F-PROT Professional

Windows 3.1
Windows 95
Windows NT
DOS

Anti-Virus and Data Security Toolkit

User's Guide

Technical support: http://www.DataFellows.com/f-prot/support/
Your local contact: F-PROT-<country>@DataFellows.com
Data Fellows direct: Anti-Virus-Support@DataFellows.com

Please see “Technical Support” on page 17 for more information about your technical support options.

1 Welcome!

Welcome to F-PROT Professional for Windows from Data Fellows. This easy-to-use anti-virus toolkit will protect your computer from virus infections, giving you peace of mind by ensuring that your valuable data is safe.

In developing F-PROT products we place special emphasis on the following issues:

- Centralized administration and maintenance capabilities
- Transparency for end user
- Real-time protection
- Wide support for operating system and hardware platforms
- Treating anti-virus as an integral part of the customer's total data security solution
- Making a lasting commitment to our customers

We feel that Anti-Virus is more of a service concept rather than just another software product. We have built our global partner network around technical competence instead of just logistical capabilities. We can provide unarguably the best global solution with support for a large number of languages and expert local technical support in all major countries.

We believe the only workable anti-virus architecture must be based on background real-time anti-virus being deployed automatically throughout the organization and administered remotely with efficient industry standard network mechanisms.

F-PROT Pro for Windows covers the most commonly used operating systems; Windows 3.X, Windows 95, Windows NT and DOS. As outlined in F-PROT Professional Product Architecture (available from www.DataFellows.com) F-PROT provides you with a consistent feature set for every platform:

- Real-time protection – Gatekeeper
- On demand scanning
- System and network management features
- Other utilities such as recovery from a crashed disk

Computer viruses are one of the most potentially harmful threats to the security of information on workstations and personal computers. The number of viruses has increased from only a handful several years ago to thousands today. While some viruses are only harmless pranks, others have been programmed to destroy data and thus do pose a real threat.

A computer virus is a parasitic program capable of independently replicating itself. Viruses attach themselves to other programs, boot sectors of hard disks and diskettes, or to application macros of document files. All viruses are harmful, whether they contain instructions to purposefully destroy data, slow down the system, or cause some other kind of damage, or whether they simply consume disk space and make the system less reliable.

Many anti-virus experts recommend that the way to remove a virus from the disk is to delete the infected programs and re-install them from original write-protected setup disks, or restore them from a recent, clean backup. Such radical disinfection is not necessarily practical. If the virus is a boot sector infector, there are no files which you could re-install; if it is a macro virus, you will risk losing the contents of the documents where the macros are stored. Even with a normal program virus, disinfection using the original setup disks or backup tapes may be tedious because of the sheer number of files requiring re-installation.

F-PROT includes comprehensive disinfection features which help you recover from a virus effortlessly. The disinfection works by finding the viral code from within the infected programs, documents or boot sectors, and removing that code. The system is restored to its original, clean state.

F-PROT will help you eliminate the risk of virus infection. When a virus is discovered, this efficient anti-virus tool removes it and prevents data loss.

1.1 What's New in F-PROT Professional 3.0?

- F-PROT 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-PROT, including a large library of technical information for the administrator and continuously updated virus descriptions, updates and support for the end user
- 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
- New Tool Tips orient the new user to the F-PROT Professional interface
- The new F-PROT 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-PROT 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

1.2 About This Guide

This guide describes F-PROT Professional for Windows 3.1, Windows 95, and Windows NT. It discusses F-PROT Professional for Windows systems in general and mentions a specific operating system only where it requires special consideration. For information about F-PROT Professional for OS/2, please refer to the F-PROT Professional for OS/2 manual.

This guide is divided into the sections summarized below, progressing from an overall tour of F-PROT Professional toward further practical depth. The final sections are intended primarily for administrators and advanced users, with auxiliary information about viruses, anti-virus mechanisms and installation, and F-PROT Professional for DOS.

- **Welcome!** This section includes an easy-read Quick Start guide to help you get F-PROT installed and working immediately, and technical support contact information in case you have any questions.
- **Using F-PROT Professional** gives a guided tour around F-PROT Professional and describes its features, along with instructions for use. Signs of possible infection are listed and instructions outlined on disinfecting the virus under various operating environments. First you will find the main features listed and explained, and then you will be shown how to use them in the protection of your systems and data. This section will help you to take full advantage of F-PROT's capabilities.
- **Administering F-PROT Professional** describes the administrative tasks and the tools available. It contains an overview of the program for the network administrator in a network environment.
- **Appendix A: Background Information on Viruses** provides background information on viruses in general. It describes some of the most common virus types and their working mechanisms.
- **Appendix B: F-PROT Professional Structure** characterizes the structure of files and directories in F-PROT Professional, and their naming conventions.
- **Appendix C: Microsoft Systems Management Server** describes how F-PROT can be installed through the Microsoft Systems Management Server (SMS) to all kinds of Windows environments:
- **Appendix D: Autoinst Configuration** describes the format of Autoinst.INI, the configuration file for the F-PROT Autoinst installation tool.
- **Appendix E: F-PROT Professional for DOS** contains information about using F-PROT Professional for DOS.
- **Glossary** - A list of helpful words and concepts especially designed for new users.

1.3 F-PROT Quick Start

This section provides a “crash course” on how to get the program installed and working.

☞ **In this section, any reference to administrator only applies to users running F-PROT installed with network functionality.**

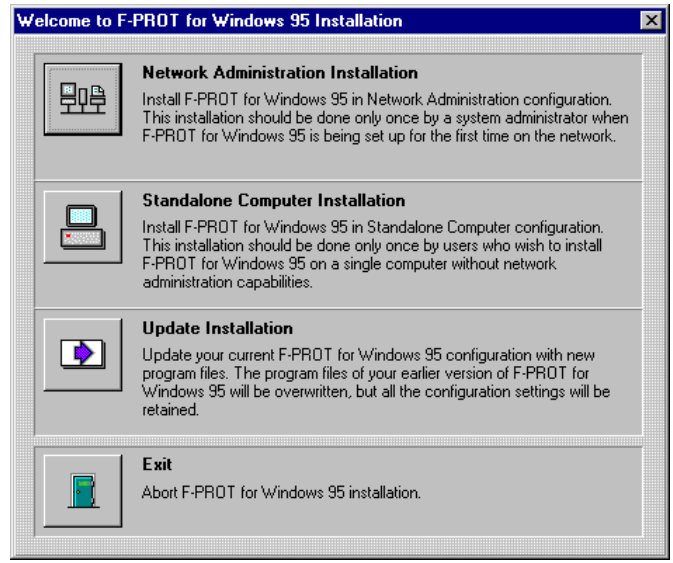
Installing F-PROT Professional

The following steps will help you install F-PROT. Before starting installation, close all running Windows applications.

Insert the F-PROT Professional installation disk number one into the diskette drive.

If you are running Windows 95 or Windows NT 4.x, click the **Start** button, point to **Settings,** and click the Control Panel icon. Once in the Control Panel folder, double-click the Add/Remove Programs icon, choose “Install”, and Setup.exe will be located automatically in one of your diskette drives. If Setup.exe has not been located automatically, click **Browse** and select the location of the Setup.exe file. Click **Finish,** and installation of F-PROT will begin. Alternatively, choose **Run** from the **Start** menu, and type in the path and name of the Setup.exe file, for example, A:\Setup.

In Windows 3.1 or Windows NT 3.x, choose **Run** from the Program Manager **File** menu and type in the path and name of the Setup.exe file, for example, A:\Setup.exe.



In the "**Welcome to the F-PROT Professional Installation"** dialog box there are four options to choose from:

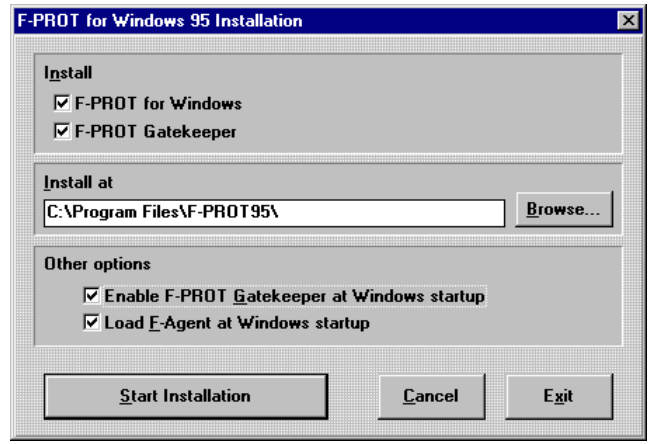
- Network Administration Installation
- Stand-Alone Computer Installation
- Update Installation
- Exit

Network Administration Installation

If you are the administrator of a network of computers, install F-PROT on the administration workstation using the **Network Administration Installation** option. Then, make necessary changes to the settings and distribute the program to your network's users. For more information on this topic, see "Distributing F-PROT Installations" on page 82.

Stand-Alone Computer Installation

Choose the Stand-Alone Computer Installation option if you are installing F-PROT for the first time on any computer which is not connected to a network.



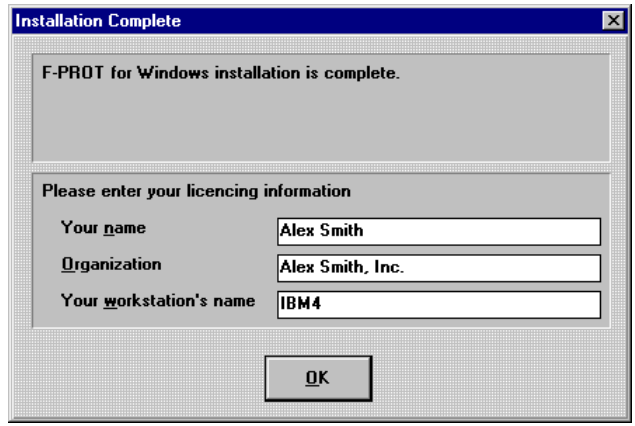
Make sure that the check boxes **F-PROT Professional** and **F-PROT Gatekeeper** are both marked if you are installing both programs. F-PROT Gatekeeper is the program providing dynamic protection against viruses. It functions transparently in the background, looking for viruses whenever you access files or diskettes. If you would like to install only one of the programs, leave its corresponding check box selected, and click the other check box to clear it.

Then, specify the name of the destination directory for F-PROT installation. The default destination directory is usually a good choice. Click **Browse** to search for the required directory on the computer drives, if needed.

The **Load F-Agent at Windows Startup** check box is selected by default, which causes F-Agent to start automatically together with your Windows session. F-Agent is needed for executing the scheduled F-PROT scans, and can also be used for changing F-PROT Gatekeeper settings, if needed.

Click **Start Installation**. You can quit installation by choosing **Exit**. Clicking **Cancel** will return you to the previous screen.

When the installation is otherwise complete, the program will ask for your name, the name of your organization, and your workstation’s name, which are shown in the report files for identification.



After you have entered the names and clicked OK, the installation will be completed. Under Windows 3.1, if you included F-PROT Gatekeeper in the installation, the dialog box will be displayed, asking whether you would like to have Windows restarted in order to make the F-PROT Gatekeeper driver active.

Choose between the **Restart Windows Now** and **Don't Restart Now** options. The F-PROT program folder will be created with the icons for F-PROT Professional, F-Agent, and the ready-made tasks. If F-Agent was specified to be loaded at start-up, Setup will add its icon to the Startup folder.

Update Installation

Choose this option if you already have F-PROT installed on your computer. This option will allow to update program files of F-PROT , while preserving your original settings.

Special Considerations for Windows NT

Under Windows NT, the setup program needs administrative rights in order to install the F-PROT Gatekeeper device driver in the system. This means that the very first installation of F-PROT must be done under an account that has administrative rights on the workstation. The account you use for your day-to-day work may or may not have these rights, depending on the security settings made by your system administrator.

F-PROT Professional for Windows NT contains built-in features to ensure that updating an already-installed copy of F-PROT can usually be done using a normal account that has no administrative rights in the system.

See the documentation that came with your Windows NT license for information about the access rights.

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.

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-PROT 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-PROT.

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:\F-PROT.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-PROT 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-PROT with the following parameters:

```
F-PROT.EXE /HARD /ALL /DISINF
```

and press [ENTER].

F-PROT removes the virus and gives you a short report of the results.

☞ **If you run into problems, point your browser to the F-PROT Support Center at http://www.DataFellows.com/f-prot/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.

Scanning for Viruses

The F-PROT 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.

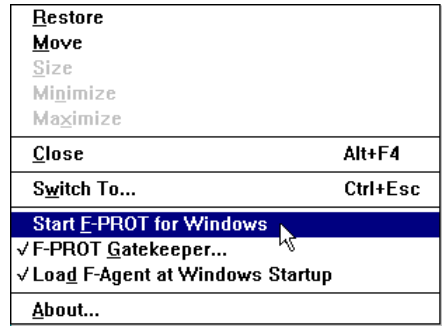
For additional protection, you can run the F-PROT interactive virus scanner and search for viruses on the hard disk, floppy disks, CD-ROMs, and network disks. You can even automate the scanning by saving the necessary settings as a task and scheduling the task to run periodically.

Launching F-PROT Professional

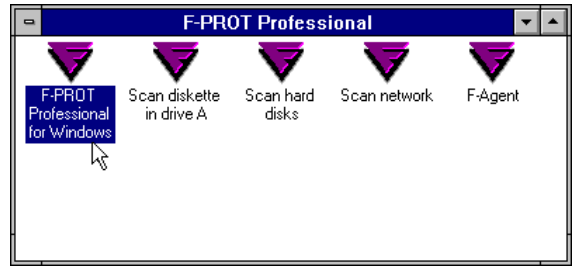
To start F-PROT , double-click the F-PROT icon in the taskbar which is available under Windows 95 and Windows NT 4.0.

If you're not running F-Agent, choose F-PROT Professional 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-PROT for Windows command from the menu.



If you're not running F-Agent, double-click the F-PROT icon in the F-PROT Professional program group in Program Manager.



F-PROT Professional 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-PROT 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-PROT program group or the Windows 95 and Windows NT 4.x Start menu.

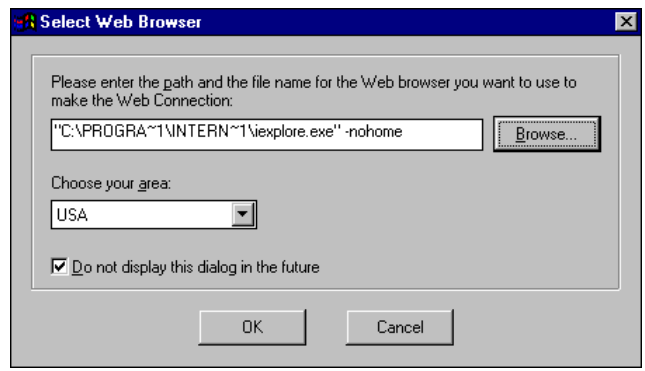
You can also perform scans by dragging and dropping files and directories into the F-PROT window, or on top of the F-PROT or F-Agent icon on the desktop. The dropped objects will be scanned automatically.

1.4 Technical Support

Data Fellows Technical Support is available on the World Wide Web, through electronic mail and online through your F-PROT client. If you suspect that your computer is infected with a virus, please see “What to Do When a Virus Is Found” on page 59 for more information.

Web Club

The F-PROT Professional Web Club provides help and assistance to F-PROT 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/f-prot/webclub/

For advanced support, the F-PROT Professional Support Center is available on the web:

- http://www.DataFellows.com/f-prot/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-PROT license, you get free technical support through email. Please contact the F-PROT Professional reseller from whom you bought your F-PROT Professional license for basic technical assistance, at:

- F-PROT-<yourcountry>@DataFellows.com
- Example: F-PROT-Japan@DataFellows.com

If there is no authorized F-PROT Professional 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-PROT 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-PROT, 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-PROT, you can find a README file in the F-PROT program group in the Windows Program Manager. The README file contains the very latest information, which you may find useful.**

2 Using F-PROT Professional

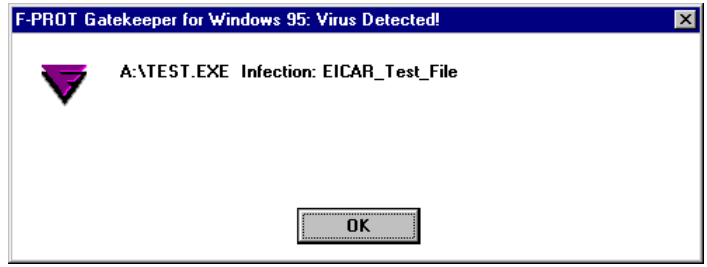
This section gives a guided tour around F-PROT Professional and describes its features, along with instructions for use. Signs of possible infection are listed and instructions outlined on disinfecting the virus under various operating environments. First you will find the main features listed and explained, and then you will be shown how to use them in the protection of your systems and data. This section will help you to take full advantage of F-PROT's capabilities.

2.1 Constant Guard with F-PROT Gatekeeper

The F-PROT 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.

F-PROT Gatekeeper

F-PROT 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-PROT Gatekeeper will automatically display a warning:

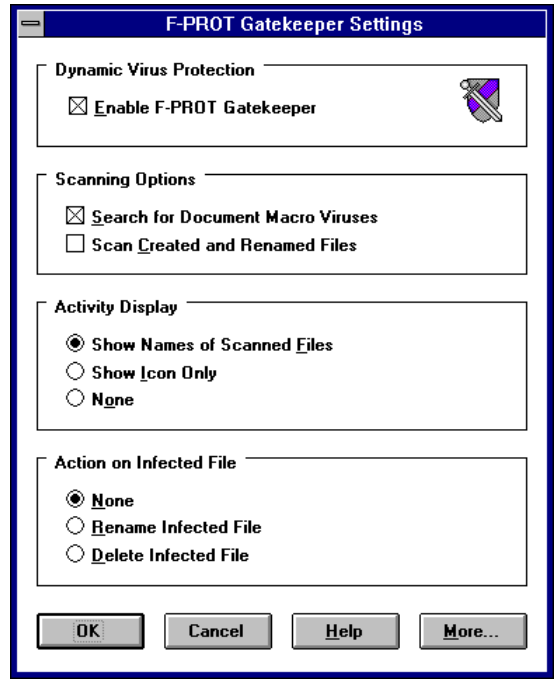


To check whether F-PROT Gatekeeper is active, open the **F-Agent** menu. If the **F-PROT Gatekeeper…** item on this menu is checked, then the Gatekeeper is active.

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

F-PROT Gatekeeper Settings

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



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

- Enable or disable F-PROT Gatekeeper.
- Set the F-PROT 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-PROT Gatekeeper Technical Information

F-PROT 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-PROT 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.

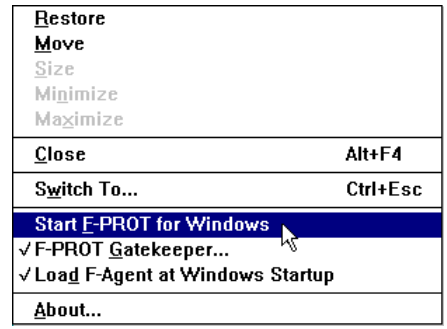
F-PROT Gatekeeper monitors also disk operations. It checks the boot sectors of the diskettes used in the computer, first when a diskette is inserted in the diskette drive and subsequently each time something is read from the diskette or written to it.

F-PROT 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-PROT tasks, thus eliminating the need for F-PROT to remain active all the time. In case of a network installation, F-Agent also provides communication between individual workstations and the F-PROT 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-PROT for Windows**, **F-PROT Gatekeeper…**, and **Load F-Agent at Windows Startup**.

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

If F-PROT Gatekeeper is installed, the **F-PROT Gatekeeper…** command of the **F-Agent** menu can be used to enable F-PROT 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.

2.2 Using the Toolbar and Task List

The F-PROT interface has two display modes: toolbar and 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-PROT you need most often.

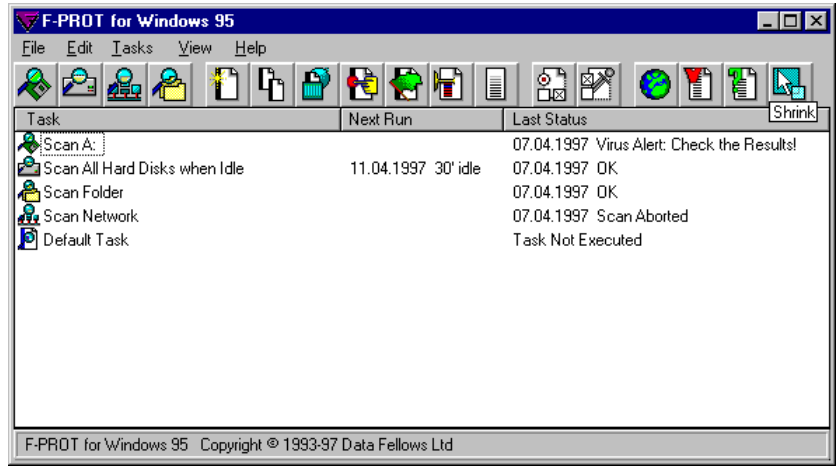
The default buttons on the toolbar give shortcuts for the following actions:

- 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-PROT Professional settings
- Edit settings of F-PROT Gatekeeper
- Connect to F-PROT Web Club
- View virus descriptions
- Access online help
- Toggle between Toolbar and Task List modes

In addition, almost any F-PROT 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-PROT Professional 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-PROT Professional 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.

2.3 Working with Scanning Tasks

F-PROT 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-PROT 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.

Task Management

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

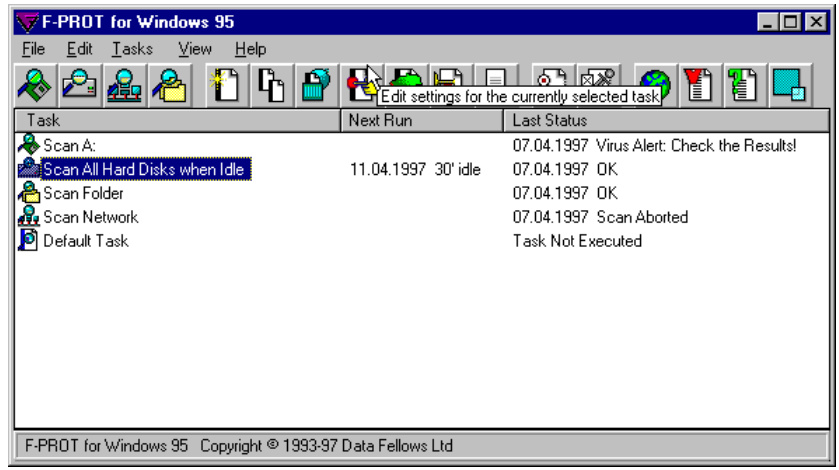
- Scan Drive A:
- Scan Hard Disks
- Scan Network Drives
- Scan a Folder

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

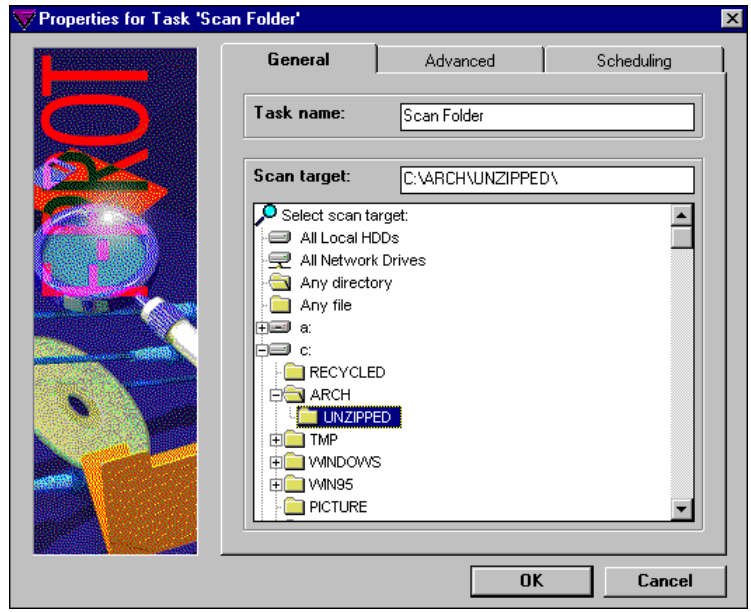
To customize tasks and create tasks, you may edit the parameters of a pre-configured task or create an entirely new task. To edit tasks or to create new tasks, first display the tasklist by either clicking **Enlarge** on the toolbar, or choosing **Enlarge to Tasklist** from the **Edit** menu.

Editing Task Parameters

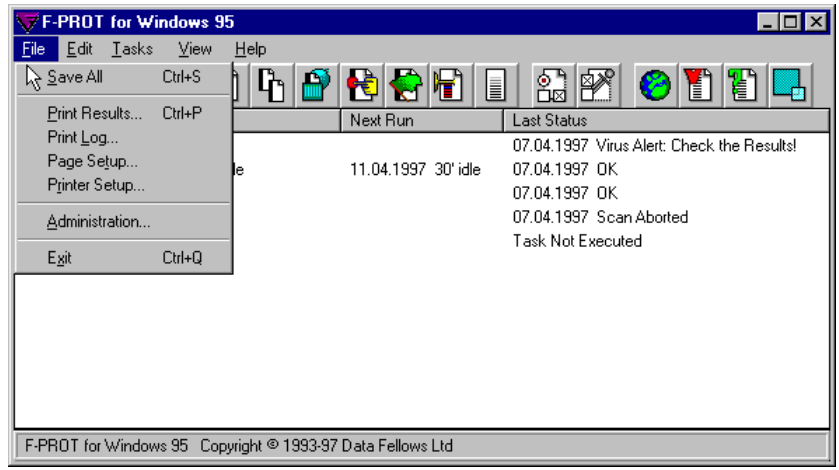
An existing task can be modified by double-clicking on it in the task list, or by selecting it on the task list and then either pressing Alt+Enter or clicking **Edit settings** button on the toolbar. Another option is to select the task on the task list and then to choose **Settings** from the **Tasks** 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” on page 28 for more information.

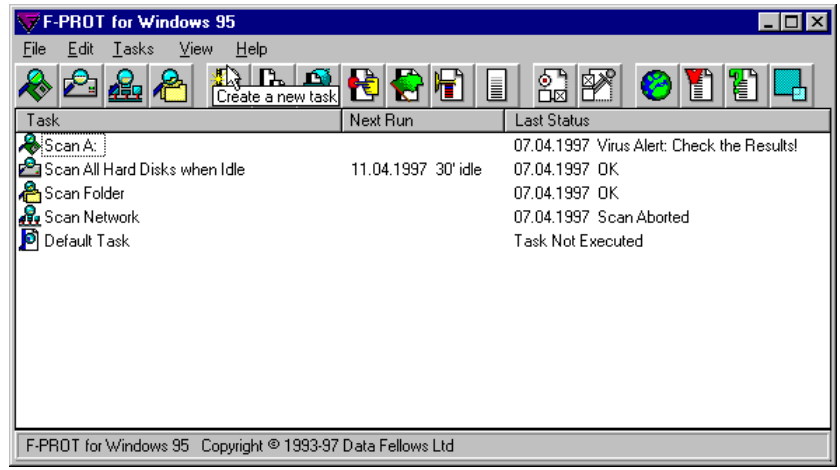


Copying Tasks

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-PROT Professional 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-PROT Professional 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-PROT Professional. 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-PROT Professional will request a confirmation.

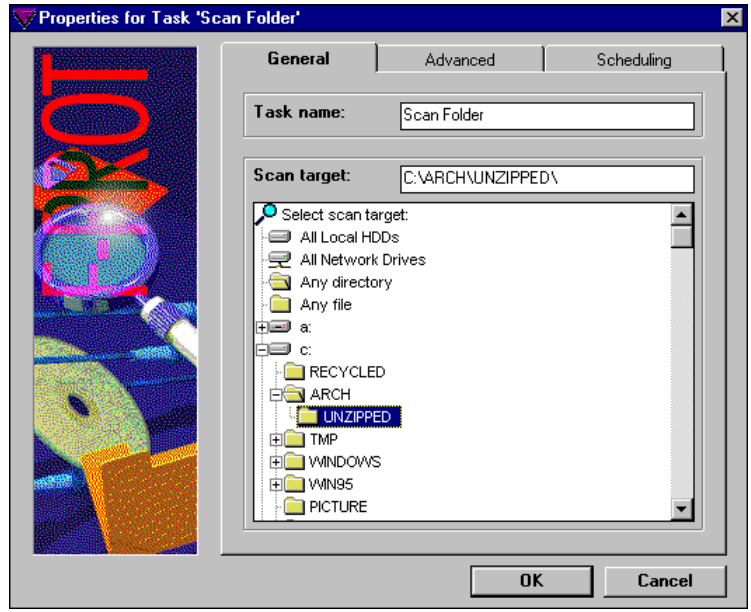
Task Properties and Scheduling

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**.

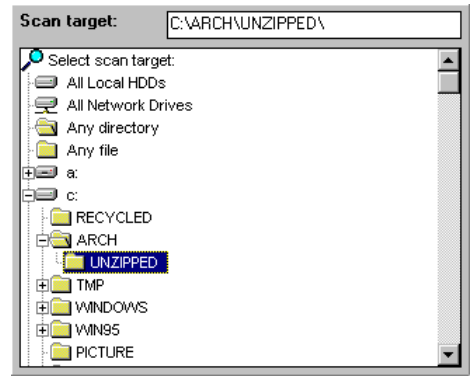
General Properties

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



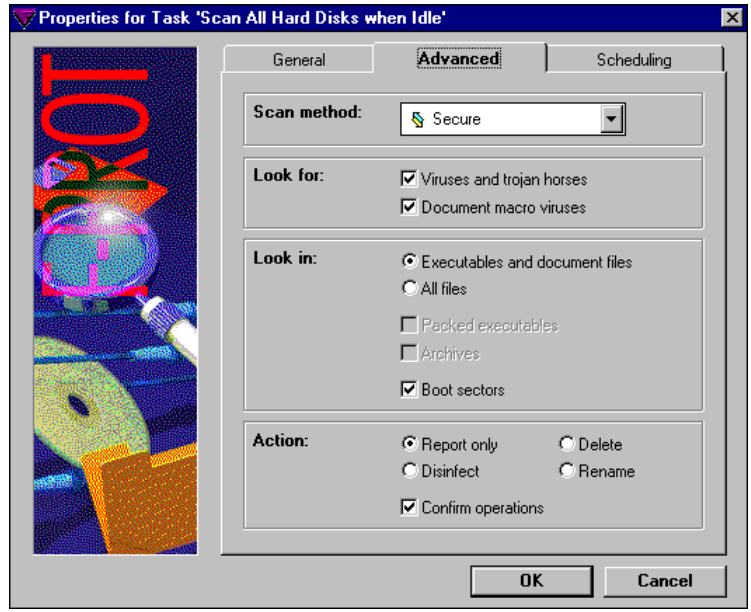
The **Task Name** is given in the upper box of the **General** page. If needed, delete the current entry and type in the task name of your choice.

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.

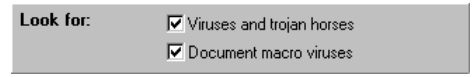


Advanced Properties

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

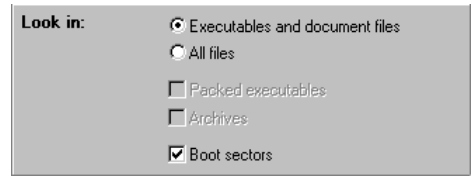


The first item to be defined is the **Scan method**. The menu normally includes the Secure Scan option. Secure Scan is a very reliable tool in searching for known viruses and their new variants.



Under **Look for,** you can specify the viruses which F-PROT Professional 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-PROT 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-PROT Professional 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.

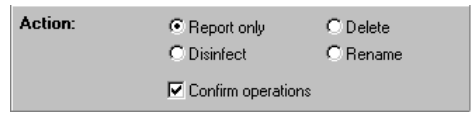
Use the **Archives** option to scan inside several archive file formats such as files compressed with the ZIP and LZH algorithms. In order to scan inside compressed files you must check the "Look in Archives" checkbox in the "Advanced" page of the task properties dialog. If "Look in Executables and document 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/f-prot/support/compressed-file-formats.htm

If the **Boot Sectors** box is selected, F-PROT Professional 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-PROT Professional on infected files when it finds a virus.



The following four choices are available:

- **Report Only**. If this option is selected, F-PROT 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-PROT will attempt removing viruses from the infected files or boot sectors. F-PROT Professional 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.

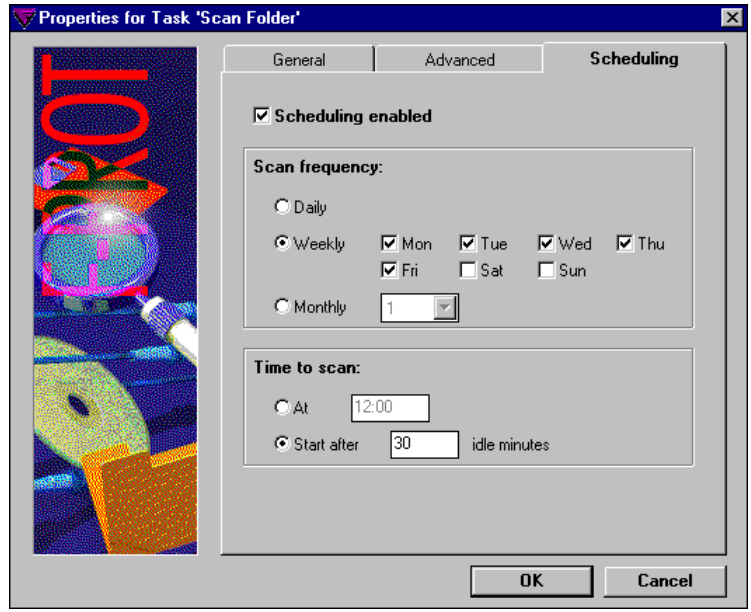
If the **Confirm operations** check box below is selected, F-PROT Professional will ask for confirmation before doing anything to infected files. If the task was started interactively, F-PROT Professional will ask for confirmation every time a virus is found. In case of a scheduled task, all the confirmations 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-PROT Professional will proceed with disinfection, deletion and renaming files without asking for confirmation.

F-PROT Professional 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.

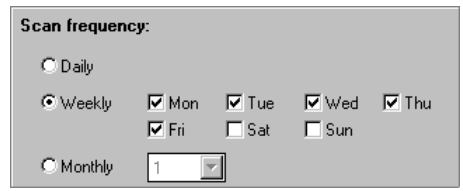
Schedule Properties

Tasks can be scheduled for execution at specific times. In order to have the scheduled tasks executed without running F-PROT Professional, 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-PROT Professional 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.

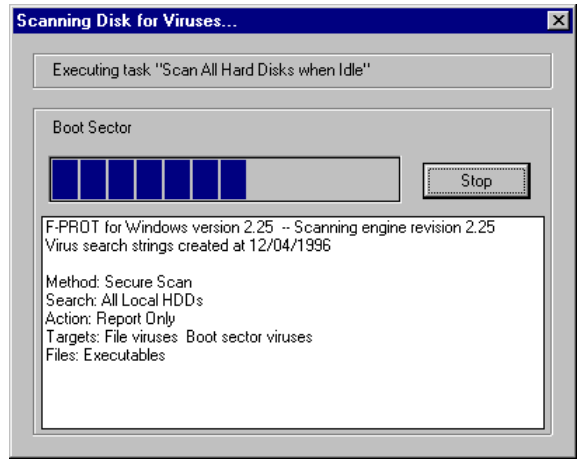
Executing a Task

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-PROT, 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.

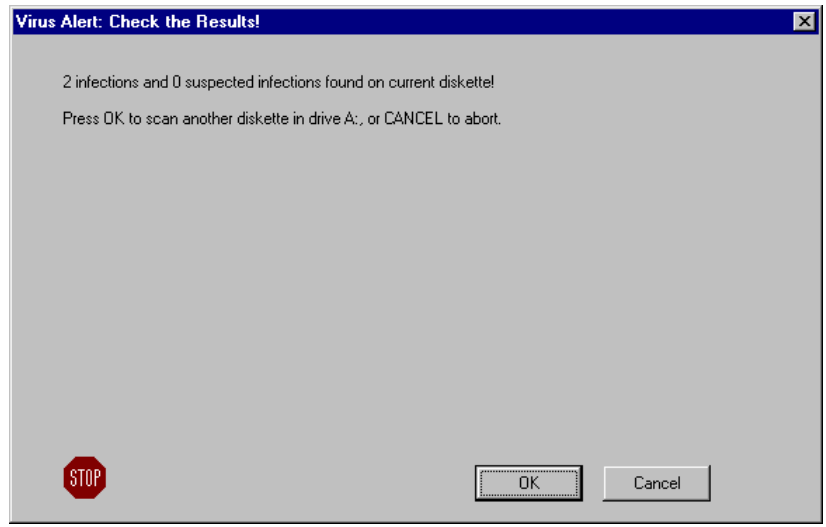


A task may be aborted at any time by clicking **Stop** in the dialog box. The program will ask for confirmation before terminating scan.

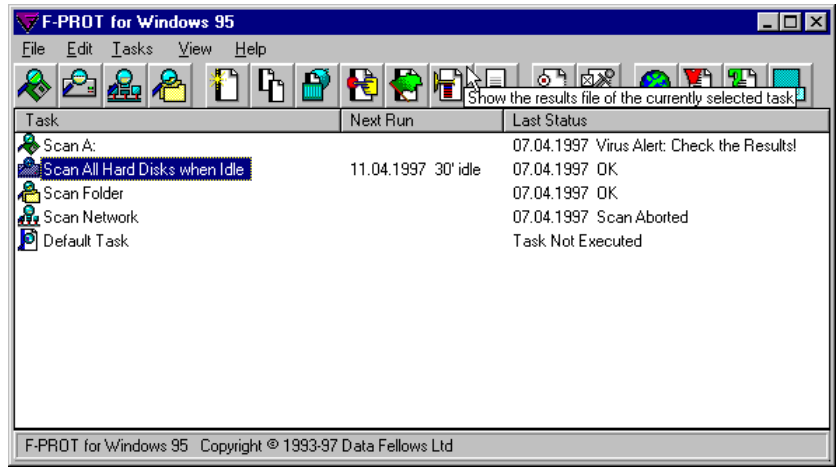
Viewing Task Results

Viewing Task Execution Reports

After executing a scanning task, F-PROT Professional produces a report on the task results. If a virus is found, 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-PROT is executing scans in its minimized mode.

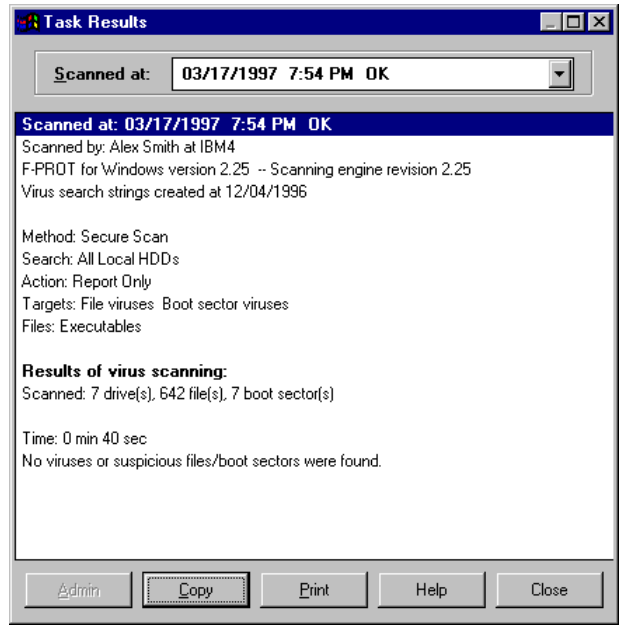


To view a results report, switch from the toolbar to the task list mode. To do this either select **Enlarge to Tasklist** from the **Edit** menu or click **Enlarge** on the toolbar.



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.

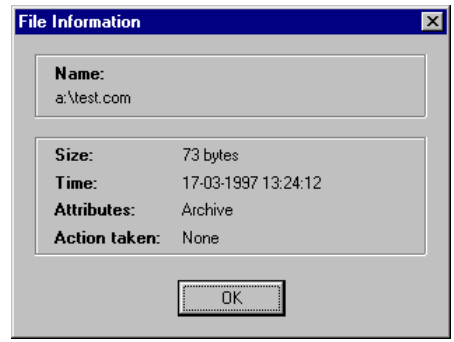


Each task result report shows the execution time and results of a specific executed task at the latest scan or the preferred number of scans, and includes the name of the user, the name or ID of the workstation, and the version of F-PROT Professional.

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-PROT World Wide Web server. Choose **Virus Descriptions on the Web** from the **Help** menu to access the server. For background information, see “Appendix A: Background Information on Viruses” on page 103.

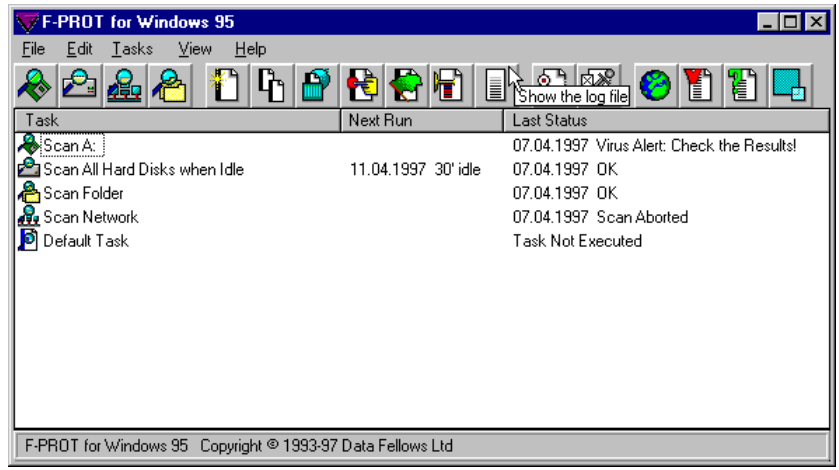
General information about the infected file can be obtained by double-clicking on its name in the report, which opens the **File Information** dialog box. In this dialog box, the file’s size, attributes and creation time are shown.



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**.

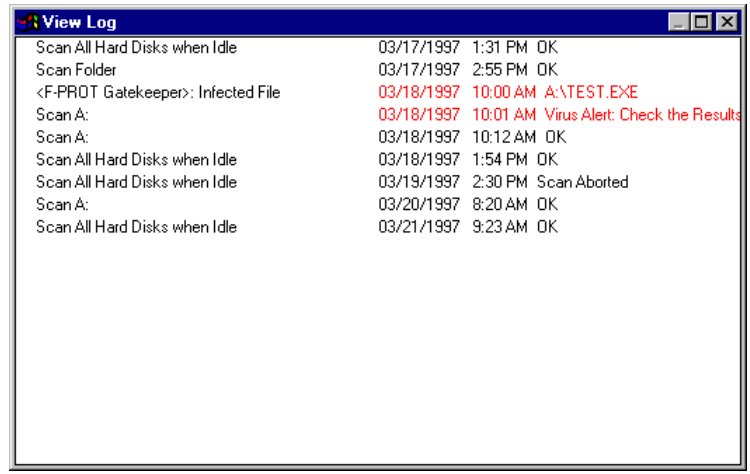
Viewing the Scan Log

Information about the executed tasks and F-PROT 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-PROT 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.

2.4 Setting F-PROT Preferences

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

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

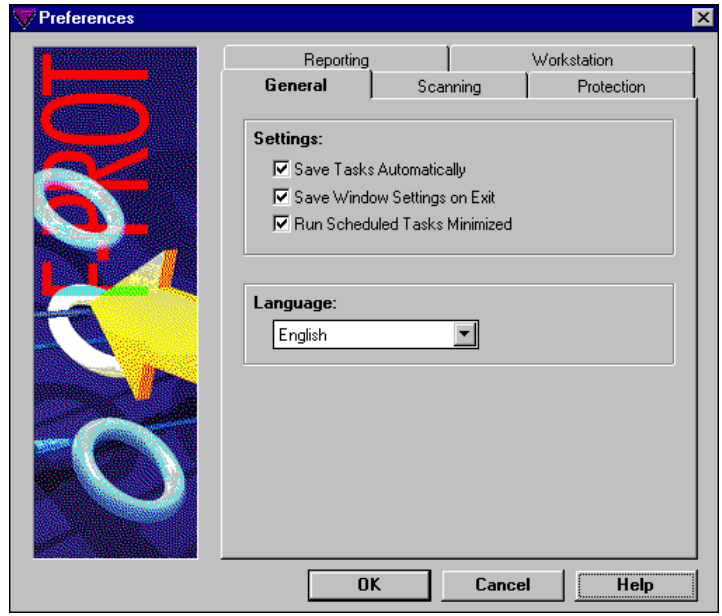
To access the **Preferences** dialog box, choose **Preferences** from the **Edit** menu or click the **Open the Preferences dialog** button on the toolbar. Once the **Preferences** dialog box is displayed, click on the tab corresponding to the Preferences you would like to modify. The following Preferences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

General Preferences

Use the **General** Preference dialog box to define the ways in which F-PROT Professional operates.



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

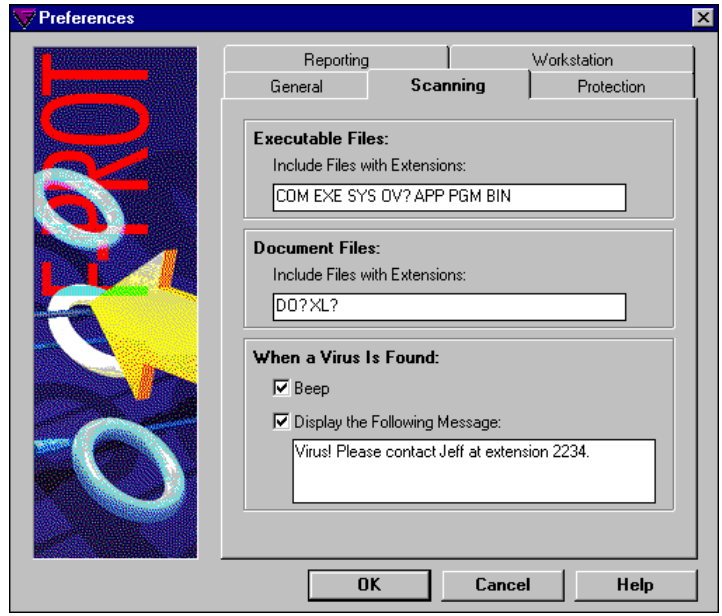
The **Save Window Settings on Exit** check box, if selected, causes F-PROT Professional to save the location and settings of its main window when it is closed. The next time the program is started, it starts in the same mode as in the end of its previous session. By default, this check box is selected.

The **Run Scheduled Tasks Minimized** check box, if selected, makes all the scheduled F-PROT Professional 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-PROT usage, and to specify the way, in which F-PROT Professional informs you about the detected viruses.



In the **Executable Files** box select the extensions of the files, which F-PROT Professional 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-PROT Professional 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.

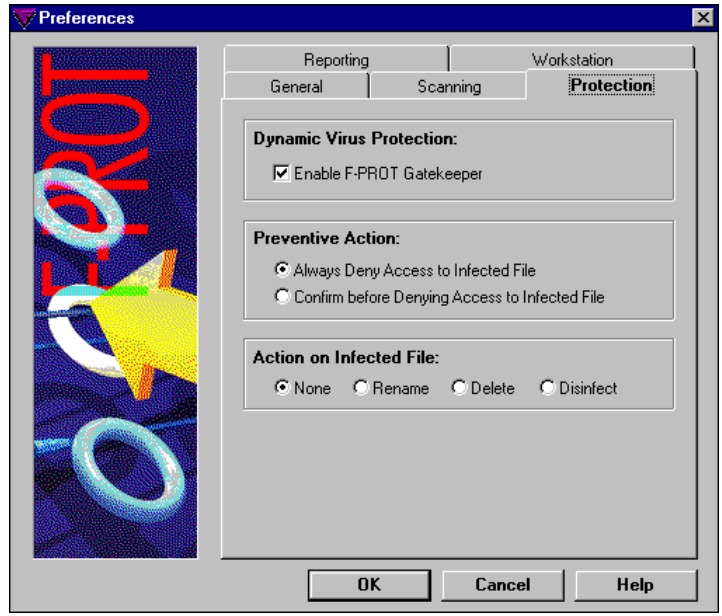
Under **When a Virus Is Found,** select the type of notification in the event a virus is found. Instruct the computer to beep by selecting the **Beep** check box. If you wish to have a message displayed, select the **Display the Following Message** check box and type in the message to be displayed when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

To test the functionality of Scanning Preferences, see the section, “The EICAR Test File”.

Protection Preferences

In the **Protection** Preference, you can enable and configure F-PROT Gatekeeper. F-PROT 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-PROT 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-PROT administrator.

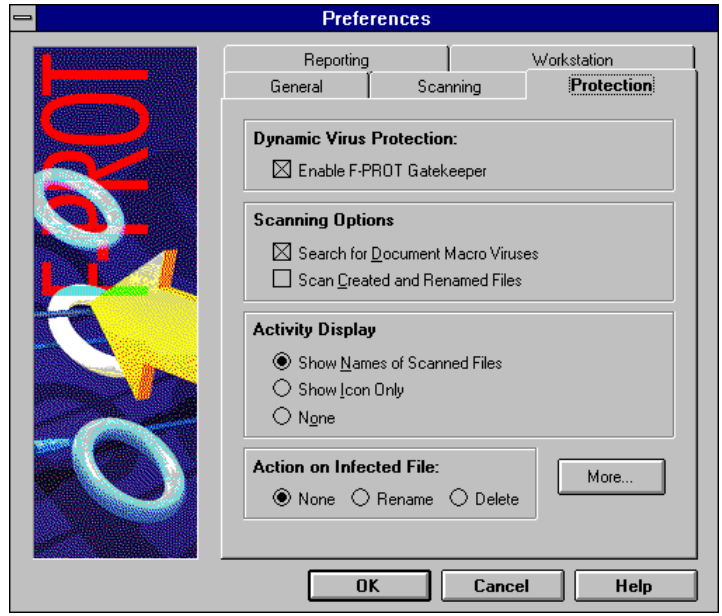


Select the **Enable F-PROT Gatekeeper** check box under **Dynamic Virus Protection** to activate F-PROT Gatekeeper. If this check box is selected, the other options of the dialog box become available.

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-PROT 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-PROT Professional for Windows 3.1, the "**Protection** Preferences" dialog box is a little different. Below are the instructions on using the **Protection** Preferences in F-PROT Professional 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-PROT 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-PROT Professional for Windows 3.1 offers the available choices for the actions taken by F-PROT Gatekeeper on the infected files. Click either

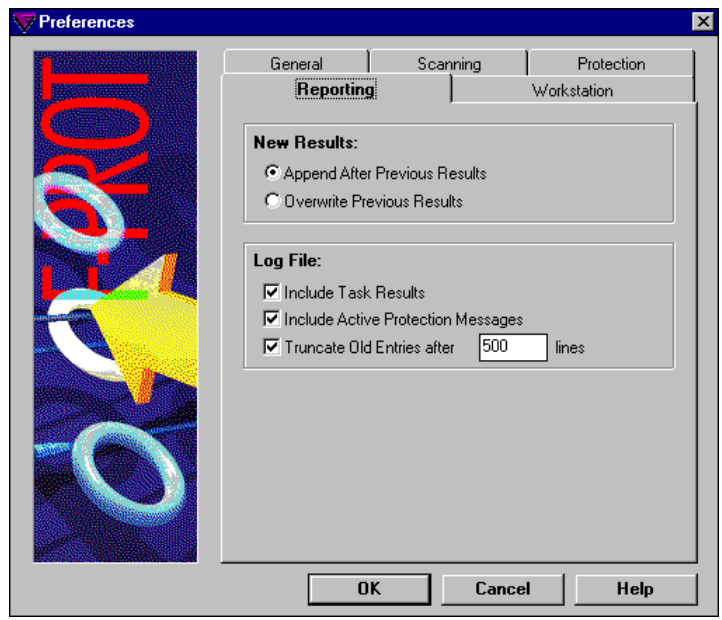
of the following: **None,** to take no actions except for notifying; **Rename**, to rename the infected file; and **Delete** to delete the infected file.

The **Protection Preference** dialog box in F-PROT Professional for Windows 3.1 includes the following **Scanning Options** for F-PROT 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.

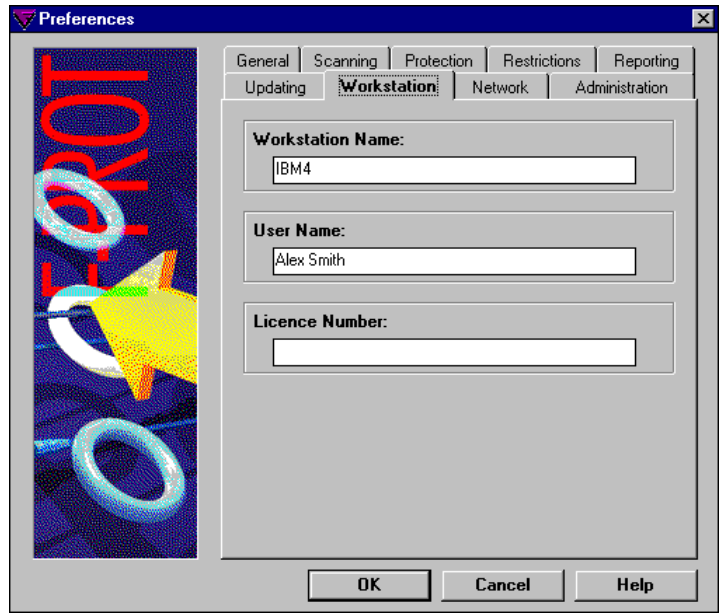


Under **New Results**, select the way in which F-PROT Professional will store the task results reports. Select either **Append After Previous Results**, if you wish to keep the previous results reports saved, or **Overwrite Previous Results**, if you do not need to keep the previous results reports. 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-PROT Professional 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-PROT 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-PROT Professional, the names are needed to communicate with the F-PROT administrator.

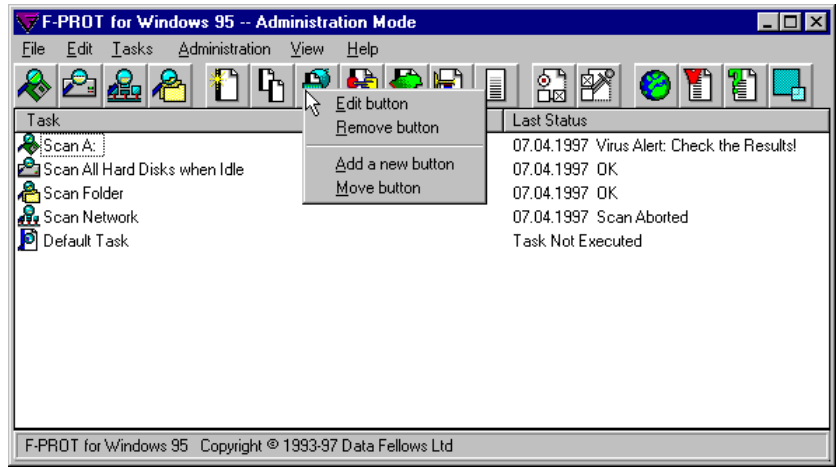
2.5 Modifying the Toolbar

The F-PROT 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-PROT Professional settings
- Edit settings of F-PROT Gatekeeper
- Connect to F-PROT 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.

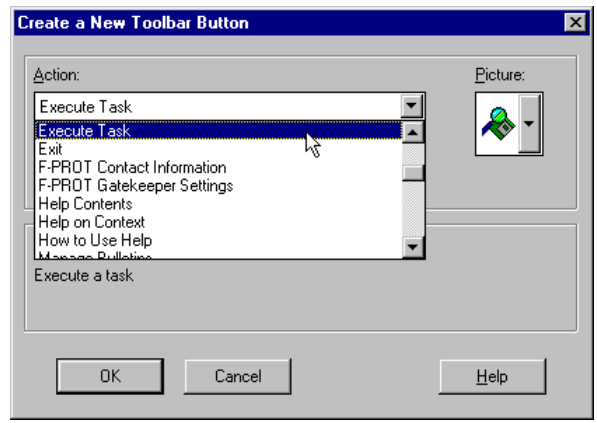
Additionally, you can create custom shortcut buttons to suit your particular needs. Almost any function can be linked to a specially created button.



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.



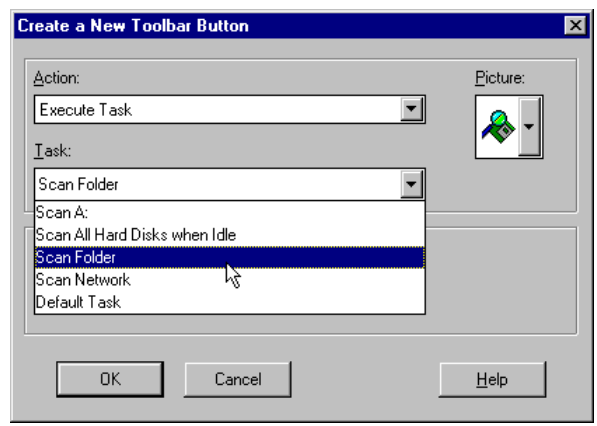
On the **Picture** list, choose the picture for the new button.

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

Action	Function
About F-PROT	Shows the F-PROT Professional splash screen.
Administration Mode	Begins/ends administration mode.
Administrator Help on Web	Connects to Administrator FAQ page on F-PROT Web server.
Delete Task	Deletes the currently selected task.
Distribute Task	Distributes the selected task. Enabled only when F-PROT Professional 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-PROT Professional.
F-PROT Contact Information	Shows contact information for your F-PROT vendor.
F-PROT Gatekeeper Settings	Allows to edit settings of F-PROT 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-PROT Professional 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-PROT Professional is in administration mode.
Start Task	Executes the currently selected task.
Undistribute Task	Removes the selected task from local workstations. Enabled only when F-PROT Professional is in administration mode.
View Infected Files	Opens a dialog where infected files may be viewed. Enabled only when F-PROT Professional 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-PROT Professional is in administration mode.
View User Reports	Opens the User Reports dialog. Enabled only when F-PROT Professional is in the administration mode.
Virus Information	Displays the **Virus Information** dialog box.
Virus Information on Web	Connects to F-PROT Web server to view virus descriptions.
Web Club	Connects to F-PROT 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.

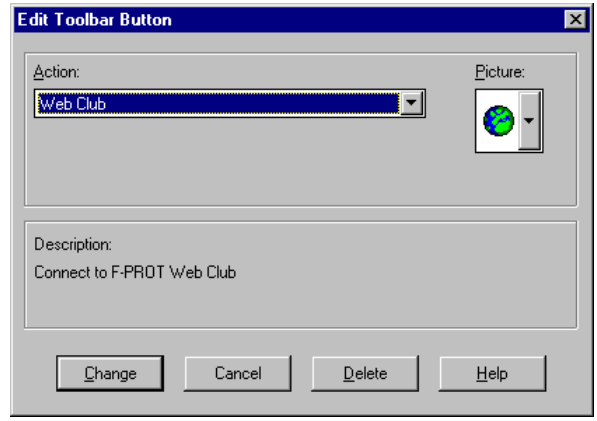
There is a shortcut way to create a new task button. Grab the task from the task list by pressing CONTROL and clicking on the task with the mouse, then drag and drop it on the toolbar, while keeping CONTROL pressed down. The new button, named according to the selected task, will appear on the toolbar.

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.

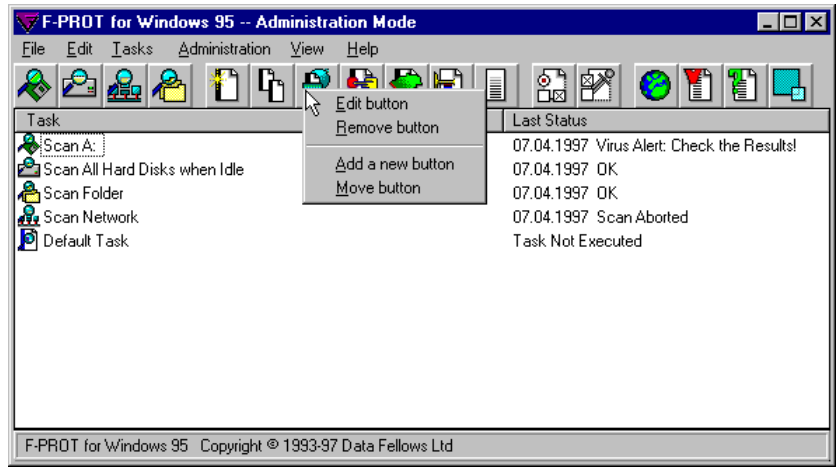
Select the desired action and picture for the button.

After making the desired modifications, confirm the changes by clicking **Change**. Clicking **Delete** will delete the button. F-PROT Professional 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-PROT Professional 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-PROT Professional 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.

2.6 Network Features

While F-PROT Professional 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.

Updates

The administrator can automatically update F-PROT Professional 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

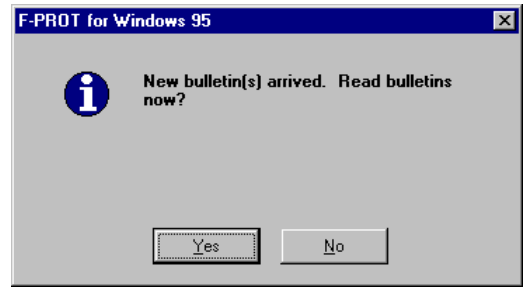
The administrator can design scanning tasks and distribute them to local workstations through the network. F-PROT Professional programs on individual workstations pick the tasks up automatically and add them to their own task lists. If the tasks have been designed to run on a schedule, the local programs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

Messaging

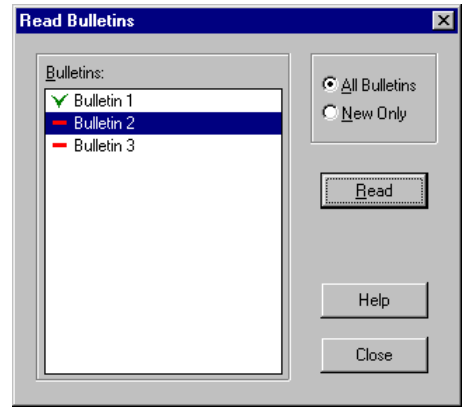
F-PROT Professional supports communication between users and the system administrator in the form of messages and bulletins. A user may send messages to administrator, and the administrator may send general bulletins to all the users.

In addition, F-PROT Professional 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-PROT Gatekeeper can be set up to send a message to administrator each time it detects a virus.

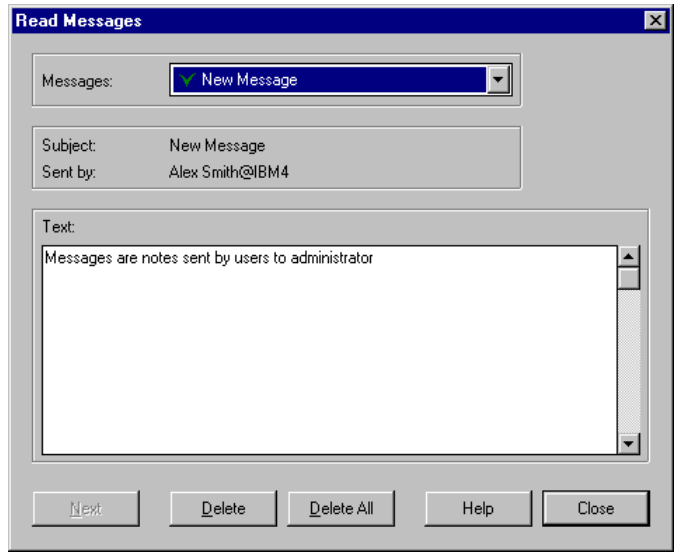
The administrator can send bulletins to all users simultaneously. When you launch F-PROT, it will notify you of any new bulletins.



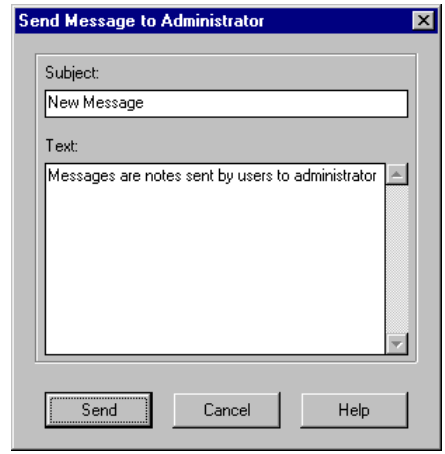
You can access the list of the bulletins either directly from this dialog by clicking **Yes**, or later by choosing **Read Bulletins** from the **Edit** menu.



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



To send a message to your F-PROT 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-PROT Professional 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-PROT Professional 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.

2.7 Menus

F-PROT 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-PROT Professional. 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-PROT Professional.

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-PROT Professional 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-PROT Professional.

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-PROT Professional is in its toolbar mode.

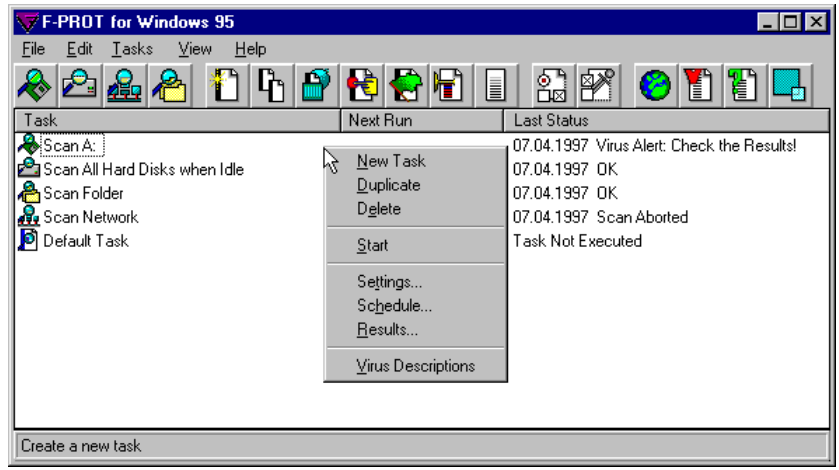
View Menu Command	Function
Large Icons	Displays each task as a large icon.
Small Icons	Displays each task as a small icon.
List	Displays the tasks in the form of the list.
Details	Default. Displays the tasks in the form of a list with the Next Run and the Last Status fields.

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-PROT Web club.
Virus Descriptions on the Web…	Connects to F-PROT WWW server to view virus descriptions.
Contact Information…	Provides contact information for your F-PROT vendor.
About…	Information about F-PROT Professional for Windows.

F-PROT Professional 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-PROT task list. This commands in this menu correspond to items in some of the normal menus.

2.8 What to Do When a Virus Is Found

Don’t Panic

If F-PROT 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 sector 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 section to disinfect the computer.
- If there is a problem in recovering from the infection, ask your system administrator to contact your local F-PROT Professional Business Partner for technical assistance. For more information about your technical support options, see “Technical Support” on page 17.

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-PROT for Windows’ Help Menu and in Viruses/Information menu in F-PROT 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 section you will find detailed instructions for all operating systems and all types of viruses.

If you run into problems during disinfection because F-PROT reports “A new or modified variant” of the virus and refuses to disinfect it, please contact F-PROT Support. See “Technical Support” on page 17 for more information.

You might have a new virus, which we need to analyse in order to add exact detection and disinfection of it to F-PROT.

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-PROT 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-PROT. 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-PROT Professional remove the virus.

If F-PROT 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.

Macro Virus Disinfection on a DOS-Only System

To disinfect Macro Viruses on a DOS system, run the F-MACRO program from F-PROT 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-PROT Professional remove the virus. If F-PROT Professional 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-PROT 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-PROT 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-occuring.

Viruses on a Diskette Boot Sector

If F-PROT 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-PROT Professional remove the virus. If F-PROT Professional 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-PROT 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” on page 13.

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:F-PROT.EXE /HARD /ALL /DISINF
```

and press [ENTER]. You’ll then see this message:

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

If F-PROT 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 section see "Creating a Rescue Disk" on page 13, 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.

Manually Repairing the MBR

If F-PROT 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-PROT 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-PROT 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-PROT Professional 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-PROT Professional for DOS diskette. To run F-PROT from the diskette, type

```
F-PROT <press ENTER>
```

F-PROT 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 section, “Creating a Rescue Disk”.

After F-PROT 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-PROT Professional remove the virus.

If F-PROT Professional 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-PROT Professional 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 section, “Manually Repairing the MBR” or the section, “Manually Repairing the Boot Sector”. Contact F-PROT Support if needed.

Viruses Resident in Memory

If F-PROT 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-PROT. 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 section, “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-PROT Professional for DOS diskette. To run F-PROT from the diskette, type

```
F-PROT <press ENTER>
```

F-PROT 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 section, “Creating a Rescue Disk”.

After F-PROT 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-PROT Professional 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-PROT.

If F-PROT Professional 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-PROT Professional 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 section, “Manually Repairing the MBR” or the section, “Manually Repairing the Boot Sector”. Contact F-PROT Support if needed.

3 Administering F-PROT Professional

This section describes the administrative tasks and the tools available. It contains an overview of the program for the network administrator in a network environment.

3.1 Overview of F-PROT Professional Administration

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

F-PROT Professional 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-PROT 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-PROT Professional aims to provide invisible protection for end user data and program files. To this end F-PROT Professional 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-PROT Professional provides a wealth of features to make your work easier.

Implementation Steps

The steps involved in setting up F-PROT Professional 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-PROT Professional task list to create the task base suitable for your organization. For more information, see “Working with Scanning Tasks” on page 25.

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. For more information, see “Modifying the Toolbar” on page 46.

4. Modify the Preferences.

Edit the F-PROT Professional Preferences, so that they are suitable for the users. Hide at least the **Network**, **Administration**, **Scanning** and **Restrictions** Preferences in the **Preferences** dialog box. For more information, see “Setting F-PROT Preferences” on page 39.

5. Create the installation directory.

If you choose to perform the complete installation on workstations, use the **Distribute F-PROT Installations** command in the F-PROT **Administration** menu to create the suitable installation directory. For more information, see “Distributing F-PROT Installations” on page 82.

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

3.2 Network Installation

Overview

There are three basic ways in which the F-PROT Professional 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-PROT Professional is installed locally to all workstations. Remote installation means that only one installed copy of F-PROT Professional exists on the network drive, and all the workstations run the same copy.

Network Installation

There are two options for installing F-PROT 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-PROT Professional 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-PROT 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-PROT 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.

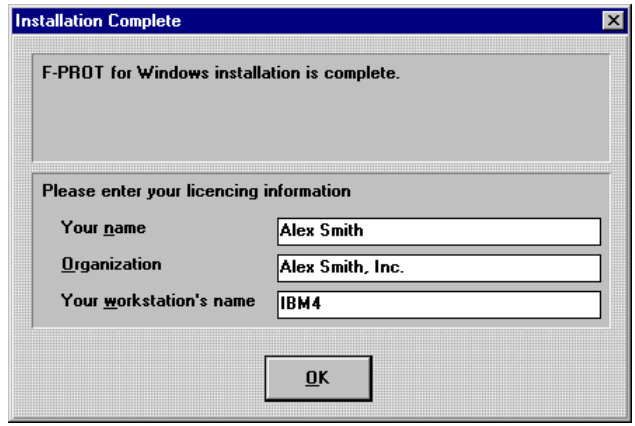
Installing F-PROT on the Administration Workstation

To start the implementation of F-PROT Professional, you should first install F-PROT on a workstation in the Network Administration configuration. When you choose the Network Administration Installation option, you implicitly designate the administration workstation.

- Run the Setup program from the installation diskette as described in “Installing F-PROT Professional” on page 9.
- Choose the Network Administration Installation option.

- Choose the target directory for the copy of F-PROT on the Administration workstation. You should install F-PROT to the local hard drive rather than a network drive.
- Choose a shared communication directory for all F-PROT Professional users. The communication directory should be on a shared disk, so that all F-PROT users have access to it.
- Type in the administration password.
- Check the Enable F-PROT Gatekeeper at Windows Start-Up and Load F-Agent at Windows Start-Up options. It is recommended that you keep F-Agent active at all times; it runs the scheduled tasks and notifies you of messages received from the other workstations.

Click **Start Installation**. When the installation is complete, the program will ask your name, the name of your organization, and your workstation’s ID.

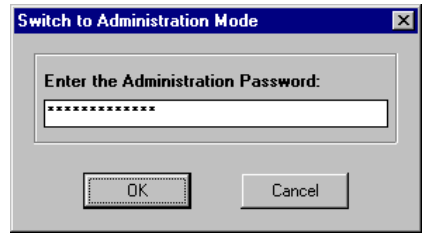


This information will be used in identifying the computers in reports and virus alerts.

Entering the Administration Mode

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

When the **Administration Workstation** check box is selected in Preferences, F-PROT Professional asks for the administration password at start-up.



If the user does not enter the correct password, F-PROT 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” on page 79 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.

3.3 Systems Management

F-PROT 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-PROT update bulletins or other virus related messages to users.

F-PROT 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-PROT installations and updates can also be done through Microsoft Systems Management Server (SMS). See "Microsoft Systems Management Server" on page 131 for more information. The latest information about SMS support is available at:

- http://www.DataFellows.com/f-prot/sms/

F-PROT 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/f-prot/snmp/

Network-Aware Functions

Update Distribution

F-PROT 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-PROT 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

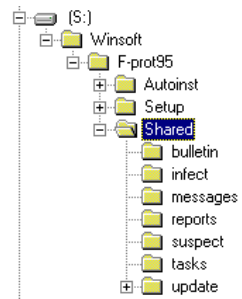
The results of tasks' execution can be set to be sent from user workstations to the Administration workstation, along with any infected files found by F-PROT Professional.

User Messages and Administrator Bulletins

F-PROT is designed to support communication between users and administrator. Such communication facilitates efficient administration and management of the F-PROT 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-PROT Professional 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-PROT Professional programs on user workstation then copy the new files from the communication directory to the appropriate directories on local hard disks.



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

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.

Novell NetWare

To change the communication directory’s privileges under Novell NetWare, use the SYSCON and FILER utilities to grant read, write, modify, create and delete privileges. For more information on how to use SYSCON and FILER, consult the NetWare documentation.

To change the privileges from the command line under NetWare version 3.11 or earlier, you can also use these commands:

- Read access rights:
  ```
  GRANT R F FOR SYS:F-PROT\BULLETIN TO GROUP EVERYONE
  ```
- Write access rights:
  ```
  GRANT W C E F FOR SYS:F-PROT\MESSAGES TO GROUP EVERYONE
  ```
- Read and write access rights:
  ```
  GRANT R W C E F FOR SYS:F-PROT TO GROUP EVERYONE
  ```

To change the communication directory's privileges under Novell NetWare version 4.0 or later, use commands like:

```
RIGHTS SYS:F-PROT R W C E F M /NAME=EVERYONE
```

Here, "everyone", is the name for a group object containing all user objects that are to use F-PROT.

You can also use

Microsoft Windows NT Server

To change the communication directory's privileges under Windows NT Server 3.51, select the directory in File Manager and choose the Permissions command from the Security menu.

Under Windows NT Server 4.0, select the directory in Windows NT Explorer, press Alt+Enter, click on the Security tab and and click the Permissions button.

Microsoft Windows for Workgroups

If you are using the built-in file sharing of Windows for Workgroups, use the File Manager to share the communication directory with read and write access, without requiring a password.

Microsoft LAN Manager

To change the communication directory's privileges under Microsoft LAN Manager, use:

```
NET ACCESS N:\F-PROT /ADD USERS:RWCD
```

UNIX

To change the communication directory's privileges under most UNIX systems, use:

```
chmod 777 /usr/local/f-prot/
```

Refer to the chmod man page for information how to set directories read-only or write-only.

Artisoft LANtastic

To change the communication directory's privileges under Artisoft LANtastic, use:

```
NET_MGR
```

Use the Shared Resources Management feature of the menu-driven application to give read, write, create, file lookup and delete privileges to the directory for appropriate groups. In LANtastic for Windows, use the Network Manager application. For more information on how to use NET_MGR and Network Manager for Windows, consult the LANtastic documentation.

Banyan VINES

To change the communication directory's privileges under Banyan VINES, use:

```
SETARL N:\F-PROT
```

Use the menu-driven application to give read, write and delete privileges for appropriate groups. For more information on how to use SETARL, consult the VINES documentation.

3.4 Customizing the User Interface

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

Creating A Task Base

Create the F-PROT task base by modifying the task list of F-PROT installed on the Administration workstation. The tasks can be added, modified, scheduled, and removed as described in this User's Guide.

Consider the needs of your organization and check the User's Guide 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" on page 93 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-PROT. While this is not always possible, the most often needed functions should be linked to the toolbar. See "Modifying the Toolbar" on page 46 for more information.

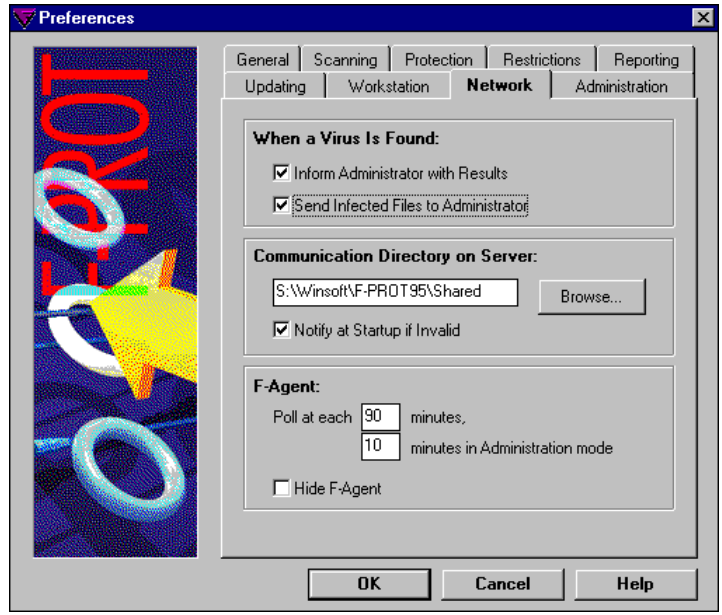
Editing Preferences

Before distributing the program to users, customize the F-PROT Professional Preferences. Instructions on how various Preferences affect the program and how they can be modified can be found in the User's Guide, section 6.3, "Setting Up Preferences."

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

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-PROT Professional send you the task results and copies of infected files from local workstations. Samples will always be sent in an encrypted format. Whenever F-PROT 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-PROT 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” on page 74 for more information.

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

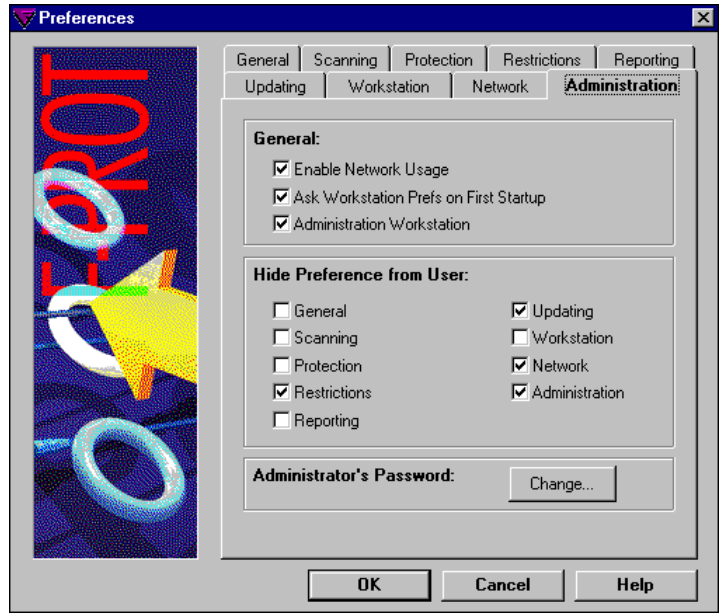
Administration Preferences

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-PROT asks for the workstation ID and user name the first time it is started on a workstation. F-PROT 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.

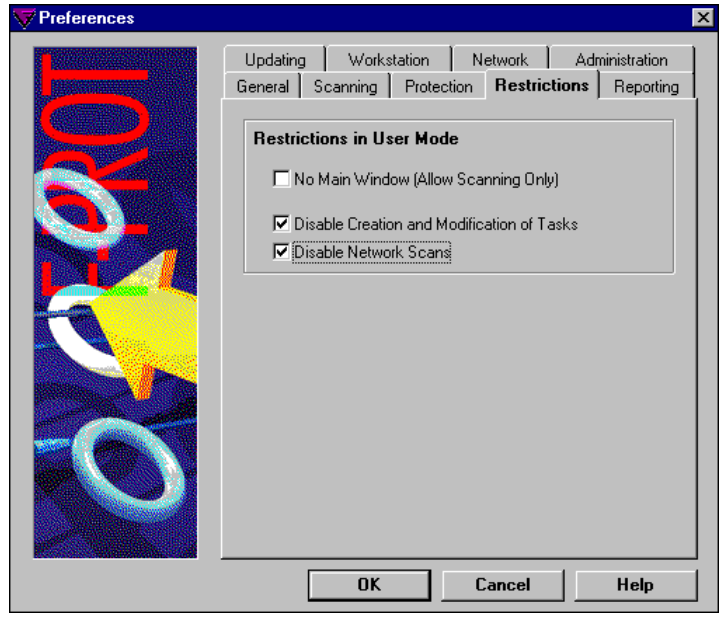


You can hide some of the Preferences from the users. If a Preferences is hidden, the users cannot edit it, and the choices, you have made, stay in effect. It is recommended that you hide at least **Network**, **Administration**, **Restrictions**, and **Updating** Preferences.

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.

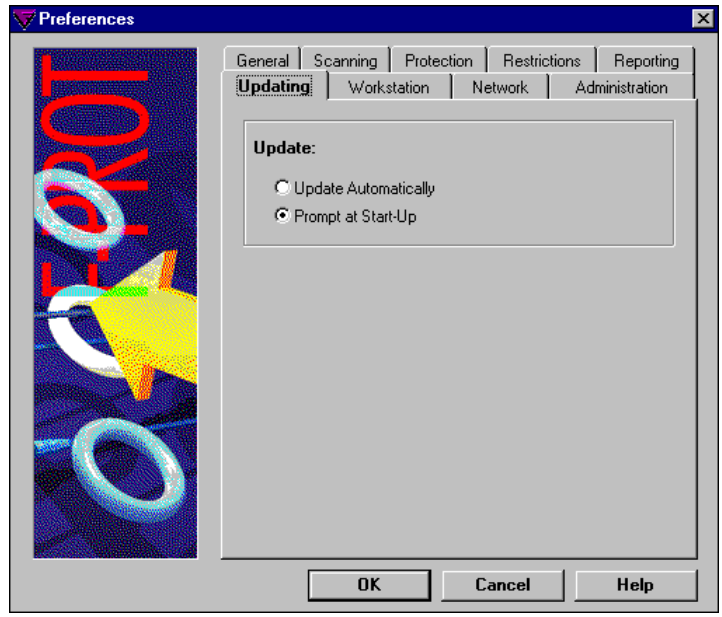
Restrictions Preferences

Use the **Restrictions** Preferences to restrict the use of F-PROT Professional 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-PROT updates on the workstations: **Update Automatically** or **Prompt at Start-Up**.



3.5 Distributing F-PROT Installations

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

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

F-PROT 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” on page 131 for more information. The latest information about SMS support is available at:

- http://www.DataFellows.com/f-prot/sms/

Installation with Autoinst

Autoinst is a utility program that enables the system administrator to have any version of F-PROT Professional 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-PROT Preferences stored in the in configuration files on workstations throughout the network.

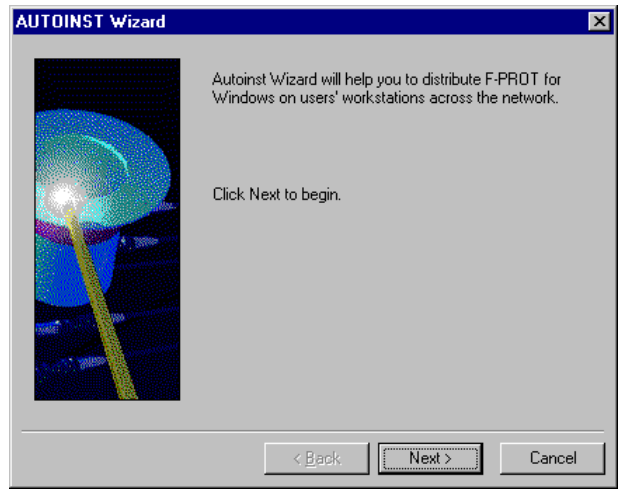
You should use the Autoinst Wizard to create the installation script. However, not all the options are available through the Wizard. If you need to fine-tune the settings, you should write a customized Autoinst script. See “Appendix D: Autoinst Configuration” on page 145 for more information.

To distribute installations using Autoinst, first perform the Network Administration installation on the Administration workstation. Then do the desired modifications to the F-PROT Preferences, toolbar, and the task base. Then choose **Distribute F-PROT Installations** from the

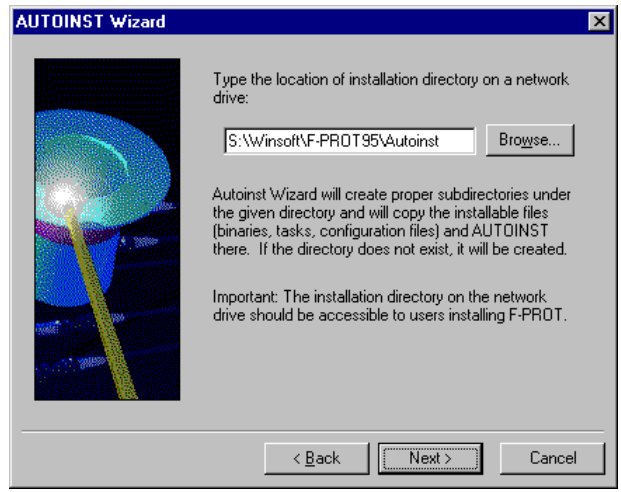
Administration menu, and select **By Creating Installation Directory for Autoinst**. Autoinst Wizard will start.

Autoinst Wizard

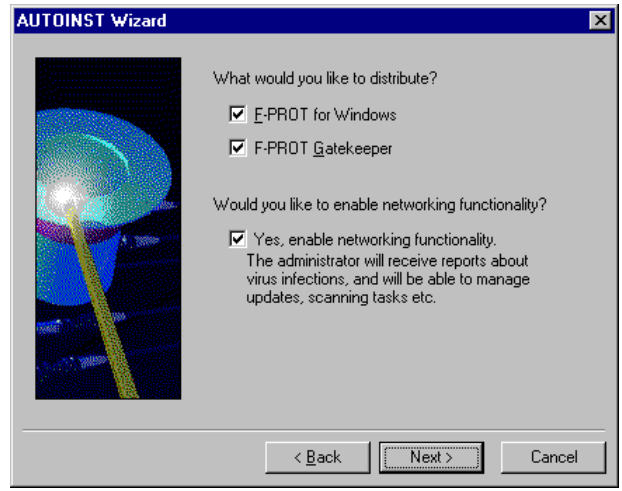
Autoinst Wizard makes it easy to write the Autoinst configuration file, create the shared Autoinst installation directory, and make all the necessary files available for distribution.



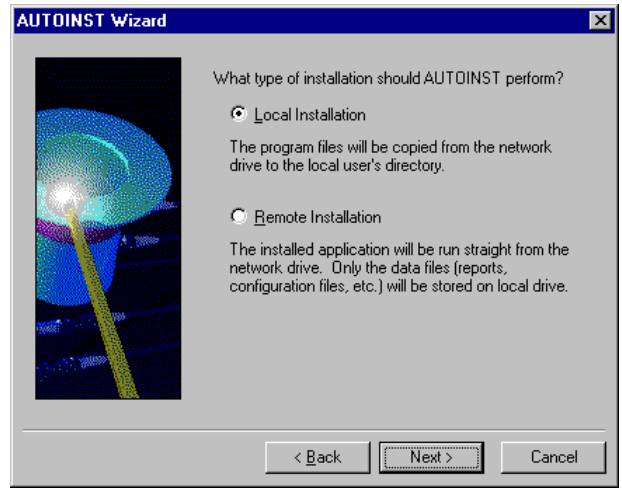
You can move freely back and forth within Autoinst Wizard by clicking **Back** and **Next**. You can exit the wizard at any time by clicking **Cancel**. The most important steps in the Wizard are described below.



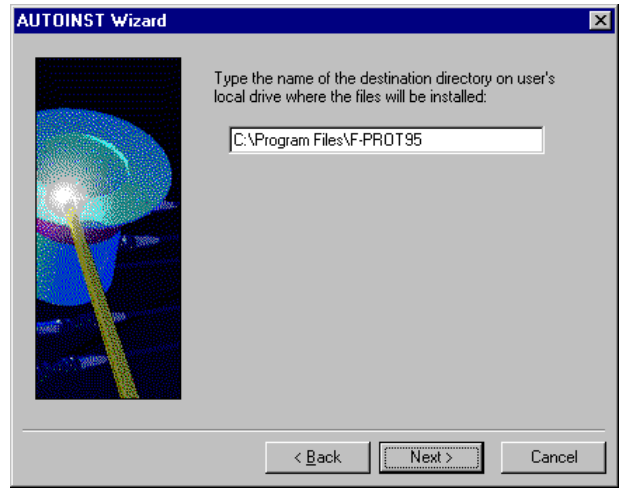
Enter the name and location of the Autoinst directory, which should be accessible from all workstations. If the specified directory does not exist, the wizard will create it, prompting for your confirmation first.



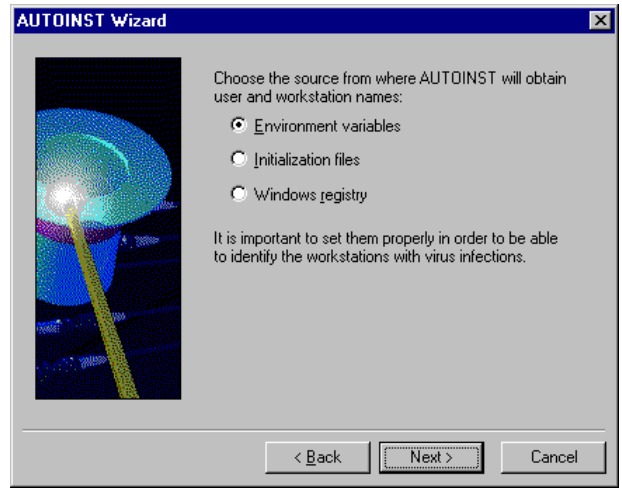
Select the check boxes corresponding to the programs you wish to distribute. Select the **Yes** check box to have the networking functionality enabled, if you plan to distribute scanning tasks, bulletins, and updates, and receive mail from workstations.



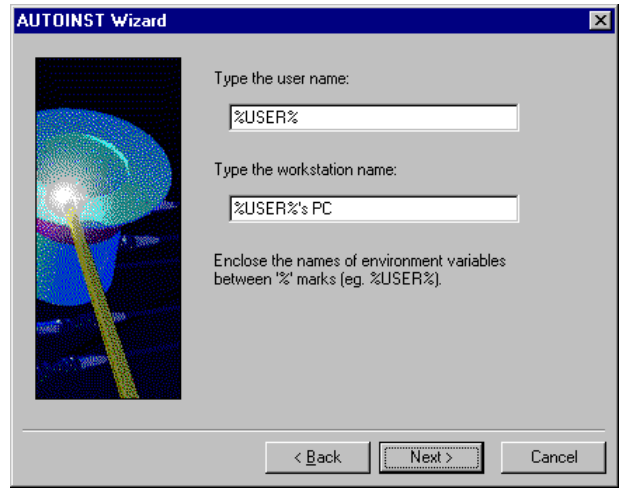
Choose the type of installation Autoinst should perform. Choose **Remote Installation** if you wish F-PROT Professional or F-PROT Gatekeeper to reside on the server. In this case, only the data files, such as reports, configuration files, and others, will be copied to the local workstations' hard disks.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



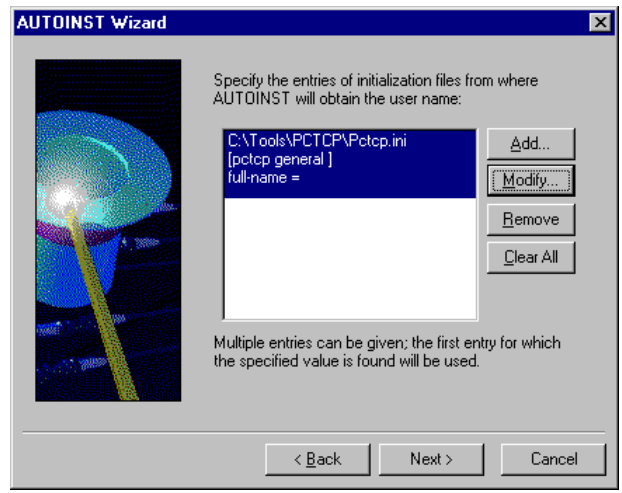
Choose the name of the destination directory on the local workstations' hard disks where the files will be installed. If the specified directory does not exist on some of the workstations, Autoinst will create it.



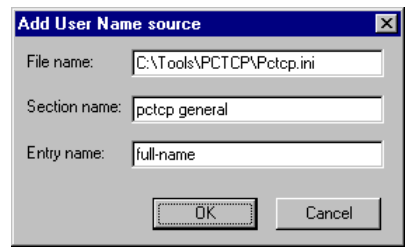
Select the source from which Autoinst will obtain the user name and the workstation ID, both of which will serve to identify the origin of mail received from workstations. Depending on your choice, various dialog boxes will be displayed upon clicking **Next**.



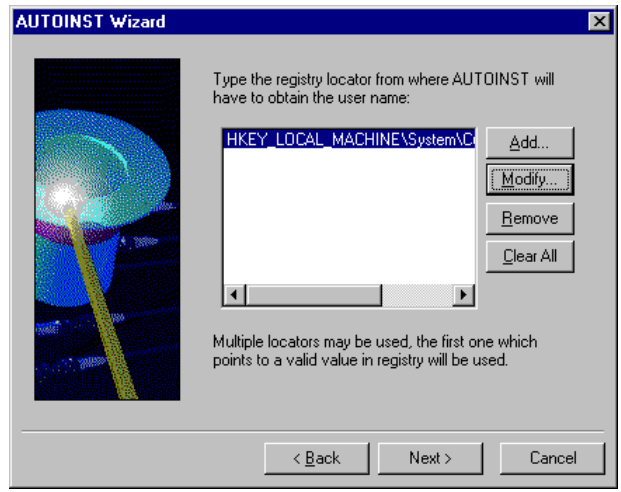
If you selected environment variables as the source from which Autoinst will obtain user name and workstation name, type in the names of the both environment variables in the provided boxes, enclosing each variable between the % characters.



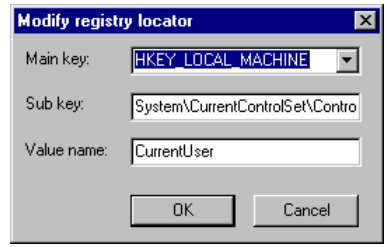
If you chose initialization files as the source of user and workstation names, add the entries that specify the user name to the provided list. If you list multiple entries, the first of them that yields result will be used. To add entries, click **Add**.



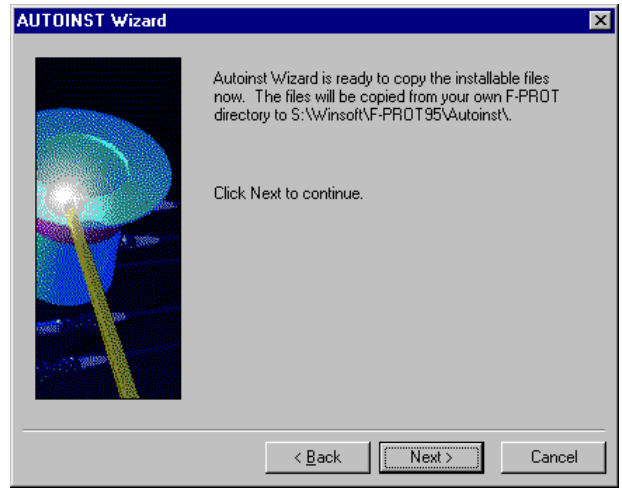
In the dialog box, type in the **File name**, **Section name** and **Entry name,** and click **OK**. The new entry will appear on the list. To edit the entry, select it on the list and click **Modify**. Edit the entries in the displayed dialog box. To delete an entry, select it on the list, and click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



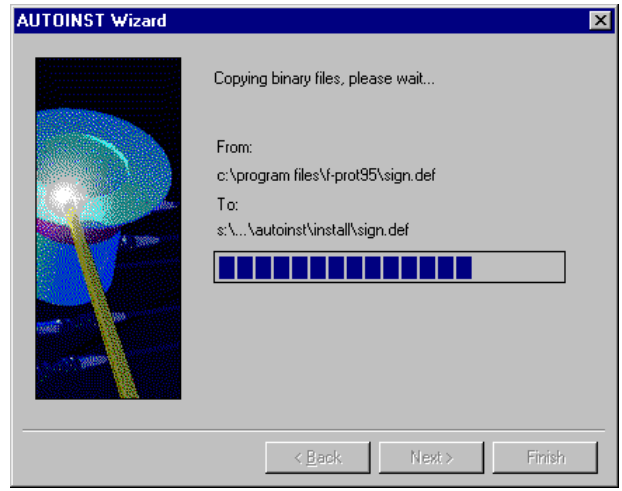
If you chose Windows registry as the source of user and workstation names, add the registry locator for the user name by clicking **Add**. You can list multiple entries; in this case the first one pointing to the valid value will be used.



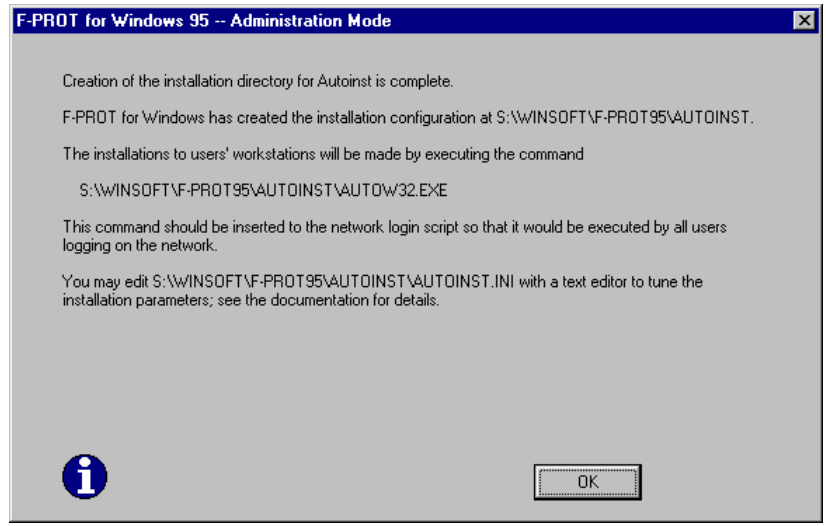
In the **Add registry locator** dialog box, enter the **Main key**, the **Sub key** and the **Value name**. The Main key can be selected from the list; the available options are: HKEY_CLASSES_ROOT, HKEY_CURRENT_USER, HKEY_LOCAL_MACHINE, HKEY_USERS.



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-PROT Preferences or the settings of F-PROT Gatekeeper before distributing the programs to the users. The customization is done through the standard Preferences dialog.

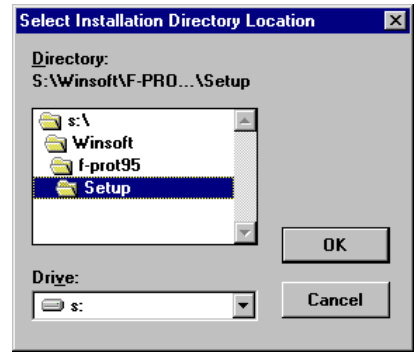


The final message box tells you where the Autoinst installation directory has been created and the name of the Autoinst command file, located in the Autoinst directory. Insert this command into the workstations' login scripts, so that it is executed at log-on. The wizard has also created the Autoinst.INI 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 "Appendix D: Autoinst Configuration" on page 145.

Installation with Setup.exe

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

1. Perform the Network Administration installation of F-PROT 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-PROT 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-PROT 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.

3.6 Distributing Updates

The easiest way to update F-PROT 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-PROT updating function uses the F-PROT root directory as the source directory.

☞ **Important: If you are sending updates through F-PROT, 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.**

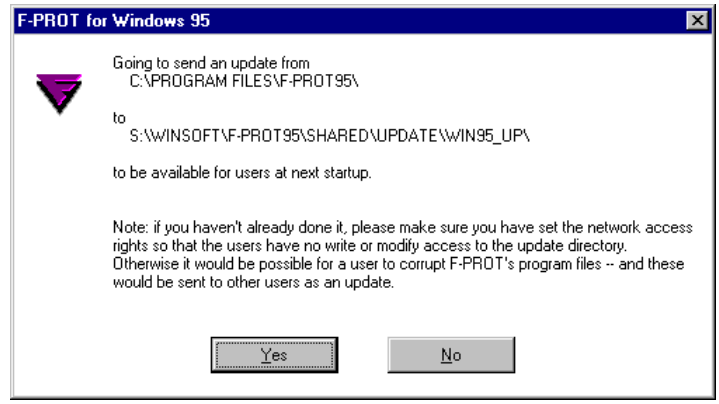
Updating the Administration Workstation

To update a new version of F-PROT 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-PROT from a server, make sure that nobody is using F-PROT 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-PROT 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-PROT Professional root directory to the UPDATE directory on the shared disk.



When you send an update to users, all programs installed under the F-PROT Professional root directory are copied to the shared disk. If you have programs like F-CHECK or F-PROT 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-PROT.

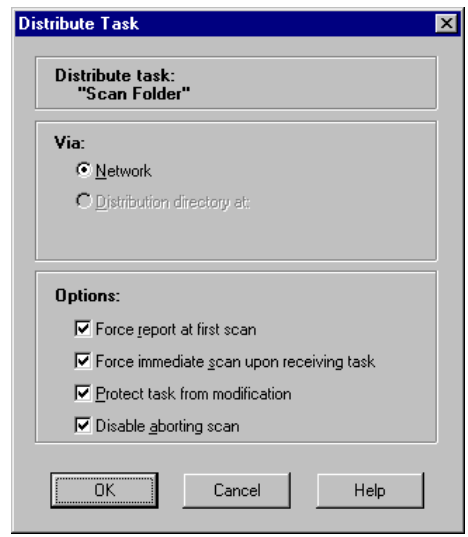
On workstations, F-PROT Professional, when started, checks the UPDATE directory. If a new version has become available, F-PROT updates itself. If the UPDATE directory contains other programs, F-PROT Professional also copies them to the local hard disk.

3.7 Distributing Tasks

Tasks can be created on the administration workstation and distributed to users via the network. F-PROT 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.

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 **Network** as the distribution method. 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.

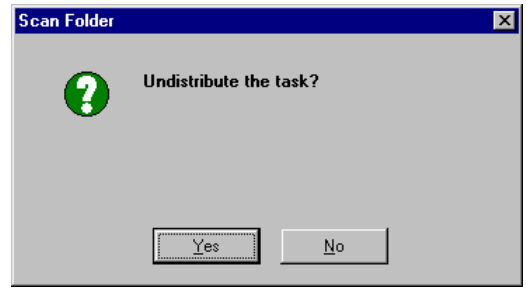
After you have chosen the desired options, click **OK** to copy the task file to the TASKS directory on the shared disk. When F-PROT programs on the local workstations notice that a new task has become available, they copy the task to the local hard disks and add it to their local task lists.

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

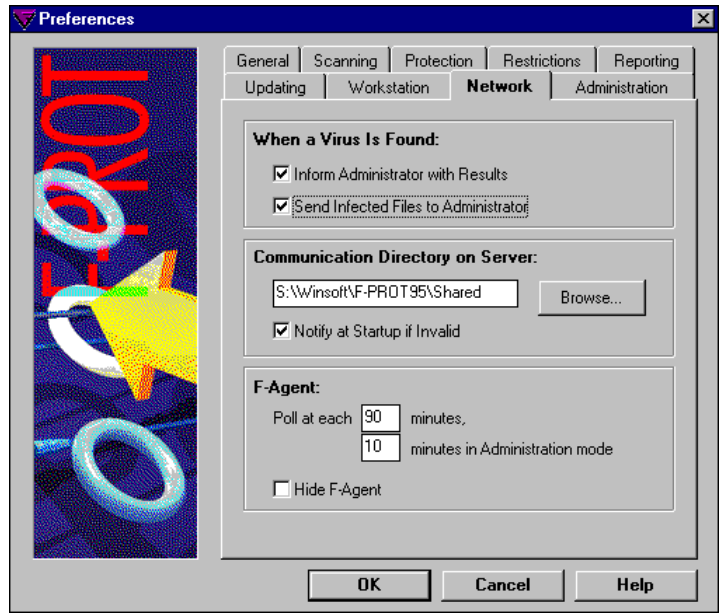
Remove a task that you have previously distributed by selecting it on the task list and choosing **Undistribute Selected Task** from the **Administration** menu.



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-PROT on local workstations notices that an Undistribute file has appeared on the shared disk, the corresponding task is deleted from the local hard disks.

3.8 Collecting Reports and Infected Files

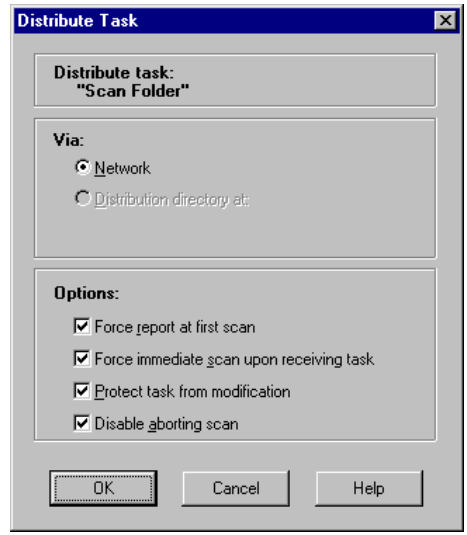
Use the **Network** Preferences to set up the actions to be taken by F-PROT Professional when it discovers a virus on a user workstation. Here you can select whether or not the task reports and any infected or suspected files are to be sent to administrator.



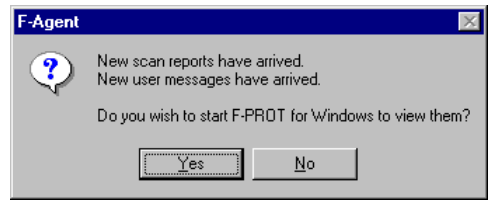
When the **Inform Administrator with Results** check box is selected and incorporated into the users' versions of F-PROT Professional, a task results report is sent to administrator whenever a virus is found during a scan execution. Whenever F-PROT Gatekeeper finds a virus, it sends corresponding message 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-PROT, 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-PROT Installations" on page 82.

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-PROT Professional should be started to view the messages.

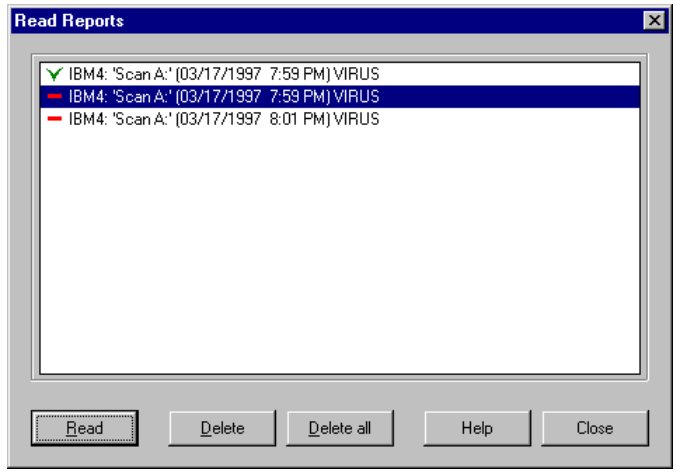


WARNING: If you want to test the performance of F-PROT Professional by scanning a large number of files infected with various viruses, be sure to switch this option off. Otherwise, every infected file will be copied to the INFECT directory. This operation will consume a vast amount of time and disk space.

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.

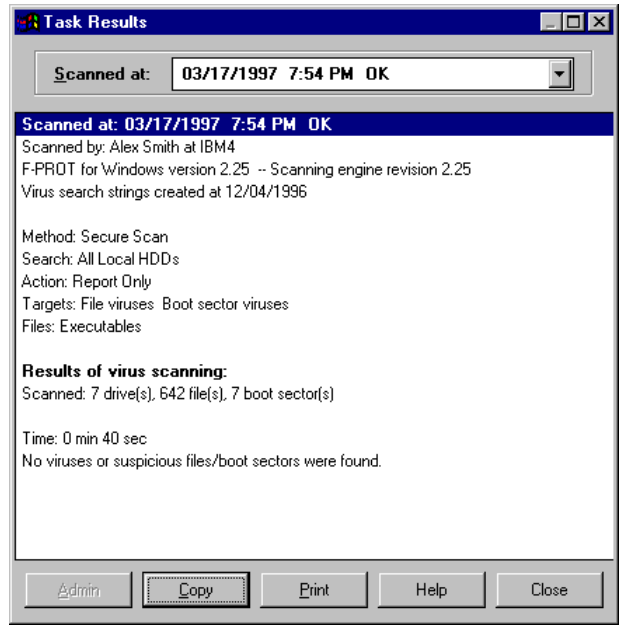
The reports list is similar to the log file. Each report is represented by one line which contains the originating workstation ID, the name of the task, the time of execution, and the report status.



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-PROT 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-PROT Professional 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-PROT 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-PROT reports an unknown virus or a new variant of a known virus, please contact Data Fellows or your local distributor. See "Technical Support" on page 17 for more information.**

3.9 Managing Messages

F-PROT Professional 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.

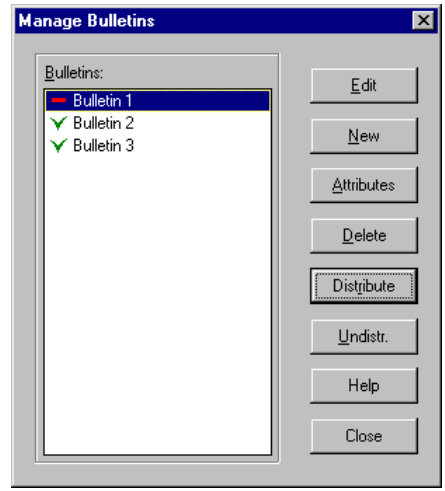
Messages are notes that the users send to the administrator. F-PROT Gatekeeper, when it finds a virus on a user workstation, also sends a message to administrator. The messages identify the sender and the originating workstation.

Both messages and bulletins are transferred over the network by being copied to the appropriate F-PROT Professional directory on the server disk. When F-PROT 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-PROT Professional run in User mode copies bulletins from the shared BULLETIN directory to the local BULLETIN directory and appends them to the local Bulletin List.

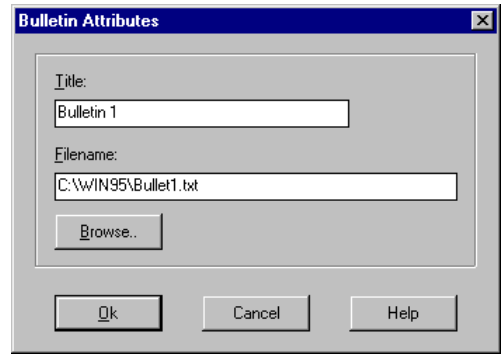
Sending Bulletins to Users

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-PROT Professional 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**.

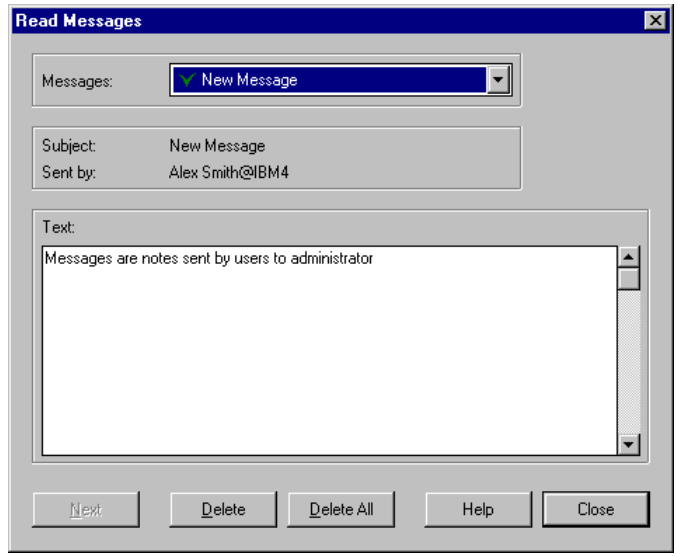
You can also remove a bulletin from circulation by selecting it on the Bulletin list and clicking **Undistribute**. This makes F-PROT Professional send the Undistribute file to the shared disk. The Undistribute file has the same name as the corresponding bulletin, but has the extension .del. When F-PROT 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.



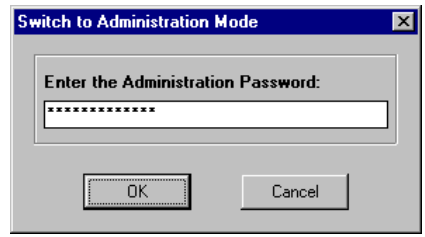
The **“Read Messages”** dialog box contains the following buttons:

- **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.

3.10 Administration Menu

The Administration menu is the administrator's main tool for controlling F-PROT. 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-PROT 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-PROT Professional 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-PROT web server.

4 Appendix A: Background Information on Viruses

This section provides background information on viruses in general. It describes some of the most common virus types and their working mechanisms.

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-PROT Professional which you can access through the Help menu.

4.1 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.

4.2 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-PROT 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-PROT 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.

4.3 Common Virus Types

The following section 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

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-PROT Professional 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-PROT Professional. 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-PROT 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.

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-PROT Professional detects, identifies and disinfects all the file 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 document 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-PROT Professional detects, identifies and disinfects all the file viruses that are in the wild.

4.4 Advanced Methods Used by Viruses

The following section 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 mutation viruses;
- retroviruses;
- application specific viruses;
- 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.

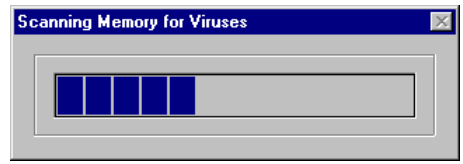
A good example is the virus called Brain, the first known stealth virus. Brain is a boot sector virus which transfers the original contents of the boot sector to a suitable location on the disk. Too large to fit completely on the boot record, it needs to store a part of its own code on the data area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

When you start F-PROT Professional for Windows 3.1 or Windows 95, its first task is to scan the computer's memory. F-PROT Professional 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-PROT 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-PROT Professional for DOS. To learn how to create a startup diskette for emergency use, see "What to Do When a Virus Is Found" on page 59. For information about using F-PROT Professional for DOS, see "Appendix E: F-PROT Professional for DOS" on page 163.

F-PROT Professional 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-PROT 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-PROT Professional utilizes many techniques against the tampering of F-PROT 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-PROT Professional detects, identifies and disinfects all the file viruses that are in the wild.

4.5 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-PROT Web server's library for more technical information.

4.6 Testing Your Anti-Virus Protection

To test whether F-PROT operates correctly, you can use a special test file which is detected by F-PROT 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*
```

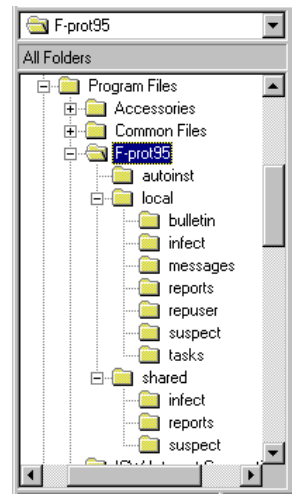
Save this file to any name with a .com extension, for example EICAR.COM. Make sure that you save the file in the standard MS-DOS ASCII format. Now you can use this file to see what is looks like when F-PROT detects a virus. Naturally, the file is not a virus. When executed without any virus protection,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

5 Appendix B: F-PROT Professional Structure

This section characterizes the structure of files and directories in F-PROT Professional, and their naming conventions. This section explains the use of various files used for F-PROT Professional installation, on administrator and user workstations and on the network server.

Workstation Directories and Files

This section describes the files and directories installed on both administrator and user workstations. The directories are: the root directory, and its two subdirectories: LOCAL and SHARED.



Root Directory

During F-PROT installation, the root directory is created on the local hard disk. In various operating environments the default path and name of the root directory are the following:

Platform	Directory
Windows 3.1	C:\Windows\F-PROTW
Windows 95	C:\Program Files\F-PROT95
Windows NT 3.X	C:\WinNT\F-PROTNT
Windows NT 4.0	C:\Program Files\F-PROTNT

The root directory can also be installed elsewhere and given any other name.

All the executable files and the Help file reside in the F-PROT root directory. However, the system file, F-PROTW.CFG, is installed not in the F-PROT Professional directory, but in the local Windows directory.

LOCAL Directory

The LOCAL directory contains subdirectories and files which F-PROT uses in its normal operations. The seven subdirectories arranged under LOCAL are: BULLETIN, INFECT, MESSAGES, REPORTS, REPUSER, SUSPECT and TASKS.

LOCAL/BULLETIN Directory

On administration workstation, the BULLETIN directory under LOCAL contains the bulletins which administrator sent to users. On a user workstation, this directory holds bulletins delivered from administrator.

LOCAL/INFECT Directory

On administration workstation, the INFECT directory under LOCAL contains the infected filessent from the user workstations and their accompanying information files.

LOCAL/MESSAGES Directory

On administration workstation, the MESSAGES directory under LOCAL contains the messages received from the users.

LOCAL/REPORTS Directory

The REPORTS directory under LOCAL contains reports from the tasks executed on the local workstation.

LOCAL/REPUSER Directory

On administration workstation, the REPUSER directory under LOCAL holds the task reports sent from user workstations.

LOCAL/SUSPECT Directory

On administration workstation, the SUSPECT directory under LOCAL holds suspected filessent from user workstations and their accompanying information files.

LOCAL/TASKS Directory

The TASKS directory under LOCAL contains the F-PROT tasks in the form of task files.

SHARED Directory and its Subdirectories

The subdirectories under SHARED are used for temporary storage of files sent to administrator when the network connection is down. The reports and files to be sent to administrator are stored in their respective directories until the network connection is re-established, at which time the files are sent on to administrator. The subdirectories under SHARED are: INFECT, SUSPECT and REPORTS.

SHARED/INFECT Directory

The INFECT directory under SHARED temporarily stores the infected files sent from workstations until the network connection is re-established.

SHARED/REPORTS Directory

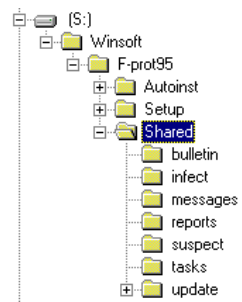
The REPORTS directory under SHARED temporarily stores the task reports from user workstation until the network connection is re-established.

SHARED/SUSPECT Directory

The SUSPECT directory under SHARED temporarily stores the suspected files sent from the workstation until the network connection is re-established.

Network Server Directories and Files

Files and directories on shared disk serve to provide file exchange between users and administrator.



Communication Directory

The F-PROT communication directory is created during F-PROT Professional installation. This directory can be given any name. Even when more than one platform is used, the same communication directory is used for communication between the platforms. See “Communication Directory” on page 74 for more information.

The communication directory contains seven communication subdirectories: BULLETIN, INFECT, MESSAGES, REPORTS, SUSPECT, TASKS, and UPDATE, and two encrypted files: Comm.inf and Fpwnet.cfg.

The file Fpwnet.cfg allows to run F-PROT in administration mode at any network workstation.

Comm.inf keeps track of the bulletins, messages, tasks, reports, and infected and suspected files, that are circulated through the shared disk.

☞ **Comm.inf and Fpwnet.cfg are encrypted.**

The communication subdirectories on the server are:

BULLETIN Directory on the Server

The BULLETIN directory on the network server is used for transferring the bulletins issued by administrator. From this directory, bulletins are distributed to all F-PROT Professional users connected to the network.

INFECT Directory on the Server

The INFECT directory on the network server is used for transferring infected files found on the local workstations. While on the server, these files are encrypted and renamed. When transferred to administration workstation, they are decrypted, but do not revert to their original names to prevent their accidental execution.

MESSAGES Directory on the Server

The MESSAGES directory on the network server is used for transferring the messages sent by users. From this directory, the messages are sent on to administration workstation.

REPORTS Directory on the Server

The REPORTS directory on the network server is used for transferring task reports sent from local workstations. From this directory, messages are sent on to administration workstation.

SUSPECT Directory on the Server

The SUSPECT directory on the network server is used for transferring suspected files found on the local workstations. While on the server, these files are encrypted and renamed. When transferred to administration workstation, they are decrypted but do not revert to their original names.

TASKS Directory on the Server

The TASKS directory on the network server is used for transferring tasks issued by administrator. From this directory, the tasks are distributed to all users connected to the network.

UPDATE Directory on the Server

The UPDATE directory on the network server is used to automatically distribute new versions of F-PROT to the users. The directory names vary by platform as follows:

- Windows 3.1: \UPDATE
- Windows 95: \UPDATE\WIN95_UP
- Windows NT: \UPDATE\WINNT_UP

The latest version of the program is copied into the appropriate UPDATE directory.

The update process is facilitated by the update list stored in the file Update.ini, which is located in the appropriate UPDATE directory of the shared disk.

F-PROT automatically updates the LastChange parameter in Update.ini. This parameter is checked by the local programs to determine whether a new version has become available. The local programs can then update themselves automatically. A corresponding value is also stored in local F-PROTW.CFGs.

```
[LastChange]
LastChange=[yy-mm-dd] (=year-month-day)
```

For example:

```
[LastChange]
LastChange=94-12-30
```

Since all the contents of this directory are copied to local workstations, the directory can also be used to update or distribute other programs. In such case, the program will be copied to the local F-PROT root directory.

File Descriptions

The following files are used for F-PROT Professional installation:

SETUP.EXE

The installation program, SETUP.EXE, is used for installing F-PROT Professional on workstations and/or on the server.

Program Files

F-PROT consists, in fact, of two separate programs, Launcher and Main Program, each of which has its own functions. When a user starts F-PROT Professional, the **Launcher** is

executed first. The Launcher performs certain preliminary tasks and then starts the **Main Program**.

When F-PROT is run in user mode, the Launcher (F-PROTW.EXE, F-PROTNT.EXE, or F-PROT95.EXE, depending on the operating environment) checks whether a new version of the program has become available. If a new version has appeared in the shared UPDATE directory, Launcher reads the Update Preferences to find out whether the program should be updated without notifying the user.

If the user's confirmation is required before updating, Launcher requests it. Otherwise, it proceeds directly to copying the new program version to the local F-PROT root directory. Having done this, it executes the Main Program

If F-PROT Professional is run in administration mode, Launcher skips the version check and immediately starts the Main Program.

The Main Program (FPWM.DLL, FPWM32.DLL) is the visible part of the application. When started, it executes the Memory Check at the beginning of its first scan. Then, if in user mode, it checks the shared disk for new tasks, user-defined signatures, and bulletins. It also checks the local INFECT, SUSPECT and REPORT directories for reports and infected and suspected files that should be sent to the administrator. If it finds any such items, it copies them from or to the shared disk.

Having completed these preliminary tasks, the Main Program informs the user of new bulletins and continues its normal routine, periodically checking the shared disk for new tasks, signatures and bulletins.

When executed in administration mode, the Main Program first checks the shared disk directories MESSAGES, INFECTED, SUSPECT and REPORT for user messages, infected and suspected files, and reports from other workstations. It then informs the administrator of its findings. Afterwards, it periodically checks the shared disk for messages, reports, and infected or suspected files.

F-PROTW.CFG

F-PROTW.CFG is the F-PROT system file. It contains the User Profile and other information needed for the program's successful execution. F-PROTW.CFG is located not in the F-PROT root directory, but in the Windows root directory. F-PROTW.CFG is encrypted.

User Profile Files

A User Profile file contains the user Preferences. At the same time, the User Profile file can also act as the F-PROT Professional system file, F-PROTW.CFG. The administrator can create and save several different User Profiles and move the User Profile files onto the shared disk to be installed directly from the network.

On a user workstation, a User Profile file acts as the system file, F-PROTW.CFG. Therefore, all User Profile files must be named F-PROTW.CFG before the programs are installed onto workstations. Otherwise F-PROT will not recognize these files.

F-PROTW.INI

☞ **This section applies only to Windows 3.1x**

F-PROTW.INI is the definition file, used by both F-PROT Professional for Windows 3.1 and F-PROT Gatekeeper operating under Windows 3.1.

One use of F-PROTW.INI is to define the memory areas which are not to be scanned for viruses. Some exotic display drivers are incompatible with a memory scan. If your system uses such a driver, the latter may cause Windows to stop responding during a memory scan. Should this occur, follow the instructions below:

- Always save your work in other Windows applications before running the memory scan tests. If Windows stops responding, there is no way to continue the Windows session and it will be necessary to re-start the computer.
- Create the F-PROTW.INI file in the Windows directory. If the F-PROTW.INI file already exists, simply edit the existing file To determine which memory areas should be skipped, enter "ShowSegmentNumber=1" into the [MemoryScan] section of F-PROTW.INI, for example:
- [MemoryScan]
  ShowSegmentNumber=1
- This will make F-PROT Gatekeeper's memory scanner display the number of scanned memory segments rather than the percentage completed in the progress indicator window.
- Restart Windows to see the memory being scanned.
- When Windows stops responding, write down the segment number shown in the progress window. For example, if the window shows "Scanning Segment 1a", the segment number is "1a". After rebooting, write "AreaStatusXX=1" (in which XX stands for the segment number) into the [MemoryScan] section of F-PROTW.INI.

  For example:

```
[MemoryScan]
ShowSegmentNumber=1
AreaStatus1a=1
```

- Then run the memory scan again. If Windows stops responding again (this time in another segment), simply write another "AreaStatus" line to F-PROTW.INI. It is very unlikely that Windows will stop responding more than once or twice. Finally, comment out or remove the "ShowSegmentNumber=1" entry from F-PROTW.INI or set the value to zero.

Remember, the memory scan hanging problem is caused by incompatibilities with certain video drivers. Therefore, if you change your video driver, try removing the "AreaStatusXX=1" entries and running the memory scan again to see what happens.

AUTOINST.INI

AUTOINST.INI is the configuration file for Autoinst, the utility program for F-PROT automatic installation or updating on workstations logged on to a network. The workstations normally call

a login batch script (LOGIN.BAT, for instance) when they log on to the network. The login batch script is modified to invoke Autoinst. Autoinst then performs the installation according to the instructions it finds in AUTOINST.INI.

The program files and configuration files are placed on a network drive by the administrator. Autoinst copies them to the local drive and makes necessary changes to the user's WIN.INI, SYSTEM.INI files and/or makes the necessary registrations. Autoinst also handles updating and uninstallation, and can be used for changing configuration (preferences) of workstations throughout the network.

See "Installation with Autoinst" on page 82 and "Appendix D: Autoinst Configuration" on page 145 for more information.

UPDATE.INI

UPDATE.INI is an ASCII file which Autoinst uses to determine whether or not to update (copy) files to the destination directory. This file is also used by F-PROT Professional for automatic updating by F-PROTNT.EXE, F-PROTW.EXE, or F-PROT95.EXE, depending on the platform.

Autoinst opens the UPDATE.INI file located in the source directory and the other UPDATE.INI file located in the destination directory to compare the file dates. If either the source or the destination directory does not contain UPDATE.INI, or if the date strings of the two files are different, Autoinst copies the files. If the dates are identical, the files are not copied.

Note that UPDATE.INI affects only the copying of program files. It has no effect on whether the configuration files are copied, or edited on the local drive according to the settings specified in Autoinst.INI.

Example of UPDATE.INI:

```
[LastChange]
LastChange=95-03-15
```

Note that when the program files are copied, UPDATE.INI is also copied. Therefore, the two copies will be identical after the first run, and program files are not copied upon subsequent runs. Be sure to change the date in UPDATE.INI before sending an update.

In order to enable automatic updating of Gatekeeper (via the comm directory) without starting the on-demand scanner, the administrator should use UPDATE.INI to set

```
[Updating]
AgentPollUpdates=1
```

FPW-PREF.INI

F-PROT Professional allows to update files, such as VIRSTOP.EXE (a TSR in the DOS version), from the network server to local workstations. When F-PROT Professional starts, it checks the file FPW-PREF.INI. Copy this file to the directory which contains F-PROTW.EXE.

FPW-PREF.INI should contain lines like the following:

```
[Update]
Source=V:\MASTER\F-PROT
Destination=C:\F-PROT
```

The FPW-PREF.INI file causes F-PROT Professional to update files from the server directory V:\MASTER\F-PROT to the local directory C:\F-PROT each time it starts up.

For example, to update the file VIRSTOP.EXE (a TSR in the DOS version) on all the workstations, the administrator only needs to update VIRSTOP in the master directory on the server. Then F-PROT Professional will make sure that all the workstations run an up-to-date copy of VIRSTOP.

Search String Files

The Search String Files contain the search strings F-PROT uses for detecting viruses. F-PROT Professional has its own search string database, in the file SIGN.DEF. This file is specifically encrypted, so that it can be accessed only by F-PROT.

Task Files

Parameters of each F-PROT task parameters are are stored in an encrypted task file, located in the local TASKS directory. When F-PROT is started, it reads all the task files and displays the corresponding tasks on the task list.

F-PROT Professional contains one default task, which is hard-coded into the program and cannot be deleted. When F-PROT is installed, it creates the task file for the default task and displays the task as Default task on the task list. Although the default task cannot be deleted, its parameters can be modified normally.

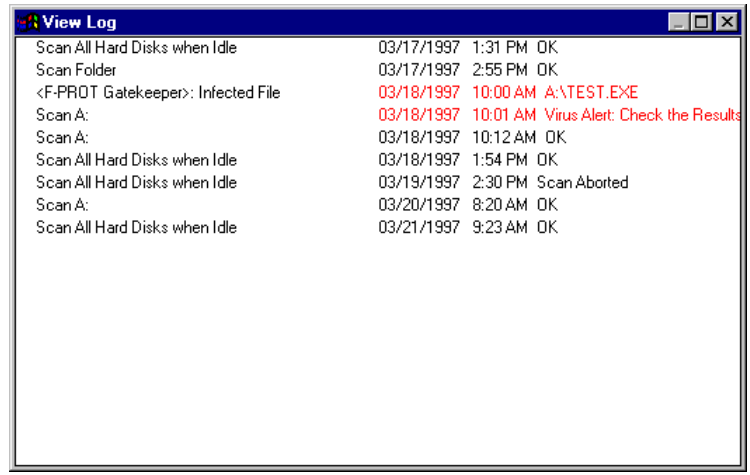
Other pre-configured tasks may also be included in the program. Such tasks are stored in normal task files, and do not differ from ordinary, user-defined tasks.

User-defined task files have the extension FPT. The file name is generated from the first 8 letters of the task name. For example: “Scan Network File Servers with Secure Scan” becomes “SCANNETW.FPT”. In case of a duplicate name, F-PROT replaces the last four letters of the task file name with a four-digit number. For example: “SCAN0001.FPT”, “SCAN0002.FPT”.

The tasks distributed by the administrator are named in the same way as the user tasks, except that the file extension is FPA.

The Log File

The log file, F-PROTW.LOG, contains one line per executed task. A log entry consists of the task name, its execution time and result.



The log file is stored at the LOCAL directory.

Task Result Files (Reports)

A results file (report) contains the results of one or several tasks. If the **Append** option is selected in the **Reporting** Preference, the file contains the results of several consequent scans, otherwise it contains the results of only one task.

The result file name is the same as the corresponding task file name, but its extension is FPR (F-PROT Result File), for example: SCANNETW.FPR. Results files are in binary format and cannot be browsed with a text editor. On local workstations, the results files are stored in the REPORTS directory. On administration workstation, reports from user workstations are stored in the REPUSER directory.

The reports can be inspected while inside the program. Warnings of viruses are shown in red. Headings are in larger font sizes.

A results file has the following elements:

- The heading, which states the task name and execution time. The user name and the workstation name are given below.
- The brief description of the task parameters.
- The summary of results. For example:

```
‘Scanned 1 disk(s), 14 file(s). No viruses found.’, or
‘Scanned 1 disk(s), 14 file(s). Alert! Found 2 virus(es) in 30 file(s).
Disinfected 0 file(s).’
```

- If infections have been found, the infected files are arranged under entries that state the infecting virus. For example:

```
‘Found the Jerusalem virus in
C:\APPS\BIN\QEDIT.EXE
C:\DOS\FORMAT.COM’, or
‘Found the Vienna virus in
C:\COMMAND.COM’
```

Double-clicking on the infected file name opens a window where the file is described in more detail. Double-clicking on the infecting virus name displays the description of the virus.

Infected And Suspected Files

Infected and suspected files are the files which have a confirmed or suspected virus infection. When such files are sent from local workstations to administrator, they are renamed to prevent spreading of infection through accidental execution of the files.

The substitute name for an infected file is formed by concatenating the letters INF and the current five-digit infected file count number, which may contain leading zeros. The renamed files have the extension VIR, for example: INF00015.VIR

The substitute name of a suspected file is similarly formed by concatenating the letters SUS and the running five-digit suspected file count number, which can include leading zeros, for example: SUS00015.VIR

When infected and suspected files are sent to administrator, each of them is accompanied by the information file, which contains the name of the infecting virus, the local workstation's name, the name of the original file and its directory path. The information files have the extension INF. Their names are formed by concatenating the letters INF and the running five-digit count number, which may include leading zeros, for example: INF00015.INF

Message Files

Message files are simple text files sent from users to the administrator. Besides the actual message, a message file contains, in its first three lines, the subject of the message, the ID of the sending workstation, and the sender's user name.

Message files have the extension TXT. Their names are concatenations of the letters MSG and the running five-digit message count number, which may include leading zeros, for example: MSG00130.TXT.

Bulletin Files

Any file, regardless of its format, can serve as a bulletin file , as long as both its sender and recipient possess the application needed to read the file. In practice, this means the text editor or other application with which the bulletin file was created.

Each bulletin is accompanied by the separate file having the extension INF. The INF file contains the name of the bulletin, the name of the application used to create the bulletin, and the name of the bulletin file. When a bulletin is copied from the shared BULLETIN directory to a local workstation, this information is incorporated into the local F-PROTW.CFG.

The name of each INF file is the concatenation of the letters BUL and the running five-digit bulletin count number, which may include leading zeros, for example: BUL00015.INF.

COMM.INF

The COMM.INF file tracks all tasks, messages, bulletins, search strings, reports, and infected files sent through the network. COMM.INF is located on the shared disk, and is accessed periodically by the local F-PROT programs which check for new tasks, bulletins, messages, and reports. The COMM.INF file is encrypted.

TMP.~NF

Every time F-Agent or F-PROT running on a workstation starts reading the shared communications directory, the semaphore file named TMP.~NF is created in the communications directory, unless it already exists. As long as the semaphore file exists, F-Agent or F-PROT from no other workstation can access the communications directory. After reading the needed information, F-PROT deletes the TMP.~NF, so that other workstations are able to access the communications files.

6 Appendix C: Microsoft Systems Management Server

This section describes how F-PROT can be installed through the Microsoft Systems Management Server (SMS) to all kinds of Windows environments:

- Windows 3.1 and 3.11
- Windows for Workgroups
- Windows 95
- Windows NT 3.51 and NT 4.0

This section provides you, the network system administrator, with information about the steps you should take in order to easily deploy F-PROT with SMS. It is assumed that you are familiar with SMS as well as the Autoinst methods of F-PROT. See Appendix D: Autoinst Configuration for information about the usage of Autoinst on Windows environments.

For information on using SMS, see the documentation in the Microsoft Windows NT Server Resource Kit, and the section "**Microsoft Systems Management Server**" on page 131.

6.1 Preliminary Steps

Before you can install F-PROT with SMS:

- Make sure that all potential client workstations have SMS clients software with Package Command Manager (PCM).
- Use queries to identify which clients have enough disk space to install F-PROT.
- Divide the potential client workstations to separate machine groups based on the operating systems.
- Prepare F-PROT source files for distribution using Autoinst.
- Create a Package Definition File (PDF) for each type of installation.

The latest PDFs for use with F-PROT templates are available at:

- http://www.DataFellows.com/f-prot/sms/

Designing the Management Network

You can use the following information to create queries for F-PROT.

Platform	Hard disk space required
Windows 3.1	4.0 MB
Windows 95	4.0 MB
Windows NT	5.0 MB

Remember to include the operating system with the queries so you can easily create a machine group for each operating system. Later you will use these machine groups to target F-PROT Professional installation jobs. Please remember also that as time progresses and further developments are created, more disk space may be required on any of these systems. Web Club updates will provide this information.

Windows NT 4.0 Service Pack 2 has known problems with the most anti-virus programs running on NT 4.0. Therefore it is not recommended to install F-PROT for Windows NT or F-PROT for Windows NT Server into a system that has Service Pack 2 installed, unless you have also installed the HotFix Microsoft created for this version of the NT kernel.

The kernel fix for Service Pack 2 is available at Microsoft's FTP site at:

- ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/NT40/hotfixes-postsp2/krnl-fix

See also Microsoft's Knowledge Base article Q141239 which is available at:

- http://www.microsoft.com/kb/articles/q141/2/39.htm

Preparing F-PROT Professional Installation for Distribution

In order to successfully distribute F-PROT Professional installations through the use of Microsoft Systems Management Server, the installation packages have to be prepared before the distribution. Since SMS uses Autoinst for installing and configuring F-PROT for Windows on client workstation side, an Autoinst installation kit has to be created.

To create Autoinst installation kit, do the following:

1. Launch F-PROT.
2. Log in as F-PROT Administrator.
3. Choose "Distribute F-PROT Installations" from the Administration menu.
4. Choose the "By Creating Installation Directory for Autoinst" option.
5. Enter the correct path for the shared directory in the Create Installation Directory At field. This is where the Autoinst installation package will be created. Note that this directory has to be visible to SMS.
6. Choose OK to start the creation of the Autoinst installation package. F-PROT program files will be copied to new destination directory.
7. Optionally, adjust the user profile of F-PROT for Windows by Choosing Modify and making the desired changes in the dialog that opens.
8. When F-PROT has transferred all the program files and you have optionally modified the User Profile, the creation of the Autoinst installation package is complete.

The Autoinst installation directory should now contain the following subdirectories and files:

File/Directory	Description
Install	Contains program files needed for installation.
Preferen	Contains configuration files for installation.
Tasks	Contains default set of task files.
AutowXX.exe	Autoinst application for various versions of Windows.
Autoinst.ini	Configuration file used by Autoinst.

On 32-bit Windows platforms, Autow32.exe is run. On Windows 3.1 and Windows for Workgroups, Autow31.exe is run. The Autoinst.ini file is common for all Windows platforms.

The following sections cover only those of Autoinst settings that are significantly important for SMS distribution.

The Autoinst initialization file, Autoinst.ini, meets the requirements of the distribution environment. Note: if you are using Autoinst Tuner for modifying Autoinst.ini file, which is highly recommended, the section names in code samples will refer to corresponding tab sheets names in Autoinst Tuner.

Source Directories of Autoinst Installation

Autoinst supports relative path names for the source and target directory paths, since SMS needs the directories to be referred with relative names. By default, the following entries should have the values:

```
[Install]
InstallFrom=INSTALL\
[Preferences]
PreferencesFrom=PREFEREN\
[FPW]
TasksFrom=TASKS\
```

Target Directory

Autoinst needs to know the target installation directory path in client workstation. By default this entry points to C:\F-PROTW directory but can be changed freely.

```
[Install]
InstallFrom=INSTALL\
InstallTo=C:\F-PROTW
```

Creating Program Group and Icons

Autoinst.ini file has entries for creating F-PROT Professional program group or folder as well as the appropriate program icons in client workstation after the installation .By default, entries are not in use. To activate them, remove the semicolon in the beginning of the desired line.

```
[FPW]
TasksFrom=TASKS\

; GroupName=F-PROT Professional
; Icon0=0,0,0,F-PROT for Windows
; Icon1=2,0,scana.fpt,Scan Drive A:
; Icon2=2,1000,scanallh.fpt,Scan All Hard Drives
```

In Windows NT environment, the program group and icons will be created under common group.

Installing F-Agent Service Under Windows NT

F-Agent Service needs an account to be correctly registered. F-Agent Service can be installed either under the generic Local System account or a specific account. F-Agent Service needs an access to shared F-PROT communication directory in order to receive updates, distributed tasks etc. therefore it is recommended that it is installed under a specific account; the account has to be given full access to F-PROT communication directory as well as to log in locally with service rights.

Since the password for the account can be delivered through Autoinst.ini and will not encrypted, it is strongly recommended to give only the minimum set of rights to that account, just enough to meet the requirements stated above. The account name and password will be given in following entries.

```
ServiceAccountName=F-PROT-GROUP
ServiceAccountPassword=PASSWORD
```

See http://www.datafellows.com/F-PROT/sms/ for the latest information about automating this process.

To enable F-Agent Service automatically after installation the following entry has to be set to a non-zero value.

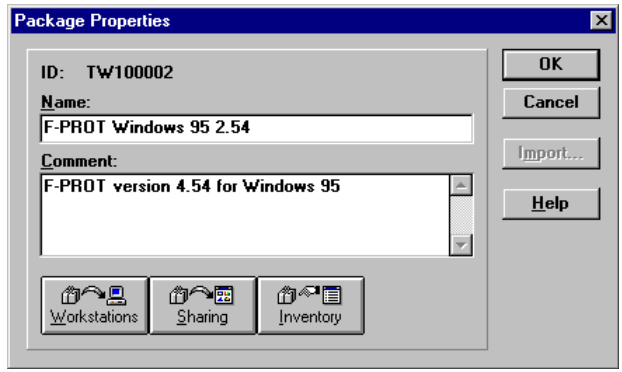
```
[F-Agent]
EnableAsService=1
```

6.2 Distributing F-PROT to Windows Workstations

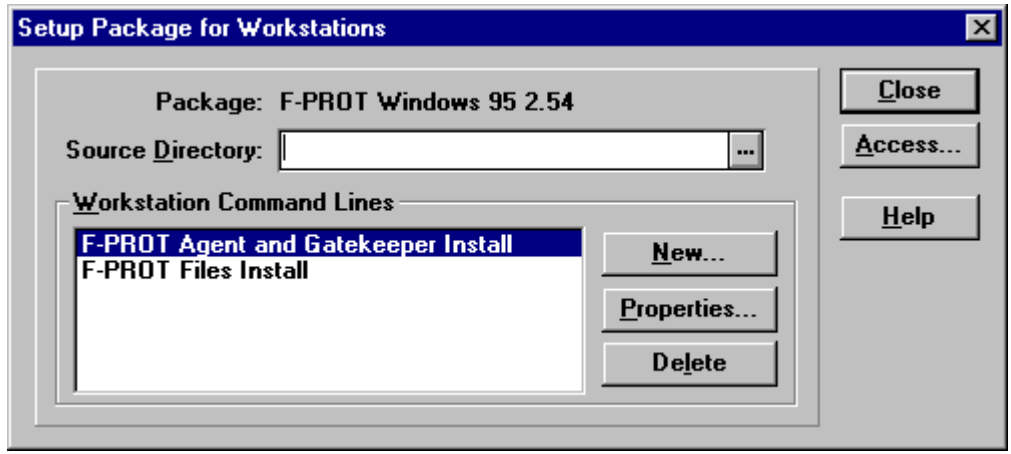
Creating the F-PROT package

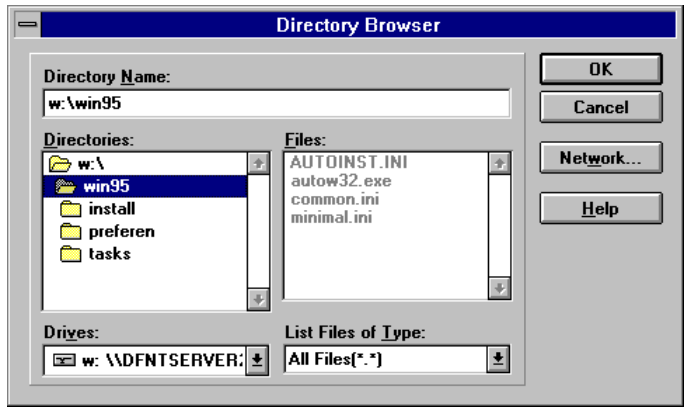
Before you can send F-PROT installation job to the target clients you must create the F-PROT package with SMS Administrator.

1. In the SMS Administrator, open the Packages window. From the File menu, choose New to get the “Package Properties” dialog box.
2. Choose Import. Find the right PDF file for the clients. For Windows 95 the PDF file is F-PROT95.PDF and for Windows 3.x the file is F-PROTW.PDF. The file is located in the F-PROT source directory.



3. Choose Workstations. In the source directory box enter the full UNC name for the source directory you made in step 2.2. You can also press ellipsis box and browse for the source directory. When browsing choose Network even if the source directory is within the same computer because this way SMS automatically converts the source directory into an UNC name.



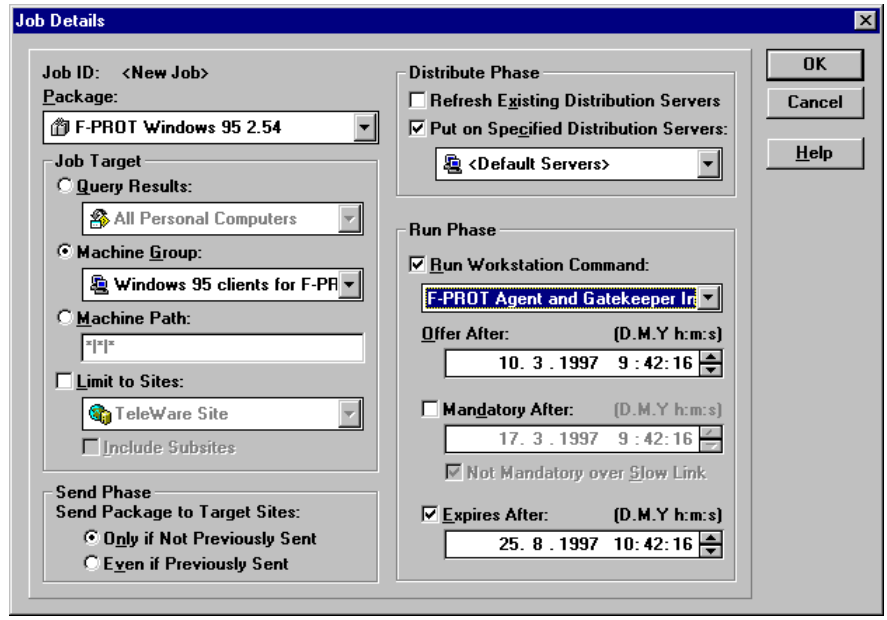


4. Choose OK in all open dialog boxes. When the package has been created and appears in the Packages windows, you can use it to create a job.

Creating the F-PROT installation job

When the package is ready you can create a job to install F-PROT to client workstations

1. In the SMS Administrator, open the Jobs window. From the File menu, choose New.
2. Check that the job type is Run Command on Workstation and choose Details.



3. Choose the F-PROT package and appropriate Job Target. Select the right machine group if you have created it.

4. If this is the first installation with F-PROT, the default Send Phase and Distribute Phase settings are correct. If you have already sent and distributed the package to the distribution servers and you want to send additional commands to workstations, clear the check marks in the Distribute Phase.

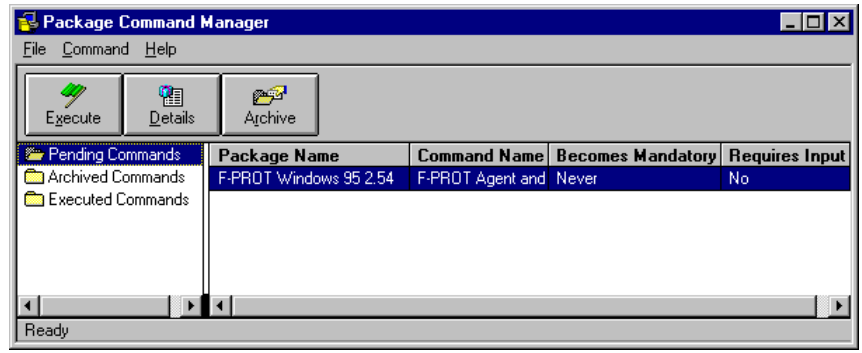
5. Select the right command for the clients. You have two choices:

- **F-PROT Agent and Gatekeeper Install** installs F-PROT Professional program files to client workstations and activates F-Agent and Gatekeeper.

- **F-PROT files Install** only copies F-PROT Professional program files to the workstations but does not enable either F-Agent or Gatekeeper after the installation.

Installing F-PROT to the client Workstations

After the sending and distributing of the F-PROT package is ready, the users see the F-PROT package when they next time log on the network (if SMSLS is in their logon script) or they run RUNSMS.BAT batch file.


Package Command Manager
File Command Help
Execute
Details
Archive
Pending Commands
Archived Commands
Executed Commands
Package Name
Command Name
Becomes Mandatory
Requires Input
F-PROT Windows 95 2.54
F-PROT Agent and
Never
No
Ready

6.3 Distributing F-PROT to Windows NT Workstations

Installation Methods

Installation of F-PROT Professional for Windows NT is more complicated than with Windows or Windows 95 because of Windows NT's security features. Gatekeeper for NT is based on kernel mode device drivers, which will be installed as system drivers. To be able to install the drivers properly, local administrator or equal rights are needed.

Since many users don't have administrator rights to their workstations, you have two choices:

1. You grant users Administrator privileges during the installation
2. You use Package Command Manager Service

Package Command Manager Service

Package Command Manager is normally installed as an application on SMS clients. Because it runs as an application, it only has the privileges assigned to the user account from which the application is run.

Fortunately Microsoft now provides Package Command Manager (PCM) service to Windows NT clients that are member of Windows NT domain and have SMS 1.2 installed. PCM service can be downloaded from Microsoft's website at:

- http://www.microsoft.com/SMSMGMT/pcmserv.htm

It will be a part of SMS 1.2 Service Pack 2, which is scheduled for release in the first quarter of 1997.

PCM service requires a user account that has administrator privileges on the client computer. It then can install software with administrative privileges. Thus, it can install software that PCM application cannot (e.g. F-PROT). However, you must keep in mind that PCM introduces a security risk. If users on any of the workstation could replace the PCMSVC32.EXE file with their own application, they could run any application with administrator privileges.

Also with PCM service you can install software completely in background so that users do not have to do anything. With the PCM application users must log on to activate PCM and must

execute a job or if it is a mandatory job it will be executed automatically within five minutes. However, with PCM service users do not see any dialog boxes and they do not log on to a workstation to install software.

See the PCM service documentation for more details about installing the PCM service.

Creating the F-PROT Package

Before you can send F-PROT Professional installation job to the target client workstations you must create the F-PROT package with SMS Administrator.

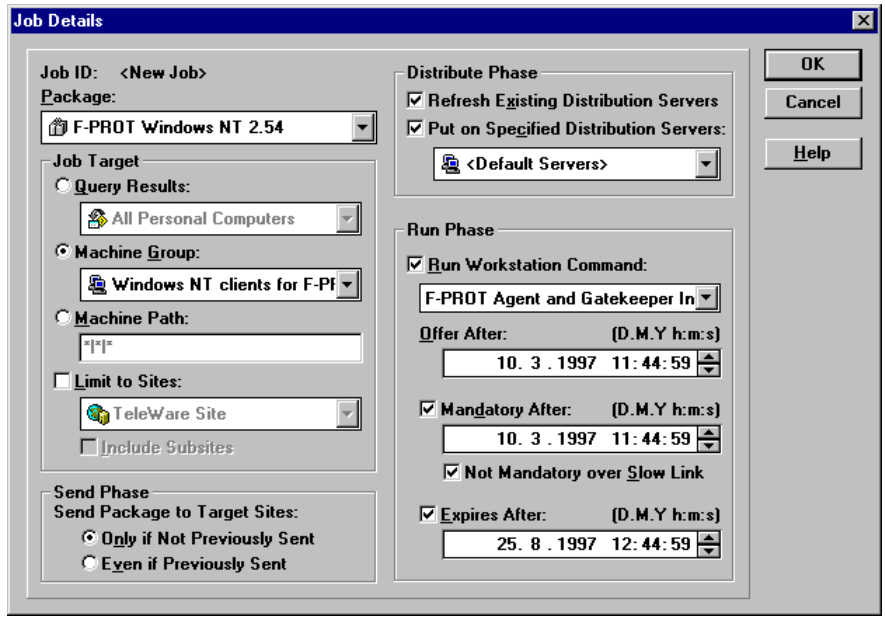
1. In the SMS Administrator, open the Packages window. From the File menu, choose New to get the “Package Properties” dialog box.
2. Choose Import. Find the right PDF file for the clients. For Windows NT the F-PROT PDF file is F-PROTNT.PDF. The file is located in the F-PROT source directory.
3. Choose Workstations. In the source directory box enter the full UNC name for the source directory you made in step 2.2. You can also press ellipsis box and browse for the source directory. When browsing choose Network even if the source directory is within the same computer because this way SMS automatically converts the source directory into an UNC name.
4. Choose OK in all open dialog boxes. When the package has been created and appears in the Packages windows, you can use it to create a job.

Creating the F-PROT installation job

When the package is ready you can create a job to install F-PROT to client workstations.

1. In the SMS Administrator, open the Jobs window. From the file menu, choose New.

2. Check that the job type is Run Command on Workstation and choose Details.



3. Choose the F-PROT package and appropriate Job Target. Select the right machine group if you have created it.

4. If this is a first installation of F-PROT Professional for Windows NT, the default Send Phase and Distribute Phase settings are correct. If you have already installed the package on distribution servers and you want to send additional commands to workstations, clear all check marks in the Distribute Phase.

5. Select the right command for the clients. You have two choices: "F-PROT Agent and Gatekeeper Install" installs F-PROT files to clients and activates gatekeeper. "F-PROT files Install" only copies F-PROT files to the workstations. F-PROT files install can be run with only user privileges.

6. If you want to use PCM Service and install F-PROT in background, you must check Mandatory After and insert correct date and time. PCM service installs software only after the job becomes mandatory.

Install Using Package Control Manager Service

If you are using the Package Control Manager (PCM) service the software is installed when the job becomes mandatory. However, the PCM service will not run jobs while the PCM application is running. If you have not replaced old PCMWIN32.EXE with a modified one, you must make

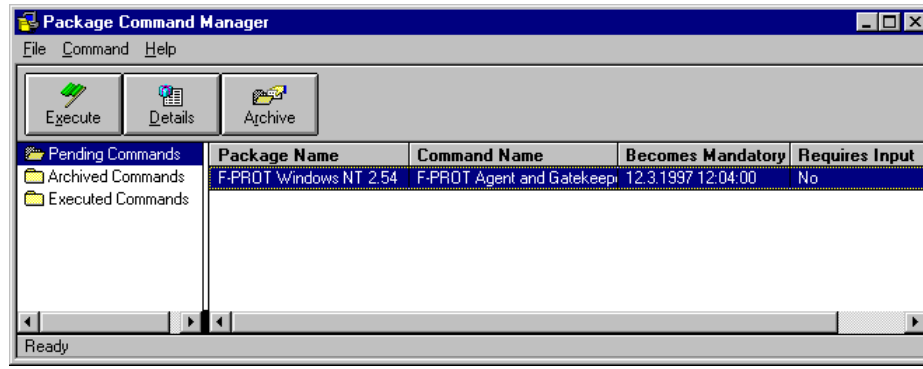
sure that PCM application is not running. To make sure that the PCM application is not running, either disable or remove the PCM application or make sure that no user is logged on.

Any packages sent to Windows NT clients with the package properties Automated and System (Background) Task (like F-PROT installation by default) must be performed by the PCM service rather than by the PCM application. A modified version of PCMWIN32 is available from Microsoft. It will not attempt to run jobs that are Mandatory and that have the package properties Automated and System (Background) Task. Those jobs will wait until the PCM application is not running and will be run then by the PCM service. See the PCM service documentation for more details.

PCM application is running although its window is not visible. You can close the PCM application by logging out or by stopping it using Windows NT Task Manager (NT 4.0 only).

Install Using PCM Application

After the sending and distributing of the F-PROT package is ready, the users see the F-PROT package when they next time log on the network (if SMSLS is in their logon script) or they run RUNSMS.BAT batch file.



7 Appendix D: Autoinst Configuration

This section describes the format of Autoinst.INI, the configuration file for the F-PROT Autoinst installation tool. Note that Data Fellows is constantly adding new features to Autoinst and therefore, new settings are being added for Autoinst.INI all the time. The latest settings which are not covered in this manual can be found in Autoinst Technical Specification. The latest version of this document is available online at Data Fellows WWW server at:

- http://www.DataFellows.com/f-prot/support/autoinst/

The latest information about the keywords supported by Autoinst is available at:

- http://www.DataFellows.com/f-prot/support/autoinst/autoinst-file-format.htm

If you don't have access to the Internet, ask your F-PROT support for that information. For more information about your technical support options, see "Technical Support" on page 17.

7.1 Using Autoinst

Autoinst is a utility program that enables the system administrator to have any version of F-PROT Professional 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-PROT 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, the following information will be useful.

F-PROT 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" on page 131 for more information. The latest information about SMS support is available at:

- http://www.DataFellows.com/f-prot/sms/

Security Issues

Please note the following:

- Autoinst and its initialization file should be write protected by the administrator, so that workstations have read-only access to them.
- The source directory should be write protected by the administrator.
- Autoinst is checksum-protected, which means that it can detect changes to its own code.

Invoking Autoinst

The installation parameters for Autoinst are stored in an inifile. The name of the inifile can be specified on the command line:

```
Autoinst [switches] [inifile]
```

If no name is specified, Autoinst will use the file Autoinst.INI, which is located in the same subdirectory. Throughout this document, the inifile for Autoinst will be referred to as Autoinst.INI.

There are five sample INI files in the Autoinst directory under the F-PROT directory. The INI file for installing F-PROT Gatekeeper, COLO.INI, may look like this:

```
; This INI file for Autoinst can be used to install F-PROT Gatekeeper
; locally to workstations. Communication between F-PROT Gatekeeper
; and F-PROT Professional for Windows is installed.
;
; Modify drive letters and directories to suit your system.
;
; Sections [Administration] and [F-Agent] are not needed if F-PROT
; Professional for Windows is already installed at users' workstations.
[Autoinst]
ShowErrorMessages=1
; set ShowProgress=3 and StopAtExit=1 for troubleshooting purposes
ShowProgress=0
StopAtExit=0
ContactAdmin=Autoinst error! Please contact your network administrator!
NoVersionInfoDisplay=0
WindowMode=0
WindowTitle=F-PROT Gatekeeper Installation
WriteAtStartup=
WriteAtStartup=Performing F-PROT Gatekeeper Automatic Installation.
WriteAtStartup=
WriteAtInstall=Installing F-PROT Gatekeeper files on your hard drive,
WriteAtInstall=please wait while the files are being copied.
WriteAtInstall=
WriteAtExit=F-PROT Gatekeeper installation is complete.
WriteAtExit=
WriteAtExit=If you experience any problems, contact your network
administrator!
WriteAtExit=
[Local]
; the WindowsDirectory= entries are only used by Autoinst for DOS
WindowsDirectory=C:\WINWG
WindowsDirectory=C:\WINDOWS
WindowsDirectory=C:\WIN3
WindowsDirectory=C:\WIN31
WindowsDirectory=C:\WFW
[Install]
SoftwareID=FPW
InstallFrom=V:\F-PROTW\SOURCE
InstallToWin=F-PROTW
[Administration]
AdministrationEnabled=1
CommunicationDirectory=V:\F-PROTW\COMM
UserName=%USER%
WorkstationName=%USER%'s PC
[Preferences]
LastChange=95-03-22
set=F-PROTW.CFG|Network|RptAdmin|1
set=F-PROTW.CFG|Network|InfAdmin|0
[Gatekeeper]
Enable=Always
AccessSettings=1
[F-Agent]
```

```
Load=Always
```

7.2 Configuration File Sections

Autoinst

The [Autoinst] section of Autoinst.INI specifies the settings for the Autoinst program itself, for example:

```
[Autoinst]
ShowErrorMessages=1
ContactAdmin=Please contact your network administrators!
ShowProgress=1
```

The ShowErrorMessages= entry specifies whether Autoinst shows error messages when it encounters problems while performing its actions. If there is an error, Autoinst displays the message, which describes the error, along with the text specified in the ContactAdmin= entry.

The ErrorNoWinDir= entry specifies whether Autoinst displays the error message if no Windows directory is found; the default value is 1.

The ShowProgress= entry determines whether Autoinst displays information about the progress of its actions. It may have values from 0 to 3. ShowProgress=3 is useful for troubleshooting, as Autoinst will then display the most detailed information about its actions.

The InstallIfWinOnly= entry specifies whether the software should be installed in any case, or only if Windows is found on the system. The default value is 0 (always install). The following options are available:

Option	Function
Win31	Install if Windows 3.1x is installed
Win95	Install if Windows 95 is installed
WinNT	Install if Windows NT is installed

These values can be used in any combinations, separated by white spaces, for example: InstallIfWinOnly=Win31 Win95.

The StopAtExit= entry specifies whether Autoinst terminates after performing all its actions; the default value is 0. If the specified entry value is other than zero, Autoinst stops and displays the following message: “Autoinst has terminated. Press Enter to continue.” A nonzero value is useful for troubleshooting, as this will give you a chance to examine Autoinst’s output.

Autoinst can be forced to show special messages, specified in the inifile. Multiple entries can be written; in this case the messages are displayed in the order of their appearance in the inifile. Empty entries are shown as empty lines.

The texts specified in the WriteAtStartup= entries are shown at start-up; the texts specified in the WriteAtInstall= entries are shown before the program files are copied; and the texts specified in the WriteAtExit= entries are displayed in the end. If WriteAtExit= is specified, the default exit message is not shown.

If the NoVersionInfoDisplay= entry is set to zero, no copyright and version information for Autoinst is shown.

The WindowMode= and the WindowTitle= entries are only valid for the Windows version of Autoinst. Unlike the DOS version, Autoinst for Windows also obtains information about the local Windows directory from Windows. Other from that, the Windows version of Autoinst behaves exactly the same as the DOS version and accepts the same parameters.

The WindowMode= entry in the [Autoinst] section determines the visibility of the Autoinst for Windows window. The following options are available:

Option	Function
0	The window is shown normally (default)
1	The window is shown minimized (iconized)
2	The window is not shown

In any case, the window is shown if an error occurs, or if a stop at exit has been specified.

The title on the caption of the Autoinst window can be specified in the WindowTitle= entry of the [Autoinst] section. If it is not given, the window is titled “AUTOINST”.

The Autoinst for Windows obtains information about the local Windows directory from Windows. Hence, the WindowsDirectory entries in the [Local] section are ignored.

If F-PROT or the Gatekeeper is installed by the Windows version of Autoinst, F-PROT, F-Agent, and F-PROT Gatekeeper are unloaded upon installation in order to be able to update the program files of these applications. Then, F-Agent or F-PROT Gatekeeper will be reloaded, if so specified.

Local

Autoinst normally alters the workstation’s local WIN.INI and SYSTEM.INI files; for that it needs to know the location of the workstation’s Windows directory. While the Windows version of Autoinst obtains this information from Windows, Autoinst for DOS uses the WindowsDirectory= entry in the [Local] section of Autoinst.INI to determine the location of the Windows directory. It

is possible for different PCs in the network to keep their Windows directories in different locations, so multiple paths can be given, for example:

```
[Local]
WindowsDirectory=C:\Windows
WindowsDirectory=C:\WINWG
```

Autoinst searches these paths for certain Windows files to determine which path matches the proper Windows directory.

Autoinst accepts environment variables in "WindowsDirectory=" entries in order to support network installations of Windows. The environment variable name must be enclosed in double quotation marks, e.g.:

```
WindowsDirectory=H:\HOME\"USER"\WINDOWS
```

Install

The [Install] section of an Autoinst.INI file specifies the source directory on a network drive, from which the files will be copied, and the destination directory on a local drive, where the files will be installed, for example:

```
[Install]
InstallFrom=V:\GATEKEEP
InstallTo=C:\WINDOWS\GATEKEEP
```

If the InstallFrom entry is not present, or is empty, no error messages are produced, but the InstallTo= or InstallToWin entry is ignored. If the InstallFrom= is not empty, but the specified directory does not exist or is invalid (does not exist and creation fails), Autoinst displays an error message.

Note that you may specify an UNC pathname (\\servername\directory\directory) in the InstallFrom= entry. The entry may also specify a relative pathname (no drive/root directory). In that case, the path is relative to the directory where Autoinst resides.

The source directory should be write-protected by the administrator.

If the destination directory does not exist, it will be created.

Instead of the InstallTo= entry, InstallToWin= can be used. It specifies the destination path relatively to the user's Windows directory, for example:

```
InstallToWin=GATEKEEP
```

This installs the program files to C:\WINDOWS\GATEKEEP if the workstation's Windows directory if C:\WINDOWS. If both the InstallTo= and InstallToWin= are specified, InstallTo= will be used. Both InstallTo= and InstallToWin will be ignored, if InstallFrom= is not given.

- **If any files are present in the destination directory, specified in the entry InstallTo= or InstallToWin=, Autoinst assumes that an update is being performed**

Autoinst can be used for remote installations. In such installations, Autoinst does not copy the files from a network drive to a local drive, but the installed application is run directly from the network drive. In order to change the inifiles appropriately, Autoinst needs to know where the

application resides. Its location is specified in the [Install] section using the InstallRemote entry, for example:

```
InstallRemote=V:\GATEKEEP
```

InstallFrom= takes precedence over InstallRemote=.

Note that you may specify an UNC pathname (\\servername\directory\directory) in the InstallRemote= entry. The entry may also specify a relative pathname (no drive/root directory). In that case, the path is relative to the directory where Autoinst resides.

The SoftwareID= entry should be changed only when installing software other than F-PROT Or the Gatekeeper. For keeping track of installed software, Autoinst stores the installed software's ID and location in the [DFAPPS] section of the user's WIN.INI file, for example:

```
[DFAPPS]
FPW=C:\WINDOWS\GATEKEEP
```

Autoinst assumes that the software, which it installs, is either F-PROT Or the Gatekeeper, or both. If you wish to install other software, specify its ID in the [Install] section, for example:

```
SoftwareID=MySoftware
```

No entry is written to WIN.INI, if a "null" software is specified:

```
SoftwareID=0
```

☞ **Do not use a different software ID when installing F-PROT Or the Gatekeeper; either leave the Software ID entry out, or set SoftwareID=FPW.**

Administration

Both F-PROT and the Gatekeeper can be set up in a networked environment, so that information about infected files is sent to administrator. In F-PROT there are also other administrator-user communication features. However, all these features work only if the communication directory has been established on a shared drive. The administrator should properly install F-PROT on the system to set up the communications directory and to manage the information.

Once this has been done, the administrator can specify the communication parameters in the [Administration] section of Autoinst.INI, for example:

```
[Administration]
AdministrationEnabled=1
CommunicationDirectory=V:\GATEKEEP\SHARED
SpoolDirectory=C:\WINDOWS\GATEKEEP\SHARED
UserName=%USER%
WorkstationName=%USER%'s PC
```

All the settings in the [Administration] section will only take effect if the AdministrationEnabled= entry has a value other than zero.

The UserName= and WorkstationName= entries specify the names of the environment variables that hold the user and workstation names for the local workstations, respectively. The environment variables must be entered between the % characters.

These names are needed in order to identify the infected computer: upon finding an infected file, F-PROT Or the Gatekeeper sends a message, containing the user name and the workstation name, to the administrator. To make identification possible, Autoinst fetches the values of the specified environment variables and stores them in the F-PROTW.CFG file.

The user and workstation names can also be obtained from the initialization files, rather than from the environment variables. The UserNameFromIni= and the WorkstationNameFromIni= entries can be specified for this purpose. The syntax of these entries is “inifile|section|entry," for example:

```
UserNameFromIni=C:\TOOLS\PCTCP\PCTCP.INI|pctcp general|full-name
```

The above means, that the user name can be obtained from the C:\TOOLS\PCTCP\PCTCP.INI file, namely from the “full-name=” entry in the [pctcp general] section. If the full pathname of the initialization file is not specified, it is assumed that the file is in the user’s Windows directory. Multiple "UserNameFromIni=" and "WorkstationNameFromIni=" entries may be given. In that case, the first entry for which the specified value is found, will be used.

All these parameters are stored in the F-PROT Or the Gatekeeper configuration file, F-PROTW.CFG. Autoinst will simply take the values from Autoinst.INI, and store them in F-PROT.CFG.

☞ **If one of the names has not been specified and administration has been enabled, F-PROT Or the Gatekeeper will prompt the user for it upon activation.**

If administration was enabled, Autoinst creates the appropriate subdirectory structure on the local workstation. F-PROT and the Gatekeeper will use these directories for temporary storage of data before it is sent to the shared communication directory on a network drive. These subdirectories are created under the directory specified in the SpoolDirectory= entry. If no such entry is present, the SHARED directory under the program files directory is used. The following subdirectories are created:

Name	Function
INFECT	Stores infected files
REPORTS	Stores reports and messages
SUSPECT	Stores suspected files

The SpoolDirectory= entry should always be specified if remote installations are made. If this entry is not present with a remote installation, Autoinst shows an error message.

If administration was enabled, Autoinst makes the following changes to the settings of the installed F-PROT : 1) Enable network features, 2) Switch to the user mode, 3) Disable the stand-alone installation setting.

Preferences

The settings for F-PROT and the Gatekeeper are stored mainly in F-PROTW.CFG, and partially in other files, such as DFAPPS.INI and F-PROTW.INI.

Autoinst copies the files to the local workstation's Windows directory from the directory specified in the PreferencesFrom= entry in the [Preferences] section, for example:

```
[Preferences]
PreferencesFrom=V:\GATEKEEP\USERS
```

However, the files previously residing in the local workstation Windows directory are not overwritten. This ensures that the changes users have done to the settings are retained.

Note that you may specify an UNC pathname (\\servername\directory\directory) in the PreferencesFrom= entry. The entry may also specify a relative pathname (no drive/root directory). In that case, the path is relative to the directory where Autoinst resides.

The administrator can create different configurations for different user groups by specifying separate Autoinst.INI configuration files with pointers to various Preferences directories.

If the PreferencesFrom= entry is not specified, the files F-PROTW.CFG, DFAPPS.INI, and F-PROTW.INI are copied, if present, from the source directory specified in the InstallFrom= or the InstallRemote= entry of the [Install] section.

The administrator can force certain setting to be set to certain values each time Autoinst is run. This is done by specifying these values in the [Preferences] section of Autoinst.INI. The entry format is:

```
set=filename|section|entry|value
```

<Filename> refers to a file in the local workstation's Windows directory. Note that this feature also allows system administrators to change settings of the files WIN.INI, SYSTEM.INI, and others.

The administrator can specify that the changes to F-PROT Preferences are to be made only at certain times. This is done by adding the following entry to the [Preferences] section:

```
LastChange=YY-MM-DD
```

The specified date will be written into WIN.INI as:

```
[DFAPPS]
SOFTWARE_ID|PrefsLastChange=YY-MM-DD
```

If Autoinst is run, and the respective dates in Autoinst.INI and WIN.INI match, no changes are made to the settings. Note that in that case, none of the entries in [Administration], [FPW], [Gatekeeper] and [F-Agent] sections will have any effect. If the LastChange= entry is not present, the changes are made every time.

Autoinst can be used for adding groups to Program Manager. To do that, the administrator has to prepare a groupfile and store it in the source directory specified in the PreferencesFrom= entry; Autoinst copies it to the user's Windows directory. To add this group to the Program

Manager program groups, the administrator should write its name in the AddGroup= entry of the [Preferences] section, for example:

```
AddGroup=F-PROTW.GRP
```

Note that this feature should only be used with DOS Autoinst, as the Windows versions of Autoinst can create the program group by themselves; see the FPW section for more information.

Certain initialization files, such as F-PROTW.CFG, are encrypted to prevent users from changing the settings manually. Autoinst decrypts such files before making changes there, and re-encrypts them afterwards.

Gatekeeper

The administrator can force some of the F-PROT Gatekeeper's preferences to be set in the [Gatekeeper] section of the Autoinst.INI. The settings that are not specified there, retain the values stored in F-PROTW.CFG.

Enabling F-PROT Gatekeeper

The Enable= entry determines whether F-PROT Gatekeeper is enabled upon Windows startup. The same settings apply to Gatekeepers for all Windows platforms.

For F-PROT Gatekeeper for Windows 3.1x, Autoinst adds A-PROT.EXE to the RUN= line of WIN.INI and adds the line device=c:\path\F-PROTW.386 to the [386Enh] section of SYSTEM.INI if F-PROT Gatekeeper is to be enabled. If F-PROT Gatekeeper is not to be enabled, Autoinst makes sure these changes are removed from WIN.INI and SYSTEM.INI.

For F-PROT Gatekeeper for Windows 95 and F-PROT Gatekeeper for Windows NT, the appropriate changes are made to the system registry. Because of that, only Autoinst for 32-bit Windows (AUTOW32) can be used for installing F-PROT Gatekeeper for these platforms.

The following options are available:

Option	Function
Enable=Always	Will always enable F-PROT Gatekeeper
Enable=Never	Will always disable F-PROT Gatekeeper
Enable=OnInstall	Will enable F-PROT Gatekeeper only if an installation is performed
Enable=OnUpdate	Will enable F-PROT Gatekeeper only if an installation or update is performed
Enable=NotOnInstall	Will disable F-PROT Gatekeeper only if an installation is performed
Enable=NotOnUpdate	Will disable F-PROT Gatekeeper only if an installation or update is performed

Uninstalling F-PROT Gatekeeper

Autoinst can also be used for uninstalling the software. If Uninstall=1 was specified, Autoinst removes all the F-PROT Gatekeeper's files from the local workstations. It also removes references to F-PROT Gatekeeper from WIN.INI and SYSTEM.INI files or the registry.

The Uninstall= option has precedence over other options; if is was specified, all the other options are ignored.

Other Entries

The AccessSettings= entry specifies whether the user can access the F-PROT Gatekeeper settings dialog in order to enable or disable the Gatekeeper or otherwise change its settings.

The ConfirmDosSessionKill= and the ConfirmWinDenyAccess= entries specify the values for the respective settings (only applies to F-PROT Gatekeeper for Windows 3.1x).

The F-PROTW.386= entry can be used for specifying the alternative path to the device driver (only applies to F-PROT Gatekeeper for Windows 3.1x). If F-PROTW.386= was specified, the device= entry in the SYSTEM.INI file will not determine the installation destination. Instead, it will be written exactly as specified in the F-PROTW.386= entry. This enables the VxD to be loaded from a different location, than the rest of F-PROT Gatekeeper, for example:

```
F-PROTW.386=c:\F-PROTW.386
```

An appropriate entry is also written to F-PROTW.INI. F-Agent will use it when it enables Gatekeeper.

F-Agent

The Load= entry in the [F-Agent] section determines whether F-Agent will be loaded upon Windows startup. WIN.INI or the registry will be appropriately changed.

There are six available options:

Option	Function
Load=Always	Will always load F-Agent
Load=Never	Will never load F-Agent
Load=OnInstall	Will load F-Agent only if an installation is performed
Load=OnUpdate	Will load F-Agent only if an installation or update is performed
Load=NotOnInstall	Will not load F-Agent if an installation is performed
Load=NotOnUpdate	Will not load F-Agent if an installation or update is performed

Autoinst for 32-bit Windows also supports installation of F-Agent as a service under Windows NT. In order to install F-Agent as a service, set EnableAsService=1.

FPW

The settings for F-PROT Professional for Windows 3.1, F-PROT Professional for Windows 95, and F-PROT Professional for Windows NT are specified in the [FPW] section.

If Uninstall=1 is specified, Autoinst removes all the F-PROT files from the local workstations, and removes references to these files from the workstations' WIN.INI and SYSTEM.INI files or the registry.

The LocalDirectory= entry specifies the root of F-PROT local data directories. These directories, namely BULLETIN, INFECT, MESSAGES, REPORTS, REPUSER, SUSPECT, and TASKS, are used for storing task files, reports, bulletins, and other items. If no LocalDirectory= entry is present, a directory named LOCAL is created under the program files directory and serves as a root for these data directories.

The LocalDirectory= entry should be always specified when remote installations are made, because the user's data files must reside on the local workstation. If the LocalDirectory= entry is missing, and the local programs directory is unknown, the tasks are not copied during installation, because Autoinst does not know the location of the local TASKS directory. Autoinst will give an error message, if it does not find this entry during a remote installation.

☞ **The local data directories will always be created, even if only F-PROT Gatekeeper is being installed. Autoinst assumes that F-PROT is being installed, if the SoftwareID= is set to the default value FPW.**

The TasksFrom= entry specifies the directory from which the task files are to be copied during installation. Parameters of each F-PROT task are stored in an encrypted task file, located in the local TASKS directory. When F-PROT is started, it reads all the task files and displays the corresponding tasks on the task list.

Note that you may specify an UNC pathname (\\servername\directory\directory) in the TasksFrom= entry. The entry may also specify a relative pathname (no drive/root directory). In that case, the path is relative to the directory where Autoinst resides.

Since the tasks must be in sync with the user's F-PROTW.CFG, the new tasks cannot be copied over the previously installed tasks. Therefore, they are copied only if there are no tasks in the local workstation's TASKS directory.

The Windows versions of Autoinst supports the creation of a Start menu folder (or Program Manager program group in Windows 3.1 and Windows NT 3.x) for F-PROT. The parameters of this group are also given in the [FPW] section. The GroupName= entry specifies the name of the Program Manager group to be created or updated, for example:

```
GroupName=F-PROT for Windows
```

The IconX= entries specify the program items to be created or updated: X denotes a number from 0 to 15. The entries have the following format:

```
IconX=ICON_TYPE, DRIVE_ID, TASK_NAME, ICON_TITLE
```

ICON_TYPE can take the following values:

Value	Function
0	Start F-PROT Professional for Windows
1	Start F-Agent
2	Execute a task with F-PROT Professional for Windows

DRIVE_ID specifies the drive to be scanned by the task: 0 corresponds to Drive A:, 1 to Drive B:, 2 to Drive C:, etc. 1000 denotes All HDDs, and 1001 denotes All Network Drives.

TASK_NAME specifies the name of the task file for the task to be launched when the icon is double-clicked; it is used only if the ICON_TYPE is set to 2.

ICON_TITLE is the text that appears below the icon in the Program Manager.

An example of the group parameters:

```
GroupName=F-PROT Professional for Windows
Icon0=0,0,0,F-PROT for Windows
Icon1=2,0,scana.fpt,Scan Drive A:
Icon2=2,1,scanb.fpt,Scan Drive B:
Icon3=2,1000,scanallh.fpt,Scan All Hard Drives
Icon4=2,1001,scannetw.fpt,Scan Network
Icon5=1,0,0,F-Agent
```

TSRLoad

The [TSRLoad] section specifies the load options of TSR programs like VIRSTOP. These programs can be installed on a workstation with Autoinst just like any other software.

The ID= entry defines the program's identifier, for example:

```
[TSRLoad]
ID=VIRSTOP
```

This identifier is used in subsequent entries for specifying the load options for that program. Multiple TSRs can be installed by using multiple ID= entries and their options.

The <id>= entry, where "<id>" stands for the ID, as defined by the ID= entry, specifies the name of the TSR's program file, for example:

```
VIRSTOP=virstop.exe
```

This entry is required; an error occurs if it is not present. Neither the drive, nor the path needs to be specified, since they are determined by the location of the installation, as specified in the [Install] section. However, the full pathname can be given here, if installation of a file already present on the system is desired. In any case, an error occurs if the file is not found on the system.

The <id>|LoadFrom= entry specifies the full pathname of the load file, from which the TSR will be loaded, for example:

```
VIRSTOP|LoadFrom=C:\AUTOEXEC.BAT
```

This entry is required, an error occurs if it is not present. The specified file must already exist, otherwise an error occurs as well.

The <id>|LoadPos= entry specifies the position of the TSR's load command inside the load file. The following options are available:

Option	Function
BeginFile	The command will be written at the beginning of the load file (default)
EndFile	The command will be written at the end of the load file
LineNumber,<n>	The command will be inserted before line number <n>. Negative line numbers denote lines from the end of the file:-1 for the last line, -2 for the last but one line.
RelativeToLineWith,<increment>,<substring>	The command will be inserted <increment> lines after the first line containing <substring>. Increment can be negative for inserting the command before the line containing <substring>
BeforLineWith,<substring>	The command will be inserted immediately before the line containing <substring>
AfterLineWith,<substring>	The command will be inserted immediately after the line containing <substring>

For example, the following entry will cause the command to be written immediately before the line containing "win.com":

```
VIRSTOP|LoadPos=RelativeToLineWith,-1,win.com
```

The <substring> parameter is case insensitive.

The <id>|LoadPrefix= entry, if present, causes a string to be inserted before the command. The prefix is inserted immediately before the command, without any spaces in between. It is useful for making drivers to be loaded from CONFIG.SYS, or for specifying the LOADHIGH option, for example:

```
VIRSTOP|LoadPrefix="LH"
VIRSTOP|LoadPrefix="device="
```

☞ **The quotation marks are required.**

The <id>|LoadSuffix= entry, if present, causes a string to be appended to the command. The suffix will be appended immediately after the command, without any spaces between them. It is useful for specifying load options for programs, for example:

```
VIRSTOP|LoadSuffix="/COPY"
```

☞ **The quotation marks are required.**

The <id>|ReplaceOption= entry specifies what action should be taken if there already is a command that loads the executable, which is specified in the <id> entry. The following options are available:

Option	Function
RetainOld	The old command will always be retained; no change will be made to the load file
RetainOldIfSame	The default option. The old command will be retained only if it exactly matches the new command (same path, same name, same suffix)
ReplaceOld	The old command will always be replaced

The <id>|ReplaceAtOldPos= entry, if not zero, forces the new command to be inserted at the location of the old command, if the latter exists in the load file. In that case, the <id>|LoadPos= entry will be ignored.

☞ **Unless the <id>|ReplaceAtOldPos= entry is present and has a value other than zero, the position of the new command is determined by the <id>|LoadPos= entry.**

7.3 Special Considerations for 32-Bit Platforms

The settings described below only apply to the 32-bit Windows version of Autoinst (AUTOW32.EXE).

In addition to the "UserName=", "UserNameFromIni=", "WorkstationName=" and "WorkstationNameFromIni=" settings (see [5.2]), the "UserNameFromRegistry=" and "WorkstationNameFromRegistry=" entries are supported. They will be used only if none of the other entries are present. Multiple "UserNameFromRegistry=" and "WorkstationNameFromRegistry=" entries may be used: the first one that points to a value in the registry will take effect.

The format for the values of both these entries (called "registry locators") is:

MAINKEY [\ SUBKEY] \\ [VALUENAME]

where:

Option	Function
MAINKEY	main key name, must be one of: HKEY_CLASSES_ROOT", "HKEY_CURRENT_USER", "HKEY_LOCAL_MACHINE", "HKEY_USERS"
SUBKEY	subkey name, may be missing
VALUENAME	name of registry value, may be missing if the default value is to be used

For example, the following are valid locator specifiers.

All items present:

```
UserNameFromRegistry=HKEY_LOCAL_MACHINE\Network\Logon\\username
```

No subkey:

```
UserNameFromRegistry=HKEY_LOCAL_MACHINE\\user-name
```

No value name:

```
UserNameFromRegistry=HKEY_LOCAL_MACHINE\Network\Logon\\
```

No subkey nor value name:

```
UserNameFromRegistry=HKEY_LOCAL_MACHINE\\
```

8 Appendix E: F-PROT Professional for DOS

F-PROT Professional for DOS is included in your F-PROT Professional for Windows license to let you boot the computer up from a trusted diskette if it refuses to start Windows. This section contains information about using F-PROT Professional for DOS.

The original diskette should be write-protected and kept in a safe place, because it may be needed in case of a virus outbreak. We also recommend that you create a Rescue Disk for use when you discover a problem. This will make it easier to recover from disk crashes, virus infection, or data loss caused by an error.

F-PROT Professional for DOS performs at two levels:

1. VIRSTOP is a memory-resident background scanning program. The main purpose of VIRSTOP is to prevent the execution of programs infected with known viruses.
2. Further protection against virus infection is given by the disk-based program, F-PROT Professional, which offers more comprehensive virus scanning as well as facilities to recover from virus infections.

8.1 Installing F-PROT Professional for DOS

To install F-PROT Professional for DOS, follow the steps listed below:

1. Start your computer preferably from a clean write-protected diskette.

2. Insert the write-protected F-PROT Professional for DOS diskette into the appropriate drive and switch to that drive. This is usually drive A:.

3. Type **A:install** and press Enter

If the version you are installing has more than one language, you will first be asked the installation language. After you select the language, the main installation screen appears.

This screen shows the command line switches that will be set when VIRSTOP is installed and running. If your computer is not short of memory, deselect **\DISK** by moving to **VIRSTOP,** using the ARROW keys, and then pressing ENTER. A menu will be displayed.

Press the SPACEBAR to toggle the switch setting to **No**, and press ENTER to make the change. Press ESC twice to get back to the main menu and move to **Start Installation.** Press ENTER to start installation.

Important: If you are running Windows, we recommend that you use Gatekeeper from F-PROT for Windows, and do not install VIRSTOP at all.

4. Before the installation is complete, a message will be displayed, asking whether you would like to change the message which VIRSTOP gives whenever it finds a virus. Press **y** if you wish to have a customized message displayed. Write the message to the message line and press enter.

5. When the installation is complete, you will be queried whether you want F-PROT to scan the hard disk immediately. We recommend that you press **y**.

Once the hard disk has been scanned and found to be clean, the following message appears:

```
No viruses or suspicious files/boot sectors were found.
```

F-PROT Professional for DOS is now installed.

6. The virus-stopping program, VIRSTOP, can be activated at once by restarting the computer. To do this, remove diskette from the drive A: and press CONTROL ALT DEL simultaneously. From now on whenever you start your computer, the background virus stopper, VIRSTOP, is actively checking for viruses each time files or disks are used. If VIRSTOP finds a problem, it gives a signal and displays a message on the screen. In this case, follow the displayed instructions.

7. Run F-TEST program from the F-PROT directory to check whether VIRSTOP is properly installed and working.

F-PROT Professional for DOS can be used directly from the supplied diskette, but the hard disk installation speeds it up and makes it easier to use. F-PROT Professional for DOS takes up about two megabytes of hard disk space. However, some of the files can be omitted to save storage space. The files essential for normal operation of F-PROT Professional for DOS with the background-checking program VIRSTOP active in memory are: F-PROT.exe, VIRSTOP.exe, Sign.def, and English.tx0 or another .tx0 language file. If you choose this minimum configuration, you will not be able to change the language used or view the virus descriptions. Otherwise, the program will function normally.

Important: While F-PROT for DOS does not search for Windows-based macro viruses, you can use F-MACRO to scan for macro viruses from within DOS. The latest version of F-MACRO is available at:

- http://www.datafellows.com/F-PROT/macro/

8.2 Using DOS F-PROT in Interactive Mode

When F-PROT Professional for DOS is installed on the hard disk, as described in the section 14.1, “Installing F-PROT Professional for DOS,” it is located on the hard disk, drive C:, in the F-PROT directory.

To start F-PROT Professional for DOS, type:

```
C:\
cd \F-PROT
F-PROT
```

F-PROT will load the stored virus information and scan for the known viruses. Then, the main menu is displayed.

Functions of F-PROT Professional for DOS

Using F-PROT Professional for DOS you can do the following:

- Scan for viruses.
- Configure F-PROT Professional to present information in various ways.
- Look up information on known viruses or add information on new viruses.
- Obtain information about the program.
- Quit the program.

Scanning for Viruses

When **Scan** is chosen from the main menu, a sub-menu, showing the current option selections, is displayed.

The following options are available for scanning parameters:

Method	Secure Scan
	Heuristic Analysis
Search	Hard disk
	Diskette drive
	Network
	<User -specified>
Action	Report only
	Disinfect/Query
	Automatic disinfection
	Delete/Query
	Automatic deletion
	Rename/Query
	Automatic renaming
Targets	Boot sector viruses (Yes/No)
	File viruses (Yes/No)
	User-defined strings (Yes/No)
	Packed files (Yes/No)
Files	Standard executables
	All files
	<User-specified>

Scanning Method

F-PROT Professional for DOS can scan for viruses using both methods: **Secure Scan** and **Heuristic Analysis**. Scanning is the virus detection method in which a file or a boot sector is read, checking for characteristics of known viruses. Heuristic (pattern-recognition) analysis, which gives a high level of protection against new viruses, uses a set of rules to detect suspicious code. The heuristic algorithms used by F-PROT Professional detect new, previously unknown viruses.

VIRSTOP uses the **Quick Scan** scanning method. As it name implies, the **Quick Scan** is faster, but less secure, than **Secure Scan**, and cannot find some complicated encrypted viruses and some viruses, written in high-level languages.

Where to Search

The **Search** command is used to select the drives and directories F-PROT Professional for DOS should search for viruses. The following options are available:

Hard Disk	Scans all partitions on the internal hard disk.
Diskette Drive	Scans one of the diskette drives. Some removable hard disks also show in the **Diskette Drive** menu, due to drivers used.
Network	Scans all the network drives. By using this option, a network server's hard disk, except for its boot sectors, can be scanned for viruses from a workstation.
User Specified	Scans a drive, directory, or file, specified by the user. If a directory is selected, F-PROT checks all of its subdirectories as well.

Action on Finding a Virus

The **Action** command is used to choose the action to be taken on the infected file when the virus is found. The following options are available:

Report only	Default action; lists the name of the infected files.
Disinfect/Query	F-PROT prompts for confirmation before it attempts to disinfect the file. If the infection cannot be removed, the file is deleted. F-PROT asks for confirmation before deleting the file.
Automatic disinfection	The file is disinfected without confirmation request.
Delete/Query	The file is overwritten several times and then deleted. F-PROT asks for confirmation before deleting the file/
Automatic deletion	The file is deleted without confirmation request.
Rename/Query	F-PROT renames the file, asking for confirmation first. The extensions are changed from .exe to .vxe, from .com to .vom.
Automatic renaming	The file is renamed without confirmation request.

Target Virus Type

The **Targets** command of the main menu is used to specify the types of viruses to search for. The default is to search for boot sector viruses, file viruses, and to search within packed files. The available options are described below:

Select **Boot sector viruses (Yes/No)** alone if you are cleaning up after an attack by a specific boot sector virus.

Select **File viruses (Yes/No)** alone if you are cleaning up after an attack by a specific file virus.

Select **User-defined strings (Yes/No)** if you have manually updated F-PROT Professional for DOS with new search strings.

Select **Packed files (Yes/No)** to have F-PROT search for viruses in packed files. Regardless of whether the infection occurred before or after packing, F-PROT Professional for DOS can find viruses in files packed with LZEXE, PKLITE, EXEPACK, DIET, and ICE. If the infection occurred after packing, F-PROT can find it in archives packed with other tools, as well.

Files To Be Scanned

The **Files** command is used to select which types of files F-PROT should scan. Most viruses will only infect standard executable files.

The default choice, **Standard executables**, is to scan the usual executable file types with the extensions: .com, .exe, ov?, app, .pgm, and .sys. This option is recommended for normal scanning.

All files should be selected if you are cleaning up after a virus attack. This will ensure that the virus is not hiding in some obscure overlay file.

The **<User-specified>** option allows the user to add a set of file extensions, for example, XTree Gold's .xtr overlays to the list of files to be scanned.

Executing Scan

When you have selected the desired options, start the scan by choosing **Begin Scan** at the top of the **Scan** menu.

The window at the bottom of the screen will display the names of the files as they are scanned. The scanning can be canceled at any time simply by pressing ESC.

When the scan is finished, a summary of its results is displayed. If viruses or suspicious programs were found, press ENTER to view the report. Press S to save report on the disk, or press P to print it out.

Configuring F-PROT Professional for DOS

Presentation of information by F-PROT Professional for DOS can be configured using the two commands: **Language** and **Setup**.

The default language for messages is English. Use the **Language** command to view the listing of the languages supported by your version of F-PROT. If alternatives are available, choose the one you require. You will need to re-install VIRSTOP with the new language setting.

Use the **Setup** command to set up the list of information about viruses, which is available under the **Viruses** command of the main menu. This list can be displayed in two ways: by lines or by columns. By lines is the default choice. To change it, press Y after choosing the **Setup** command.

Information on Viruses

When a virus is found, it is important to get information about it. View information about viruses by choosing **Viruses** from the main menu. Use the PAGE UP and PAGE DOWN keys to move around the list and to select the virus in question. Then press ENTER to view the detailed information.

Alternatively, get straight to the detailed information by starting typing the virus name. As soon as the virus name can be uniquely identified, the detailed information is displayed.

New Virus Search Strings

In the event of a sudden new virus epidemic, the virus search strings can be added to F-PROT Professional for DOS before its next update is available. The search strings can be entered by choosing **New search strings** under **Viruses**.

After selecting **New search strings**, choose **Add a new search string.** You will be queried about the name of the virus; whether it infects .com files, .exe files, and boot sectors; and then asked to enter the hexadecimal search string.

Choose **List user-defined search strings** to view the names of the viruses whose search strings were added, the names of the objects they infect, and the search string for each virus.

Choosing **Delete a search string** displays the names of the user-defined viruses. Select the name of the virus you wish to delete. Confirmation is needed prior to deletion.

You can also directly edit the user.def file, since it is a plain ASCII file, for example:

```
CEB New_virus
000102030405060708
```

Exiting from F-PROT Professional for DOS

To exit from F-PROT, press ESC repeatedly, until you return to the main menu. Once in the main menu, choose **Quit**.

If you changed any options settings, either save the new settings by pressing Y, or exit without saving them by pressing N.

It is not recommended to save the changes on the original F-PROT Professional for DOS diskette, as it should be write-protected all the time. Use a copy instead.

Using F-PROT Professional for DOS in Command-Line Mode

F-PROT Professional for DOS is usually run without any parameters when it enters the interactive mode. It is also possible to run F-PROT in the command-line mode, which makes it easier to tailor F-PROT to perform desired searches. When F-PROT is run from a diskette in the command-line mode, it works almost as fast as when run from the hard disk.

F-PROT Professional for DOS can be started from the command line as follows:

```
F-PROT [drive, directory, or file] [parameters]
```

F-PROT will then enter the command-line mode, unless the **/inter** parameter was given. The available parameters are listed below.

/640	Only scan 640K of memory.
/all	Check all files.
/analyse	Use heuristic analysis instead of search strings.
/append	Used with **/report** to append to existing report.
/auto	Automatic deletion.
/beep	Sound an alarm if a virus is found.
/command	Force command-line mode.
/delete	Delete all infected files.
/disinf	Disinfect whenever possible.
/ext=	Specify default extensions for files to scan, use period as a separator.
/freeze	Freezes the machine if a virus is found in the memory.
/freeze2	Freezes the machine if a virus is found on the disk.
/guru	Report with more details when using heuristic analysis.
/hard	Scan all DOS partitions on the hard disk.
/help	Display this list.
/inter	Force interactive mode.
/list	List all files checked.
/mono	Use monochrome mode on color displays.
/multi	Scan multiple diskettes.
/net	Scan any network drives found.
/nobreak	Do not abort scan if ESC is pressed.
/nofloppy	Do not test if there is a diskette in drive A:
/nomem	Skip initial memory scan.
/nosub	Do not scan subdirectories.
/nowrap	Do not wrap text in reports.
/[no]boot	[Do not] scan boot sectors.
/[no]file	[Do not] scan files.
/[no]packed	[Do not] scan inside packed files.

/[no]user	[Do not] scan for user-defined patterns.
/page	Pause after each page (command-line mode)
/rename	Rename infected files to .vom or .vxe.
/report=	Send the output to a file.
/silent	Do not generate output to screen.
/version	Return with version number as an **errorlevel** value.

Some examples of useful command lines are:

```
F-PROT A:
Scan a diskette using the Secure Scan method.
F-PROT A: /multi /auto /disinf
Scan multiple diskettes with automatic disinfection.
F-PROT c: /list /report=list.txt
Make a secure scan on drive C: and send a list of scanned files to
List.txt.
F-PROT /hard /all
Scan all files on all the partitions of the hard disk.
F-PROT /hard /nofile
Scan only the memory and boot sectors for viruses.
F-PROT D: E: /all
Scan all files on drives D: and E:.
F-PROT /net
Scan all network drives.
F-PROT I:\PD
Scan a public domain directory on the file server.
F-PROT c:\ /nosub
Scan just the root directory of drive C:.
```

F-PROT scans in the command-line mode can be aborted by pressing ESC unless **/nobreak** parameter was used.

When F-PROT is run in the command line mode, it will return an exit code, which can be checked with the DOS **errorlevel** command.

0	Normal exit; nothing found.
1	Abnormal termination, unrecoverable error (usually a missing or corrupted F-PROT file.)
2	Self-test failed, program has been modified.
3	A Boot/File virus infection found.
4	Virus search strings found in memory.
5	Program terminated be ESC.
6	At least one virus was removed.
7	Out of memory.
8	Suspicious files found, not necessarily a virus.

F-PROT Professional for DOS can be executed every time the computer is started by adding the necessary command line to the Autoexec.bat file. A batch file FP.BAT is included on the installation diskettes. If this batch file is called from Autoexec.bat, it runs F-PROT on the start-up and displays the message appropriate to the exit code. This batch file can be easily modified to suit the paths and requirements of the user.

The F-PROT Professional for DOS package includes the following components:

F-PROT.EXE	The main module of F-PROT Professional for DOS, with virus scanning and disinfecting features.
VIRSTOP.EXE	The virus stopping program that offers active protection from viruses.
INSTALL.EXE	The F-PROT Professional for DOS installation program, which also configures VIRSTOP.
F-TEST.COM	A utility program for verifying that VIRSTOP is operating.
SIGN.DEF	A database, containing search strings for viruses. This file is encrypted.
SETUP.F2	Used for storing user preferences.
VERSION_N.NNZ	Used with FPUPDATE.BAT to return the version number, N.NNZ, of the package.
ENGLISH.TX0	Used for language support, along with such files as: ITALIANO.TX0, SWEDISH.TX0, VIR-HELP.ENG, VIR-HELP.ITA and others.
F-MACRO.EXE	DOS-based program which scans for macro viruses.
MACRO.DEF	Library of search strings for macro viruses, used by F-MACRO.EXE.

9 Glossary

access control

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

AUTOEXEC.BAT

The command file automatically executed during system startup in DOS.

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.

bit

The smallest unit of memory size, sets of which make up bytes, arranged in a sequential pattern to express text, numbers, or other detailed information, recognizable by the computer's processing system.

Boot

To restart the computer.

boot sector

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

byte

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

checksum

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

CMOS

Complimentary 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.

COM file

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

CONFIG.SYS

The configuration file automatically executed during system startup in DOS.

CPU

Central Processing Unit, the “brain” of the computer, usually housed in a “box”, the rectangular unit which may be separate from the monitor.

CRC

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

DOS

Disk Operating System, the most basic system type originally used on all Personal Computers.

EXE file

An “executable” file, or program file; the type of file that “runs”, as contrasted with a document or data file.

HPFS

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

kilobyte

One thousand (1 000) bytes of information.

LAN

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

MBR

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

Megabyte

One thousand (1 000) kilobytes, or one million (1 000 000) bytes, a moderately large unit measure of computer memory.

Modem

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

multipartite virus

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

mutating virus

A virus which changes (mutates) as it progresses through the host files. Physiologically cancer is a mutating virus, which alters tissues and changes itself as it proceeds with creating damage. Similarly mutating viruses in the software world can change themselves as well as the host files, making disinfection a greater challenge.

NFS

Network File System used by many Unix variants.

NTFS

NT File System used by Windows NT.

RAM

Random Access Memory, the dynamic memory used by the processor at the time of processing.

reset

To warm boot the system.

ROM

Read Only Memory, static memory storage holding information for the processor to use, not to edit or delete.

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.

SMS

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

stealth virus

A virus which hides itself from view by intercepting disk access requests. When an anti-virus program tries to read files or boot sectors to find the virus, it feeds the reading program a clean image of the object being read.

time bomb

Destructive action triggered at some specific date or time.

timestamp

The creation or last modification time recorded for an object.

trojan horse

Program that purposefully does something the user that starts it does not expect.

virus

Parasitic program capable of attaching itself to files or disks and replicating itself repeatedly.

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.

10 Index

L

M

N

P

R

S

T

U

W