Contents

What's New

F-Secure Anti-Virus Quick Start

Using F-Secure Anti-Virus

Administering F-Secure Anti-Virus

What to Do When a Virus Is Found

Background Information on Viruses

Technical Support

What's New in F-Secure Anti-Virus?

- The Countersign Technology framework provides an API (application programming interface) for plugging in anti-virus detection modules
- Various types of archive contents (for instance, ZIP, ARJ and LZH) are seen as directories and files by the detection modules. The same applies for all sorts of compound documents like OLE files and mail server databases.
- The Network Management services provide a means of communicating detection engine alerts, reports and messages to the administrator. In addition, the administrator is provided with remote configuration and policy management services to the anti-virus utilities.
- Installs over any currently installed anti-virus product. Future versions of F-Secure Anti-Virus (to be released later this fall) will provide a method of combining the currently installed anti-virus product into the F-Secure Anti-Virus Framework.
- F-Secure Anti-Virus Gatekeeper real-time scanner technology is now also available for Windows NT workstation and server systems as well as Windows 3.x and Windows 95 environments, including automatic update support
- The Data Fellows Web Club allows internet connections to the latest information directly from F-Secure Anti-Virus, including a large library of technical information for the administrator and continuously updated virus descriptions, updates and support for the end user
- Uses an advanced heuristic analysis to detect previously unknown viruses therefore limiting the risk of false alarms.
- Advanced change detection method. This checksum technology uses Data Fellows' advanced cryptography technology developed for military users of Data Fellows data encryption products to protect both the method of detecting change on the users system as well as protecting the F-Secure Checksum database.
- Unobtrusive background operation for all major platforms.
- F-Secure Anti-Virus Macro Control — a revolutionary solution: the only product on the market to use a "certification" approach to document and spreadsheet macros in the enterprise. F-Secure Macro Control checks for locally known macros that have been created for the general use within an organization.
- Installs desktop versions of F-Secure Anti-Virus automatically to multi-platform environments from a single workstation.
- Send updates to users with a single mouse click.
- Receive reports from workstations when a virus is found.
- Receive copies of infected files from workstations automatically.
- Receive copies of suspicious files from workstations automatically.
- Mandate workstations to perform scan from a central location.
- Send F-Secure Anti-Virus update bulletins or other messages to users.
- Remotely change any setting or configuration in workstation installations.
- Advanced, network independent centralized management system.

- Clear and easy-to-use interface with Windows 95/NT 4.0 look-and-feel.
- Customizable toolbar with instant Tool-Tips, which orient the new user to the F-Secure Anti-Virus interface.
- Right-mouse-click support for Windows 95 and Windows NT 4.0 Explorer and Desktop.
- Easy-to-use Wizard for creating automatic network installation.
- Extensive and easy-to-understand virus description database, explaining what all the common viruses actually do.
- Direct links to the Data Fellows Anti-Virus WWW services providing the most up-to-date information.
- A Wizard makes automatic installation easier, allowing the administrator to create an automatic network installation and update script directly from the Administrator menu.
- Extremely fast scanning is supported for ZIP and other compressed file archives.
- The new F-Secure Anti-Virus Service automatically manages updates on Windows NT, even if no one is using the computer.
- Right-mouse-click support for Windows 95 and Windows NT Explorer enables direct virus scanning.
- Installation and updates supported under the Microsoft Systems Management Server (SMS) on Windows networks.
- Automatic alerting capabilities strengthened with industry standard Simple Network Management Protocol (SNMP) support.
- Comprehensive F-Secure Anti-Virus collection of virus descriptions available online directly from the report window.
- New Windows 95 compatible user interface gives fresh look, eliminating confusion for new users and bringing many improvements in ease-of-use.
- Multi-language support enhanced, task and button names reflect language change.

Web Club

The F-Secure Anti-Virus Web Club provides help and 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 World Wide Web browser, and your location.

To connect to the Web Club directly from within your web browser, open this location:

- http://www.DataFellows.com/anti-virus/webclub/

For advanced support, the F-Secure Anti-Virus Support Center is available on the web:

- http://www.DataFellows.com/anti-virus/support/

Data Fellows 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. The first time you use this option, you will need to enter the path and name of your WWW browser, and your location.

To connect to the Virus Information Database directly, open this location:

- http://www.DataFellows.com/vir-info/

Scanning for Viruses Inside Archived Files

F-Secure Anti-Virus supports scanning inside several archive file formats, such as the files compressed with the ZIP and LZH algorithms. Data Fellows constantly increases support for various compressed file formats. Please see this Web page for the latest information:

- http://www.DataFellows.com/anti-virus/support/compressed-file-formats.htm

Launching F-Secure Anti-Virus

To start F-Secure Anti-Virus, double-click the F-Secure Anti-Virus icon in the taskbar which is available under Windows 95 and Windows NT 4.0.

If you’re not running F-Agent, choose F-Secure Anti-Virus from the Start menu.

In Windows 3.1 and NT 3.x, click the F-Agent icon on the desktop and choose the Start F-Secure Anti-Virus for Windows command from the menu.

If you’re not running F-Agent, double-click the F-Secure Anti-Virus icon in the F-Secure Anti-Virus program group in Program Manager.

Scanning for Viruses

The F-Secure Anti-Virus Gatekeeper device driver provides you with real-time protection from viruses as you access files. This shields your computer from all kinds of viruses automatically without manual intervention or configuration.

For additional protection, you can run the F-Secure Anti-Virus interactive virus scanner and search for viruses on the hard disk, floppy disks, CD-ROMs, and network disks. You can even automate the scanning by saving the necessary settings as a task and scheduling the task to run periodically.

F-Secure Anti-Virus includes several ready-made tasks, to perform, for example, the following scans:

- Scan Diskette in Drive A:
- Scan Hard Disks
- Scan Folder
- Scan Network

F-Secure Anti-Virus toolbar contains buttons for starting these tasks. Clicking a button will start the corresponding task. Place the mouse pointer over a toolbar button to view the button’s name.

These tasks can also be executed by selecting their corresponding icons from the F-Secure Anti-Virus program group or the Windows 95 and Windows NT 4.x Start menu.

You can also perform scans by dragging and dropping files and directories into the F-Secure Anti-Virus window, or on top of the F-Secure Anti-Virus or F-Agent icon on the desktop. The dropped objects will be scanned automatically.

See Working with Scanning Tasks for more information on managing the scanning tasks.

Creating a Rescue Disk

It is a good idea to create a diskette that contains copies of the most important system areas of your hard disk to get your system running in case you ever have a problem starting your computer. This disk will also help you recover from certain types of virus infections.

More:

Standard Rescue Disk

Windows NT Rescue Disk

Manual Rescue Disk Creation

Standard Rescue Disk

Before you begin the creation of a Rescue Disk, you must make absolutely sure that your computer is free of viruses. Otherwise, a virus that has infected your computer before the installation of F-Secure Anti-Virus may spread to the Rescue Disk also. You can verify the cleanness of your system by booting the computer from a clean, write-protected boot diskette and running a virus check with F-Secure Anti-Virus.

1. Turn off the power in your computer.
2. Insert the boot diskette in the diskette drive and switch the computer on. If you do not have a boot diskette, you may use the MS-DOS SETUP diskette. After the SETUP program has started, exit it by pressing the [F3] function key twice.
3. When the boot process is complete, remove the boot diskette and insert the Disinfection Disk in the drive.
4. Write the command
   ```
   A:\FSAV.EXE /HARD
   ```
   on the command line and press [ENTER].

If your computer will not boot from a diskette, set drive A: to be the boot drive in the computer's BIOS settings. Remember to switch this setting back after you have booted the computer.

F-Secure Anti-Virus checks all available hard disks as well as the computer's memory for viruses, and gives you a report of the results. If the system seems to be clean, you can begin the creation of a Rescue Disk. On the other hand, if the program detects a virus in your system, run F-Secure Anti-Virus with the following parameters:

```
FSAV.EXE /HARD /ALL /DISINF
```

and press [ENTER].

F-Secure Anti-Virus removes the virus and gives you a short report of the results.

If you run into problems, point your browser to the F-Secure Anti-Virus Support Center at http://www.DataFellows.com/anti-virus/support.

Next, write system information to the floppy so it can be restored later. You should keep your Rescue Disk write-protected at all times and store it in a safe place. However, at this stage you must remove the write-protection temporarily so that system information can be copied to the diskette. Alternatively, you can copy the F-RESCUE.EXE file to another floppy and use that as your Rescue Disk.

Start the system information copying by executing F-Rescue. Write the following command:

```
A:\F-RESCUE
```

and press [ENTER].

When the F-Rescue program starts, it asks the user to select the appropriate function:

```
There is one hard drive in Your system.
Select option:
1) Backup system information
2) Restore system information
0) Exit
```

Select option 1 and press [ENTER].

After this, the program asks you to describe the system and the computer. Fill in all the requested information and confirm by pressing [ENTER].

```
Starting backup of Your system information
Please give information to identify this workstation
User Name............:Demo Name
Computer Name........:Demo Computer
```

After this, the F-Rescue program will automatically copy system information to the Rescue Disk. After the program has finished, all the necessary information has been copied to the diskette and you can remove it from the drive. The Rescue Disk is now ready for use.

Remember to write-protect your Rescue Disk, and keep it write-protected at all times!

Windows NT Rescue Disk

To create an NT Rescue Disk, execute the NT utility RDISK (Repair Disk Utility). It is located in SYSTEM32 directory under Windows NT’s own directory. When RDISK has started, choose option “Create Repair disk” and follow directions on screen. This diskette can be used to recreate your boot sectors.

Manual Rescue Disk Creation

If you are unable to create a Rescue Disk automatically, you can create it manually by following these instructions:

Format a clean diskette as a system diskette. Insert the diskette into drive A:, open MS-DOS prompt and type:

```
FORMAT A: /S <ENTER>
```

Using the COPY command, copy the following programs from the DOS area of your hard disk onto the Rescue Disk:

```
FDISK.EXE
SYS.COM
```

On MS-DOS and Windows 3.1 systems, these files are typically located in C:\DOS. On Windows 95 systems, they can usually be found in the C:\WINDOWS\COMMAND directory.

Constant Guard with F-Secure Anti-Virus Gatekeeper

The F-Secure Anti-Virus Gatekeeper and F-Agent modules provide consistently perpetual protection from macro viruses and other attackers, from the background, both when files and diskettes are opened and at regularly scheduled intervals.

More:

F-Secure Anti-Virus Gatekeeper

F-Agent

F-Secure Anti-Virus Gatekeeper

F-Secure Anti-Virus Gatekeeper functions transparently in the background, looking for viruses whenever you access diskettes or files. If you try to open, copy, or move an infected executable file, F-Secure Anti-Virus Gatekeeper will automatically display a warning:

To check whether F-Secure Anti-Virus Gatekeeper is active, open the F-Agent menu. If the F-Secure Anti-Virus Gatekeeper… item on this menu is checked, then the Gatekeeper is active.

Click this command, if you would like to disable F-Secure Anti-Virus Gatekeeper or modify its settings. This will open the “F-Secure Anti-Virus Gatekeeper Settings” dialog box. You can also open a dialog box for modifying the Gatekeeper settings by using the Protection Preferences of F-Secure Anti-Virus.

More:

F-Secure Anti-Virus Gatekeeper Settings

F-Secure Anti-Virus Gatekeeper Technical Information

F-Secure Anti-Virus Gatekeeper Settings

You can change the F-Secure Anti-Virus Gatekeeper settings by opening the F-Agent menu in Windows and choosing the F-Secure Anti-Virus Gatekeeper command. The program will then display the F-Secure Anti-Virus Gatekeeper Settings dialog on the screen.

With the F-Secure Anti-Virus Gatekeeper settings, you may do the following, depending on your platform:

- Enable or disable F-Secure Anti-Virus Gatekeeper.
- Set the F-Secure Anti-Virus Gatekeeper’s ability to identify viruses by name. Switching off this option saves memory and is useful in computers that are low in memory.
- Determine whether or not the user should confirm the program’s actions after a virus has been detected.
- Determine what should be done to infected files. The options are renaming files, deleting files or leaving the files as they are.

F-Secure Anti-Virus Gatekeeper Technical Information

F-Secure Anti-Virus Gatekeeper’s functioning is based on Dynamic Virus Protection Technology. This technology employs a device driver which monitors the software interrupts used in opening files and managing disk partitions.

This means that F-Secure Anti-Virus Gatekeeper is notified every time a file is opened. If the file happens to be an executable one or a document file containing macros, the program checks it automatically for viruses.

F-Secure Anti-Virus Gatekeeper monitors also disk operations. It checks the boot sectors of the diskettes used in the computer, first when a diskette is inserted in the diskette drive and subsequently each time something is read from the diskette or written to it.

F-Secure Anti-Virus Gatekeeper works both in Windows and in DOS sessions opened from Windows.

F-Agent

F-Agent runs in the background mode to launch the scheduled F-Secure Anti-Virus tasks, thus eliminating the need for F-Secure Anti-Virus to remain active all the time. In case of a network installation, F-Agent also provides communication between individual workstations and the F-Secure Anti-Virus administrator.

When F-Agent is loaded, its icon is displayed on the desktop, in the taskbar status area under Windows 95 and Windows NT 4.x. Click the icon with the left mouse button in Windows 3.1 and with right mouse button in Windows 95 and Windows NT 4.x to view the F-Agent menu.

The commands available from this menu are: Start F-Secure Anti-Virus for Windows, F-Secure Anti-Virus Gatekeeper…, and Load F-Agent at Windows Startup.

Click Start F-Secure Anti-Virus for Windows to launch F-Secure Anti-Virus. In Windows 95 and Windows NT 4.x, F-Secure Anti-Virus can also be started by double-clicking the F-Agent icon on the desktop.

If F-Secure Anti-Virus Gatekeeper is installed, the F-Secure Anti-Virus Gatekeeper… command of the F-Agent menu can be used to enable F-Secure Anti-Virus Gatekeeper and change its settings. If the Gatekeeper is already active, this command will be marked with a check mark. In this case, the command can be used for disabling Gatekeeper, if needed.

Use the Load F-Agent at Windows Startup command to have F-Agent loaded at Windows start-up. If the command is checked, meaning that F-Agent is loaded at start-up, the command can be used to disable loading, if needed. In both cases, you will be asked for confirmation. In case of a network installation, some of the above commands may be hidden by administrator.

Using the Toolbar and Task List

The F-Secure Anti-Virus interface has two display modes: toolbar and task list.

More:

Toolbar

Task List

Toolbar

In the toolbar mode, the window contains a number of buttons and menus, providing you with easy access to all the features of F-Secure Anti-Virus you need most often.

The default buttons on the toolbar give shortcuts for the following actions:

- Scan drive A:
- Scan the Hard Drive
- Scan Network Drives
- Scan a Folder
- Create a new task
- Duplicate, edit, execute, and delete scanning tasks
- Execute a pre-configured task
- Read results of a task
- Show the log file
- Modify F-Secure Anti-Virus settings
- Edit settings of F-Secure Anti-Virus Gatekeeper
- Connect to F-Secure Anti-Virus Web Club
- View virus descriptions
- Access online help
- Toggle between Toolbar and Task List modes

In addition, almost any F-Secure Anti-Virus feature can be linked to a newly created button. To see what a particular button does, place the mouse pointer over it and the name will appear in a small window.

Task List

In the task list mode, the full-sized window shows the list of scanning tasks, in addition to the buttons and menus.

To toggle between the two display modes, click on the Enlarge/Shrink button..

The task list displays the name of each task; the next time it is scheduled to be executed, or its Next Run; and its Last Status, the result of the last execution. A task can be selected from the task list by clicking on it with the mouse or by using the arrow keys.

When you open the F-Secure Anti-Virus task list after installation, it already contains several tasks. The Default Task cannot be deleted, but its settings can be modified, including the name. In addition to the Default Task, F-Secure Anti-Virus includes several ready-made tasks, which perform, for example, the following scans:

- Scan Drive A:
- Scan Hard Disks
- Scan Network Drives
- Scan a Folder

The toolbar contains shortcut buttons for starting these tasks. Clicking a button will start the corresponding task.

Working with Scanning Tasks

F-Secure Anti-Virus supports saving the scan settings to a scanning task to make it easy to run the scan again when needed. Each scanning task has a name and a set of parameters, which contain the information needed to execute that particular scanning task. The scanning parameters are stored on the hard disk as a file.

Tasks and parameters can be edited or removed. When F-Secure Anti-Virus is launched, it reads task files and shows them on the task list. When a scan of a new kind is needed, it is first created as a task, then executed according to parameters.

More:

Task Management

Task Properties and Scheduling

Executing a Task

Viewing Task Results

Task Management

F-Secure Anti-Virus contains one default task which is unremovable but whose parameters can be modified. F-Secure Anti-Virus also includes a number of ready-made tasks:

- Scan Drive A:
- Scan Hard Disks
- Scan Network Drives
- Scan a Folder

These ready-made tasks are included for your convenience. They are in no way special compared with the tasks you can create yourself.

To customize tasks and create tasks, you may edit the parameters of a pre-configured task or create an entirely new task. To edit tasks or to create new tasks, first display the tasklist by either clicking Enlarge on the toolbar, or choosing Enlarge to Tasklist from the Edit menu.

More:

Editing Task Parameters

Copying Tasks

Creating New Tasks

Deleting Tasks

Editing Task Parameters

An existing task can be modified by double-clicking on it in the task list, or by selecting it on the task list and then either pressing Alt+Enter or clicking Edit settings button on the toolbar. Another option is to select the task on the task list and then to choose Settings from the Tasks menu or from the right-click-shortcut menu.

All the above actions open the Properties for Task dialog box, where the task properties can be edited.

If the option Save Tasks Automatically in the General page of the Preferences for Task dialog box is not active, save the edited task by choosing Save All from the File menu. Please see Task Properties and Scheduling for more information.

Copying Tasks

To make a new task by copying and modifying an old one, select the task to be copied on the task list. Then click the Make a Copy button on the toolbar. Alternatively, choose Duplicate from the Tasks menu or from the right-click-shortcut menu. F-Secure Anti-Virus will create a task, called “Copy of ‘Source Task’”, place it on the task list, and open the Properties for Task dialog box. In this dialog box you can set up properties of the new task.

Creating New Tasks

To create an entirely new task, click Create a new task on the toolbar. Alternatively, choose New Task from either the Tasks menu or the right-click-shortcut menu. F-Secure Anti-Virus will create the task called “Untitled Task,” place it on the task list, and open the Properties for Task dialog box.

When a task has been created, it must be saved before you exit F-Secure Anti-Virus. Save the new task by choosing Save All from the File menu. New and modified tasks can also be saved automatically on exit, if so defined in the General Preferences.

Deleting Tasks

Any task can be deleted from the task list, except for the Default Task and, in case of a network installation, the tasks distributed by administrator. To delete a task, first select it on the task list using the mouse or the arrow keys. Then, delete the selected task by either pressing the delete key, or clicking the Delete button on the toolbar. Alternatively, choose Delete from the Tasks menu or from the right-clicking short-cut menu.

When a task is deleted, any corresponding to it report is also removed. Before removing the task from the task list and deleting the corresponding task file, F-Secure Anti-Virus will request a confirmation.

Task Properties and Scheduling

Task parameters, or properties, are defined in the Properties for Task dialog box. This dialog box is automatically displayed whenever a new task is created. To modify parameters of an existing task, select the task on the task list and click the Edit Settings button on the toolbar. Alternatively, choose Settings from either the Tasks menu or the right-clicking shortcut menu. Selecting the task and pressing Alt+Enter, or double-clicking on the task name will also open the Properties for Task dialog box.

The Properties for Task dialog box contains three pages: General, Advanced, and Scheduling.

More:

General Properties

Advanced Properties

Schedule Properties

General Properties

The General page of the Properties for Task dialog box specifies the task name, and the file, folder or disk to be scanned.

The Task Name is given in the upper box of the General page. If needed, delete the current entry and type in the task name of your choice.

In the Scan Target box, enter the name and the path of the file, folder, or disk to be scanned. It is more convenient to enter this information for disks and folders by selecting them from the list. Double-click on the disks drives and folders to view their contents.

Advanced Properties

Use the Advanced page of the Properties for Task dialog box to set the following task properties: the scan method; viruses which F-Secure Anti-Virus should look for; files, folders, or disks to be searched; and the action to be taken on the infected files.

The first item to be defined is the Scan method. The options available are: F-PROT, AVP, and F-PROT+AVP. Both scanners are very reliable in searching for known viruses and their new variants.

Under Look for, you can specify the viruses which F-Secure Anti-Virus will be looking for. Both the Viruses and Trojan Horses check box and the Document macro viruses check box are selected by default. If needed, click a check box to clear it.

Viruses are basic pieces of malicious, self-replicating software. Unlike them, Trojan Horses, which are often confused with viruses, cannot replicate themselves. They are simple traps and time-bombs hidden inside other programs.

Under Look In, specify the type of files which should be scanned. The default option is Executables and document files. Selecting Executables and document files limits the search for viruses only to document files and the files containing executable code. F-Secure Anti-Virus uses file extensions specified in the Scanning Preferences to determine whether a file is an executable or a document file. The commonly used extensions for executable files are: .com, .exe, .sys, and .ov?. For document files, the commonly used extensions are: .do? and .xl?.

Use the “Scanning Preference” dialog box to re-define executable and document files, if needed.

All files means exactly what it says. If this option is selected, F-Secure Anti-Virus will search all the files, regardless of their extension: executables, documents, and others. This setting should not be used under normal conditions, because it slows down the scans considerably and may generate false reports. Viruses cannot run from files that have no executable content. All infections in such files are due to programming errors by virus authors. However, if a virus has been discovered and subsequently removed from the system, this option may be used for cleaning up the stray infections out of non-executable files.

Use the Archives option to scan inside several archive file formats such as files compressed with the ZIP and LZH algorithms. In order to scan inside compressed files you must check the “Look in Archives” checkbox in the “Advanced” page of the task properties dialog. If “Look in Executables and document files” is selected (on the same page) then files with ZIP and LZH extensions will be scanned along with those whose extensions are listed in the Scanning Preferences page (this also means that self-extracting archives will be scanned). If “Look in All files” is selected then files with all extensions will be scanned.

We constantly increase support for compressed file formats, with recursive scanning and other archive formats to be added in upcoming versions. Please see this web page for the latest information:

- http://www.DataFellows.com/anti-virus/support/compressed-file-formats.htm

If the Boot Sectors box is selected, F-Secure Anti-Virus will check the boot sectors of hard disks and diskettes for boot sector viruses. This check box is selected by default.

Under Action:, specify the action to be taken by F-Secure Anti-Virus on infected files when it finds a virus.

The following four choices are available:

- Report Only. If this option is selected, F-Secure Anti-Virus reports the detected viruses, but does nothing to the infected files. You will be able to choose the required action after reading the task results report.

- Disinfect. F-Secure Anti-Virus will attempt removing viruses from the infected files or boot sectors. F-Secure Anti-Virus is able to disinfect most known viruses. If a file cannot be disinfected, the program would ask the user whether to delete the file.
- Delete. The infected files will be first overwritten, and then deleted from the system.
- Rename. Infected executable files will be given a different file extension to eliminate the risk of further spreading of the virus in case of unintentional execution of the infected file. The file name extensions are changed from .com to .vom, and from .exe to .vxe.

If the Confirm operations check box below is selected, F-Secure Anti-Virus will ask for confirmation before doing anything to infected files. If the task was started interactively, F-Secure Anti-Virus will ask for confirmation every time a virus is found. In case of a scheduled task, all the confirmations will be requested in one batch. The Confirm operations check box is selected by default. If you click the check box to clear it, F-Secure Anti-Virus will proceed with disinfection, deletion and renaming files without asking for confirmation.

F-Secure Anti-Virus can also be instructed to beep or display a message every time it finds a virus. This is not given as a task parameter, but can be selected from the Scanning Preference dialog box.

Schedule Properties

Tasks can be scheduled for execution at specific times. In order to have the scheduled tasks executed without running F-Secure Anti-Virus, F-Agent should be active at all times.

Begin with selecting the Scheduling Enabled check box in the upper area of the page. This will enable the scheduling options.

To schedule a task to run automatically, use the Scheduling tab of the Properties for Task dialog box.

Under Scan frequency, there are three general options for how often the task will be executed:

- Daily: Execute the scan every day.
- Weekly: Select the check boxes corresponding to the days of the week when you wish the task to run.
- Monthly: Enter the day of the month on which you wish the task to be executed.

Under Time to scan, there are two alternatives for setting the time of the day when the task should be performed.

Enter the desired time by clicking the At option button and typing in the numbers for hours and minutes. If two or more tasks are scheduled to run at the same time, the task that appears first on the task list takes precedence.

Alternatively, click the Start after _ idle minutes option button and type in the number of idle minutes after which F-Secure Anti-Virus should perform the task. Tasks that use this option are run once per day, according to the order in which they appear on the task list. If the machine is not idle during the day, the task will be rescheduled for the following day.

The Scheduling page can also be accessed directly from the task list by selecting the task and choosing Schedule from the Tasks menu or from the right-click-shortcut menu. Double-clicking on the task’s Next Run field will also display the Scheduling page.

Executing a Task

A task can be executed either by scheduling it or by running it interactively.

To run a task interactively, select the task on the task list and press Enter, or click Execute the currently selected task on the toolbar. You can also choose Start from the Tasks menu or from the right-click-shortcut menu. If the toolbar contains a shortcut button for the task you wish to execute, just click the shortcut button without selecting the task on the task list.

If the task is the first one in the current session of F-Secure Anti-Virus, then the program first scans the computer’s memory. After that, the “Scanning Disk for Viruses” dialog box appears. The task name is displayed in the upper part of the dialog box, along with the scan status, the name of the scanned file, and the progress indicator.

The lower part of the window displays a preliminary report, which lists the scan method; the name of the file, folder, or disk being scanned; the action to be taken on infected files; the types of the target viruses; and the types of scanned files.

A task may be aborted at any time by clicking Stop in the dialog box. The program will ask for confirmation before terminating scan.

Viewing Task Results

Viewing Task Execution Reports

After executing a scanning task, F-Secure Anti-Virus produces a report on the task results. If a virus is found on a diskette, the Virus Alert: Check the Results! message box is displayed on the screen and you can view the results report immediately by clicking Report in the Scan Finished dialog box. This dialog box and the Virus Alert message box, if relevant, are displayed on the screen even if F-Secure Anti-Virus is executing scans in its minimized mode.

To view a results report, switch from the toolbar to the task list mode. To do this either select Enlarge to Tasklist from the Edit menu or click Enlarge on the toolbar.

Select the task on the task list and either click Show the results file of the currently selected task on the toolbar, or choose Results from the Tasks menu or the right-click-shortcut menu. The task results are presented in a separate window.

Depending on your preferences, the new report may either overwrite the report about the previous execution of the task, or can be appended to the existing list of reports.

Each task result report shows the execution time and results of a specific executed task at the latest scan or the preferred number of scans, and includes the name of the user, the name or ID of the workstation, and the version of F-Secure Anti-Virus.

Below these, the report states the scan execution time, the scan results, and the following scan parameters: the scan method; the name of the scanned file, folder, or disk; the action taken on the infected files; the types of the target viruses; and the types of scanned files.

Further in the report, more detailed results are given. There is a separate entry for each virus infection. If you double-click on a virus name, the Virus Information dialog box, which contains virus descriptions, will be displayed. Virus descriptions are also available at the F-Secure Anti-Virus World Wide Web server. Choose Virus Descriptions on the Web from the Help menu to access the server. For background information, see Background Information on Viruses.

General information about the infected file can be obtained by double-clicking on its name in the report, which opens the File Information dialog box. In this dialog box, the file’s size, attributes and creation time are shown.

If the computer is connected to a network, the report can be sent to administrator by clicking Admin in the Task Results dialog box. The report can also be printed out by clicking Print.

Viewing the Scan Log

Information about the executed tasks and F-Secure Anti-Virus Gatekeeper scans that found a virus is stored in the log file by default. You can have the log include only one type of entries, or change the length of the log, by using the Reporting Preferences.

To view the log, click Show the log file on the toolbar or choose Log from the Tasks menu. The log contains one line per each executed task or scan, beginning with the task name. Each log entry for a task execution consists of the task name, execution time and the result status. Each log entry for a virus-finding F-Secure Anti-Virus Gatekeeper scan includes the time of the scan, and the name of the infected file.

Virus alerts are shown in red.

The maximum length of the log, 500 lines by default, can be set in the Reporting Preferences dialog box.

Printing Task Results

If the computer is connected to a printer, you can print out the log and the task results.

To print results of an executed task directly from the task list, select the task and then choose Print Results option from the File menu. You can also print the results report can from the Task Results dialog box by clicking Print.

To print the log, choose Print Log from the File menu.

Choose Printer Setup from the File menu to open the standard printing dialog box. In the dialog box, select the printer, paper size, and other printer settings.

Choose Page Setup from the File menu to define page parameters, including print margins.

Setting F-Secure Anti-Virus Preferences

Preferences control the way in which F-Secure Anti-Virus functions. There are several different preferences, each responsible for some portion of the program’s functionality.

If F-Secure Anti-Virus is installed with network functionality, the F-Secure Anti-Virus administrator pre-defines the preferences and may decide to hide some of them from the users. In this case, some preferences may be unavailable.

To access the Preferences dialog box, choose Preferences from the Edit menu or click the Open the Preferences dialog button on the toolbar. Once the Preferences dialog box is displayed, click on the tab corresponding to the Preferences you would like to modify. The following Preferences are available in the Preferences dialog box:

Preference	**Function**
General	Controls the program settings and sets the language.
Scanning	Determines which files the program will accept as scan objects, and how it will inform you if a virus is found.
Protection	Controls whether F-Secure Anti-Virus Gatekeeper is enabled and what actions it takes if a virus is found.
Reporting	Controls task result reports and the log file.
Workstation	Used for setting the user name and the workstation ID.

To access a particular Preference, click its corresponding tab in the Preferences dialog box. The instructions on using various Preferences follow.

More:

General Preferences

Scanning Preferences

Protection Preferences

Reporting Preferences

Workstation Preferences

General Preferences

Use the General Preference dialog box to define the ways in which F-Secure Anti-Virus operates.

The Save Tasks Automatically check box, if selected, enables automatic saving of any new or modified task at the closing of F-Secure Anti-Virus. This check box is selected by default.

The Save Window Settings on Exit check box, if selected, causes F-Secure Anti-Virus to save the location and settings of its main window when it is closed. The next time the program is started, it starts in the same mode as in the end of its previous session. By default, this check box is selected.

The Run Scheduled Tasks Minimized check box, if selected, makes all the scheduled F-Secure Anti-Virus tasks, executed through F-Agent, run with the minimized display. By default, this check box is selected.

In the General Preference, you may also choose your preferred language from the Language: list of available choices.

Scanning Preferences

Use the Scanning Preferences to re-define executable and document files for F-Secure Anti-Virus usage, and to specify the way, in which F-Secure Anti-Virus informs you about the detected viruses.

In the Executable Files box select the extensions of the files, which F-Secure Anti-Virus will consider to be executable. The default set of the executable files extensions is the following: .com, .exe, .sys, .ov?, .app, .pgm, .bin. If you need to re-define executable files, type in the new extensions and delete those you do not need.

Similarly, in the Document Files box select the extensions of the files, which F-Secure Anti-Virus will consider to be document files. The default set of the document files extensions is the following: .do?, .xl?. If you need to re-define document files, type in the new extensions and delete those you do not need.

Under When a Virus Is Found, select the type of notification in the event a virus is found. Instruct the computer to beep by selecting the Beep check box. If you wish to have a message displayed, select the Display the Following Message check box and type in the message to be displayed when a virus is found.

To test the functionality of Scanning Preferences, see Testing Your Anti-Virus Protection.

Protection Preferences

In the Protection Preference, you can enable and configure F-Secure Anti-Virus Gatekeeper. F-Secure Anti-Virus Gatekeeper is the program for providing dynamic protection against viruses. It functions transparently in the background, looking for viruses whenever you access diskettes or files.

F-Secure Anti-Virus Gatekeeper detects the same viruses as does the fully executed scan, works for both Windows and DOS sessions under Windows, and in case of a network installation communicates directly with F-Secure Anti-Virus administrator.

Select the Enable F-Secure Anti-Virus Gatekeeper check box under Dynamic Virus Protection to activate F-Secure Anti-Virus Gatekeeper. If this check box is selected, the other options of the dialog box become available.

Under Preventive Action, select between Confirm before Denying Access to Infected File and the default Always Deny Access to Infected File.

Under Action on Infected File, select the action to be taken by F-Secure Anti-Virus Gatekeeper on the infected files. Click either of the following: None to take no action except notifying; Rename, to rename the infected file; Delete to delete the infected file; and Disinfect to disinfect the infected file.

In F-Secure Anti-Virus for Windows 3.1, the “Protection Preferences” dialog box is a little different. Below are the instructions on using the Protection Preferences in F-Secure Anti-Virus for Windows 3.1.

In order to go to the Preventive Action selection, click More in the “Protection Preferences” dialog box.

Under Preventive Action, there are four options for F-Secure Anti-Virus Gatekeeper actions when it finds the virus. Two options are available when the virus is found under Windows, and two options are available when the virus is found under DOS session.

Under When Virus is Found under Windows, choose either Confirm Before Denying Access to Infected File, or the default Always Deny Access to Infected File.

Under When Virus is Found under DOS Session, choose either Confirm before Terminating the DOS Session, or the default Always Terminate the DOS Session.

The Action on Infected File selection in F-Secure Anti-Virus for Windows 3.1 offers the available choices for the actions taken by F-Secure Anti-Virus Gatekeeper on the infected files. Click either of the following: None, to take no actions except for notifying; Rename, to rename the infected file; and Delete to delete the infected file.

The Protection Preference dialog box in F-Secure Anti-Virus for Windows 3.1 includes the following Scanning Options for F-Secure Anti-Virus Gatekeeper: Search for Document Macro Viruses and Scan Created and Renamed Files.

The Activity Display is a small window that displays the status of progress in real time. Choose from the following available options: Show Names of Scanned Files, Show Icons only, and None.

Reporting Preferences

In the Reporting Preferences you can configure the log, and determine whether the task results reports will be stored in the program, or overwritten by the next scan.

Under New Results, select the way in which F-Secure Anti-Virus will store the task results reports. Select either Append After Previous Results, if you wish to keep the previous results reports saved, or Overwrite Previous Results, if you do not need to keep the previous results reports. In the latter case, only the latest report will be available for viewing.

Under Log File, select the appropriate check boxes for configuring the F-Secure Anti-Virus log. Click the Task Results check box to have the task results included in the log. Click the Active Protection Messages check box to have F-Secure Anti-Virus Gatekeeper messages included in the log.

To set the maximum length of the log file, click the Truncate Old Entries checkbox and type in the number. The default maximum is 500 lines.

Workstation Preferences

The Workstation Preference is used to set the workstation name and the user name. In case of a network installation of F-Secure Anti-Virus, the names are needed to communicate with the F-Secure Anti-Virus administrator.

Modifying the Toolbar

The F-Secure Anti-Virus toolbar contains ready-made shortcut buttons which provide convenient shortcuts to perform the following actions:

- Scan drive A:
- Scan the Hard Drive
- Scan Network Drives
- Scan a Folder
- Create a new task
- Duplicate, edit, execute, and delete scanning tasks
- Execute a pre-configured task
- Read results of a task
- Show the log file
- Modify F-Secure Anti-Virus settings
- Edit settings of F-Secure Anti-Virus Gatekeeper
- Connect to F-Secure Anti-Virus Web Club
- View virus descriptions
- Access online help
- Toggle between Toolbar and Task List modes

These buttons can be edited or moved around within the toolbar.

Additionally, you can create custom shortcut buttons to suit your particular needs. Almost any function can be linked to a specially created button.

More:

Creating Buttons

Editing Buttons

Deleting Buttons

Moving Buttons Around

Creating Buttons

To create a new button, click on the toolbar with the right mouse button. A menu will be displayed. Choose Add a new button from the menu. The Create a New Toolbar Button dialog box will be displayed, where the new button can be defined.

The same dialog can be accessed by double-clicking an empty spot on the toolbar while holding down the Control key.

On the Picture list, choose the picture for the new button.

On the Action list, choose the action to be linked to the button. Available actions are the following:

Action	Function
About F-Secure Anti-Virus	Shows the F-Secure Anti-Virus splash screen.
Administration Mode	Begins/ends administration mode.
Administrator Help on Web	Connects to Administrator FAQ page on F-Secure Anti-Virus Web server.
Delete Task	Deletes the currently selected task.
Distribute Task	Distributes the selected task. Enabled only when F-Secure Anti-Virus is in administration mode.
Duplicate Task	Makes a copy of the currently selected task.
Edit Preferences	Opens the Preferences dialog box.
Edit Task Settings	Opens Properties for the currently selected task.
Enlarge/Shrink	Displays/hides task list.
Execute Task	Executes a task.
Exit	Exits F-Secure Anti-Virus.
F-Secure Anti-Virus Contact Information	Shows contact information for your F-Secure Anti-Virus vendor.
F-Secure Anti-Virus Gatekeeper Settings	Allows to edit settings of F-Secure Anti-Virus Gatekeeper.
Help Contents	Displays help items.
Help on Context	Searches for help items on context.
How to Use Help	Displays advice on how to use help.
Manage Bulletins	Opens the Manage Bulletins dialog box. Enabled only when F-Secure Anti-Virus is in administration mode.
New Task	Creates a new task.
Page Setup	Opens a normal page setup dialog.
Print Log	Prints the log without preview.
Print Results	Prints the results of a selected task without preview.
Printer Setup	Opens a normal printer setup dialog.
Read Bulletins	Displays the Read Bulletins list.
Save All	Saves the program settings.
Schedule Task	Opens the Schedule dialog box for the selected task.
Search for Help On	Searches for help on a chosen topic.

Send Message	Opens the Send Messages dialog box.
Send Update	Opens the Update dialog. Enabled only when F-Secure Anti-Virus is in administration mode.
Start Task	Executes the currently selected task.
Undistribute Task	Removes the selected task from local workstations. Enabled only when F-Secure Anti-Virus is in administration mode.
View Infected Files	Opens a dialog where infected files may be viewed. Enabled only when F-Secure Anti-Virus is in administration mode.
View Log	Opens the Log file.
View Task Results	Displays results of a task.
View Task Results	Displays results of the currently selected task.
View User Messages	Opens the Read Messages dialog box. Enabled only when F-Secure Anti-Virus is in administration mode.
View User Reports	Opens the User Reports dialog. Enabled only when F-Secure Anti-Virus is in the administration mode.
Virus Information	Displays the Virus Information dialog box.
Virus Information on Web	Connects to F-Secure Anti-Virus Web server to view virus descriptions.
Web Club	Connects to F-Secure Anti-Virus Web Club.

If you choose either of Execute Task, Schedule Task or View Task Results actions, click the task of your choice on the Task list, located below the Action list..

After you have selected the action and the picture to be linked to the button, click OK, and the new button appears on the toolbar.

There is a shortcut way to create a new task button. Grab the task from the task list by pressing Control and clicking on the task with the mouse, then drag and drop it on the toolbar, while keeping Control pressed down. The new button, named according to the selected task, will appear on the toolbar.

Editing Buttons

To modify an existing button, double-click the button, while holding Control down. This will display the Edit Toolbar Button dialog box, where the button’s properties can be freely edited. The same dialog can be accessed by first right-clicking the button and then selecting the Edit button from the displayed menu.

Select the desired action and picture for the button.

After making the desired modifications, confirm the changes by clicking Change. Clicking Delete will delete the button. F-Secure Anti-Virus will ask for confirmation before deleting the button.

Deleting Buttons

To delete a button, click on it with the right mouse button and choose Remove button from the displayed menu. Alternatively, double-click the button while holding Control down to go to the Edit Toolbar Button dialog box and click Delete at the bottom of the dialog box. F-Secure Anti-Virus will ask for confirmation before deleting the button.

Buttons can also be deleted by dragging them off the toolbar, while holding Control down. In this case F-Secure Anti-Virus will request confirmation as well.

Moving Buttons Around

To move buttons within the toolbar, press Control and grab the button with the mouse by clicking on it and keeping the button of the mouse pressed down. The button can be dragged around the toolbar and dropped in a suitable place by simply releasing the mouse button.

Network Features

While F-Secure Anti-Virus can be used on a stand-alone computer without any network connections, it is designed to support communication between a user and the system administrator via the network. Some examples of network features are given below.

More:

Updates

Tasks

Messaging

Cross-Platform Compatibility

Updates

The administrator can automatically update F-Secure Anti-Virus on the users' computers via the network. Depending on the Updating Preferences, a user need not be aware that an the update is taking place.

Tasks

The administrator can design scanning tasks and distribute them to local workstations through the network. F-Secure Anti-Virus programs on individual workstations pick the tasks up automatically and add them to their own task lists. If the tasks have been designed to run on a schedule, the local programs will execute automatically.

Messaging

F-Secure Anti-Virus supports communication between users and the system administrator in the form of messages and bulletins.. A user may send messages to administrator, and the administrator may send general bulletins to all the users.

In addition, F-Secure Anti-Virus can be set up to automatically send the task result report to administrator each time when it finds a virus on a network workstation. F-Secure Anti-Virus Gatekeeper can be set up to send a message to administrator each time it detects a virus.

The administrator can send bulletins to all users simultaneously. When you launch F-Secure Anti-Virus, it will notify you of any new bulletins.

You can access the list of the bulletins either directly from this dialog by clicking Yes, or later by choosing Read Bulletins from the Edit menu.

Select a bulletin from the list, and click Read to view it.

To send a message to your F-Secure Anti-Virus administrator, choose Send Message from the Edit menu. Enter the subject and the text of the message in the displayed dialog box and click Send.

Cross-Platform Compatibility

F-Secure Anti-Virus is available for a number of platforms, including:

- Windows 3.1
- Windows 95
- Windows NT
- OS/2

All Windows versions are compatible with each other and the OS/2 version. All these different versions may also co-exist on the same network and share tasks, messages etc. This means that the system administrator may use F-Secure Anti-Virus for Windows NT, for example, and still get reports from users that run Windows 3.1, Windows 95 or OS/2. He can also send out tasks that are executed on each workstation regardless of what operating system it is running.

Menus

F-Secure Anti-Virus in a Stand-Alone Computer installation configuration has the following five menus: File, Edit, Tasks, View, and Help. The View menu is not available for some operating systems. In addition to these menus, there is also the shortcut menu, which can be displayed by clicking the right mouse button on the task list. The shortcut menu contains commands from the Tasks and the Help menus.

Some of the menu commands, described below, are only present on network workstations, and are not present in case of the Stand-Alone Computer installation of F-Secure Anti-Virus. In case of Network workstation installation, there is also one hidden menu, Administration, which is only visible in Administration mode. Administration mode on network workstations can be turned on with a password from the File menu by choosing Administration.

File Menu Command	**Function**
Save All (Control+S)	Saves all unsaved tasks, Preferences, and window settings.
Print Results… (Control+P)	Prints the results of the selected task.
Print Log…	Prints the log.
Page Setup…	Sets margins.
Printer Setup…	Standard printer setup.
Administration…	Switches to the Administration mode, first asking for the administration password. When in Administration mode, use this command to switch to User mode.
Exit (Control+Q)	Exits F-Secure Anti-Virus.

Edit Menu Command	**Function**
Send Message…	Opens a dialog for sending messages to administrator. If this command is dimmed, network communication is installed, but not active, as when you are not logged in.
Read Bulletins…	Opens the list of bulletins.
Enlarge to Tasklist	Enlarges the interface to the full-size window when F-Secure Anti-Virus is in the toolbar mode.
Shrink to Toolbar	Shrinks the window into a toolbar, if it is in full size mode.
Preferences…	Opens the Preferences dialog box for configuring the settings of F-Secure Anti-Virus.

Tasks Menu Command	**Function**
New Task (insert)	Creates a new task named “Untitled Task.”
Duplicate	Makes a copy of the selected task. The new task is named “Copy of” + the old task’s name, cutting it at the maximum allowable name length. The new task is automatically selected.
Delete (del)	Asks for confirmation, then deletes the selected task.
Start (enter)	Executes the selected task.

Settings (alt+enter)	Opens the Properties for Task dialog box, where the selected task parameters can be modified.
Schedule (Control+enter)	Opens the Schedule dialog box, where the selected task can be scheduled.
Results (Control+R)	Opens the results file of the selected task, to view, copy, or print it. This command acts as a print preview for results.
Log(Control+L)	Opens the log file with the list of task execution times and results, to view or print it. This command acts as a print preview for the log file.

All the above commands, except for Log and Results, are disabled when F-Secure Anti-Virus is in its toolbar mode.

View Menu Command	**Function**
Large Icons	Displays each task as a large icon.
Small Icons	Displays each task as a small icon.
List	Displays the tasks in the form of the list.
Details	Default. Displays the tasks in the form of a list with the Next Run and the Last Status fields.

Please note that the various view options are not available under Windows 3.1.

Help Menu Command	**Function**
Contents	On-line help index.
Help on Context (F1)	Context-sensitive help.
Search for Help On.	Searches for help on given topics.
How to Use Help	Instructions on how to use Help.
Virus Descriptions	Displays descriptions of a variety of viruses.
Web Club…	Connects to F-Secure Anti-Virus Web club.
Virus Descriptions on the Web…	Connects to F-Secure Anti-Virus WWW server to view virus descriptions.
Contact Information…	Provides contact information for your F-Secure Anti-Virus vendor.
About…	Information about F-Secure Anti-Virus for Windows.

F-Secure Anti-Virus Help acts in accordance with the Windows Help structure. To learn more about Windows Help, choose How to Use Help.

Shortcut Menu Command	**Function**
New Task	Creates a new task named “Untitled Task.”
Duplicate	Makes a copy of the selected task. The new task is named “Copy of” + the old task’s name, cutting it at the maximum allowable name length. The new task is automatically selected.
Delete	Asks for confirmation, then deletes the selected task.

Start	Executes the selected task.
Settings	Opens the Properties for Task dialog box, where the selected task parameters can be modified.
Schedule	Opens the Schedule dialog box, where the selected task can be scheduled.
Virus Descriptions	Displays descriptions of a variety of viruses.

The shortcut menu can be accessed by clicking the right mouse button on the F-Secure Anti-Virus task list. This commands in this menu correspond to items in some of the normal menus.

Overview of F-Secure Anti-Virus Administration

There is more to being the F-Secure Anti-Virus administrator than just maintenance. You can determine how the program actually functions and how F-Secure Anti-Virus appears when installed on the user workstations.

F-Secure Anti-Virus provides protection and features for everyone:

- Average end users
- Sophisticated end users
- System administrators

The normal end user should not be bothered with anti-virus issues. The transparent protection of F-Secure Anti-Virus Gatekeeper ensures that the end-user does not need to know that an anti-virus program is protecting the system unless a virus tries to enter the system.

The sophisticated end user and the system administrator are more interested in computer viruses and want to know how their information is protected.

F-Secure Anti-Virus aims to provide invisible protection for end user data and program files. To this end F-Secure Anti-Virus features:

- Automatic background scanning of every executed file with the most sophisticated scanner available.
- Scanning tasks designed by the system administrator and executed automatically at pre-scheduled times or when the computer is idle.
- An easy-to-use toolbar interface for scanning hard drives and diskettes at the click of a mouse. The toolbar is completely drag-and-drop customizable. Both the administrator and the end users can customize the user interface.

F-Secure Anti-Virus provides a wealth of features to make your work easier.

More:

Implementation Steps

Implementation Steps

The steps involved in setting up F-Secure Anti-Virus for your organization are:

1. Install the program on the Administration workstation. If the computer is connected to the network, the installation will also create the shared communication directory structures on the server disk.
2. Create the task base. Add, modify, schedule, and remove tasks on F-Secure Anti-Virus task list to create the task base suitable for your organization. For more information, see Working with Scanning Tasks.
3. Modify the toolbar. Add, modify, and remove the buttons on the toolbar. The toolbar should correspond to the task base and to the specific needs arising from your system.
4. Modify the F-Secure Anti-Virus Preferences, so that they are suitable for the users. Hide at least the Network, Administration, Scanning and Restrictions Preferences in the Preferences dialog box.
5. Create the installation directory. If you choose to perform the complete installation on workstations, use the Distribute F-Secure Anti-Virus Installations command in the F-Secure Anti-Virus Administration menu to create the suitable installation directory.

In order to customize F-Secure Anti-Virus separately for various user groups, repeat steps 2 through 5 for each customization.

Network Installation

Overview

There are three basic ways in which the F-Secure Anti-Virus system can be set up on the workstations:

- Complete installation with network functionality
- Remote installation with network functionality
- Stand-alone installation without network functionality

Complete installation means that F-Secure Anti-Virus is installed locally to all workstations. Remote installation means that only one installed copy of F-Secure Anti-Virus exists on the network drive, and all the workstations run the same copy.

More:

Network Installation

Stand-Alone Installation

Network Installation

There are two options for installing F-Secure Anti-Virus and the Gatekeeper on network workstations. The preferable method is to install both programs on every workstation. The server will act as the communications relay. Under such configuration, all the network functions and communications capabilities are available. Only the directories needed for communication over the network are created on the server. F-Secure Anti-Virus tasks and updates are distributed automatically to every workstation connected to the network.

In some situations, for example, when workstations have insufficient hard disk space, it may be necessary to install F-Secure Anti-Virus and the Gatekeeper to run on the server. In this case, the users run the copy of the program stored in the server on their own workstations. Only the files and directories necessary for communicating through the network are installed on individual workstations. Communication to and from individual workstations works as well as in the previous option, but the programs cannot be used if the network connection breaks down.

Stand-Alone Installation

If there is no network available, F-Secure Anti-Virus and the Gatekeeper are installed separately on each workstation. In this case, the communications system cannot be used, and each user is individually responsible for reporting possible infections to administrator. New versions of the programs must be distributed on diskettes.

Entering the Administration Mode

Any workstation where F-Secure Anti-Virus is installed can be used as the administration workstation simply by running F-Secure Anti-Virus on it in administration mode. Please note that it is recommended to avoid running F-Secure Anti-Virus in administration mode on more than one workstation at a time.

When the Administration Workstation check box is selected in Preferences, F-Secure Anti-Virus asks for the administration password at start-up.

If the user does not enter the correct password, F-Secure Anti-Virus will still start, but only in user mode. The administration password can be changed in the Administration Preferences dialog box by clicking Change. See Administration Preferences for more information.

The program can be switched from user mode to administration mode on any workstation by choosing the Administration command from the File menu and entering the administration password in the dialog box.

Systems Management

F-Secure Anti-Virus has a wealth of network-related features:

- Easily send software updates over the network with one menu command.
- Receive reports from workstations every time a virus is found.
- Receive copies of infected files.
- Receive copies of suspicious files.
- Send new tasks to workstations and thus scan workstations over the network.
- Send F-Secure Anti-Virus update bulletins or other virus related messages to users.

F-Secure Anti-Virus is not dependent on some specific brands of network software. Its communications system works as long as all the workstations on the network can treat a part of the server's hard disk as a shared logical disk. Practically, all PC network systems support this, including Novell NetWare, Windows NT Server, Windows for Workgroups, Banyan Vines, IBM AS/400 PC Support, Microsoft LAN Manager, Artisoft LANtastic, Digital Pathworks, Sun PC-NFS and FTP Software PC/TCP.

F-Secure Anti-Virus installations and updates can also be done through Microsoft Systems Management Server (SMS). See "Microsoft Systems Management Server" in the F-Secure Anti-Virus manual for more information. The latest information about SMS support is available at:

- http://www.DataFellows.com/anti-virus/sms/

F-Secure Anti-Virus also supports the industry standard Simple Network Management Protocol (SNMP). The latest information about supported network management platforms is available at:

- http://www.DataFellows.com/anti-virus/snmp/

More:

Network-Aware Functions

Communication Directory

Network-Aware Functions

Update Distribution

F-Secure Anti-Virus supports automatic updating over the network. Whenever you install a new version to the installation directory, the program can be automatically updated on all the workstations connected to the network.

Task Distribution

With F-Secure Anti-Virus you can send pre-configured tasks to user workstations through the network. Use this feature to develop uniform scanning practices for the whole organization and to target specific threats, such as new viruses. When the distributed tasks are no longer needed, they can be removed from all the workstations simultaneously.

Reporting

The results of tasks' execution can be set to be sent from user workstations to the Administration workstation, along with any infected files found by F-Secure Anti-Virus.

User Messages and Administrator Bulletins

F-Secure Anti-Virus is designed to support communication between users and administrator. Such communication facilitates efficient administration and management of the F-Secure Anti-Virus system. Communication between individual users is not supported. Direct information exchange between users and administrator takes place in the form of messages and bulletins. Messages are notes that users send to administrator. Bulletins are general announcements that you can send to all users at once.

Communication Directory

When F-Secure Anti-Virus is installed, the communication structures are created in a directory on a shared disk. When you send, for example, an update to users, it is copied to the shared drive. F-Secure Anti-Virus programs on user workstation then copy the new files from the communication directory to the appropriate directories on local hard disks.

Likewise, when F-Secure Anti-Virus on a user workstation sends files to the shared directory, your program will copy them to the appropriate local F-Secure Anti-Virus directories.

More:

Access Rights

Access Rights

As administrator, you need both read and write access rights to the communication directory and all its subdirectories. User access to these directories can be limited in order to prevent accidental corruption of the communications system. Suggested access rights are listed in the following table.

Directory	Suggested Access Rights
Communication Directory	Read and Write access rights
BULLETIN	Read access rights
INFECT	Write access rights
MESSAGES	Write access rights
REPORTS	Write access rights
SUSPECT	Write access rights
TASK	Read access rights
UPDATE	Read access rights
UPDATE\WIN95_UP	Read access rights
UPDATE\WINNT_UP	Read access rights
UPDATE\OS2_UP	Read access rights

Access rights policies are necessarily different in different networks. Here, “write access” means that any user can create new files and delete files created by any user.

For the communications system to function, users must have both read and write access rights to the communication directory. This directory contains the file COMM.INF, which keeps track of all the files transferred over the network.

If you do not wish to use a supervisor account when installing, create the directory beforehand at a proper location, set the access rights, log in with a non-supervisor account, and specify the same directory when installing.

Refer to the F-Secure Anti-Virus manual for specific instructions on changing the communication directory’s privileges under Novell NetWare, Microsoft Windows NT Server, Microsoft Windows for Workgroups, Microsoft LAN Manager, UNIX, Artisoft LANtastic, and Banyan VINES.

Customizing the User Interface

After completing the installation on the Administration workstation, you may choose to customize the user interface of F-Secure Anti-Virus to fit the needs of the end-users.

More:

Creating A Task Base

Modifying The Toolbar

Editing Preferences

Creating A Task Base

Create the F-Secure Anti-Virus task base by modifying the task list of F-Secure Anti-Virus installed on the Administration workstation. The tasks can be added, modified, scheduled, and removed as described in Using F-Secure Anti-Virus.

Consider the needs of your organization and check the Using F-Secure Anti-Virus topic for the appropriate options. Decide which types of tasks are required and whether they should be scheduled or run interactively.

Users can edit or delete tasks, unless you protect the task base from modifications by setting appropriate restrictions in Preferences. You can also disable modifications to tasks when using the Distribute Selected Task command from the Administration menu. See Distributing Tasks for more information.

Modifying The Toolbar

The toolbar buttons should correspond to the task base you created, as well as to the specific needs of your organization. Ideally, the users only need the toolbar to manage their own copies of F-Secure Anti-Virus. While this is not always possible, the most often needed functions should be linked to the toolbar. See Modifying the Toolbar for more information.

Editing Preferences

Before distributing the program to users, customize the F-Secure Anti-Virus Preferences. Instructions on how various Preferences affect the program and how they can be modified can be found in Setting F-Secure Anti-Virus Preferences.

However, there are some Preferences not mentioned in the end-user documentation: Network, Administration, Restrictions, and Updating.

More:

Network Preferences

Administration Preferences

Restrictions Preferences

Updating Preferences

Network Preferences

The Network Preference contains the Inform Administrator with Results and Send Infected files to Administrator check boxes. Check the boxes to have F-Secure Anti-Virus send you the task results and copies of infected files from local workstations. Samples will always be sent in an encrypted format. Whenever F-Secure Anti-Virus Gatekeeper finds a virus, it will send a corresponding message to administrator. These messages can then be read by choosing View User Messages from the Administration menu.

This dialog box specifies the name and location of the shared communication directory. Select the Notify at Startup if Invalid check box to have F-Secure Anti-Virus notify you at start-up if the specified directory has become invalid.

This preference also allows changes to the F-Agent polling frequency. See Communication Directory for more information.

The Hide F-Agent option lets you hide the F-Agent icon from the taskbar and the desktop.

Administration Preferences

In the “Administration Preferences” dialog box, there are three general settings:

Enable Network Usage. If this check box is not selected, all network related functions will be disabled.

Ask Workstation Prefs on First Startup. If this check box is selected, F-Secure Anti-Virus asks for the workstation ID and user name the first time it is started on a workstation. F-Secure Anti-Virus will not proceed until this information is provided.

Administration Workstation. This option is used to determine whether or not the current workstation is the administration workstation.

You can hide some of the Preferences from the users. If a Preferences is hidden, the users cannot edit it, and the choices, you have made, stay in effect. It is recommended that you hide at least Network, Administration, Restrictions, and Updating Preferences.

The Administration Preferences can also be used to change the administration password. The user or administrator must know the current password in order to change it.

Restrictions Preferences

Use the Restrictions Preferences to restrict the use of F-Secure Anti-Virus in the user mode. You can prevent users from seeing the program main window by selecting the No Main Window check box. In this case, the users can still start scans from the program’s desktop icon. The other possible restrictions are: Disable Creation and Modification of Tasks, and Disable Network Scans.

Updating Preferences

In the Updating Preferences select one of the alternatives for executing F-Secure Anti-Virus updates on the workstations: Update Automatically or Prompt at Start-Up.

Distributing F-Secure Anti-Virus Installations

When you have completed the installation and customization on the Administration workstation, the program is ready for distribution. To distribute F-Secure Anti-Virus to the end-user workstations, you have two options:

- Set up an installation directory for Autoinst to have F-Secure Anti-Virus installed to workstations as they log on to the network server.
- Prepare the a setup installation directory and ask the users to run F-Secure Anti-Virus Setup from their workstations.

F-Secure Anti-Virus also supports installation through the use of Microsoft Systems Management Server (SMS). In this case, Autoinst is used for building the installation scripts. See “Microsoft Systems Management Server” in the F-Secure Anti-Virus manual for more information. The latest information about SMS support is available at:

- http://www.DataFellows.com/anti-virus/sms/

More:

Installation with Autoinst

Installation with Setup.exe

Installation with Autoinst

Autoinst is a utility program that enables the system administrator to have any version of F-Secure Anti-Virus installed or updated automatically on workstations that log on to the network. In most network environments, the workstations call a log-in batch script (for instance, LOGIN.BAT) when they log on to the network. This script is modified to invoke Autoinst. Autoinst then performs the installation according to the instructions listed in its parameter file

The administrator must place the program files and configuration files on a network drive; Autoinst will then copy them to local workstations and make the necessary changes to the users' Windows Registry or the WIN.INI and SYSTEM.INI files. Autoinst also handles updating and uninstallation, and can be used for changing the F-Secure Anti-Virus Preferences stored in the in configuration files on workstations throughout the network.

You should use the Autoinst Wizard to create the installation script. However, not all the options are available through the Wizard. If you need to fine-tune the settings, you should write a customized Autoinst script. See “Autoinst Configuration” in the F-Secure Anti-Virus manual for more information.

To distribute installations using Autoinst, first perform the Network Administration installation on the Administration workstation. Then do the desired modifications to the F-Secure Anti-Virus Preferences, toolbar, and the task base. Then choose Distribute F-Secure Anti-Virus Installations from the Administration menu, and select By Creating Installation Directory for Autoinst. Autoinst Wizard will start.

More:

Autoinst Wizard

Autoinst Wizard

Autoinst Wizard makes it easy to write the Autoinst configuration file, create the shared Autoinst installation directory, and make all the necessary files available for distribution.

You can move freely back and forth within Autoinst Wizard by clicking Back and Next. You can exit the wizard at any time by clicking Cancel. The most important steps in the Wizard are described below.

Enter the name and location of the Autoinst directory, which should be accessible from all workstations. If the specified directory does not exist, the wizard will create it, prompting for your confirmation first.

Select the check boxes corresponding to the programs you wish to distribute. Select the Yes check box to have the networking functionality enabled, if you plan to distribute scanning tasks, bulletins, and updates, and receive mail from workstations.

Choose the type of installation Autoinst should perform. Choose Remote Installation if you wish F-Secure Anti-Virus or F-Secure Anti-Virus Gatekeeper to reside on the server. In this case, only the data files, such as reports, configuration files, and others, will be copied to the local workstations' hard disks. If you choose Local Installation, Autoinst will perform the complete installation on the local workstations, which is the recommended configuration.

Choose the name of the destination directory on the local workstations' hard disks where the files will be installed. If the specified directory does not exist on some of the workstations, Autoinst will create it.

Select the source from which Autoinst will obtain the user name and the workstation ID, both of which will serve to identify the origin of mail received from workstations. Depending on your choice, various dialog boxes will be displayed upon clicking Next.

If you selected environment variables as the source from which Autoinst will obtain user name and workstation name, type in the names of the both environment variables in the provided boxes, enclosing each variable between the % characters.

If you chose initialization files as the source of user and workstation names, add the entries that specify the user name to the provided list. If you list multiple entries, the first of them that yields result will be used. To add entries, click Add.

In the dialog box, type in the File name, Section name and Entry name, and click OK. The new entry will appear on the list. To edit the entry, select it on the list and click Modify. Edit the entries in the displayed dialog box. To delete an entry, select it on the list, and click Remove. Clicking Clear All will delete all the entries.

If you chose Windows registry as the source of user and workstation names, add the registry locator for the user name by clicking Add. You can list multiple entries; in this case the first one pointing to the valid value will be used.

In the Add registry locator dialog box, enter the Main key, the Sub key and the Value name. The Main key can be selected from the list; the available options are: HKEY_CLASSES_ROOT, HKEY_CURRENT_USER, HKEY_LOCAL_MACHINE, HKEY_USERS.

Now the Autoinst Wizard is ready to copy the files. Click Next and it will start copying the files to the installation directory.

The Autoinst Wizard will ask you whether you want to customize F-Secure Anti-Virus Preferences or the settings of F-Secure Anti-Virus Gatekeeper before distributing the programs to the users. The customization is done through the standard Preferences dialog.

The final message box tells you where the Autoinst installation directory has been created and the name of the Autoinst command file, located in the Autoinst directory. Insert this command into the workstations' login scripts, so that it is executed at log-on. The wizard has also created the Autoinst.INI file, which can be further edited with a text editor to fine-tune its parameters. For more information on using Autoinst and fine-tuning Autoinst.INI, see "Autoinst Configuration" in the F-Secure Anti-Virus manual.

Installation with Setup.exe

Another option to distribute F-Secure Anti-Virus installations is to create a shared Setup installation directory. To establish a shared Setup directory:

1. Perform the Network Administration installation of F-Secure Anti-Virus on the Administration workstation.
2. Create the Setup installation directory on the server.
3. Copy the contents of the original installation diskettes to the SETUP installation directory.
4. Click Distribute F-Secure Anti-Virus Installations from the Administration menu, and choose By Modifying the Installation Directory. Select the SETUP installation directory in the dialog box and click OK. The F-Secure Anti-Virus configuration and task files will be copied to the SETUP directory.

Workstation installations can now be done by running Setup.exe on workstations from the Setup directory you created.

Distributing Updates

The easiest way to update F-Secure Anti-Virus is via the network. The best way to handle updating is first to update the Administration workstation, and then use it as the source for the update. F-Secure Anti-Virus updating function uses the F-Secure Anti-Virus root directory as the source directory.

Important: If you are sending updates through F-Secure Anti-Virus, make sure that you do not have Autoinst listed in the system’s login script. Autoinst is only used for first time installations and should be removed as soon as everyone in the network has executed it.

More:

Updating the Administration Workstation

Sending Updates To Users

Updating the Administration Workstation

To update a new version of F-Secure Anti-Virus to the Administration workstation, run Setup.exe from the new setup disks. Choose the Update Installation option. This installation replaces the old program files on your hard disk.

If the end-users run a shared copy of F-Secure Anti-Virus from a server, make sure that nobody is using F-Secure Anti-Virus at the time of updating. The setup cannot replace the necessary files if they are open.

Sending Updates To Users

After you installed a new version of F-Secure Anti-Virus on the Administration workstation, send it to the users through the network. This can be done by choosing Send Update from the Administration menu. The program will copy all the files and directories under the F-Secure Anti-Virus root directory to the UPDATE directory on the shared disk.

When you send an update to users, all programs installed under the F-Secure Anti-Virus root directory are copied to the shared disk. If you have programs like F-CHECK or F-Secure Anti-Virus for DOS installed in their own directories under the root directory, they will also be copied to the local workstations. As you can see, this feature can be used to update or distribute programs which are unrelated to F-Secure Anti-Virus.

On workstations, F-Secure Anti-Virus, when started, checks the UPDATE directory. If a new version has become available, F-Secure Anti-Virus updates itself. If the UPDATE directory contains other programs, F-Secure Anti-Virus also copies them to the local hard disk.

Distributing Tasks

Tasks can be created on the administration workstation and distributed to users via the network. F-Secure Anti-Virus programs on local workstations will automatically add the distributed tasks to their task lists. Similarly, you can automatically remove a previously distributed task from all workstations connected to the network.

More:

Sending Tasks to Users

Removing a Previously Distributed Task

Sending Tasks to Users

Send a task to users by selecting it on the task list and clicking Distribute Selected Task on the Administration menu.

In the subsequent dialog box, select either Network or Distribution directory as the distribution method. The Distribution Directory option is available only if you have distributed F-Secure Anti-Virus installations by setting up and modifying an installation Setup directory. See Installation with Setup.exe for more information.

Click the check boxes below to select the desired options.

If the Force report at first scan check box is selected, the local programs send the results of this task directly to administrator.

If the Force immediate scan upon receiving task check box is selected, the task is executed immediately after being copied to local workstations.

If the Protect task from modification check box is selected, the users cannot modify the task parameters.

If the Disable aborting scan check box is selected, the users cannot terminate a scan during its execution.

After you have chosen the desired options, click OK to copy the task file to the TASKS directory on the shared disk. When F-Secure Anti-Virus programs on the local workstations notice that a new task has become available, they copy the task to the local hard disks and add it to their local task lists.

A distributed task remains in the shared TASKS directory until removed by administrator. If a workstation is not connected to the network because it is switched off or not logged on to the network, or for other reasons, the task will be retrieved as soon as the contact with the server is regained.

The task files distributed by the administrator have the extension .fpa, whereas user task files are designated .fpt. On the task lists of local workstations the distributed tasks are shown in a different color.

Removing a Previously Distributed Task

Remove a task that you have previously distributed by selecting it on the task list and choosing Undistribute Selected Task from the Administration menu.

The Undistribute Selected Task command sends the Undistribute file to the TASKS directory on the shared disk. The Undistribute file has the same name as the corresponding task file but is differentiated by the extension .del. When F-Secure Anti-Virus on local workstations notices that an Undistribute file has appeared on the shared disk, the corresponding task is deleted from the local hard disks.

Collecting Reports and Infected Files

Use the Network Preferences to set up the actions to be taken by F-Secure Anti-Virus when it discovers a virus on a user workstation. Here you can select whether or not the task reports and any infected or suspected files are to be sent to administrator.

When the Inform Administrator with Results check box is selected and incorporated into the users' versions of F-Secure Anti-Virus, a task results report is sent to administrator whenever a virus is found during a scan execution. Whenever F-Secure Anti-Virus Gatekeeper finds a virus, it sends corresponding message to administrator. The messages can be read by choosing View User Messages from the Administration menu.

When the Send Infected Files to Administrator check box is selected and incorporated into the users' versions of F-Secure Anti-Virus, infected and suspected files are automatically sent to administrator. The files are transferred to the INFECT and SUSPECT directories, respectively, and the reports go to the REPORTS directory. For more information on these directories, see Distributing F-Secure Anti-Virus Installations.

You can also have the results of some specific task sent to you by selecting the option "Force Report at First Scan" in the "Distribute Selected Task" dialog box. Selecting this option makes the receiving workstations send results of the distributed task to administration workstation.

The administrator's F-Agent watches for new messages and reports from users. When new messages arrive, the administrator is asked whether F-Secure Anti-Virus should be started to view the messages.

WARNING: If you want to test the performance of F-Secure Anti-Virus by scanning a large number of files infected with various viruses, be sure to switch this option off. Otherwise, every infected file will be copied to the INFECT directory. This operation will consume a vast amount of time and disk space.

More:

Viewing User Reports

Infected and Suspected Files

Viewing User Reports

Reports can be browsed by choosing View User Reports from the Administration menu. This opens the “Read Reports” dialog box, in which the user reports are listed.

The reports list is similar to the log file. Each report is represented by one line which contains the originating workstation ID, the name of the task, the time of execution, and the report status.

The dialog box contains the following buttons:

- Read, to access a selected report;
- Delete, to remove a report from the report list and the local hard disk;
- Delete All, to remove all reports from the report list and the local hard disk;
- Help, to access context-sensitive Help; and
- Close, to exit the dialog box.

The actual report can be inspected by either double-clicking on the corresponding entry in the Report list, or by selecting the entry from the list and clicking the Read button on the lower pane of the dialog box. The report is displayed in a separate window.

Infected and Suspected Files

F-Secure Anti-Virus recognizes two types of ‘at risk’ files: infected and suspected ones. Infected files are those files in which the program has detected a recognized virus infection. Suspected files are those files that F-Secure Anti-Virus determines to may have a virus infection. When a file of either kind is sent from a local workstation to the network server, it is encrypted and renamed to prevent the infecting virus from spreading as a result of unintentional execution of the file. When the file is moved to the administration workstation, it is decrypted but does not revert to its original name.

Each infected or suspected file is accompanied by the information file, which contains the original name of the file, the directory path for the workstation on which it was found, the name of the infecting virus, and the ID of the local workstation.

The infected files can be viewed by choosing View User Infected Files from the Administration menu. F-Secure Anti-Virus displays the list of infected files, giving the name of the virus, the name of the infected workstation, and the name of the infected file on the local workstation, complete with the directory path. Below the list, the program displays the current file name and location of the file on the administration workstation.

If F-Secure Anti-Virus reports an unknown virus or a new variant of a known virus, please contact Data Fellows or your local distributor. See Technical Support for more information.

Managing Messages

F-Secure Anti-Virus supports communication between users and administrator in the form of bulletins and messages. These are files that are circulated via the network shared disk.

Bulletins are general messages that administrator sends simultaneously to all the users.

Messages are notes that the users send to the administrator. F-Secure Anti-Virus Gatekeeper, when it finds a virus on a user workstation, also sends a message to administrator. The messages identify the sender and the originating workstation.

Both messages and bulletins are transferred over the network by being copied to the appropriate F-Secure Anti-Virus directory on the server disk. When F-Secure Anti-Virus is run on the administration workstation, any new messages that appear in the shared MESSAGES directory are copied to the local MESSAGES directory and added to the Message List. Likewise, F-Secure Anti-Virus run in User mode copies bulletins from the shared BULLETIN directory to the local BULLETIN directory and appends them to the local Bulletin List.

More:

Sending Bulletins to Users

Reading Messages

Sending Bulletins to Users

Before you can send a bulletin, you must first create it. Since a bulletin is simply a file sent through the network, you can write, draw or compile the bulletin file with any text editor or other application you want. Users must have the same application available in order to read the bulletin.

To send a bulletin to users, choose “Manage Bulletins” from the Administration menu. This will open the “Manage Bulletins” dialog box, which contains options for editing and deleting old bulletins and creating new ones. The bulletins are distributed and undistributed from this dialog.

To create a new bulletin, click New to open the “Bulletin Attributes“ dialog box where you can define the bulletin.

In this dialog box, first name the bulletin. F-Secure Anti-Virus will thereafter recognize the bulletin by that name, regardless of its original file name.

The next step is to enter the actual name and directory path of the bulletin file. If necessary, use the Browse button to locate the bulletin file.

After you have defined the bulletin in this dialog box, click OK to return to the “Manage Bulletins” dialog. The new bulletin will be on the list, and you can send it to users by selecting it on the list and clicking Distribute.

You can also remove a bulletin from circulation by selecting it on the Bulletin list and clicking Undistribute. This makes F-Secure Anti-Virus send the Undistribute file to the shared disk. The Undistribute file has the same name as the corresponding bulletin, but has the extension .del. When F-Secure Anti-Virus programs on local workstations find the Undistribute file in the shared BULLETIN directory, the corresponding bulletin from the local BULLETIN directory is deleted.

Bulletins can be edited by clicking Edit in the “Manage Bulletins” dialog box. Bulletins can be converted into Write format for editing.

Reading Messages

Read the user messages by choosing “View User Messages” from the Administration menu. In the dialog box, choose the message from the list. By default, the first unread message will be opened and marked as read.

The dialog box identifies the sender and displays the subject of the message. The message text is displayed in the lower portion of the dialog box.

The “Read Messages” dialog box contains the following buttons:

- Next, to select the next unread message and display its contents;
- Delete, to remove the currently selected message;
- Delete All, to delete all the messages;
- Close, to exit the dialog box; and
- Help, to access the context-sensitive Help.

Administration Menu

The Administration menu is the administrator's main tool for controlling F-Secure Anti-Virus. The menu contains commands needed to administer the system.

Since the Administration menu is only visible when the program is run in Administration mode, it is hidden from normal users. To switch to Administration mode on some other workstation, simply choose the Administration command from the File menu and enter the administration password in the dialog box.

The Administration menu contains the following commands:

Command	**Function**
Distribute F-Secure Anti-Virus Installations	Modifies installation directory, creates installation directory for Autoinst.
Manage Bulletins	Opens the bulletin list.
View User Messages	Opens the Read Messages dialog box.
View User Reports	Opens the Read Reports dialog box.
View User Infected Files	Displays the list of infected files sent from workstations.
Distribute Selected Task	Prompts for the task options, then makes task available in the network TASKS directory.
Undistribute Selected Task	Sends an Undistribute file to the shared disk. The corresponding task will be removed from user workstations.
Send Update	Copies everything under the F-Secure Anti-Virus root directory (except what is under the LOCAL and SHARED directories) to UPDATE directory on the shared disk.
Administrator Support on the Web	Connects to the Administrator's support page on the F-Secure Anti-Virus Web server.

Don't Panic

If F-Secure Anti-Virus reports that your computer is infected with a virus, don't panic! Sometimes a badly thought out attempt to remove a virus will do much more damage that the virus might have done. The worst thing to do is to format the hard disk since that way you may lose a lot of information and end up spending a lot of work restoring your system to its original state. Further, some viruses cannot be removed even with a hard disk format.

The first actions on discovering a virus infection should be:

- Inform the system administrator.
- Put a note on the infected computer, so that it will not be used before it has been disinfected.
- If you still feel like panicking, go get a cup of coffee. The virus will wait.
- If the virus is a macro virus, notify the people you have shared documents with.

- If the virus is a boot sectorGlossbootsector infector, notify the people you have shared diskettes with.
- If the virus is a program file infector, notify the people you have shared program files with.
- Follow the instructions in this topic to disinfect the computer.
- If there is a problem in recovering from the infection, ask your system administrator to contact your local F-Secure Anti-Virus Business Partner for technical assistance. For more information about your technical support options, see Technical SupportTechnicalSupport.

At this point, it would probably be a good idea to read the description on the operation of the virus. Such descriptions are available in F-Secure Anti-Virus for Windows' Help Menu and in Viruses/Information menu in F-Secure Anti-Virus for DOS. Latest virus descriptions are viewable at Data Fellows' web site at:

- http://www.DataFellows.com/vir-info/

Disinfecting the System

On a Windows system, macro viruses are the most common. However, there are several other types of viruses, each of which requires a different method for disinfection. In this topic you will find detailed instructions for all operating systems and all types of viruses.

If you run into problems during disinfection because F-Secure Anti-Virus reports “A new or modified variant” of the virus and refuses to disinfect it, please contact F-Secure Anti-Virus Support. See Technical Support for more information.

You might have a new virus, which we need to analyze in order to add exact detection and disinfection of it to F-Secure Anti-Virus.

Make sure you check all places where the virus might have ended: disks, network drives, backup tapes, removable drives, files sent to other people via e-mail, and all other places which you have accessed during the time the virus has been in your system.

Viruses in Document Files

If F-Secure Anti-Virus for Windows or Gatekeeper finds a virus in a document file (DOC, XLS, etc) on the hard drive or network drive, you have a macro virus. These never stay resident in memory, so you do not need to boot from a clean diskette. Just make sure you do the disinfection after exiting Word and Excel to make sure they are not locking any document files.

To disinfect, run F-Secure Anti-Virus. Open up the Settings for “Scan Hard Drive” task and make sure that the Action is set to Disinfect. Then start the task from the task bar. When the virus is found, follow the instructions given on the screen and let F-Secure Anti-Virus remove the virus.

If F-Secure Anti-Virus for Windows is unable to remove the virus, you might want to download the latest MACRO.DEF update via the internet from

- http://www.DataFellows.com/macro/

If the infection was on a network drive, it is important to make sure all workstations are cleaned at the same time to prevent re-infection. One way to do this is to force everybody off the network and include a hard drive scan made with the DOS-based F-MACRO program into the system login script.

More:
Macro Virus Disinfection on a DOS-Only System

Macro Virus Disinfection on a DOS-Only System

To disinfect Macro Viruses on a DOS system, run the F-MACRO program from F-Secure Anti-Virus for DOS directory. Execute it with a command line like this:

```
F-MACRO C: /DISINF
```

or, for example,

```
F-MACRO U: X: Y: Z: /DISINF
```

Viruses in Program Files

If a virus is found in any of the program files (COM, EXE, etc) on the hard drive or a network drive, you have a program virus. Open up the Settings for “Scan Hard Drive” task and make sure that the Action is set to Disinfect. Then start the task from the task bar. When the virus is found, follow the instructions given on the screen and let F-Secure Anti-Virus remove the virus. If F-Secure Anti-Virus cannot disinfect the virus, it will either rename the file or delete it, first asking for confirmation. The easiest way to recover such a file is to reinstall it or restore it from the backups. Contact F-Secure Anti-Virus Support if needed.

If the infection was on a network drive, it is important to make sure all workstations are cleaned at the same time to prevent re-infection. One way to do this is to force everybody off the network and include a hard drive scan made with F-Secure Anti-Virus for DOS to the system login script. Also revise the access levels users have on the directories which were infected to prevent the problem from re-occurring.

Viruses on a Diskette Boot Sector

If F-Secure Anti-Virus or Gatekeeper finds a virus on a floppy diskette boot sector, begin the “Scan floppy” task (from the Settings menu) and make sure that the Action is set to Disinfect. When the virus is found, follow the instructions given on the screen and let F-Secure Anti-Virus remove the virus. If F-Secure Anti-Virus cannot disinfect the virus, it will either rename the file or delete it, first asking for confirmation.

Alternatively, you may simply copy the clean files from the diskette to a directory on the hard drive and throw away the diskette. Disks are cheap and this is a quick and easy way to get rid of the problem.

Viruses on the Hard Disk Boot Sector or MBR

Viruses that have infected your hard disk boot sector or the Master Boot Record (MBR) may be tricky to disinfect because they get access to your system every time you start the computer from the hard disk. For this reason, it is recommended that you boot the computer from a floppy diskette instead and use the Rescue disk to remove the virus from the hard disk.

Using the Rescue Disk

A Rescue Disk and a Disinfection Disk are included in the F-Secure Anti-Virus package. Using these diskettes, you can remove a virus infection and restore vital system information to the computer when it has been destroyed or altered. This situation may arise if the computer is switched off while an application is still active, or if a virus damages the computer's system information.

With a complete and up-to-date Rescue Disk, you can boot the computer, use the Disinfection Disk to check the system for viruses and remove possible infections, and again use the Rescue Disk to restore system information to the computer.

The following example describes the restoration of system information using the Rescue Disk after the system has been infected. For instructions on how to create a Rescue Disk and store system information on it, see Creating a Rescue Disk Creating a Rescue Disk.

Before restoring system information, you must make sure that no viruses remain in the computer. In this example we assume that the computer has been infected, so the first task is to remove the infection using the Disinfection Disk:

1. Switch off the computer and insert the Rescue Disk in the diskette drive.
2. Switch the computer back on and wait while the operating system boots from the Rescue Disk.
3. Exit F-Rescue.
4. Remove the Rescue Disk and insert the Disinfection Disk.
5. On the command line, type:
   ```
   A:\FSAV.EXE /HARD /ALL /DISINF
   ```
   and press [ENTER].

You'll then see this message:

```
F-Secure Anti-Virus will remove the virus and give you a report about
the infection and the situation after the disinfection.
```

If F-Secure Anti-Virus is unable to disinfect a boot virus automatically, you can restore the boot sector from the Rescue Disk as follows:

1. Switch off the computer and insert Rescue Disk in the diskette drive.
2. Switch the computer back on and wait while the operating system boots from the Rescue Disk.
3. After the computer boots, the F-Rescue program will be launched automatically.
4. When the F-Rescue program starts, it displays the following menu on the screen:
   ```
   1) Backup system information
   2) Restore system information
   0) Exit
   ```
5. Choose 2

You will now be shown the Restore menu, where you have the following options:

```
1) Restore MBR and first tracks
2) Restore extended partition info
3) Restore DOS Boot sectors
```

```
4) Restore CMOS Setup information
5) Make hard disk bootable
6) Select single element to restore
0) Exit to DOS
```

If you are recovering from a boot virus, the important choices here are 1, 2 and 3.

Option 1

With this option, you can restore the Main Boot Records of the computer’s hard disks, as well as the disks’ first tracks.

Depending on your system, you may have to make the following further choices:

```
Physical disk #0, 540 MB
Physical disk #1, 320 MB


To which disk # do you wish to restore MBR (A for All, N for None)?
```

Choose A to restore all boot sectors.

Option 2

This option allows you to recover the original extended partition information of your computer’s hard disks. Depending on the system, you may have to make the following further choices:

```
Physical disk #0, 540 MB
Physical disk #1, 320 MB


To which disk # do you wish to restore extended partition info (A for
All, N for None)?
```

Choose A to restore all areas.

Option 3

You can also restore the operating system’s original boot sector. Depending on your computer, you may have to make the following further choices:

```
Physical disk #0, 540 MB
Physical disk #1, 320 MB


To which disk # do you wish to restore boot sectors (A for All, N for
None)?
```

Choose A to restore all DOS boot sectors.

Option 4

This function restores the original CMOS start-up settings. CMOS is the system’s battery-backed memory which contains information about the system configuration. This information is needed during the computer’s boot-up.

```
You are about to restore CMOS, are you sure (Y/N)?
```

To restore the CMOS settings, you just need to write Y and press [ENTER].

To keep your Rescue Disk current, you must update it every time you make changes to the system. The Rescue Disk must be updated as described in the topic Creating a Rescue Disk, every time you make one of the following changes in your computer:

- When you update your operating system
- When you update the computer's BIOS or CMOS
- When you change the number, size or partitioning of your hard disk drives
- When you change the amount of RAM in your computer
- When additional devices are connected to the system (for instance, a CD-ROM -drive)

The Rescue Disk must be updated every time the system configuration is changed. The diskette must be stored write-protected and in a safe place.

More:

Manually Repairing the MBR

Manually Repairing the Boot Sector

Special Considerations for Windows NT

Manually Repairing the MBR

If F-Secure Anti-Virus is unable to disinfect a MBR boot virus and restoring the MBR from a backup created by F-Rescue or NT's RDISK fails, you can try to manually recreate the MBR area. MBR (Master Boot Record) is one sector (512 bytes) located at the very start of your hard drive. These instructions work with many (but not all) DOS, Windows, Windows 95, Windows NT, OS/2 and even PC-based Unix systems.

To attempt repair, use a startup system diskette with DOS version 5 or higher and make sure that the file FDISK.EXE is on that diskette. Write-protect the diskette.

Cold start the infected computer from this diskette. Do not rely on just pressing Control + Alt + Delete; instead press the Reset button or turn the computer off and then back on.

Check if you are able to access all partitions on the hard disk(s) normally. For example, if command dir C:\ produces a normal file list of drive C:, then you know that partition of C: is recognized. Test other partitions too. If partitions are not recognized, it might be because the virus encrypts the partition data or overwrites it. In this case, the generic disinfection method described below is not possible. Do not continue or you will lose your data. Contact F-Secure Anti-Virus Support instead.

If you can access C: and other partitions, type in the command

```
FDISK /MBR
```

This will overwrite the code part of the MBR, in effect killing the virus. If you are using Novell DOS 7.0, you need to select this option from the menu, instead of giving a command-line switch.

Now re-start the computer normally from the hard disk and re-check that everything is operating normally. Do not forget to check your diskettes for the infection as well.

Manually Repairing the Boot Sector

If F-Secure Anti-Virus is unable to disinfect a boot sector virus and restoring the boot sector from a backup created by F-Rescue or NT's RDISK fails, you can try to manually recreate the boot sector. Boot sector consists of a single sector (512 bytes) located at the start of every partition. A single hard drive can have many boot sectors. These instructions work with many (but not all) DOS, Windows and Windows 95 systems.

Use a startup system diskette and make sure that the SYS.COM file is on that diskette. The DOS version on the diskette should be EXACTLY the same as the one on the hard disk. Write-protect the diskette.

Cold start the computer from the diskette and give the command

```
SYS C:
```

In addition to copying the system files over, which is not necessary to remove the virus, this will overwrite DOS boot sector with clean code, killing the virus.

Now re-start the computer normally from the hard disk and re-check that everything is operating normally. Do not forget to check your diskettes for the infection as well.

Special Considerations for Windows NT

If Windows NT fails to boot, it might be caused by a boot virus. Since NT cannot be booted from a diskette, you must run F-Secure Anti-Virus for DOS instead. Reboot the machine with the Rescue Disk or a clean startup DOS system diskette. The first diskette of DOS installation diskette set will do. It would be easiest to use a self-made bootable diskette. Instructions on how to make the Rescue Disk are in the section “Creating a Rescue Disk.”

Turn off the power of the infected computer, insert the clean startup disk and start the machine. If the machine does not boot from the diskette, make sure your CMOS Setup settings are configured to boot from the diskette (remember to turn this setting back on after you are done).

After the computer re-starts and the prompt appears, remove the startup disk. Insert the F-Secure Anti-Virus for DOS diskette. To run F-Secure Anti-Virus from the diskette, type

```
FSAV <press ENTER>
```

F-Secure Anti-Virus will start and the memory test should find no viruses. If it does, you must re-create the boot diskette on a clean machine, following the instructions in the topic Creating a Rescue Disk.

After F-Secure Anti-Virus has started, open up Scan menu, make sure that the Target menu is set to Hard Drive and Action is set to Disinfect, and choose Begin Scan. When the virus is found, follow the instructions given on the screen and let F-Secure Anti-Virus remove the virus.

If F-Secure Anti-Virus for DOS is unable to remove a boot sector virus, try using your NT Rescue Disk (created beforehand with RDISK (NT utility) or during NT installation). Cold reboot from the NT Rescue Disk and choose ‘Recreate boot sectors’ option.

If F-Secure Anti-Virus for DOS is unable to remove a boot sector virus but you have do not have a working NT Rescue Disk, it might be possible to remove the virus manually. See Manually Repairing the MBR or Manually Repairing the Boot Sector for more information. Contact F-Secure Anti-Virus Support if needed.

Viruses Resident in Memory

If F-Secure Anti-Virus finds a virus during initial memory test, you will need to reboot the machine with the rescue disk or a clean startup DOS system diskette so that the virus does not get re-loaded to memory, and re-run F-Secure Anti-Virus. The first diskette of a DOS installation diskette set will do. It would be easiest to use a self-made bootable diskette. Instructions on how to make such a Rescue Disk are in the topic Creating a Rescue Disk."

Turn off the infected computer, insert the clean startup disk and start the machine. If the machine does not boot from the diskette, make sure your CMOS Setup settings are configured to boot from the diskette (remember to turn this setting back on after you are done).

After the computer re-starts and the prompt appears, remove the startup disk. Insert the F-Secure Anti-Virus for DOS diskette. To run F-Secure Anti-Virus from the diskette, type

```
FSAV <press ENTER>
```

F-Secure Anti-Virus will start and the memory test should find no viruses. If it does, you must re-create the boot diskette on a clean machine, following the instructions in Creating a Rescue Disk.

After F-Secure Anti-Virus has started, open up the Scan menu, make sure that the Target menu is set to Hard Drive and Action is set to Disinfect, and choose Begin Scan. When the virus is found, follow the instructions given on the screen and let F-Secure Anti-Virus remove the virus.

If you get an error message which says that low-level access to hard drive is prevented and asks you to use the LOCK command, you are using a Windows 95 boot diskette instead of a DOS boot diskette. Re-create a DOS bootable diskette or repeat the cold boot and give the LOCK command at the prompt before executing F-Secure Anti-Virus.

If F-Secure Anti-Virus cannot disinfect a file virus, it will either rename the file or delete it, first asking for confirmation. The easiest way to recover such a file is to reinstall it or restore it from the backups.

If F-Secure Anti-Virus for DOS is unable to remove a boot sector virus but you have do not have a working NT Rescue Disk, it might be possible to remove the virus manually. See the topics Manually Repairing the MBR and Manually Repairing the Boot Sector for more information. Contact F-Secure Anti-Virus Support if needed.

How Great Is the Virus Threat?

Viruses are set apart from most other information security risks by the fact that even regular back-ups are not always a sufficient precaution. Making frequent back-ups diminishes the danger of a total disaster in case of a virus attack, but since even the back-up copies can be infected or corrupted, other measures are needed.

If security is lax, a well-designed virus can spread almost unnoticeably from one computer to another. Given enough time, a virus can infect virtually all computers and even worse, back-ups in an organization. A virus can even corrupt data bit-by-bit. If the designer of such virus was sufficiently skillful and devious, the changes can be so subtle that it is almost impossible to notice them for a long time. Even if small discrepancies in the data are found, they are often thought to be the result of operator errors or other human factors. This can be the worst sort of damage, as even the backups cannot be trusted after the virus is found.

After spreading itself during the latency period, a virus can activate and wreak havoc in the computers. The extent of such damage can range from the annoying to the truly devastating. A serious virus attack can be a catastrophic experience for a company. Many companies can be left totally crippled, if the files on their computers are wiped out.

No one wants to spread a virus to partners or clients, even if the virus does no direct harm. It is difficult to be absolutely certain that a virus is “harmless”.

Even though the likelihood of a disastrous virus infection is small, the danger is real and needs to be acknowledged. The costs of developing appropriate information security guidelines and purchasing effective anti-virus software are very small compared to the possible cost of an uncontrolled virus infection.

Data Fellows maintains a comprehensive database of computer virus information which documents the various symptoms of numerous viruses. The database is available in the Internet at:

- http://www.DataFellows.com/vir-info/

The virus descriptions are also available in the online help system of F-Secure Anti-Virus which you can access through the Help menu.

Common Virus Myths

Misconceptions about viruses are as common as the viruses themselves. Users who are new to virus-protection software may find some basic information very helpful. The following myths are explained and the corresponding truth delivered.

"Viruses Spread by Themselves"

Viruses cannot run themselves. Therefore, it follows that they cannot spread spontaneously, either. A virus cannot do anything until an infected program is executed or the computer is booted from an infected diskette.

"Viruses Are Able to Spread Between Any Two Computers"

Although it is theoretically possible to create virus which could function in various computer environments, the task would be extremely complicated. In practice, it is safe to assume that DOS viruses are unable to infect other kinds of computers, such as Macintoshes, Unix computers and VAXes.

"Viruses Can Infect Also Write-Protected Disks"

If a diskette has been write-protected manually, by using either tape or the write-protect switch, it cannot be written to. Even viruses cannot infect manually protected diskettes. However, diskettes become vulnerable whenever the protection is switched off, and this is why write-protected diskettes must also be checked for viruses.

"Some Viruses Are Completely Harmless"

There are viruses which do not destroy information on purpose. In fact, most viruses do nothing but spread themselves, whereas some viruses are content to flash a message of some kind every now and then. A user may then think that the virus in question is entirely harmless. However, the truth is that there is no such thing as a harmless virus. In all cases, viruses increase the load on the computer and change program code without the user’s knowledge or approval. Even a simple and basically harmless infection may cause some programs to be unable to function. If nothing else, viruses consume disk space better used for something else.

"Only Pirated Programs Contain Viruses"

In most cases, infections spread with copied programs. Virus infections can often be traced to infected public domain and shareware programs or illegal program copies. However, the sad truth is that a very large number of virus infections have their source in original program diskettes. Global statistics show dozens of cases where a commercially distributed software has carried a virus infection. Altogether hundreds of thousands of infected diskettes have been shipped to unsuspecting customers. After all, what cause is there to be wary of packaged and write-protected program diskettes, especially if they come from a large and distinguished software house?

"Viruses Spread through E-mail and BBSs"

For the most part, the infections discovered so far have not originated in electronic bulletin board systems. People who run BBSs are usually more aware of the virus threat than the average user, and they know how to protect against viruses. In most BBSs, files are automatically scanned for viruses. In addition to this, boot sector viruses (such as Michelangelo and Form) cannot spread over data communication lines.

"Anti-Virus Programs Provide Total Protection Against Viruses"

The important thing to remember is that the programs which search for viruses – scanners – can identify only known, already discovered viruses. The advanced heuristic methods used by F-Secure Anti-Virus make it possible to detect also unknown viruses but this method does not provide identification of the viruses. This is why we provide you with a continuous update service.

An obsolete anti-virus scanner will only give the user a false sense of security, while letting new viruses slip through. Therefore, make sure that your copy of F-Secure Anti-Virus is always up to date.

"Viruses Can Wreck Computers"

A modern computer cannot be wrecked programmatically. Every now and then there are rumors about viruses which blow up monitors or break hard disks, but not a single one of these cases has been verified.

"Virus Infections Happen Only to Other People"

The risk to get a computer virus infection is naturally the lower the less data is brought to the computer from outside. In practice, no one is completely safe. On the other hand, the virus threat is often blown out of all proportions.

"Virus Infections Can Be Removed Only by Formatting the Hard Disk"

It is very rarely necessary to format the hard disk in order to get rid of a virus infection. Usually the disinfection can be accomplished by using a high-quality anti-virus program.

Common Virus Types

The following topic presents some of the most common virus types and their working mechanisms. There are four major types of viruses:

- file viruses
- boot sector viruses
- companion viruses
- macro viruses

More:

File Viruses

Boot Sector Viruses

Companion Viruses

Macro Viruses

File Viruses

The file viruses infect executable programs, usually .com and .exe files, but sometimes also overlay files. An overlay file may have any extension, but the most common ones are .ovl and .ovr. All these files contain executable code.

A file virus works by finding a suitable executable program, into which it adds its own code, typically to the end of the host file. To make sure that it will be executed with the parent program, the virus adds a jump instruction to the beginning of the program. The jump transfers control to the virus code at the end of the host code.

After being activated, a virus has free reign in the computer. Normally, the main purpose of a virus is to spread the infection. This can be done in various ways.

Resident Viruses. When an infected program is run, the virus may stay resident in memory and infect every program executed. Viruses that use this method to spread the infection are called Resident Viruses.

Direct Action viruses. Other viruses may search for a new file to infect when activated. After infecting a specified number of new lines, the virus transfers control to the original program. Viruses that use this method to spread infection are called Direct Action viruses. After the control has been returned to the original program, its execution will continue as if nothing happened.

"Time bomb". After infecting a computer, a virus can move into its active phase, with the intention to attain the specific goal set by the virus author. Transition to the active phase can happen on a specific date, or when a certain condition has been met. In its active phase, the virus can destroy data or perform other harmful actions, like formatting the hard disk. Sometimes, these viruses are relatively harmless, perhaps slowing the computer down every Friday or making a ball bounce around the screen. Still, even if a virus was not intended to cause damage, it can do so due to an incompetence of its author. In addition, a virus can be modified, so that a more harmful version of it appears.

The obvious damages done by a virus amount to deletion of data or programs, maybe reformatting or overwriting the hard disk. However, more subtle forms of damage are also possible. Some viruses may modify data or introduce typing errors into text. Other viruses have no intentional effect other than just replicating.

The actions of a virus will slow down the start of the infected program. The delay is often so slight, that it is almost impossible to notice. There are, however, a few viruses, that infect a large number of files at once after being executed. This may slow down the start of the infected program by tens of seconds.

When a virus adds its code to the program, the size of the program will change. Some viruses avert this by storing their code in an unused area in the host file. In this case, the actual size of the infected program does not change.

Most viruses try to recognize the infections existing in files and avoid re-infecting the already infected programs. Usually, viruses mark infected files with some sort of easily distinguishable marker, such as setting the time stamp of the file to a non-valid value.

F-Secure Anti-Virus detects, identifies and disinfects all the file viruses that are in the wild.

Boot Sector Viruses

A boot sector virus infects the boot sector on a hard disk or diskette. Normally, the boot sector contains code for loading the operating system files. A boot sector virus replaces the original boot sector with a copy of itself and stores the original boot sector somewhere else, or simply replaces it totally. When a computer is later started from such a diskette, the virus takes control and hides in RAM. It will then load and execute the original boot sector and everything will appear to be normal. However, all the subsequent diskettes inserted in the computer will be infected with the virus.

Every formatted diskette has a boot sector. All the system and data diskettes, all diskettes containing programs or no files at all, have codes in their boot sectors. This code is run when a computer is started from this diskette. If the diskette does not contain the operating system, the program code in the boot sector will print the a message, such as:

```
Non-system disk or disk error
```

If the diskette is infected with a virus, the virus has probably already infected the hard disk.

The best way to protect your computer against boot sector viruses is to prevent starting from diskettes. This can be usually done with the BIOS SETUP of the computer, although this option may be not available on older models.

If the computer has no hard disk, and has to be started form a diskette, always use the same diskette, and keep it write-protected.

Most boot sector viruses infect master boot records (MBRs) on hard disks. This causes some problems, since MBRs cannot be cleaned with the format command. The best way to disinfect MBR is to use F-Secure Anti-Virus. Another option is to low-level format the disk, re-partition it with fdisk, format with format and restore the contents from a backup.

Boot viruses are able to infect a PC regardless of the operating system (DOS, Windows, NT, Linux, NetWare, etc.). Non-DOS systems will usually fail to boot when this happens.

Because the size of the boot record on a diskette is limited to 512 bytes, large boot sector viruses have to hide part of their code outside the boot sector itself. Many viruses create bad sectors on the disk and store their code in these sectors. It is also possible to hide code in the area reserved for the main directory. Another option is to format an extra track and use it for storing the virus code. Only reasonably sophisticated viruses use the last option.

As there are five different diskette formats available, namely 360K, 1.2 MB, 720K, 1.44 MB, and 2.88 MB, very few viruses are able to infect all diskette types. A boot sector virus will usually hide at the top of memory, thus reducing the amount of memory that DOS sees. For example, a computer with 640K might appear to have only 639K. It should be noted, that some BIOS modules also take one or two kilobytes away from the DOS memory.

F-Secure Anti-Virus searches for boot sector viruses by checking the MBR, the boot sectors, the partition table, and other available hiding spaces.

Important: Never start a computer with a hard disk from a diskette because it is practically the only way the hard disk can become infected with a boot sector virus. On many machines you can prevent this by setting the boot order in the machine’s BIOS SETUP settings, so that the computer always boots from the hard disk even if there is a diskette in the floppy drive.

Companion Viruses

Companion viruses use a feature of DOS to force their execution. When several files with the same base name but different extensions are in the same directory, the file with the .com extension is executed first. This happens only when the command line entry does not include the extension. Companion viruses use this feature be selecting an .exe file and creating a .com file with the same name in the same directory. The .com file may be hidden and thus would not show up in the directory listing. In contains the virus code.

It is also possible to design a companion virus that takes advantage of the order of directories specified in the PATH environment variable, or a virus that would use some other way to get its code to be executed before the host program.

After being activated, such a virus executes the actual program and seizes control again after the execution of the program has ended.

F-Secure Anti-Virus detects, identifies and disinfects all the companion viruses that are in the wild.

Macro Viruses

Macro viruses are viruses written with the macro “language” of an application program, such as Microsoft Word or Microsoft Excel. These macro languages are powerful enough to be used for writing viruses.

Macro viruses typically spread further when an infected document is opened or new documents are saved. This is problematic, because people exchange documents much more than executable files or diskettes. New macro viruses are also very easy to create or modify.

The first macro viruses infecting Microsoft Word were found in August 1995. By April 1997, more than 550 macro viruses were known, and Word macro viruses were the most commonly reported virus type world wide. Although other word processors like WordPerfect and Ami Pro support accessing Word documents, they cannot be infected by Word viruses. However, it is not impossible to write similar viruses for these programs.

F-Secure Anti-Virus detects, identifies and disinfects all the macro viruses that are in the wild.

Advanced Methods Used by Viruses

The following topic presents some of the methods viruses use to hide their presence or to otherwise complicate the process of fighting against them.

The following viruses using advanced methods are described:

- stealth viruses;
- self-encrypting, polymorphic, and mutating viruses;
- retroviruses;
- application specific viruses;
- multipartition viruses.

More:

Stealth Viruses

Self-Encrypting, Polymorphic, and Mutating Viruses

Retroviruses

Multipartition Viruses

Stealth Viruses

A few years ago it seemed that the final weapon against the virus infections was found. This omnipotent technique was called checksumming. The checksummers calculate an individual, unique signature for each file. By re-calculating the signature search string and comparing it to the original one stored in database, it is possible to detect every change made to a file and ensure the integrity of the system. However, it did not take long for the first file-infecting stealth viruses to appear and crush the hopes of final victory in the battle against viruses.

A stealth virus falsifies the information read from a disk so that a program reading the disk receives incorrect data. The virus does this by intercepting the interrupt vectors used to read data from the disk and supplying the reading program with false information. This way, the program reading the disk receives information which incorrectly indicates everything to be all right. This technique can be successfully used by both file viruses and boot sector viruses.

A good example is the virus called Brain, the first known stealth virus. Brain is a boot sector virus which transfers the original contents of the boot sector to a suitable location on the disk. Too large to fit completely on the boot record, it needs to store a part of its own code on the data area of the disk.

If a computer is started from an infected diskette, the virus is executed first. After taking control, Brain executes the original boot sector. Everything looks normal to the user, but Brain observes all disk reads and writes. Whenever a program attempts to read the contents of the boot sector, Brain responds by delivering the original boot sector code from its hiding place on the disk. Since the program actually sees the original code, everything appears to be in order, even though any diskette is infected. Brains also redirects all write attempts to the boot sector, protecting its own code.

Similar stealth methods are also used in viruses that infect files.

A stealth virus can intercept all disk reads to present false information. For this reason, F-Secure Anti-Virus has to check RAM memory before execution. If a stealth virus is already active, it can easily falsify all disk reads. Even a stealth virus cannot hide its code in memory completely, and it is always possible to find an active virus by checking all available memory before starting a virus scan. This is exactly what F-Secure Anti-Virus does.

When you start F-Secure Anti-Virus for Windows 3.1 or Windows 95, its first task is to scan the computer’s memory. F-Secure Anti-Virus checks the memory in the 0 - 1088 KB range, which is accessible to DOS viruses. Windows viruses are searched for by using specific system checks.

If F-Secure Anti-Virus for Windows finds a virus in the memory, it activates a dialog box to save all the open jobs, and then exits Windows. Once the Windows session is closed, the computer should be re-started from a clean diskette and scanned with F-Secure Anti-Virus for DOS. To learn how to create a startup diskette for emergency use, see What to Do When a Virus Is Found. For information about using F-Secure Anti-Virus for DOS, see the F-Secure Anti-Virus manual.

F-Secure Anti-Virus for Windows NT does not need to perform a memory scan at all because Windows NT protects system memory and private memory areas of each program automatically.

Self-Encrypting, Polymorphic, and Mutating Viruses

Most virus scanners operate by searching for virus search strings. Viruses that change their code between infections make it impossible to recognize the virus by using a search string.

Mutating viruses change their code and sometimes even their functionality between generations of the same virus.

The most common mutation technique is encryption. Many mutating viruses encrypt their code with a simple encryption algorithm using as encryption key, for instance, the time of the day. This makes all generations of a single virus different from each other, except for the decryption routine in the beginning of the virus code.

To make it impossible or inconvenient to use the decryption routine as a search string, virus writers often try to minimize the size of the virus. This is based on the fact that very short search strings can not be used because the possibility of finding the same byte sequence in normal programs increases, causing unwanted false alarms.

Most viruses encrypt themselves only at the time of infection, but there are some that do it while they are resident in memory. Whale is one of these very complex and sophisticated viruses.

The Bulgarian virus writer Dark Avenger created a virus mutation engine in 1991, called MtE. The MtE could easily be incorporated into any virus. The result was a virus which was functionally similar to the original virus, but was attached to the host program in one of an endless variety of versions. The MtE was distributed through underground bulletin boards as an object file that could be linked to any old or new virus.

It is extremely hard to isolate a search string from an MtE-encrypted virus that could be found in the next generation of the same virus. The encryption algorithm used by MtE is so advanced that only a single common byte can be found in all MtE-encrypted files. Furthermore, the location of this byte varies. The common instruction is JNZ (Jump if Not Zero), which can be found in practically every program available.

The MtE uses many different encryption algorithms and randomly adds extra bytes to the decryption routines.

MtE is not the only known mutation generator. There are dozens of different mutation engines in circulation, and there are several polymorphic viruses that have been created without the help of an external generator.

There are other methods to generate mutating viruses, besides encrypting their code. One is to build the virus from very small modules that can be swapped inside the code without any functional harm.

F-Secure Anti-Virus finds polymorphic viruses with its emulator-based scanning engine.

Retroviruses

The actions of some viruses are intentionally directed against known anti-virus programs. A virus may search for files from an anti-virus package and delete them. An active virus can identify the execution of an anti-virus product and simply crash the computer. As a result, the user may think that the virus scanner itself causes the crashes.

Other viruses do not aim for the destruction of an anti-virus product. A more devious way to incapacitate an anti-virus program is to make certain changes to the program itself. The virus scanner would still appear to be working normally, but it would not find any viruses.

The Peach virus is a good example of a retrovirus. It is a standard file virus, but has some features hat are directed against anti-virus software. When Peach infects .exe files, it checks a certain byte from the file’s header information. If the byte has a certain value, the file will not be infected. Peach apparently is trying to verify whether the file is a certain known program. Virus experts have yet to find out which program Peach is trying to avoid.

After being executed twenty seven times, Peach attacks the Central Point Anti-Virus (CPAV) software if it is installed in the same computer. CPAV saves its search strings in a single file on a disk and does not check for existence of the search string file. Peach deletes this file and CPAV will appear to work normally, but in fact will not recognize any viruses because of the absence of the search string file.

Due to the existence of retroviruses, F-Secure Anti-Virus utilizes many techniques against the tampering of F-Secure Anti-Virus files.

Multipartition Viruses

Multipartition viruses use multiple infection techniques. They can infect various types of executable files, boot sectors, master boot records (MBRs), FATs, and directories.

Multipartition viruses have a better chance of surviving a cleaning operation than viruses of other types. Even if the virus is disinfected from all program files, it will infect them again, if not removed from the boot sector.

Tequila is one example of a multipartition virus. It infects both .exe files and the master boot record. The virus features encryption mechanisms and advanced hiding abilities.

F-Secure Anti-Virus detects, identifies and disinfects all the multipartition viruses that are in the wild.

Signs Of Infection

If you experience the following symptoms, you might be infected by a new, unknown virus:

- Increased use of memory.
- Computer operating very slowly.
- Delay every time an application is executed.
- Inexplicable changes in executable or other files.
- A change in the latest alteration date of files, without apparent reason.
- Abnormal write-protection errors.
- Windows fails to start or install.
- Windows warns that 32-bit disk access is turned off.
- Inability to save Word documents to any other directory except TEMPLATE.
- Disks fail to work normally.

Unfortunately, these early warnings of a possible virus infection are not usually obvious and can be caused by a wide variety of reasons.

If the virus has an activation routine and it has passed into the active phase, it is usually very easy to detect:

- Files disappear.
- The hard disk is formatted.
- The computer does not start.
- Information changes.
- Certain files cannot be loaded or executed.
- The virus gives some other visible signs like writing messages to the screen or playing music.

Choose Virus Descriptions on the Web from the Help menu to access the F-Secure Anti-Virus Web server’s library for more technical information.

Testing Your Anti-Virus Protection

To test whether F-Secure Anti-Virus operates correctly, you can use a special test file which is detected by F-Secure Anti-Virus as though it were a virus. This file, known as EICAR Standard Anti-Virus Test File, is also detected by several other anti-virus programs. EICAR is the European Institute of Computer Anti-virus Research.

To create the EICAR test file, use any text editor to create the file with the following single line in it:

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

Save this file to any name with a .com extension, for example EICAR.COM. Make sure that you save the file in the standard MS-DOS ASCII format. Now you can use this file to see what is looks like when F-Secure Anti-Virus detects a virus. Naturally, the file is not a virus. When executed without any virus protection, EICAR.COM displays the text ‘EICAR-STANDARD-ANTIVIRUS-TEST-FILE!’ and exits.

Contacting F-Secure Anti-Virus Technical Support

Data Fellows Technical Support is available on the World Wide Web, through electronic mail and online through your F-Secure Anti-Virus client. If you suspect that your computer is infected with a virus, please see What to Do When a Virus Is Found for more information.

More:

Web Club

Virus Descriptions on the Web

Electronic Mail Support

Web Club

The F-Secure Anti-Virus Web Club provides help and 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 World Wide Web browser, and your location.

To connect to the Web Club directly from within your web browser, open this location:

- http://www.DataFellows.com/anti-virus/webclub/

For advanced support, the F-Secure Anti-Virus Support Center is available on the web:

- http://www.DataFellows.com/anti-virus/support/

Virus Descriptions on the Web

Data Fellows 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. The first time you use this option, you will need to enter the path and name of your WWW browser, and your location.

To connect to the Virus Information Database directly, open this location:

- http://www.DataFellows.com/vir-info/

Electronic Mail Support

If the online services at www.DataFellows.com do not cover your question, you are welcome to contact Data Fellows Technical Support by electronic mail.

With the purchase of an F-Secure Anti-Virus license, you get free technical support through email. Please contact the F-Secure Anti-Virus reseller from whom you bought your F-Secure Anti-Virus license for basic technical assistance, at:

- Anti-Virus-<yourcountry>@DataFellows.com
- Example: Anti-Virus-Japan@DataFellows.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@DataFellows.com

To be able to provide you with the best possible advice, we ask you to include the following information in your support request:

- The version number of F-Secure Anti-Virus you are using
- The version number of your operating system (DOS, Windows)
- Information about your computer: brand and model, amount and usage of memory, BIOS version, monitor type
- What kind of LAN you are using, the type of your network adapter, the network operating system's version number
- The types, names and version numbers of the device drivers used in your computer (mouse, SCSI etc.)
- A description of the problem: possible error messages given by F-Secure Anti-Virus, when does the problem to occur
- The contents of the computer's AUTOEXEC.BAT and CONFIG.SYS files, or a report given by MSD (MSD is a diagnostic program included in both DOS and Windows)

After you have installed F-Secure Anti-Virus, you can find a README file in the F-Secure Anti-Virus program group in the Windows Program Manager. The README file contains the very latest information, which you may find useful.

Licensing Agreement

The F-Secure Anti-Virus computer programs (software) are licensed, not sold, to you by Data Fellows Ltd (Data Fellows) for use only under the following terms. Data Fellows reserves any rights not expressly granted to you. You own the disks on which the software is submitted, but Data Fellows retains ownership of all copies of the software itself. The software is protected by copyright law.

You will receive a pre-specified number of base packages (normally one), which include the F-Secure Anti-Virus software with the proper documentation. In addition to this, you will receive a pre-specified number of additional manuals and one short user's guide, of which you can freely make copies for your use.

This License Allows You to:

1. Install and use the F-Secure Anti-Virus software only on the number of computers specified in the invoice you received with the software.
2. Extend the size of your F-Secure Anti-Virus license by purchasing additional licenses. The total number of computers using F-Secure Anti-Virus software is limited by the arithmetic sum of the sizes of the individual licenses you have purchased.
3. Create as many copies of the F-Secure Anti-Virus Setup disk as you need for installation and backup purposes.
4. Transfer the software and all rights under this license to another party together with a copy of this license and all written materials accompanying the software, provided that the other party reads and accepts the terms and conditions of this license. You loose the right to use the software and all other rights under this license when transferring the software.
5. You can freely install the software to the home computers of those employees that belong to the users of this software at the office. The installation may be done from either the delivered diskettes or from copies made of them according to the license conditions.

Other Terms:

1. After purchase you are provided with free updates and technical support for a pre-specified period of time. After this, the software can be updated for an annual fee.
2. The update interval is 1 to 3 months. A technical bulletin of the current virus situation will be annexed to each update. The updates will be delivered on a number of installation diskettes per base package to the persons registered as base package users.
3. If so requested, the updates can be delivered to a number of locations against a separate fee.

Restrictions:

1. You may not distribute copies of the software to another party or electronically transfer the software from one computer to another, if one of the computers belongs to another party.
2. The software contains trade secrets of Data Fellows and to protect them you may not decompile, reverse engineer, disassemble, or otherwise reduce the software to a human perceivable form.
3. You may not modify, adapt, translate, rent, lease, resell, distribute, or create derivative works based

upon the software or any part thereof. However, we want to encourage companies in providing value added services to F-Secure Anti-Virus customers. Please contact us directly if you are interested in the above mentioned activities.

Limited Warranty and Disclaimers:

Limited Warranty on Media. Data Fellows warrants the diskettes on which the software is recorded to be free from defects in materials and faulty workmanship under normal use for a period on thirty (30) days from the date of delivery. Any implied warranties on the disks, including implied warranties of merchantability and fitness for a particular purpose, are limited in duration to 30 days from the date of delivery. Data Fellows will, at its option, replace the diskette(s) or refund the purchase price of the diskette(s). Data Fellows shall have no responsibility to replace of refund the purchase price of a diskette damaged by accident, abuse, or misapplication.

Disclaimer of Warranty on Software. The software is provided “as is” without warranty of any kind. Data Fellows expressly disclaims all implied warranties, including but not limited to the implied warranties of merchantability and fitness for a particular purpose especially. Data Fellows does not guarantee the software or any accompanying written materials in terms of their correctness, accuracy, reliability, or otherwise. The entire risk as to the results and performance of the software and written materials is assumed by you.

Complete Statement of Warranty. The limited warranties provided in preceding paragraphs are the only warranties of any kind that are made by Data Fellows on this product. No oral or written information or advice given by Data Fellows, its dealers, distributors, agents, or employees shall create a warranty or in any way increase the scope of this warranty, and you may not rely on any such information or advice. This warranty gives you specific legal rights. You may have other rights, which vary from state to state.

Limitation of Liability. In no event will Data Fellows or its employees be liable to you for any consequential, incidental, or indirect damages arising out of the use of or inability to use the software or accompanying written materials. This includes damages for loss of business profits, business interruption and loss of business information. Data Fellows is not responsible for the software’s ability to repel a specific virus or for damages caused by an unsuccessful virus prevention.

The liability of Data Fellows to you for actual damages for any cause whatsoever is limited to the money paid for the software that caused the damages.

Termination:

This license is effective until terminated. It will terminate immediately without notice if you fail to comply with any of its provisions. 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. Disputes related to this license agreement will be dealt with in the district court of Helsinki, Finland.

Disclaimer

All product names referenced herein are trademarks or registered trademarks of their respective companies. Data Fellows Ltd. disclaims proprietary interest in the marks and names of others. Although Data Fellows Ltd. makes every effort to ensure that this information is accurate, Data Fellows Ltd. will not be liable for any errors or omission of facts contained herein. Data Fellows Ltd. reserves the right to modify specifications cited in this document without prior notice.

Companies, names, and data used in examples herein are fictitious unless otherwise noted.

Glossary of Terms

access control

archive file

Autoexec.bat

background task

BAT file

BIOS

booting

boot sector

boot sector virus

CMOS

cold boot

Config.sys

CRC

device driver

disinfection

exit code

FAT

file server

Heuristic Analysis

latency period

MBR

Path

partition table

search string

SMS

SNMP

time bomb

timestamp

Trojan Horse

TSR

warm boot

worm

write-protection

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.

archive file

A file compressed to an archive by an application designed for that purpose, such as Arj or PKZip. Since packed files cannot be directly read or executed in the archive form, they must first be extracted to their normal form in order to perform operations on them.

Autoexec.bat

A command string file that is automatically executed when a DOS computer is started. Autoexec.bat contains, among other things, the run commands for automatically executable files and parameters for environment variables.

background task

Task executed by the system but not shown in the foreground window (running but not visible).

BAT file

File containing DOS commands used for automating repetitive tasks.

BIOS

Basic Input/Output System. The part of the operating system that takes care of the most hardware-specific tasks. This part is stored on ROM on most PCs.

booting

The start-up of a computer. During start-up, the computer reads the SETUP information after which it loads the operating system into memory either from a diskette or from a hard disk. The programs defined in the files Autoexec.bat and Config.sys are also executed.

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 like, for example, MS-DOS.

boot sector virus

A virus that hides its code in the boot sector of a disk or a diskette and which is therefore automatically executed when a computer is turned on. Most boot sector viruses stay active in memory after their execution.

CMOS

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

cold boot

To restart the computer by cycling the power.

Config.sys

A text file that is automatically read when the computer is booted. Contains the run commands for device drivers and parameters for the hardware.

CRC

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

device driver

A program that controls devices, such as the hard disk and the mouse. The start-up commands for device drivers are usually stored in the Config.sys file for automatic execution during the computer start-up.

disinfection

A function of F-Secure Anti-Virus, which cleans files, boot sectors, and the like of viral code. After disinfection, the functioning of the cleaned objects is restored. If viruses have corrupted their victims' data during infection, disinfection is not possible.

exit code

A code string, usually a number or a number sequence a program transfers to the operating system when it terminates its execution. The exit code generally relays information about the program execution and the termination status, for example, whether the execution has terminated normally or not.

FAT

File allocation table. The allocation table used with the DOS operating system. FAT contains information about the location of files and bad (unusable) sectors on a disk.

file server

A network-connected computer, on which data and applications shared by the network users are located.

Heuristic Analysis

One of the virus scanning methods. A Heuristic Analysis search is based on identifying viruses by their functional characteristics, and not by their search strings among normal program code.

latency period

A phase between initial infection and the activation of a virus. During this period the virus does nothing else but infects more victims.

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.

Path

An environment variable that indicates the directories which are searched when an execution command is given.

partition table

Part of the main boot record (MBR) of a hard disk. Contains information on how the physical disk is divided (partitioned) into logical entities.

search string

A character string belonging to a virus.

SMS

Microsoft Systems Management Server. An administration tool used for installing and updating software components on Windows platforms.

SNMP

Simple Network Management Protocol. A standard protocol which enables centralized management of hardware and software from a number of vendors in a heterogeneous network.

time bomb

Destructive action triggered at some specific date or time.

timestamp

The creation or last modification time recorded for an object.

Trojan Horse

A program in which a trap is hidden inside normal program code. These traps are sprung by triggers defined beforehand and perform functions that, from a user's point of view, are usually unpleasant.

TSR

Terminate and stay resident program. A program which after its execution stays active in memory as a background program.

warm boot

To restart the computer without cycling the power.

worm

Parasitic program capable of replication by inserting copies of itself into machines in a network.

write-protection

A protection of diskettes that prevents writing on them.