Contents

Overview

F-Secure Anti-Virus has been designed for corporate network environments. The virus detection features operate in real-time and transparently. The program requires little or no action by the users, which minimizes the need for training and support. The centralized policy-based management features provide an anti-virus solution that is easy to maintain and low in cost.

F-Secure Anti-Virus Gatekeeper

F-Secure Anti-Virus Gatekeeper's functioning is based on Dynamic Virus Protection technology. This technology employs a device driver which monitors the operating system services used in opening files and managing disk partitions.

The Real-Time Protection feature provided by F-Secure Anti-Virus Gatekeeper gives you continuous protection against viruses as files are opened, copied, moved, renamed and downloaded from the Web.

Real-time Protection functions transparently in the background, looking for viruses whenever you access files on the hard disk, diskettes, or network drives. If you try to access an infected file, Real-time Protection will automatically stop the virus from executing. It will then either remove it from the file or display a warning, as specified in the security policy.

> F In order to prevent boot sector viruses from spreading, Real-time Protection also checks for diskettes when the computer is shut down or restarted. This may cause a buzzing sound if there is no diskette in the disk drive. This buzzing sound is normal.

To see if Real-time Protection is active, double-click the F-Secure Settings and Statistics icon in the System Tray in the lower right corner of the screen. If the status of F-Secure Anti-Virus is 'Enabled', Real-time Protection is active and providing continuous protection.

Scanning for Viruses Manually

There is no need to scan files manually. The real-time detection features of F-Secure Anti-Virus Gatekeeper ensure the strongest protection against viruses automatically. The information in here is for reference in case you want to run a manual scan.

You can start a virus scan with any of the following:

- Shortcut menu (right-click on afile, folder or disk)
- F-Secure Settings and Statistics menu on the System Tray (right-click on the ‘F’ (F-Secure) icon in the system tray)
- Windows Start menu (right-click on the menu)

During manual scanning, the *Manual Scan Statistics* dialog box displays a progress indicator and statistics for the scan. The scan can be interrupted by clicking **Stop**. A report is generated after the scan is completed. You can view the report in your Web browser by clicking **Show Report**.

More:

Shortcut Menu

F-Secure Settings and Statistics Menu on the System Tray

Starting a Scan from the Windows Start Menu

Shortcut Menu

To scan a file, folder, or disk for viruses, right-click its icon, and choose ‘Scan Folders for Viruses’ from the shortcut menu. Any file, folder, or drive can be scanned this way, regardless of extension.

F-Secure Settings and Statistics Menu on the System Tray

You can display the F-Secure Settings and Statistics menu by right-clicking on the ‘F’ (F-Secure) icon in the system tray.

To start a scan, choose one of the Scan actions on the menu.

If you choose *Scan Target*, you will then need to select the folder or disk to scan.

Starting a Scan from the Windows Start Menu

The F-Secure Anti-Virus program group contains shortcuts for scanning your hard disks, diskettes, and folders.

To start a scan, select one of the following scan commands on the menu: *Scan all local hard disks, Scan diskette* or *Scan folder*. If you select *Scan folder*, you will need to select a folder or disk to scan.

Disinfection Wizard

If a virus is found while you are using the computer, F-Secure Anti-Virus will start the Disinfection Wizard by default.

1. The first screen displays the names of the detected viruses.
   For more information about a virus, click on its name, and then click the **Virus Info** button. The Virus Information page will display a list of detected viruses.
   You can browse the entire virus information database by clicking the check box. If the virus is very new, it may not be in the database. If you do not see a description, you may find it in the Virus Information Database at our Web site.
   The F-Secure Virus Information Database is an extensive virus knowledge database that contains information on thousands of viruses. The database is updated every day. To access this database, click the **Web Club** button.
2. Then, a list of infected files will be displayed.
   In the ***Action to Take*** box, choose the action to be taken on the infected files.
3. The files will now be disinfected and the results of the disinfection action will be displayed.
4. Disinfection Report will be generated. If you do not want a report to be generated, clear the ***Generate Report*** check box.

The disinfection report is automatically displayed in your default Web browser. The report is sent to the administrator if the program is centrally managed.

> F Note**.** The administrator can configure F-Secure Anti-Virus to automatically remove viruses from the computer without prompting for any action. In this case, Disinfection Wizard does not run.

Settings

You can view and modify F-Secure Anti-Virus settings by opening the *F-Secure Settings and Statistics* dialog box and double-clicking the ‘F’ icon in the system tray. F-Secure Settings and Statistics will open and display a list of installed F-Secure products.

You can either double-click the *F-Secure Anti-Virus* application, or click **Properties** to open the *F-Secure Anti-Virus Properties* dialog box. In the *F-Secure Anti-Virus Properties* dialog box, you can specify different settings for the three kinds of scanning operations: Real-time Protection, Manual Scanning and Updates. The *F-Secure Anti-Virus Properties* dialog box also has information on scan statistics.

Statistics

Displays results of the real-time scan.

Real-time Protection

Settings for transparent, continuous protection provided by F-Secure Anti-Virus while it runs in the background, scanning files as they are accessed.

Manual Scanning

Settings for the scanning tasks that are started manually.

Updates

Settings for enabling automatic virus definition database update reminders for manual updates. The **Update Now** button makes immediate updates possible.

Real-time scans should be restricted so that they do not use a large amount of system resources, which can occur when scanning compressed files and other special files.

Because manual scans are only performed when desired, they can be set to scan larger groups of files, which will consume more system resources.

Real-time Protection

To enable or disable real-time protection with F-Secure Anti-Virus, select or clear the ***Enable Protection*** check box.

More:

Action to Take on Infected Files

Scanning Options

Action to Take on Infected Files

In the ***Action to Take on Infected Files*** box, you can choose what action F-Secure Anti-Virus will take when an infected file is detected. Choose one of the following actions:

Ask after scan

Starts the Disinfection Wizard when an infected file is detected.

Disinfect automatically

Disinfects the file automatically when a virus is detected.

Rename automatically

Renames the file automatically when a virus is found.

Delete automatically

Deletes the file automatically when a virus is found.

Scanning Options

Under ***Scanning Options***, you can choose which files will be scanned in real-time.
The following options are available:

All files

All files will be scanned, regardless of their file extension. This option is not recommended because it might slow down system performance considerably.

Files with these extensions

Files with specified extensions will be scanned. To specify files that have no extension, type '.' You can use the wildcard '?'. Enter each file extension separated by a space. This option is recommended for real-time protection.

Exclude files with these extensions

You can specify files that will not be scanned.

Exclude objects

You can specify individual files or folders that will not be scanned. To do so, click the **Select** button, and browse for the files or folders you want to exclude from scanning.

Scan inside compressed files

Select this check box to scan inside compressed files, such as ZIP, ARJ, and LZH files. Scanning inside large compressed files might use a lot of system resources and slow down the system. Therefore, it is not recommended with real-time protection.

Manual Scanning

The settings for manual scan operations can be specified in the *Manual Scanning* page of the *F-Secure Anti-Virus Properties* dialog box.

More:

Action to Take on Infected Files

Scanning Options

Action to Take on Infected Files

In the ***Action to Take on Infected Files*** box, you can choose what action F-Secure Anti-Virus will take when an infected file is detected.

One of the following options can be chosen:

Ask after scan

Starts the Disinfection Wizard when an infected file is detected.

Disinfect automatically

Disinfects the file automatically when a virus is detected.

Rename automatically

Renames the file automatically when a virus is found.

Delete automatically

Deletes the file automatically when a virus is found.

Scanning Options

Under ***Scanning Options***, you can choose which files will be scanned during the manual scanning operation.

The following options are available:

All files

All files will be scanned, regardless of their file extension. This option is not recommended because it may slow down system performance considerably.

Files with these extensions

Files with specified extensions will be scanned. Enter each file extension separated by a space. You may use the wildcard '?'.

Exclude files with these extensions

You may specify files that will not be scanned.

Exclude objects

You can specify individual files or folders that will not be scanned. To do so, click the **Add** button, and browse for the files or folders that you want to exclude from scanning.

Scan inside compressed files

Select this check box to scan inside compressed files, such as ZIP, ARJ, and LZH files. This option can be readily used because manual scanning tasks do not affect the performance of the system.

The **Scan Now** button can be used to scan a folder for viruses at any time.

Updates

The Updates page has information on installed scanning engines and virus database updates. It also has a direct link from the **More Information** button either to F-Secure's web site or to an ISP site.

More:

Installed Scanning Engines

Virus Database Updates

Remind me about updates

Update Now

Update Reminder

More Information

Installed Scanning Engines

In the ***Installed Scanning Engines*** box you can find information on the currently installed scanning engine names, the individual database dates and their revision numbers. The scanning engines used are F-Secure F-Prot, F-Secure AVP or F-Secure Orion.

Virus Database Updates

The ***Virus Database Updates*** section informs you about the current status of the virus definition databases. It will, for example, inform of any immediate updates that should be made if virus definition databases are old.

Remind me about updates

With the ***Remind me about updates*** check box you can enable the automatic virus definition database update reminders. You can determine how often an update dialog appears by inserting a number in the ***days*** box.

The availability of the update reminder functionality is determined by policy settings. If manual updates have been forbidden by the policy settings, both the ***Remind me about updates*** check box and ***[X] days*** box are not available. The adminstrator can change the allowance status for these options from the F-Secure Administrator policy:

`FSAV\Data Fellows\F-Secure Anti-Virus\Settings\Virus Database Updates\Update Reminder\Reminder Status`

The default status for Standalone Mode is **allowed** and for Centrally Managed Mode **not allowed**.

Update Now

The **Update Now** button starts the manual virus definition database update. Whether this feature is available or not is determined by policy settings.

If the following F-Secure Administrator policy setting

`FSAV\Data Fellows\F-Secure Anti-Virus\Settings\Virus Database Updates\Allow Manual Updates`

is set to **true**, the **Update Now** button can be used. If F-Secure Anti-Virus has been installed with Centrally Managed configuration, it will start normal update polling from either Management Server or from wherever virus definition databases are distributed. Standalone Mode starts downloading new databases from F-Secure's own site or from an ISP site.

A dialog is shown during the download process. The update can be cancelled by pressing the **Cancel Update** button.

Update Reminder

If manual virus definition database updates are allowed, then update reminders are also enabled. If the ***Remind me about updates every [X] days*** check box has been checked and X days have passed since the last update, or update reminder, a dialog is shown.

If you press the **Update Now** button in this dialog box, the manual virus definition database update starts. If you press the **Remind Me Later** button, the update reminding is postponed by the number of days chosen as the reminding interval. If you press the **Update Options** button, the *F-Secure Anti-Virus Properties* dialog opens with the *Database Management* tab active.

More Information

The **More Information** button opens a default web browser at either F-Secure's or ISP's site. The URL can be changed in F-Secure Administrator at:

`FSAV\Data Fellows\F-Secure Anti-Virus\Settings\Virus Database Updates\Information Site`

Note that the URL must contain the protocol and site name, for example http://www.company.com

Statistics

The *Statistics* page of the *F-Secure Anti-Virus Properties* dialog box displays results of the real-time scan for the current session.

Technical Support

F-Secure Technical Support is available by e-mail and from our Web site. You can access our Web site from within F-Secure Anti-Virus or from your Web browser.

More:

Web Club

Virus Descriptions on the Web

Electronic Mail Support

Web Club

The F-Secure Anti-Virus Web Club provides assistance to F-Secure Anti-Virus users. To enter, choose the Web Club command from the Help menu. The first time you use this option, enter the path and name of your Web browser, and your location.

To connect to the Web Club directly from within your Web browser, go to:
http://www.F-Secure.com/webclub/

For advanced support, the F-Secure Anti-Virus Support Center is available at:
http://www.F-Secure.com/support/

Virus Descriptions on the Web

F-Secure Corporation maintains a comprehensive collection of virus-related information on its Web site. To view the Virus Information Database, choose the Virus Descriptions On the Web command from the Help menu.

Alternatively, you can access the Virus Information Database at:
http://www.F-Secure.com/vir-info/

Electronic Mail Support

If you have questions about F-Secure Anti-Virus not covered in the manual or online services at *www.F-Secure.com*, you can contact your local F-Secure distributor or F-Secure Corporation directly.

For basic technical assistance, please contact your local F-Secure Business Partner. Send your e-mail to:

Anti-Virus-<country>@F-Secure.com

Example: Anti-Virus-Norway@F-Secure.com

If there is no authorized F-Secure Anti-Virus Business Partner in your country, you can request basic technical assistance from:

Anti-Virus-Support@F-Secure.com

Please include the following information with your support request:

Version number of F-Secure Anti-Virus (including the build number).

Name and version number of your operating system (DOS, Windows). Include the build number.

A detailed description of the problem, including any error messages displayed by the program, and any other details which could help us replicate the problem.

When contacting F-Secure support by telephone, please do the following to save time:

Be at your computer so you can follow instructions given by the support technician, or be prepared to write down instructions.

Have your computer turned on, and (if possible) in the state it was in when the problem occurred; or you should be ready to replicate the problem on the computer with minimum effort.

If you have a virus infection, make sure that you have run the latest fsupdate. The fsupdate can be downloaded from the Web Club.

Corporation Information

F-Secure Corporation (formerly Data Fellows) is one of the world's leading developers of data security products. The company develops, markets and supports anti-virus, data security, and cryptography software products for corporate computer networks. It has headquarters in San Jose, California, and Espoo, Finland, with branch offices in several countries, including the UK, France, Germany, Japan, Hong Kong, and Canada. Corporate partners, VARs and other distributors are located in over 80 countries around the world. F-Secure products have been translated into more than 20 languages.

F-Secure software products have received numerous international awards and citations. The company was named one of the Top 100 Technology companies in the world by Red Herring magazine in its September 1998 issue. F-Secure Workstation Suite 4.0 was awarded five stars, the highest rating, by SECURE Computing Magazine in its July 1999 issue. F-Secure Anti-Virus was awarded Editor's Choice by the German PC Professionell Magazine in its July 1999 issue. Other commendations include Hot Product of the Year 1997 (Data Communications Magazine); and Best Anti-Virus product (SVM Magazine, May 1997) and the 1996 European Information Technology Prize.

F-Secure Corporation has tens of thousands of customers in more than 100 countries. These include many of the world's largest industrial corporations and best-known telecommunications companies; major international airlines; several European governments, post offices and defense forces; and several of the world's largest banks. Customers include NASA, the US Air Force, the US Department of Defense Medical branch, the US Naval Warfare Center, the San Diego Supercomputer Center, Lawrence-Livermore National Laboratory, IBM, Unisys, Siemens-Nixdorf, EDS, Cisco, Nokia, Sonera (formerly Telecom Finland), UUNet Technologies, Boeing, Bell Atlantic, and MCI.

The F-Secure Product Family

All F-Secure products are integrated into the F-Secure Framework, which provides a three-tier, scalable, policy-based management infrastructure for minimizing the cost of security management.

F-Secure Workstation Suite consists of malicious code detection and removal, unobtrusive file and network encryption, and personal firewall functionality, all integrated into a policy-based management architecture.

F-Secure Anti-Virus, with multiple scanning engines (including F-PROT and AVP), is the most comprehensive, real-time virus scanning and protection system for all major desktop and server platforms. It is a three-tiered solution aimed at the corporate market, and includes a wealth of features for network management and centralized deployment.

F-Secure Content Scanner protects networks against viruses arriving through e-mail, web downloads, and database replication. It works with Microsoft Exchange Server, Lotus Domino, and firewall products from Check Point and other leading vendors.

F-Secure VPN+ provides a software-based, IPSec-compliant virtual private network solution for large corporate networks as well as remote and small office networks. By combining F-Secure VPN+ products, companies of any size can use cost-effective public networks, or the Internet, to create secure VPNs without the need to install special hardware.

F-Secure FileCrypto is the first and only product to integrate strong real-time encryption directly into the Windows file system. It automatically encrypts data before being stored on the hard disk, protecting sensitive information in the most demanding situations. FileCrypto also allows users to send encrypted, self-extracting packages by e-mail to other users.

FSecure SSH provides secure remote login, terminal, and other connections over unsecured networks. It is the most widely used secure remote administration tool.

F-Secure NameSurfer is the solution for remote Internet and intranet DNS administration. Its easy-to-use WWW user interface automates and simplifies DNS administration.

F-Secure Distributed FireWall is a software-based firewall product that offers complete protection to a widely distributed, mobile workforce from one centrally managed location.

Glossary of Terms

Access control
AUTOEXEC.BAT
Background task
BAT file
BIOS
Bit
Boot
Boot sector
Byte
Checksum
CMOS
Cold boot
COM file
CONFIG.SYS
CounterSign
CPU
CRC
DOS
EXE file
HPFS
Kilobyte
LAN
MBR
Megabyte
Modem
Multipartite virus
Mutating virus
NFS
NTFS
On-access scanner
On-demand scanner
RAM
Real-time scanner
Reset

Access control

The procedure which grants or denies users or processes to use a system. Usually this involves authentication of the user, verifying of access rights, monitoring and logging.

AUTOEXEC.BAT

The command file automatically executed during system start-up in DOS.

Background task

Task that is running, but not shown in the active window.

BAT file

File containing DOS commands used for automating repetitive tasks.

BIOS

Basic Input/Output System. The part of the operating system that handles the most hardware-specific tasks. On most PCs, the BIOS is stored in ROM.

Bit

The smallest unit of memory size recognizable by a computer. Sets of bits make up bytes, arranged in a sequential pattern to express text, numbers, or other detailed information.

Boot

To restart the computer.

Boot sector

Boot record. An area located on the first track of diskettes and logical disks. Boot sector information enables the computer to read an operating system (such as MS-DOS, for example).

Byte

A small unit of memory size, enough to store one alphabetical or numeric character. Each byte is composed of "bits," binary units collected in sets (e.g., 00101101) which store the smallest pieces of information.

Checksum

Identifying number calculated from file characteristics, such that if the file changes even the smallest amount, this identity is changed.

CMOS

Complementary Metal Oxide Semiconductor. The battery-powered memory of PC-computers. The size of this memory is typically from 32 to 50 bytes. CMOS contains information about external details such as disks, date, and peripherals. It is not emptied when the computer is turned off, as long as the battery still has power.

Cold boot

To restart the computer by turning the power off and on.

COM file

DOS executable program with a simple structure. The maximum size is 64 kilobytes.

CONFIG.SYS

The configuration file automatically executed during system start-up in DOS.

CounterSign

The framework that integrates a variety of scanning engines to offer protection on several levels, for all possible compression and encryption schemes, implementing virtually 100% virus protection at the enterprise level under a single interface.

CPU

Central Processing Unit. The "brain" of the computer. It is usually housed in a "box," which may be separate from the monitor.

CRC

Cyclic Redundancy Check. One of the most popular checksum methods. CRC uses a 32-bit signature calculated from the contents of the file.

DOS

Disk Operating System. The most basic system type; originally used on all personal computers.

EXE file

An "executable" file, or program file; the type of file that "runs," unlike a document or data file.

HPFS

High Performance File System. The file system used by OS/2.

Kilobyte

1 024 bytes

LAN

Local Area Network. A small network within a room, building or group, which may or may not be connected to the larger worldwide Internet.

MBR

Master Boot Record. An area located on the zero track of physical hard disks. It contains the main boot program and the partition table. Main boot record is independent of operating systems and is always executed first after the computer has performed the Power-On-Self-Test (POST). The size of a main boot record is 512 bytes. The main boot program translates the partition table, which contains information on how the physical disk is divided (partitioned) into logical entities. After this, the main boot program executes the boot sector of the active partition.

Megabyte

1 024 kilobytes (one million bytes)

Modem

A telephonic piece of hardware used to connect a computer or Local Area Network to a larger network such as the Internet.

Multipartite virus

A virus composed of several parts. Every part of a multipartite virus needs to be cleaned away, to give assurance of non-infection.

Mutating virus

A virus which changes itself (mutates) as it passes through host files, making disinfection a serious challenge.

NFS

Network File System used by many UNIX variants.

NTFS

Windows NT File System.

On-access scanner

Real-time scanner, a background process that provides a constant guard against viruses.

On-demand scanner

A virus scanner which is started manually.

RAM

Random Access Memory. The dynamic memory used by the processor.

Real-time scanner

A scanner that operates in the background, allowing a user to continue working at normal speed, with no significant slowing.

Reset

To warm boot the system.