Release Notes for F-Secure Anti-Virus 5.30

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.

There are additional release notes distributed with the F-Secure Management Tools Setup and F-Secure Management Server Setup kits. Please consult them for the latest information about those components.

Technical Support

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

Sales

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

F-Secure USA	**F-Secure Europe**
F-Secure Inc.	F-Secure Corporation
675 N. First Street, 5th Floor	PL 24
San Jose, CA 95112, USA	FIN-00181, Helsinki, Finland
tel (408) 938 6700	tel +358 9 2520 0700
fax (408) 938 6701	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/.

Introduction

What Does F-Secure Anti-Virus Include?

F-Secure Anti-Virus includes the following products for securing your workstation in day-to-day use:

- F-Secure Framework
- F-Secure Anti-Virus

F-Secure Framework includes utilities for maintaining all of your F-Secure applications with policy-based management. It is an easy-to-use HTTP-based network solution which includes the F-Secure Administrator utility for centrally managing each Workstation Suite application.

F-Secure Anti-Virus provides transparent real-time protection against malicious code and viruses. Daily updates can be conveniently downloaded from the F-Secure Web site and put to use immediately. These updates provide the fastest available cure for any new virus threat. No other anti-virus software provides continuous and tested updates for every new virus threat.

F-Secure Framework

F-Secure Framework is based on a comprehensive security management architecture. The main components in the framework are described below.

F-Secure Administrator provides a centralized management console for the security of the managed hosts in the network. It enables the administrator to organize the network into logical units for sharing policies. The policies are defined in F-Secure Administrator and then distributed to the workstations through the F-Secure Management Server. F-Secure Administrator is a Java-based application which can be run on several different platforms. It can be used to remotely deploy the Management Agent on other workstations without the need for local login scripts, rebooting, or any intervention by the end user.

F-Secure Management Server is the repository for policies and software packages distributed by the administrator and also for status information and alerts sent by the managed hosts. It provides scalability by working as an extension to the Microsoft Internet Information Server (IIS). Communication between F-Secure Management Server and the managed hosts is accomplished through the standard HTTP protocol, which ensures trouble-free performance on the LAN and global internetworks. In a small LAN, the active components of F-Secure Management Server do not need to be installed. Policies and software packages can be distributed through a shared folder on a normal file server. This shared folder is referred to as the Communication directory.

F-Secure Management Agent enforces the security policies set by the administrator on the managed hosts, and provides the end user with a user interface and other services. It handles all management functions on the local workstations and provides a common interface for all F-Secure applications, and operates within the policy-based management infrastructure.

The basic architecture used by these components relies on a concept known as policy-based management. A security policy is a set of well-defined rules that regulate how sensitive information and other resources are managed, protected, and distributed. The management architecture of F-Secure software uses policies configured by the administrator for optimum control over network. Policy-based management implements many functions:

- Remotely controlling and monitoring the behavior of the products
- Monitoring statistics provided by the products and the Management Agent
- Remotely starting predefined operations
- Transmission of alerts and notifications from the products to the system administrator

Information between F-Secure Administrator and the hosts is exchanged by the transfer of policy files.

The F-Secure management architecture is based on three tiers. The tiers are:

- Management console: the administrator's workstation, running F-Secure Administrator.
- Management servers: the repositories for policy files and software packages, each running F-Secure Management Server.
- Managed hosts: the workstations, servers and gateway computers whose security is being managed, each running F-Secure Management Agent.

The functions of three-tier security management are described in greater detail in the F-Secure Management Tools Administrator's Guide manual.

F-Secure Management Agent

Version

F-Secure Management Agent Release 4.50 build 3491

What's new

1? "Last known good" communication settings are stored and used when incorrect communication settings (server address, password, etc.) have been specified. Prevents losing the management server/commdir connection in case of typos in the server policy settings.
2? "Poll now" button – allows the end user to update policies, statistics, Anti-Virus databases on demand (in addition to the normal polling interval based updating) A command-line utility FSPOLL.EXE is also provided.
3? Recovering from a corrupted incremental policy file (policy.ipf). "Last known good" copy of this file is maintained and taken into use when a file corruption is detected. Allows F-Secure products to stay fully functional in case of certain operating system crash situations where file corruption may occur.
4? Enhanced Fsdiag utility with more complete reporting
5? Changing the used management key is now possible by F-Secure Management Agent reinstallation

Fixed Problems

6? 7799:AVUTT: Fsdiag in Win 95
7? 15804:Failed conflict removal for FSAV mixes up FSMA installation
8? 15979:FSMA does not install PKI
9? 14748:FSAV 5.22 build 7072: FSAA.EXE hangs during login.
10? 11200:FSMS address in FSMA 4.21
11? 12027:Product language selection and SNMP traps
12? 16376:mprexe fails if we change domain password
13? 15563:FSMAUI localization resources show a '?' instead of national characters
14? 13467:Uninstalling fsma leaves f-secure network provider registry entry
15? 13750:FSDiag fails under Win95 on the 'set' operation
16? 13832:fsdiag fails to retrieve incremental policy and other files
17? 13885:Incremental policy file is not updated or corrupted
18? 14742:Reinstall FSMA fails under Win9x if Keep Existing Settings
19? 12710:Incremental policy in fsdiag reports
20? 7964:FSMA install fails to revert to english if language setting is missing
21? 9782:Manager and UI-plugin module crashes when Netware client installed.
22? 10875:Japanese messages forwarded to SMTP are not UTF8-encoded
23? 11627:NRB shall store the ""last known good"" communication settings
24? 12000:Algorithm that selects temporary directory (used to copy admin.pub) is bad
25? 12143:FSAV 5.2: Using fileshare installation, each NT wrk uses two connections.
26? 12350:DPF -> DPX renaming mechanism fails at some situations
27? 13146:Redefined FSMA settings during installation leave policies broken
28? 15179:Policy based installation fails when all settings are final
29? 16578:FSMA UI plugin leaks memory when settings dialog is kept open
30? 16607:NRB crashes on Win2000 if connection is lost
31? 13771:fsmainst fails to upgrade in w2k in some situations
32? 14135:Ilauncher should delete temporary copy of JAR file before launching setup
33? 14800:winhlp32.exe error in Japanese HELP file for FSMA 4.32
34? 14801:Junk characters in Japanese HELP file for FSMA 4.32
35? 12798:ILauncher gives no notification about that reboot is needed
36? 8704:FSMA setup plugin does not write conflict/error msgs for remote install
37? 10736:FSMA version differs depending on logged on user
38? 10737:Environmental variable of FSMA
39? 11634:FSMA should recover from a corrupted incremental policy
40? 13132:Log files have unnecessary empty lines
41? 14959:'Last connection to server' statistics and UI is updated in standalone mode
42? 15059:FNRB32.EXE crashes on Win2000

43? 15255:NRB doesn't send statistics after comm.method is changed to file protocol
44? 15428:Importing standalone host fails for NT and W2k
45? 16195:Occasional NRB crash on NT
46? 16395:Unsuccessful downloading of 0kb files from server
47? 15639:FIN localization resources have some errors.
48? 15711:FSM32 crash during installation.
49? 16608:FSSS window is not shown correctly in chinese environment.
50? 13692:Copyright information should be updated for 2001
51? 14310:Japanese llaunchr progress screen has error
52? 15076:Successful connection message every time connection settings change
53? 10104:FSMAINST wizard flow shows pages in incorrect order
54? 10830:sending alerts via SMTP: misprint in default message subject
55? 11626:NRB produces alerts with an extra linefeed in the end
56? 11785:PlugInSupport_VerifyConflict() cancels setup: last error message empty
57? 13019:Disabling WSS UI
58? 12054:Text in SNMP progress dialog under Japanese host is missing
59? 12490:No proper error when iLauncher moves jar to temp folder on the filled disk
60? 12360:FSMA newer version conflict detection is not disabled
61? 13342:FSMA Communication tab in Spanish needs resizing
62? 14963:Misprint in FSMA Setup
63? 14965:Previous start time of FSMA is not updated in statistics
64? 16402:Problem in Finnish FSMA
65? 14739:FSMA upgrade installation procedure
66? 8928:Feature Request for FSMA: ""Poll now"" button
67? 13676:Changing communication settings and admin.pub by reinstallation
68? 13697:FSMA uninstaller must remove all user credentials at uninstall(requirement)
69? 14151:Set Debug=1 by default for FSMA insallation
70? 9567:FSMAINST should not pass an empty string.
71? 13161:Optimize the size of FSABOUT localization DLLs
72? 16442:Simplified ""release debugging"" for FSMA 4.50

Known Problems

73? Using a separate communication directory user account can fail if the logged-in user also has mounts for the server where the communication directory is located. This is caused by the "Multiple credentials" (error 1219) problem described in Microsoft TechNet article Q173199. A workaround is to use different network host names for the communication directory path and the share used by the logged-in user. For example, using "\\192.1.2.3\commdir" as the communication directory and "\\companyserver\datafiles" as the logged-in user's share should work even though "companyserver" and "192.1.2.3" were the same machine.

74? 9255: A broken installation of Microsoft Internet Explorer (any version) is known to affect F-Secure Management Agent's communications with the F-Secure Management Server. It is recommended to reinstall or upgrade Microsoft Internet Explorer if the following kind of alerts are observed in the alert log file: "NRB switched its operation mode to Offline Mode. System error number: " (note that the system error number and system error message are missing from the alert)

F-Secure Anti-Virus

Version

F-Secure Anti-Virus Release 5.30 build 7262

IMPORTANT NOTES

- Re-installing or upgrading FSAV 5 will overwrite any virus definition databases used by the previous FSAV 5 installation, thus making the virus protection level somewhat older. In centrally managed installations the new virus definition databases will be updated by the next policy polling interval. If FSAV 5 is installed in stand-alone mode, the user should re-apply the latest virus definition databases available at http://www.F-Secure.com/.

- When upgrading Windows 95/98/NT 4.0 with FSAV 5.x to Windows 2000, it is important to first uninstall FSAV 5.x, then upgrade to Windows 2000, and then reinstall FSAV 5.x. This is because of differences in the low-level driver architecture in older Windows platforms and Windows 2000.

- Windows 2000 contains a new feature that calculates the disk space usage of installed programs and tells how frequently they have been used. This info is provided in the Add/Remove Programs list, but it may be incorrect for the F-Secure Anti-Virus modules. The Add/Remove Programs list may for example claim that F-Secure Anti-Virus has been used occasionally, even if the on-access protection is enabled all the time. This is perfectly normal and does not mean that the product is disabled or malfunctioning in any way. Very high disk space usage figures may also be reported. Always use the Explorer to find out the real disk space usage of the F-Secure products, rather than the figure reported by Add/Remove Programs.

What's New in F-Secure Anti-Virus

F-Secure Anti-Virus 5 includes significant improvements over version 4. The new version is based on F-Secure Framework, the enabling technology behind the new policy-based management architecture.

F-Secure Anti-Virus 5 is designed from the ground up for the corporate environment and large heterogeneous networks. It provides the network administrator with comprehensive security management features and a three-tier architecture that will scale from a small LAN with only a few workstations all the way up to a large WAN with hundreds of thousands of nodes distributed around the globe.

The user interface has been simplified. Every major function of the program is transparent to the user, which reduces maintenance costs. The powerful F-Secure Gatekeeper technology detects and disinfects viruses in real-time. This completely eliminates the complexity of on-demand and scheduled scanning tasks.

Software distribution and alerting functions are no longer based on file-sharing in a LAN. Instead, they work within a three-tier system that uses the HTTP protocol to work in any TCP/IP network. The HTTP protocol will work easily with your existing routers, firewalls, and other components of your network infrastructure.

F-Secure Anti-Virus 5.10 and later versions are compatible with Microsoft Windows95, Windows98, Windows NT 4.0 and Windows 2000 operating systems.

F-Secure Anti-Virus 5.11 and later versions support on-demand updating of virus definition databases using the FSUPDATE-utility (http://www.F-Secure.com/download-purchase/updates.html).

F-Secure Anti-Virus 5.20 introduces new virus definition database functionality through the local user interface and F-Secure Administrator management console. New functionality is illustrated in F-Secure Anti-Virus User's Guide.

F-Secure Anti-Virus 5.22 contains the following major changes from previous release:

- Localization support for Chinese, Spanish and Italian languages.
- Platform support for Windows ME.
- Ability to disable real-time scanning of files accessed over network (applies to outbound access only).
- The HTML-scanning report lists the active scanning engines and their definition database dates.
- The HTTP-update mechanism (Update now) uses Windows' proxy settings, if defined.

F-Secure Anti-Virus 5.30 contains the following major changes from previous release:

- Evaluation support for try-before-you-buy installations (30-day trial period).
- Command-line scanner beta version included for preview (see …\f-secure\anti-virus\readcmd.rtf for more information).
- Status indicator of real-time protection activity in the Windows system tray (can be disabled through policy, see user's manual for instructions).
- Removal of unused virus definition databases from the program folder.
- Manual scanning reports are attached in the SMTP-alerts (configurable in centrally managed installations only).
- Added TAR and TGZ extensions to scanned compressed files (scanning of compressed files is enabled by default in manual scanning only).
- Dynamic detection of BackWeb to determine whether *Update now* should be enabled.

Administration

- The F-Secure Administrator utility provides central administration under three-tier management architecture. The administration tasks include software distribution, updating, alerting, and configuration management.
- F-Secure Anti-Virus is scalable to enterprise-wide networks through distributed F-Secure Management Servers and the HTTP protocol.
- The F-Secure Management Agent provides statistics from each workstation and sends alerts when a virus is found.
- Copies of infected and suspicious files are sent through the F-Secure Management Server to the administrator.
- The administrator can create and distribute policies that specify different settings for manual scans and real-time protection.
- F-Secure Anti-Virus is fully integrated with all of the F-Secure Workstation Suite applications through the F-Secure Administrator utility.
- Alerts, reports, and messages are viewed in F-Secure Administrator.
- Improved support for the industry-standard SNMP protocol.
- Installation and updates are supported under the Microsoft Systems Management Server (SMS) on Windows networks.

End-User Interface

- F-Secure Anti-Virus is fully integrated with all the F-Secure Workstation Suite applications.
- A new and simple user interface makes the most common functions available from a shortcut menu.
- A new Disinfection Wizard guides the user through the removal of viruses from the system.
- The new and easy-to-use virus information database on the F-Secure Web site can be conveniently accessed.
- All F-Secure Anti-Virus settings can be centrally managed by the administrator.
- The administrator can determine what is visible in the user interface, thus controlling the level of transparency to the user.

Following list contains the most important fixes and known problems in this release of F-Secure Anti-Virus 5. The numbers refer to F-Secure's internal change-tracking database entries. For more detailed information, contact Anti-Virus-Support@F-Secure.com.

Most Important Fixed Problems

- 14108, "FSAV causes BSOD on NT TSE"
- 14247, "BSOD with FSAV 5.11"
- 14370, "FSAV 5.20 causes computer to reboot several times before login [#13165,#13620]"
- 13049, "Exception in AVP during NW logon (Crash at AVP95(01) + 0001557D)"
- 13165, "FSAV 5.20 causes BSODs [#13620,#14370]"
- 15269, "Disable stack switching in Win9x FSAV5 [#13552]"
- 15473, "F-Prot 3.08/09 causes hang-ups in ODS. [#15260]"
- 12414, "FSAV 5.20 conflicts with Acer NeoMagic ZV+ [#13657]"
- 13556, "FSAV.HLP missing [#13346]"
- 14232, "No warnings when all scanning engines are disabled"
- 13238, "FSAV 5.21/NT Update now does not remind me as specified"
- 15382, "Change the level of trap 'no scanning engines loaded' to 'Security alert'"
- 5052, "SMTP report sent by FSMA doesn't say which virus it is"
- 6856, "Date and Time Formats are not localized in FSAV 5 [#14280, #14282]"
- 11326, "F-TESTW does not detect FSAV5 GK95"
- 12321, "Uninstall doesn't work if one AV engine has been disabled"
- 14323, "FSAV 5.x: Unnecessary signature DBs should be removed by FSAV [14397]"
- 10921, "DW doesn't start for user stopped ODS."
- 15852, "BSoD when scanning WBEM files."
- 14222, "AV 5 makes using Netscape messanger slow [#16134]"
- 15850, "GK does not detect a virus in file with Japanese file name"
- 15934, "FSAV 5.30 could not apply new virus definition databases. [#15399]"
- 13547, "FSAV5: Banyan access doesn't work with active GK [#6540]"
- 15184, "DEFRAG Freeze with GK"
- 13631, "Scandisk doesn't work with FSAV 5.20 if real-time scanning is enabled"
- 16708, "FSAV upgrading fails because renaming of database files fails"

Known Problems

- Using the Offline-file synchronization feature in Windows 2000 may cause slowdowns with large number of files. This can be worked around by excluding the Offline files storage folder from real-time scanning. By default, the offline storage folder is located at <nt-system-root>\csc. To exclude the folder, use the "Exclude objects" function on the "Real-time Protection" page of F-Secure Anti-Virus settings.

- Real-time protection always causes some overhead on file I/O, which can cause problems for time-critical file operations such as creating CD-R/CD-RW images.

- Starting manual scans on drives that reside on Banyan shares cause unstability for F-Secure Anti-Virus. Workaround is available through Anti-Virus-Support@F-Secure.com if you experience this problem in your Banyan environment. (related Change Tracking System entry: #16876).

- 13178, "Do not allow install if machine does not meet memory requirements [#10584]": Although F-Secure Anti-Virus 5 has minimum system requirements (see "System requirements" in this document), they are not checked during setup, allowing the product to be installed on systems without enough resources.

- 15447, "FSMUIAV.DLL not initialized if FSMA isn't running": In some environments the user may be able to login before F-Secure Management Agent is started, causing the F-Secure Anti-Virus settings and statistics to be unavailable. This can be worked around by waiting a moment before logging into the system. Even if this problem occurs, the real-time virus protection is fully functional.

- 12682, "FSAV confilcts with the installation of Sandstone dictionary SW": F-Secure Anti-Virus 5 and Sandstone dictionary software (http://www.sandstone.fi/) have interoperability problems on Windows 9x platforms.

- 9741, "FSAV5 Doesn't find an infected MBR when scanning manually" If FSAV 5 detects an infection on MBR of a hard disk, the user should set the real-time protection's "Action on infection" setting to "Disinfect automatically" and reboot; this will remove the infection.

- 5727, "'Unable to scan' situation is not handled for password protected archives": F-Secure Anti-Virus 5 is not able to scan inside password-protected archives, but as soon as any infected file is extracted from such an archive, F-Secure Anti-Virus 5 will detect the infection.

- 7079, "LS120 drive inaccessible when FSAV upgraded to 5.01": LS120-drives may become inaccessible if F-Secure Anti-Virus 5 is installed. This problem can be worked around by disabling the F-Secure AVP scanner plug-in.

- 10620, "Problems with removal of resident CIH.1003 virus with FSAV 5": F-Secure Anti-Virus 5 may not be able to completely remove a resident CIH.1003 virus. For instructions on removing the virus, go to http://www.f-secure.com/v-descs/cih.htm.

- 13011, "FSAV 5.21 build 6460: Eudora slow to start when GK active.": Some newer Eudora versions may take a long time to load if real-time scanning is enabled. This is because the file "eudora.ini" gets scanned repeatedly. You can workaround this by excluding "eudora.ini" from scanned files.

- 12307, "FSAV unable to disinfect from folder C:_Restore in WinME": F-Secure Anti-Virus can not disinfect/delete/rename infections found under the special system folder "_Restore" of Windows ME. Infections are detected normally, however.

Installation

Key Codes for Installation

The key code for the installation is printed on a sticker on the CD-ROM cover.

Installation Order

Please consult F-Secure Management Tools Administrator's Guide for full step-to-step instructions.

Installing into environment with F-Secure Management Tools already installed:

1. Select "View Packages" in F-Secure Administrator.
2. Select "F-Secure Management Agent" in the "Installation Packages" dialog and select "Delete".
3. Copy the accompanied JAR-file to the communication directory path "..\install\entry".
4. Select "Refresh" in the "Installation Packages" dialog.
5. F-Secure Administrator starts verifying the signature of the new installation packages. After this, you are ready to distribute F-Secure Anti-Virus 5 in the policy domain.

Installing into environment without previous installation of F-Secure Management Tools.

1. Install FSMS (optional). This step is not required if you only want to use the communication directory.
2. Run F-Secure Management Tools Setup.
3. Run F-Secure Administrator from the Start menu. When FSA is run for the first time, it launches the Setup Wizard to collect required information. This wizard will also initialize the communication directory and generate the administration key-pair. FSA may display the wizard again later if some required information is no longer available.
4. Once the main window of FSA is visible, you have to define the policy domain structure. You can start with a very simple flat structure which contains only a single domain where all hosts are placed directly under that root domain. Select the domain pane and choose the New Domain from the Edit menu.
5. After you have a root policy domain, you can start adding hosts: (1) Install FSAV 5 to some host(s) and choose Autoregistered Hosts from the Edit menu to import the hosts into the domain. (2) Choose Import Hosts from the Edit menu to browse the NT domain and to install FSMA to the selected hosts. (This does not work in the beta version.) (3) Choose New Host from the Edit menu. Note that this is suitable mainly for testing FSA alone. Because in this case there is no actual managed host(s), the status information, alerts, and reports are not available.
6. Select "Policy" tab in the Properties pane. Change policy values under the Settings subtree as required.
7. Choose Distribute from the File menu to generate the policy file(s).

Additional information:

- F-Secure Management Tools Setup. See the F-Secure Management Tools Administrator's Guide, Section 3.2.
- F-Secure Workstation Suite Setup. See the F-Secure Workstation Suite Administrator's Guide, Chapter 3.
- F-Secure Management Server. See the F-Secure Management Tools Administrator's Guide, Section 2.2.

F-Secure Intelligent Installation™

F-Secure Anti-Virus 5 includes the F-Secure Intelligent Installation™ method which provides the administrator with a method to distribute the software and update all Windows NT workstations in a domain from a single point. Hosts will be installed or updated without any end-user intervention and without need of giving the local administrator rights to end-users.

System Requirements

The system requirements for F-Secure Anti-Virus are:

- Microsoft Windows 2000, Windows NT 4.0, Windows 95, Windows 98 or Windows ME running on Intel Pentium hardware
- 32 MB of RAM (64 MB recommended minimum for Windows NT platforms)
- 30 MB free hard disk space
- Ethernet network interface or a dialup/DHCP interface

    The recommended Microsoft Windows NT 4.0 installation is with Service Pack 6

The system requirements for F-Secure Management Tools are listed in the F-Secure Management Tools Setup 'Readme' file. The system requirements for F-Secure Management Server Setup are listed in the F-Secure Management Server Setup 'Readme' file.

Uninstallation

Uninstalling the F-Secure Anti-Virus requires some manual operations. Administrator rights are required for uninstalling.

To uninstall the F-Secure Anti-Virus, do the following steps:

- Uninstall all F-Secure components by using Add/Remove Programs in the Windows Control Panel. Note that F-Secure Management Agent must be uninstalled last.
- Reboot the computer.
- Remove the remaining files in C:\Program Files\F-Secure.
- Remove the remaining shortcuts in the Start Menu.

Known Problems

- CTS #3419 Setup does not launch properly if Microsoft Outlook 98 is running
  *The following text is from InstallShield Support web site (support.installshield.com)
  Document ID: Q102626*
  Symptoms
  When I run Setup.exe on my system, which has Microsoft® Outlook® 98 running and is connected to a Microsoft Exchange Server, the setup initialization reaches 100%, but then nothing happens. If I wait a long time, the first dialog box appears and the installation proceeds normally.
  Cause
  This problem occurs due to some timing issues between Setup.exe and the Microsoft Exchange Server.
  Workaround
  Close Outlook 98 before running Setup.exe. Generally, you should not have any other applications running when you run an installation.

F-Secure License Terms

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	In Europe
E-mail: US-Sales@F-Secure.com	E-mail: Helsinki@F-Secure.com
Telephone: (408) 938-6700	Telephone: +358 9 2520 0700
Toll Free: (888) 432-8233	
Fax: (408) 938-6701	Fax: +358 9 2520 5001
Postal address: F-Secure, Inc.	F-Secure Corporation
675 N. First Street, 5th floor	Tammasaarenkatu 7
San Jose, California 95112	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

Trade Register No: 425.966, VAT FI07055792   Effective June 2001