error is encountered, the corresponding message will also be printed on screen (stderr).

0	Scanning completed successfully, system is clean
1	Command line scan not allowed in policy (currently unsupported)
2	Scanning aborted by user
3	Error loading F-Secure Anti-Virus or one of its program files
4	Gatekeeper couldn’t connect to scanning engines
5	Self-test failed (currently unsupported)
6	Command line syntax error or unknown parameter
7	Execution failed, out of memory
8	Scan path not valid
10	Failed to open one of the report files, scanning successful

11	Encountered encrypted files that can’t be scanned (currently unsupported)
12	Failed to open some targets, these objects may still be infected
20	Suspicious code found, may be a virus (currently unsupported)
21	One or more viruses found, actions successful, no remaining viruses
22	One or more viruses found, actions successful, renamed viruses remain on disk
23	One or more viruses found, actions unsuccessful or not attempted, system still infected
24	Virus found in memory, scanning aborted (currently unsupported)

Known Issues

UNC paths are not checked for validity before scanning.

If there are files or directories on the policy file's exclude list and the /LIST parameter is specified, files in the excluded directories are listed in the report although the files weren't actually scanned.

The user can abort a scan by pressing Control+C, but ESC isn't supported.

The report is written by using the Windows character set. Extended characters in filenames will not show correctly if viewed with a DOS based text viewer.

Please also see the product's release notes about other known issues.