

Release Notes for F-Secure Anti-Virus Command-Line Scanner Beta 1.0.1251

This document contains late-breaking information about the product. Please refer to the manual for more information. The manual is available in Adobe Acrobat PDF format on the installation media. Printed copies of the manual can be ordered from your F-Secure business partner.

Technical Support

Web:	http://www.F-Secure.com/support/
Your local contact:	<country>@F-Secure.com
F-Secure contact:	Support@F-Secure.com

Sales

Web:	http://www.F-Secure.com/products/
Your local contact:	<country>@ F-Secure.com
F-Secure contact:	Sales@ F-Secure.com

F-Secure USA

F-Secure Inc.
675 N. First Street, 5th Floor
San Jose, CA 95112, USA
tel (408) 938 6700
fax (408) 938 6701
<http://www.F-Secure.com/>

F-Secure Europe

F-Secure Corporation
PL 24
FIN-00181, Helsinki, Finland
tel +358 9 2520 0700
fax +358 9 2520 5001
<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/>.

Copyright © 1993-2001 F-Secure Corporation All Rights Reserved.

Overview

F-Secure Anti-Virus Command-Line Scanner is part of the standard F-Secure Anti-Virus product starting with version 5.30. This tool is included in both the workstation and server versions. 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 System Agent 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 three 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 by 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 logfile.

Architecture

F-Secure Anti-Virus 5 is based on a real-time architecture where F-Secure Anti-Virus Gatekeeper, the kernel-mode device driver, 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 programmatically.

F-Secure Anti-Virus Command-Line Scanner doesn't include an embedded virus scan engine at all. Instead, it uses the instance of Gatekeeper already running in the system to invoke the device driver based virus scanner to perform the actual scans. This architecture has many 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 mechanisms of F-Secure Anti-Virus 5 are used instead to maintain the virus scan engines and virus signature databases.
- ☐ Access to all files in the system. Since Gatekeeper runs in kernel-mode, it can scan into any file. The command-line scanner uses Gatekeeper to iterate the file system and scan files which guarantees full access to the system.

The supported platforms are:

- ☐ Windows 95
- ☐ Windows 98
- ☐ Windows 98 SE
- ☐ Windows ME
- ☐ Windows NT 4.0
- ☐ Windows 2000

The utility supports the F-Secure Management Agent localization scheme and will set its language according to the relevant policy values. However, the only supported language is currently English.

Installation

F-Secure Anti-Virus Command-Line Scanner ships as a standard part of F-Secure Anti-Virus 5.30 and later. It will also work with earlier versions such as F-Secure Anti-Virus 5.22 provided that it is installed manually. To do this, copy the FSAV.EXE and FSAVCMD.ENG files to the F-Secure Anti-Virus installation directory (e.g. "c:\program files\f-secure\anti-virus").

Command-Line Format

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 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.

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.
/RENAME	Rename infected COM/EXE files.
/REPORT=	Send the output to a file.
/SCANNER=	Use only single scanner ("AVP", "F-PROT" or "Orion").
/SILENT	No output.
/VERSION	Show scanner version information.

If the path includes a specific filename extension specifier 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 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.).

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:\tmp]fsav *.*  
F-Secure Anti-Virus Command Line Scanner, version 1.00.1251  
Scans files for viruses  
Copyright © 2001, F-Secure Corporation
```

```
Files  
Scanned:          604
```

```
Boot Sectors:  
Scanned:          1  
Infected:         0
```

```
Time: 00:41
```

```
No viruses found
```

Sample report when a virus was found:

```
[c:\tmp]fsav c:\tmp\eicar /report=c:\tmp\report.txt  
F-Secure Anti-Virus Command-Line scanner, version 1.00.1251  
Scans files for viruses  
Copyright © 2001, F-Secure Corporation
```

```
c:\tmp\eicar\eicar.com Infection: EICAR_Test_File
```

```
Files  
Scanned:          1  
Infected:         1  
Disinfected:      0  
Deleted:          0  
Renamed:          0
```

```
Boot Sectors:  
Scanned:          1  
Infected:         0
```

```
Time: 00:41
```

```
1 virus found
```

Report file

Contents of the report file when a virus was found:

```
F-Secure Anti-Virus Command-Line scanner, version 1.00.1251  
Scans files for viruses  
Copyright © 2001, F-Secure Corporation
```

```
11 May 2001 19:16:46
```

```
Scanning options:  
Target: c:\tmp\eicar  
Files scanned with extensions: COM EXE SYS OV? BIN SCR DLL SHS HTM HTML HTT  
VBS  
Action: Report only  
Scan inside archives: off
```

```
F-Secure F-PROT: 3.09.303, 2001-05-09 04:03:56  
F-Secure AVP: 3.55.160.3180, 2001-05-09 04:03:56  
F-Secure Orion: 1.02.14, 2001-05-09 04:03:56
```

Results of virus scanning:

c:\tmp\eicar\eicar.com Infection: EICAR_Test_File

```
Processed:      1
Infected:      1
Disinfected:    0
Deleted:        0
Renamed:        0
```

Time 00:02

To get a separate report from each scan engine for each file, use the /APPEND option:

```
FSAV c:\samples /report=foo.txt /SCANNER=F-PROT
FSAV c:\samples /report=foo.txt /SCANNER=AVP /APPEND
FSAV c:\samples /report=foo.txt /SCANNER=Orion /APPEND
```

You can then sort the report to view the report for each file successively. If there is no line in the report for some file/scanner combination, the scanner didn't find anything to report with that file.

Return codes

The utility 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.

License Agreement

BY INSTALLING OR USING THIS SOFTWARE YOU AGREE THAT YOU HAVE READ THIS LICENSE AND ITS APPENDIX, UNDERSTAND ITS TERMS, AND AGREE TO BE BOUND BY ITS TERMS AND THAT IT IS THE ONLY AGREEMENT BETWEEN US, SUBJECT TO AMENDMENTS, REGARDING THE PROGRAM AND DOCUMENTATION. PLEASE NOTE THAT YOU MAY NOT USE, COPY, MODIFY OR TRANSFER THE PROGRAM OR DOCUMENTATION OR ANY COPY, EXCEPT AS EXPRESSLY PROVIDED IN THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, DO NOT COPY, INSTALL OR USE THE SOFTWARE.

These F-Secure license terms including its appendix cover any and all F-Secure software products (the "Software") licensed by the user hereunder ("You" or "Licensee"). The Software is licensed, not sold, to you for use only under the following terms. F-Secure may revise these terms at any time and the revised terms shall automatically apply to the corresponding versions of the Software distributed with the revised terms. F-Secure reserves any and all rights not expressly granted to you. You own the media on which the Software is submitted, but F-Secure retains ownership of all copies of the Software and released updates and upgrades to the Software. You will receive a specified number of base packages, which will include the Software and related documentation. If you have received the Software via online purchase, then you will receive the software and the related documentation in electronic format.

This License Entitles You to:

- Install and use the Software on the total number of computers or other devices limited to the total number of individual users, licenses, capacity or other limitations as set forth in or on the package containing the Software or in the related documentation. The only exception is for F-Secure Anti-Virus for Workstation applications, in which case you may also install F-Secure Anti-Virus for Workstation on home computers of those employees who use F-Secure Anti-Virus for Workstation at their workplace. The home installation may be done from either supplied media or copies created according to the license terms.
- Use the Software on a network, provided that you have a licensed copy of the Software for each user that uses the Software.
- Create copies of the "setup program" for the Software for installation and backup purposes.
- Extend the number of licenses by purchasing additional licenses.

Note: If the Software has been either marked as an evaluation copy or provided to you and identified by F-Secure as an evaluation copy, you are then granted a non-exclusive license to use and evaluate the evaluation copy within your organization free of charge for thirty (30) days from the first installation or download from our website, unless more time is authorized in writing by F-Secure or its authorized partner.

Maintenance and Support

F-Secure Anti-Virus and F-Secure Workstation Suite products

Upon purchase of F-Secure Anti-Virus and F-Secure Workstation Suite products, with the exception of evaluation copies, you are provided with "support and maintenance service," which includes updates, upgrades, and technical support, for a specified period of time, usually one (1) year. Support and maintenance service can be purchased thereafter for an annual fee. You will receive upgrades, updates and technical support from the F-Secure partner from whom you have purchased and registered the Software. If you have received the software via online purchase, you will receive upgrades, updates and technical support directly from F-Secure, unless specified otherwise. On request, updates, upgrades and technical support can be provided as limited hereunder to additional locations for an additional fee. The virus detection

capability is typically updated several times every month. You can download these updates from our sites via the Internet. Software upgrades are supplied to you at least once a year, and typically three times a year. The upgrades, updates and technical support will be delivered to persons registered as the support contact.

For evaluation copies, you are not entitled to any enhancement or update to the Software. For evaluation copies, F-Secure shall have no obligation to provide maintenance or support for the Software.

Note: All F-Secure products for the NEC PC-98, Novell Netware 3.x and 4.x, OS/2, Windows NT 3.51, Windows 3.1, and DOS operating systems will only be developed, maintained, and supported as long as these operating systems are supported by the manufacturers or until end of year 2001, which ever comes first.

Other F-Secure products

Upon purchase of other F-Secure products than F-Secure Anti-Virus and F-Secure Workstation Suite products, you are provided with "electronic maintenance service," which includes updates and upgrades for a specified period of time, usually one (1) year. You can download these updates from our sites via the Internet. Maintenance service can be purchased thereafter for an annual fee. The electronic maintenance service does not include technical support, which can be purchased separately. The electronic maintenance service does not apply if you have received the software via online purchase.

For evaluation copies, you are not entitled to any enhancement or update to the Software. F-Secure shall have no obligation to provide maintenance or support for the evaluation Software.

For online purchase you are provided with the same maintenance and support services which are included in F-Secure Anti-Virus and F-Secure Workstation Suite products.

Restrictions on Use

You may not distribute copies of the Software to a third party, electronically transfer the Software to a computer belonging to a third party, or permit a third party to copy the Software.

The Software contains or may contain trade secrets of F-Secure. Thus, you may not decompile, reverse engineer, disassemble, or otherwise reduce the Software to any human-perceivable form.

You may not modify, adapt, translate, rent, lease, resell, distribute or create derivative works based upon the Software or any part thereof.

You may not use the documentation for any purpose other than to support your use of the Software. Please contact F-Secure directly (<http://www.F-Secure.com>) if you are interested in any other rights to the Software other than those granted in this Agreement.

Export Restrictions (exclusively for *cryptography products)

1) In the United States of America: The Licensee agrees to comply with the Export Administration Act, the Export Control, all regulations promulgated under such Acts, and all other United States government regulations covering the export of technical data and equipment and products produced therefrom, that are applicable to Licensee.

2) In participating States of the Wassenaar Arrangement (except the United States of America): The Licensee agrees to comply with local regulations regarding the export and/or use of cryptographic software.

3) In countries other than the United States of America: The Licensee agrees to comply with the local regulations regarding exporting and/or using cryptographic software.

In all cases, F-Secure will not be liable for the illegal export and/or use of its cryptographic software by the Licensee.

Limited Warranty and Disclaimers

Limited Warranty on Media. F-Secure warrants the media on which the Software is recorded to be free from defect in material and workmanship under normal use for 30 days from the date of delivery. Any implied warranties on the media, including implied warranties of merchantability and fitness for a particular purpose, are limited in duration to 30 days from the date of delivery. F-Secure will, at its option, replace the media or refund the purchase price of the media. F-Secure shall have no responsibility to replace or refund the purchase price of media, which is damaged by accident, abuse, or misapplication.

Disclaimer of Warranty on Software. The Software is provided "as is", without warranty of any kind. F-Secure expressly disclaims all implied warranties, including but not limited to implied warranties of merchantability or fitness for a particular purpose. F-Secure does not guarantee

the Software or related documentation in terms of their correctness, accuracy, reliability, or otherwise. You assume the entire risk as to the results and performance of the Software and related documentation.

Complete Statement of Warranty. The limited warranties provided in the preceding paragraphs are the only warranties of any kind that are made by F-Secure on this product. No oral or written information or advice given by F-Secure, its dealers, distributors, agents, or employees shall create a warranty or in any way increase the scope of the foregoing limited warranty, and you may not rely on any such information or advice.

Limitation of Liability. In no event shall F-Secure or its suppliers be liable to you for any special, consequential, incidental, or indirect damages, including, but not limited to, loss of revenue or profit, lost or damaged data or other commercial or economic loss, arising out of the use of, or inability to use, the Software or related documentation, even if F-Secure has been advised of the possibility of such damages. F-Secure is not responsible for the Software's ability to repel a specific virus or for damages caused by an unsuccessful virus prevention. Our maximum liability to you for actual damages for any cause whatsoever is limited to the amount paid by you for the Software. Nothing contained in this Agreement shall prejudice the statutory rights of any party dealing as a consumer. F-Secure is acting on behalf of its employees and licensors or subsidiaries for the purpose of disclaiming, excluding, and/or restricting obligations, warranties, and liability as provided in this clause, but in no other respects and for no other purpose.

Title

Title, ownership rights, and intellectual property rights in the Software shall remain those of F-Secure, and/or its suppliers. The Software is protected by copyright laws and international copyright and other intellectual property treaties. This license does not grant you any right to any enhancement or update to the Software.

U.S. Government Rights

If you are acquiring the Software and related documentation for or on behalf of the United States of America, its agencies and/or instrumentalities ("U.S. Government"), the following provisions apply. The Software is deemed to be "commercial software," and the documentation is deemed to be "commercial computer software documentation," pursuant to DFAR Section 227.7202, and FAR 12.212, as applicable. Any use, modification, reproduction, release, performance, display or disclosure of the Software or its related documentation by the U.S. Government shall be governed solely by both these terms and this Agreement.

High Risk Activities

The Software is not fault-tolerant and is not designed, manufactured or intended for use or resale as on-line control equipment in hazardous environments requiring fail-safe performance, such as in the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control, direct life support machines, or weapons systems, in which the failure of the Software could lead directly to death, personal injury, or severe physical or environmental damage ("High Risk Activities"). F-Secure and its suppliers specifically disclaim any express or implied warranty of fitness for High Risk Activities.

Term and Termination

Except for evaluation copies, this license is effective until terminated. It will terminate immediately without notice if you are in breach of any of its terms and conditions. Upon termination, you must destroy the Software and all copies thereof. You may terminate this license at any time by destroying the Software and all copies thereof. You shall not be entitled to a refund from F-Secure or any of its resellers as a result of termination. The terms and conditions concerning confidentiality and restrictions on use shall continue in force even after any termination. Disputes related to the license terms shall be governed by the laws of Finland, except in the case of purchases made within or on behalf of licensees residing within or

operating under the laws of the United States. In such instances, such disputes shall be governed by the laws of the State of California.

For evaluation copies, the license will terminate automatically: 1) if you fail to comply with the limitations described herein; 2) 30 days from the first installation of the Software; or 3) at the expiration of the allocated evaluation time. Upon termination of this License, you agree to destroy the Software and all copies thereof.

If any part of this Agreement is found void and unenforceable, it will not affect the validity of rest of the Agreement, which shall remain valid and enforceable according to its terms. This Agreement may only be modified in writing by F-Secure.

For purchasing the commercial versions of any F-Secure products you may contact us:

On the Web: <http://www.F-Secure.com>

By Telephone: (888) 432-8233 (in the USA) or +358-9-2520 0700 (in Europe).

By e-mail: F-Secure-Sales@F-Secure.com

All correspondence regarding this license should be addressed to F-Secure:

In the USA

E-mail: US-Sales@F-Secure.com

Telephone: (408) 938-6700

Toll Free: (888) 432-8233

Fax: (408) 938-6701

Postal address: F-Secure, Inc.

675 N. First Street, 5th floor

San Jose, California 95112

In Europe

E-mail: Helsinki@F-Secure.com

Telephone: +358 9 2520 0700

Fax: +358 9 2520 5001

F-Secure Corporation

Tammasaarenkatu 7

FIN-00180 Helsinki, Finland

Trade Register no: 425.966, VAT FI07055792

Appendix

F-SECURE ANTI-VIRUS

F-SECURE BackWeb

You may install and use F-SECURE BackWeb in conjunction with licensed F-SECURE's anti-virus and security products. F-SECURE BackWeb may be used only for receiving updates and related information on F-SECURE's anti-virus and security products. F-SECURE BackWeb shall not be used for any other purpose or service.

"BackWeb" is a trademark of BackWeb Technologies.

F-SECURE DISTRIBUTED FIREWALL CLIENT*

You may install F-SECURE DISTRIBUTED FIREWALL CLIENT only on a personal computer. You may not install F-SECURE DISTRIBUTED FIREWALL CLIENT software on a file server, an application server or any computer whose primary function is to serve other computers.

F-SECURE DISTRIBUTED FIREWALL SERVER*

You may install F-SECURE DISTRIBUTED FIREWALL SERVER on a personal computer, file server or application server.

F-SECURE FILECRYPTO *

F-SECURE INTEGRATION FOR HP OPENVIEW VANTAGEPOINT

HP OpenView VantagePoint is a trademark of Hewlett-Packard Company.

F-SECURE INTEGRATION FOR BMC PATROL

PATROL® is a registered trademark of BMC Software in the United States.

F-SECURE INTEGRATION FOR UNICENTER TNG

Unicenter TNG® is a registered trademark of Computer Associates International, Inc.

F-SECURE NAMESURFER ISP

You may install F-SECURE NAMESURFER on an unlimited number of servers within your organization in one location. The total number of hosts in your DNS database must not exceed the number of hosts you have purchased the license for. You may provide DNS administration as a service for third parties.

F-SECURE POLICY MANAGER

You may install and use F-SECURE POLICY MANAGER in conjunction with licensed F-Secure software products.

F-SECURE PLUS FOR TIVOLI ENTERPRISE

Tivoli® is a registered trademark of Tivoli Systems Inc.

F-SECURE SSH *

SSH is a registered trademark of SSH Communications Security Corp (www.ssh.com).

F-SECURE SMARTCARD EXTENSION

F-SECURE VPN+ CLIENT *

You may install F-SECURE VPN+ CLIENT only on a personal computer. You may not install F-SECURE VPN+ CLIENT software on a file server, an application server or any computer whose primary function is to serve other computers. You may not configure and/or use F-SECURE VPN+ CLIENT software to

forward traffic to other hosts. In conjunction with F-SECURE VPN+ CLIENT license you may also install and use F-SECURE DISTRIBUTED FIREWALL.

F-SECURE VPN+ GATEWAY *

You may configure F-SECURE VPN+ GATEWAY without restriction. In conjunction with F-SECURE VPN+ GATEWAY license you may also install and use F-SECURE DISTRIBUTED FIREWALL.

F-SECURE VPN+ SERVER *

You may install F-SECURE VPN+ SERVER on a personal computer, file server or application server. You may not install, configure or use F-SECURE VPN+ SERVER on any computer to forward traffic to other hosts. In conjunction with F-SECURE VPN+ SERVER license you may also install and use F-SECURE DISTRIBUTED FIREWALL.

F-SECURE WORKSTATION SUITE *

* cryptography products = products that include encryption technology