Introduction

The boom in communications networks in recent years, and especially the extraordinary growth of the Internet, has made the use of electronic mail enormously popular.

One of the greatest advantages of e-mail is the possibility of sending and receiving files. This has also become a new entry point for viruses.

Exchanging documents via electronic mail is very common practice. This, to a great extent, has facilitated the spreading of Word and Excel viruses. You must bear in mind, however, that all types of viruses can be sent and received via e-mail, not only Word and Excel viruses.

Conventional antiviruses are not capable of efficiently detecting and disinfecting viruses located in e-mail messages for the following reasons:

1. E-mail messages are normally stored in a mail database using a specific format and compression and/or encryption techniques that prevent scanning using conventional antiviruses.

2. E-mail messages and their attached files are often stored in servers that conventional antiviruses cannot access.

For the above reasons, an electronic mail antivirus must be specifically designed to detect and remove viruses in e-mail environments. For this, the main features an electronic mail antivirus should possess are the following:

- Totally automatic scanning of messages immediately upon receipt.
- Automatic scanning of messages upon opening.
- Automatic scanning of each message to be sent. In this way, you avoid the possibility of sending virus-infected messages.
- Automatic scanning of all messages that are saved.
- Scanning of all e-mail messages at any time upon user demand.
- Integration with the electronic mail program.
- Possibility of scanning compressed files.
- Possibility of scanning nested messages (messages inside other messages).

Panda Antivirus for Exchange/Outlook is an electronic mail antivirus that possesses all of the above features, together with many more, that complete its effectiveness and convert it into a powerful, but easily configured tool that prevents all risks when working with e-mail messages.

NOTE
The following products are explained in this manual:

- Panda Antivirus Exchange/Outlook
- Panda Antivirus Exchange/Outlook Network Client

The first permits the direct installation of Panda Antivirus Exchange/Outlook on one computer. The second permits you to distribute this antivirus to all the workstations of a network, thereby simplifying the network administrator's job.

Please refer to the part of the manual that corresponds to the product you have acquired.

Installation

Requirements

Panda Antivirus Exchange/Outlook requires:

- IBM compatible computer capable of running Windows 95, Windows 98 or Windows NT Workstation 3.51 or 4.0.
- MS-Exchange and/or MS-Outlook.
- 3 MB hard disk space.

Installation

To install Panda Antivirus Exchange/Outlook, insert disk number 1 in the disk drive and run the SETUP.EXE program.

The installation process consists of a series of windows in which you will be asked for the information necessary to carry out the installation.

Once the installation has concluded, we recommend you to reset the computer. The Exchange/Outlook antivirus will not begin to work until you reset Exchange/Outlook.

Uninstallation

To uninstall Panda Antivirus Exchange/Outlook, you must close the Exchange/Outlook mail program, go to the *Control Panel*, choose the *Add or Remove Programs* option and select Panda Antivirus Exchange/Outlook from the list. Once you have done this, press the *Add or Remove* button. The uninstallation will conclude in a matter of seconds. You should not try to uninstall this version by deleting the folder in which it was installed. It must always be uninstalled following the indicated procedure.

How to scan with Panda Antivirus Exchange/Outlook

On-demand scanning

To scan a specific folder, first select it. If you select a folder that contains other folders (for example, a mailbox), all dependent folders will be scanned. Once you have chosen the folder, press the Scan button in the MS-Exchange/Outlook standard button bar or select the *Scan in search of viruses* option from the *Tools* option in the MS-Exchange/Outlook main menu.

Once the scan has concluded, you will be able to view a results report containing details of any incidents found during the scan.

Panda Antivirus Exchange/Outlook also permits you to scan one or more messages. To do this, select the message or messages you want to scan. Once selected, press the on-demand scan button to start scanning.

To select several messages, click on them while pressing the Control key. If you want to select a group of messages, select the first and then click on the last while pressing the Shift key.

Real-time protection

Permanent protection allows you to work with your mail without having to worry about viruses, as Panda Antivirus Exchange/Outlook will monitor all suspicious operations for you.

The permanent protection takes care of scanning for viruses in:

- All new messages received.
- All messages you want to send.
- All messages opened, regardless of whether they were received before or after the installation of the antivirus.
- All messages you want to save.

The permanent protection can be easily enabled or disabled by pressing the corresponding button in the MS-Exchange/Outlook standard button bar.

Panda Antivirus Exchange/Outlook is capable of scanning compressed files and nested messages (messages inside other messages), thereby offering the highest possible levels of protection.

How Panda Antivirus for Exchange/Outlook works

Panda Antivirus Exchange/Outlook is completely integrated in the MS-Exchange/Outlook program. All the antivirus handling is therefore performed from the mail program itself.

Panda Antivirus Exchange/Outlook adds four buttons to the MS-Exchange/Outlook standard button bar. These four buttons are:

Scan: This button starts the scanning of the folder or messages selected at the beginning of the scanning process. All subfolders found in the selected folder will be scanned. A window permits you to follow the scanning process by showing the set of folders to be scanned, the folder that is currently being scanned and a progress bar.

Results report: This buttons displays a report of incidents found by the antivirus. This report is saved from one session to another until the user decides to delete it.

Enable or disable the antivirus: This button allows you to enable or disable the Panda Antivirus permanent protection. If this protection is disabled, the Panda Antivirus Exchange/Outlook program will not scan new messages received or sent in search of viruses. Neither will it scan messages you open to read. However, you will be able to scan a specific folder or message at any time by means of the Scan button. The startup scan for the Exchange/Outlook program will be performed even though the permanent protection is disconnected.

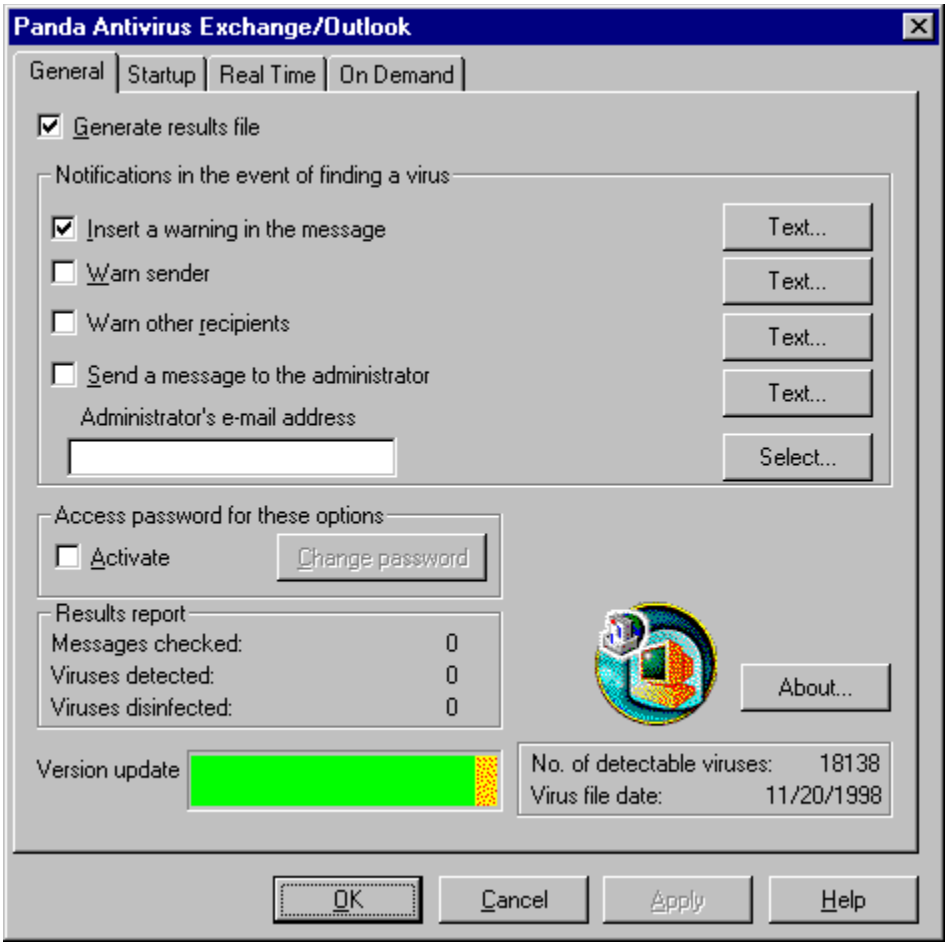
Configure: This button displays the Panda Antivirus Exchange/Outlook configuration window. Through this window you can configure the general behavior of the antivirus, its behavior at the startup of the mail program and its behavior as permanent protection and on-demand protection. You can also access the Panda Antivirus Exchange/Outlook configuration by selecting *Options* from the *Tools* option in the MS-Exchange/Outlook main menu. A page called Panda Antivirus Exchange/Outlook will appear in this options window, from which you can configure the antivirus.

Configuration of Panda Antivirus Exchange/Outlook

Panda Antivirus Exchange/Outlook permits extensive configuration of each of its functions. The configuration window is divided into several pages, each of which refers to a specific part of the antivirus.

General

The options listed on this page are of a general nature and determine the behavior of the antivirus in all cases. They are as follows:



Generate results file: If this option is checked, all the antivirus scanning operations will log the diverse incidents in a results file.

Insert a warning in the message: If this option is checked, every time a virus is found in a message, a text will be added to the message in the form of a warning. This message will be added regardless of the action you have decided to take when a virus is found. The message is customizable, thereby allowing the user to insert whatever text he/she wants.

Warn sender: If this option is checked, every time a virus is found in a message, a notification will be sent to the sender of the infected message to warn him/her of the situation. The message text the sender will receive is completely configurable, thereby enabling you to customize it.

Warn other recipients: If this option is checked when a virus is found in a message, a notification message will be sent to the other recipients of the message, if there are any. In this way, you can warn users who may not be protected against viruses. The message text the other recipients will receive can also be customized.

Send a message to the administrator: If you check this option and indicate the administrator's e-mail address, a notification message will be sent to the system administrator every time a virus is detected in a message. The text of this notification message is completely customizable.

Enable password: If this option is checked, the Panda Antivirus Exchange/Outlook configuration will be protected by a password. In this way, no unauthorized user will be able to change the antivirus configuration.

Change password: This button permits you to change the password that protects the Panda Antivirus Exchange/Outlook configuration.

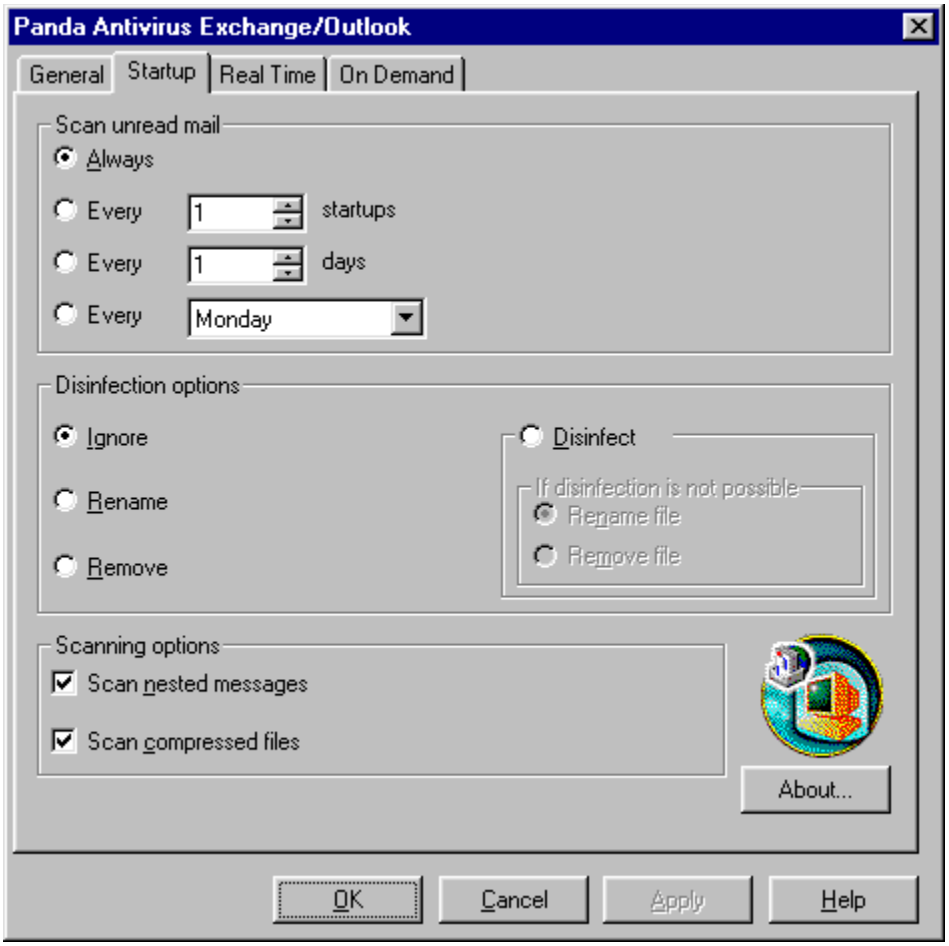
Results report: This option displays information on how many messages were scanned, how many viruses were detected and how many were disinfected.

Version update: This displays a graphic representation of the update status of the antivirus.

Version details: The number of detectable viruses and the virus file date provide information about the version of the antivirus installed.

Startup

This is where you can configure the behavior of the antivirus at the startup of the MS-Exchange/Outlook e-mail program. The available options are as follows:



Always scan unread mail: If this option is checked, every time MS-Exchange/Outlook is started up, all unread messages in the Inbox will be scanned.

Scan unread mail every certain number of startups: If this option is checked, the unread messages in the Inbox will be scanned every time your e-mail program reaches the specified number of startups.

Scan unread mail every certain number of days: If this option is checked, the scanning of the unread messages in the Inbox will only be performed when the specified number of days has passed.

Scan mail certain days: If this option is checked, the unread messages in the Inbox will only be scanned on the specified day of the week.

Disinfection – **Ignore:** If this option is checked when a virus is found, the antivirus will not carry out

any action.

Disinfection – **Rename:** If this option is checked when a virus is found, the antivirus will rename the virus-infected file.

Disinfection – **Remove:** If this option is checked when a virus is found, the antivirus will remove the infected file.

Disinfection – **Disinfect:** If this option is checked when a virus is found, the antivirus will try to disinfect the infected file.

Disinfection – **If disinfection is not possible, rename:** If the antivirus cannot disinfect an infected file, it will be renamed.

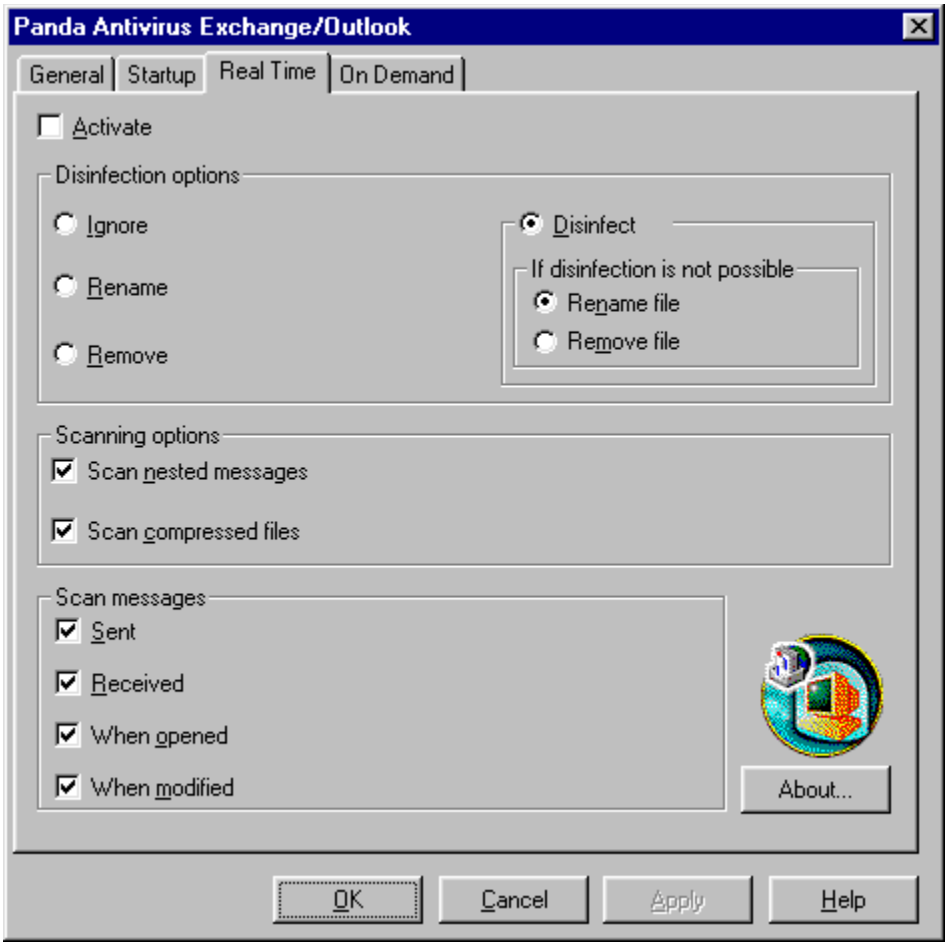
Disinfection – **If disinfection is not possible, remove:** If the antivirus cannot disinfect an infected file, it will be removed.

Scan nested messages: If this option is checked, nested messages will be scanned. In other words, if one message is found inside another, both messages will be scanned. The number of message levels that can be scanned depends on the computer's resources.

Scan compressed files: If this option is checked when a compressed file is found, it will be scanned in the same way as a normal file.

Real-time

This permits you to configure the permanent protection offered by the antivirus. The available options are as follows:



Enable: If this option is checked, the permanent protection will be enabled. This means that all incoming messages will be scanned, as well as all messages sent, opened or saved.

Disinfection – **Ignore:** If this option is checked when a virus is found, the antivirus will not carry out any action.

Disinfection – **Rename:** If this option is checked when a virus is found, the antivirus will rename the virus-infected file.

Disinfection – **Remove:** If this option is checked when a virus is found, the antivirus will remove the infected file.

Disinfection – **Disinfect:** If this option is checked when a virus is found, the antivirus will try to disinfect the infected file.

Disinfection – **If disinfection is not possible, rename:** If the antivirus cannot disinfect an infected file, it will be renamed.

Disinfection – **If disinfection is not possible, remove:** If the antivirus cannot disinfect an infected file, it will be removed.

Scan nested messages: If this option is checked, nested messages will be scanned. In other words, if one message is found inside another, both messages will be scanned. The number of message levels that can be scanned depends on the computer's resources.

Scan compressed files: If this option is checked when a compressed file is found, it will be scanned in the same way as a normal file.

Scan messages sent: If this option is checked, all messages you want to send will be scanned before sending. This prevents the sending of infected files.

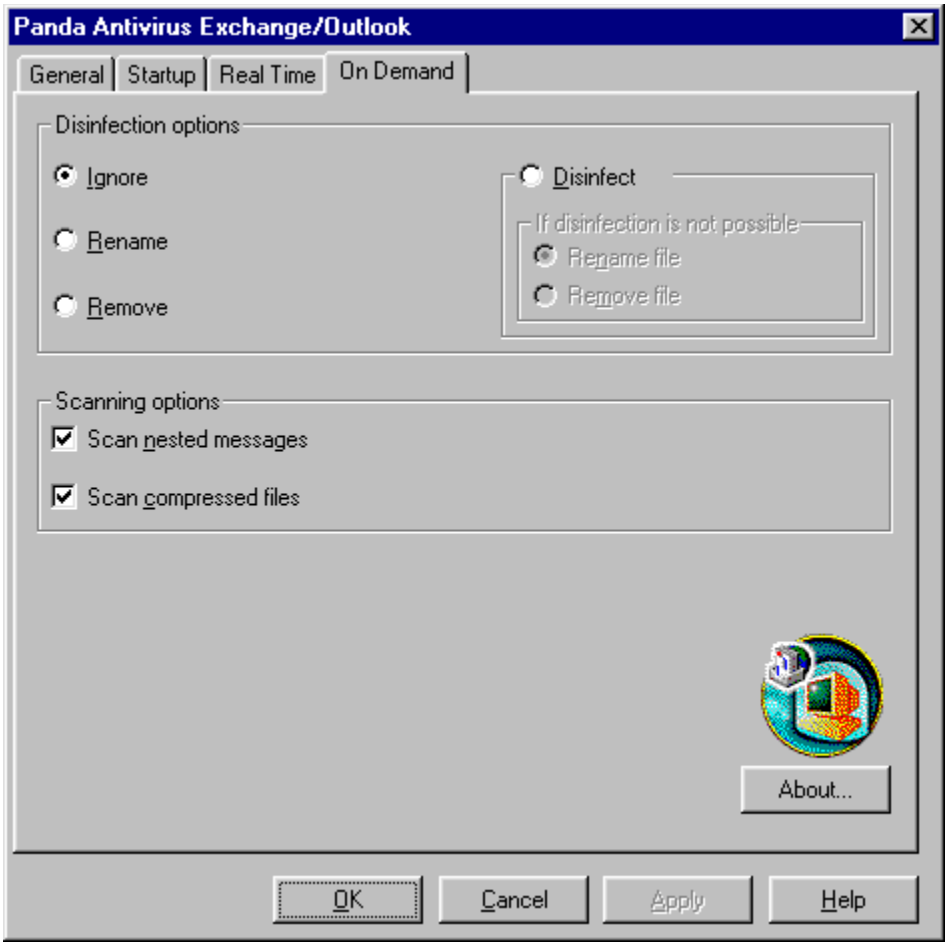
Scan messages received: If this option is checked, all messages received will be scanned immediately upon arrival, even before they are opened.

Scan messages when opened: If this option is checked, all messages opened will be scanned, regardless of when they were received.

Scan messages when modified: If this option is checked, all messages saved will be scanned.

On-demand

This is where you can configure the on-demand scanning offered by the antivirus. The available options are as follows:



Disinfection – **Ignore:** If this option is checked when a virus is found, the antivirus will not carry out any action.

Disinfection – **Rename:** If this option is checked when a virus is found, the antivirus will rename the virus-infected file.

Disinfection – **Remove:** If this option is checked when a virus is found, the antivirus will remove the infected file.

Disinfection – **Disinfect:** If this option is checked when a virus is found, the antivirus will try to disinfect the infected file.

Disinfection – **If disinfection is not possible, rename:** If the antivirus cannot disinfect an infected file, it will be renamed.

Disinfection – **If disinfection is not possible, remove:** If the antivirus cannot disinfect an infected file, it will be removed.

Scan nested messages: If this option is checked, nested messages will be scanned. In other words, if one message is found inside another, both messages will be scanned. The number of message levels that can be scanned depends on the computer's resources.

Scan compressed files: If this option is checked when a compressed file is found, it will be scanned in the same way as a normal file.

Introduction to the distribution throughout a network

The idea behind distributing the antivirus throughout a network is that of simplifying the work of a network administrator who wants to protect a series of workstations in the quickest and most comfortable way possible.

It is carried out in the following way:

1. The network administrator copies the antivirus to a server directory or a shared directory to which all users have access. This copy is performed through an installer program designed for this purpose. You must bear in mind that the antivirus is NOT being installed in the server. You are only copying the files necessary to install the antivirus in the workstations.

2. Each time a workstation connects to the network, the program will check to see if the antivirus is installed and updated. If so, it will do nothing, but if the antivirus is not installed or updated, it will proceed with the automatic installation or updating of the antivirus program.

As can be seen, the server (or shared resource) is only used as a means to distribute the antivirus to the workstations.

This general procedure is used for practically all types of networks. It is, however, performed slightly differently for each one. The procedure for the most common types of networks in current use will be explained is this manual.

How to distribute the antivirus throughout a network

Requirements

To distribute Panda Antivirus Exchange/Outlook throughout a network, you require:

- IBM compatible computer capable of running Windows 95, Windows 98 or Windows NT Workstation 3.51 or 4.0.
- 3 MB hard disk space on the server that will be used as the means of distribution.
- 3 MB hard disk space on each computer on which the antivirus is to be installed.

How to easily distribute the antivirus to all the workstations of a network

The process of distributing the antivirus to all the network workstations consists of two parts:

1. Copying the antivirus to a directory that all users can access.

2. Distribution of the antivirus to all workstations as they connect to the network by means of the RINSTALL program.

Below is a detailed description of how to perform the two previous steps. Some aspects of this installation process require knowledge of the type of network through which the antivirus is to be distributed. All this information is explained in detail for the major network types in their corresponding sections. Consult them if you should have any doubts.

Copying the antivirus to a directory that all users can access

The first step in the distribution of the antivirus through the network is the copying of files to a directory on one of the server's hard disks. It is essential that the copying of these files to the server be carried out in a virus-free environment. If this is not done, the antivirus files could be infected. As these files are distributed to all workstations that connect to the network, the virus would be distributed along with them. To obtain a safe file copy and to make sure that these files will not be infected from any workstation in the future, the copy must be carried out according to the following steps:

1. The administrator must make sure that his/her computer is virus-free. It would be advisable for the administrator to install the appropriate Panda Software antivirus on his/her computer and activate the corresponding permanent protection. You should not continue with the installation until you are sure that the computer from which you are installing the antivirus is completely virus-free.

2. Choose a directory in the corresponding server where you are going to copy the files. We recommend you to create a new directory called PAVEXCLI, to which all users have read access. It is important that no user should have *write* or *delete* access to this directory. Otherwise, any user could, accidentally or deliberately, infect or delete the antivirus files, thereby producing the serious consequences that this would imply.

3. Once you have created the target directory, just insert disk number 1 or the CD-ROM, go to the corresponding drive and run the SETUP.EXE program.

The installation process consists of a series of windows in which you will be asked for the data

necessary to carry out the installation in your computer. One of the details you will be asked for is the target directory. You must select the directory created for this purpose so that the antivirus files can be copied to it.

Distribution of the antivirus

This is where the advantage of our antivirus for networked PCs can clearly be seen. Rather than having to go from station to station installing the antivirus, this will be automatically installed as soon as a workstation connects to the network.

When a workstation connects to a network, a series of commands or programs are normally executed to prepare it to operate on a network, in the same way as a series of commands or programs are executed when a computer is booted. This series of commands and/or programs is known as a *Login Script.*

Our antivirus with network distribution capacity comes with a program called **RINSTALL**, which takes care of the automatic distribution of the antivirus. Therefore, achieving the automatic distribution of the antivirus is as easy as placing the **RINSTALL** execution in the *Login Script*.

RINSTALL will be run every time a workstation connects to the network. **RINSTALL** first checks to see if the connected workstation has the antivirus installed. If it is installed and updated, nothing is done, and the rest of the commands in the *Login Script* are executed as normal. If the workstation does not have the antivirus installed or if it is not updated, **RINSTALL** will install the antivirus. Once this has been done, the execution of the remaining *Login Script* commands continues as normal.

As the **RINSTALL** operation is completely automatic, the network administrator only needs to copy the files and modify the *Login Script* to install the antivirus protection, which will be distributed to the workstations as they connect to the server.

Distribution of the antivirus in a Novell NetWare network

To automatically distribute the antivirus to all workstations as they connect to a Novell NetWare network, you must insert the following line in the *System Login Script*:

```
#F:\PAVEXCLI\RINSTALL PAVEX.SCR
```

Consult the Novell NetWare section to obtain a more detailed explanation of these aspects.

As can be seen in the example, you must indicate the server location where the antivirus files can be found. This line must therefore come *after* the drive mapping, leaving this part of the *System Login Script* as follows:

```
MAP ROOT F:=ALFA\SYS:
#F:\PAVEXCLI\RINSTALL PAVEX.SCR
```

(assuming that the server name is ALPHA and the files are located in the SYS volume).

Distribution of the antivirus in a Windows NT network

To automatically distribute the antivirus to all workstations as they connect to the network, you must add the following line to the *Logon Script* using the Profile Manager program:

Consult the Windows NT section to obtain a more detailed explanation of these aspects.

```
F:\PAVEXCLI\RINSTALL PAVEX.SCR
```

As can be seen in the example, you must indicate where the antivirus files were copied. This line must therefore come *after* the mapping of the shared resources, leaving this part of the *Logon Script* as follows:

```
NET USE F: \\ALFA\SYS
F:\PAVEXCLI\RINSTALL PAVEX.SCR
```

(assuming that the server name is ALPHA and the shared resource is called SYS).

Distribution of the antivirus in an OS/2 network

To automatically distribute the antivirus to all workstations as they connect to the network, you must add the following line to the PROFILE.BAT (or PROFILE.CMD) file:

Consult the OS/2 section to obtain a more detailed explanation of these aspects.

```
F:\PAVEXCLI\RINSTALL PAVEX.SCR
```

As can be seen in the example, you must indicate where the antivirus files were copied. This line must therefore come *after* the mapping of the shared resources, leaving this part of the PROFILE.BAT file as follows:

```
NET USE F: \\ALFA\SYS
F:\PAVEXCLI\RINSTALL PAVEX.SCR
```

(assuming that the server name is ALPHA and the shared resource is called SYS).

Distribution of the antivirus in a Pathworks network

To automatically distribute the antivirus to all workstations as they connect to the network, you must add the following line to the connection sequence of the group of users on whose computers the antivirus is to be installed:

```
F:\PAVEXCLI\RINSTALL PAVEX.SCR
```

As can be seen in the example, you must indicate where the antivirus files were copied. Because of this, it is advisable to define the drive mapping before running RINSTALL.

Distribution of the antivirus in a Banyan-Vines network

To automatically distribute the antivirus to all workstations as they connect to the network, you must add the following line to the profile of each user whose computer is to be protected. The user profile is the sequence of commands that are executed each time a user connects to the network.

Just edit this profile with the MUSER command and add the following line:

```
POSTLOGIN F:\PAVEXCLI\RINSTALL PAVEX.SCR
```

(assuming the server drive is *mapped* to F and the files have been copied to the **PAVEXCLI** directory).

It is very advisable to define the drive mapping before running **RINSTALL** to make sure that the server's hard disk is referenced in the same way from all workstations.

Changing all user profiles one by one can be a very tedious task if there are many users. There is usually a common profile used by all users. This profile is then called from the various user profiles. The command to use for calling one profile from another is:

```
USE Sample_Profile@group@organization
```

where *Sample_Profile* is a fictitious user, and *group* and *organization* are those corresponding to the company's structure.

In this way, you need only make the necessary changes to the *Sample_Profile* for it to affect all users that call this profile from their own.

Installation of the antivirus on a workstation not connected to the network

If you want to install Panda Antivirus Exchange/Outlook on a workstation that is not connected to the network, you must carry out the following procedure:

1. Insert disk number 1 or the CD-ROM for Panda Antivirus Exchange/Outlook, go to the corresponding drive and run the SETUP.EXE program. The installation process consists of a series of windows in which you will be asked for the data necessary to carry out the installation on your computer. One of the details you will be asked for is the target directory. You must select a directory in the computer on which you are installing the antivirus, and not a server directory as previously described.

2. Once the installation process has concluded, execute the following command:

   C:\PAVEXCLI\RINSTALL PAVEX.SCR

   (if you have installed the antivirus in another drive or directory, indicate the appropriate changes).

3. When the distribution process has concluded, the antivirus program for MS-Exchange/Outlook will be installed on your computer.

4. Delete the directory in which you installed the antivirus in step 1, as it will no longer be necessary.

Solving distribution problems

If the antivirus has not been correctly distributed to one or more computers, go to that computer or computers and check the following:

1. Make sure the computer can connect to the server on which the antivirus has been copied.

2. Try running **RINSTALL** directly. Go to the server directory where the antivirus was copied and run **RINSTALL** PAVEX.SCR.

If the two previous checks were correct, check the login script and make sure that the right script was modified and that the added line corresponds to the one previously detailed in this manual.

Advanced features

How to prevent users from modifying the Panda Antivirus Exchange/Outlook configuration

If you want to prevent the users who are going to automatically receive Panda Antivirus Exchange/Outlook from changing its configuration, follow the procedure described below:

1. Install Panda Antivirus Exchange/Outlook on the network administrator's computer.

2. Open the MS-Exchange/Outlook mail program and configure the antivirus in the desired way.

3. Protect the configuration with a password. This is done in the antivirus configuration window.

4. Copy the PAVEXCLI.CFG file located in the WINDOWS\SYSTEM directory of the administrator's computer to the network directory from which the antivirus is going to be distributed.

5. Modify the *login script* to begin the distribution of the antivirus to all the network workstations.

It is essential that this procedure be carried out before the distribution of the antivirus throughout the network.

Necessary information about Novell NetWare

The distribution of the antivirus through a Novell NetWare network requires a certain knowledge of this system. The concepts you need to understand are described below, together with examples of how to correctly prepare the system.

Commands that are executed at the start of a network session

Normally, when a computer is booted, a series of commands defined in a file are run. In the case of MS-DOS or Windows, this is the AUTOEXEC.BAT file.

Likewise, it is also normal that when a computer connects to a network, a series of commands are run. This series of commands and/or programs is known as the *login script*.

The *login script* can be general (the same for all users) or specific (a different one for each user). There can also be a mixed solution, with a general login script common to all users, and another login script for each particular user.

As the *login script* is executed each time a user connects to the network, it is the ideal place to achieve the distribution of the antivirus to all the workstations. You need only run the Panda Software antivirus distribution program in the *login script* to distribute the antivirus to all workstations as they connect to the network.

System Login Script

In the case of Novell NetWare, the general login script common to all users is known as the *System Login Script*. You must edit this file to add the execution of the Panda Software antivirus distribution program. To edit the *System Login Script,* carry out the following steps:

1. If you have a Novell NetWare 3.x version, you must use the SYSCON program. If you have a Novell NetWare 4.x version, you need to use the NETADMIN program. All Novell NetWare servers have a volume called SYS, inside of which there is always a directory called PUBLIC. The two above programs (SYSCON and NETADMIN) can be found in this directory.

2. To edit the *System Login Script* with SYSCON, run the program, select *Supervisor Options* and then *System Login Script.*

3. To edit the *System Login Script* with NETADMIN, run the program and repeatedly select the two dots (..) in the box on the left until this option is no longer available. You will then see only one option (to the right it will be described as an *organization*). Select this option and press the F10 key. In the menu that appears, select the option *View or Edit Object Properties* and in the following menu select the *Login Script* option. Once you have done this, you can modify the *System Login Script.*

You must insert two lines in the *System Login Script*: the line relating to *mapping* (this concept is explained in the next section) and the line that refers to the automatic distribution of the antivirus.

Associating a drive letter

This section explains the *mapping* concept. On a computer, the hard disk is usually identified with the letter C, the disk drive with the letter A or B and the CD-ROM drive with D, E, etc., depending on the number of hard disks installed.

The volumes (“hard disks”) of a Novell NetWare server also need to be identified with a drive letter so as to be able to refer to directories and files in these volumes from connected workstations. The operation of associating a drive letter to a volume is known as *mapping.*

It is very advisable that all workstations have the same drive mappings to ensure that the different server volumes are given the same name in each case. To do this, you need only place the mapping command in the *System Login Script*. Volumes are generally mapped to letters from F onwards, but any other drive letter can be used, as long as it is not being used already. Bearing this in mind, the mapping command would be as follows:

```
MAP ROOT F:=SERVER_NAME\VOLUME_NAME
```

If the server name is ALPHA and the volume name is SYS, the command would be:

```
MAP ROOT F:=ALPHA\SYS:
```

Necessary information about Windows NT

The distribution of the antivirus through a Windows NT network requires a certain knowledge of this system. The concepts you need to understand are described below, together with examples of how to correctly prepare the system.

Commands that are executed at the start of a network session

Normally, when a computer is booted, a series of commands defined in a file are run. In the case of MS-DOS or Windows, this is the AUTOEXEC.BAT file.

Likewise, it is also normal that when a computer connects to a network, a series of commands are run. In Windows NT this series of commands and/or programs is known as the *logon script*.

In Windows NT, each user has his/her own logon script. This would mean modifying the logon scripts for all the users you are going to distribute the antivirus to. To avoid this tedious task, Panda Software has developed a utility called Profile Manager, whose functioning is explained below.

As the logon script is executed each time a user connects to the network, it is the ideal place to achieve the distribution of the antivirus to all the workstations. You need only run the Panda Software antivirus distribution program in the logon script to distribute the antivirus to all workstations as they connect to the network.

Logon scripts - Profile Manager

To install the Profile Manager program, which permits you to modify all the logon scripts simultaneously, insert the disk labeled *Windows NT Logon Script Editor* or go to the corresponding directory on the CD-ROM and run the **SETUP.EXE** program. e.g.:

```
A:\SETUP
```

Once installed, perform the following steps:

1. Run the program.
2. Select simplified mode.
3. Select *Edit domain logon scripts* from the File menu.
4. A text editor will appear at the bottom of the window. This is where the appropriate modifications are made that will affect all the logon scripts.
5. Exit the program, saving the changes.

You must insert two lines in the *Logon Script*: the line relating to *mapping* (this concept is explained in the next section) and the line that refers to the automatic distribution of the antivirus.

Associating a drive letter

This section explains the *mapping* concept. On a computer, the hard disk is usually identified with the letter C, the disk drive with the letter A or B and the CD-ROM drive with D, E, etc., depending on the number of hard disks installed.

In the case of a Windows NT network, the concept o*f mapping is* related to the concept of a *shared resource*. The whole or a part of the server's hard disk (or disks if there are several) can be shared, thereby becoming a shared resource. These shared resources are the ones that need to be mapped,

so that they can later be referred to from the workstations.

It is very advisable that all workstations have the same drive mappings to ensure that the different shared server resources are given the same name in each case. To do this, you need only place the mapping command in the *Logon Script*. Shared resources are generally mapped to letters from F onwards, but any other drive letter can be used, as long as it is not being used already. Bearing this in mind, the mapping command would be as follows:

```
NET USE  F: \\SERVER_NAME\RESOURCE_NAME
```

If the server name is ALPHA and the volume name is SYS, the command would be:

```
NET USE F: \\ALPHA\SYS
```

Necessary information about OS/2

The distribution of the antivirus through an OS/2 network requires a certain knowledge of this system. The concepts you need to understand are described below, together with examples of how to correctly prepare the system.

Commands that are executed at the start of a network session

Normally, when a computer is booted, a series of commands defined in a file are run. In the case of MS-DOS or Windows, this is the AUTOEXEC.BAT file.

Likewise, it is also normal that when a computer connects to a network, a series of commands are run. This series of commands and/or programs is known as the *login script*. In the case of OS/2, each user has a file called PROFILE.BAT (or PROFILE.CMD) that is run each time the user connects to the network.

As each user has his/her own login script, you must modify the PROFILE.BAT file for all the users you want to distribute the antivirus to. The drawback is that future modifications would also imply having to edit all the PROFILE.BAT files. This can be avoided by creating a BAT file that contains the lines necessary for the distribution of the antivirus and then calling this file from the corresponding PROFILE.BAT files. In this way, any future modifications can be made on this BAT file, which will then affect all users.

As the login script is executed each time a user connects to the network, it is the ideal place to achieve the distribution of the antivirus to all the workstations. You need only run the Panda Software antivirus distribution program in the login script to distribute the antivirus to all workstations as they connect to the network.

Associating a drive letter

This section explains the *mapping* concept. On a computer, the hard disk is usually identified with the letter C, the disk drive with the letter A or B and the CD-ROM drive with D, E, etc., depending on the number of hard disks installed.

In the case of an OS/2 network, the concept o*f mapping* is related to the concept of a *shared resource*. The whole or a part of the server's hard disk (or disks if there are several) can be shared, thereby becoming a shared resource. These shared resources are the ones that need to be mapped, so that they can later be referred to from the workstations.

It is very advisable that all workstations have the same drive mappings to ensure that the different shared server resources are given the same name in each case. To do this, you need only place the mapping command in the PROFILE file for each user. Shared resources are generally mapped to letters from F onwards, but any other drive letter can be used, as long as it is not being used already. Bearing this in mind, the mapping command would be as follows:

```
NET USE  F: \\SERVER_NAME\RESOURCE_NAME
```

If the server name is ALPHA and the volume name is SYS, the command would be:

```
NET USE F: \\ALPHA\SYS
```

Syntax of the script commands (.SCR)

You will have observed throughout this documentation that the **RINSTALL** program is always given a parameter. This parameter is the name of a file with an SCR extension (a script file). A script file is a text file that is divided into sections, each line of which contains a command. The script file determines the behavior of the **RINSTALL** program.

The SCR files suitable for **RINSTALL** can have 6 different sections:

Common Section **[COMMON]:** These commands are always executed.

DOS Section **[DOS]:** The commands in this section are executed in DOS, Windows 3.1x and Windows 95.

Windows 3.1x Section **[WIN]:** The commands in this section are executed in DOS, Windows 3.1x and Windows 95, but only if the Windows 3.1x directory is found on the workstation's hard disk.

Windows 95 Section **[WIN95]:** The commands in this section are executed in DOS, Windows 3.1x and Windows 95, but only if the Windows 95 directory is found on the workstation's hard disk.

Windows NT Section **[WINNT]:** The commands in this section are only executed in Windows NT.

OS/2 Section **[OS/2]**: The commands in this section are only executed in OS/2.

There are three types of commands:

1. **Files to be copied:** All lines that do NOT start with a number sign (#) indicate a file that should be present in the source directory and that should be copied to the target directory. By default, these files are copied only if they do not exist in the target directory or if the file in the target directory is older that the one in the source directory.

2. **Assignments**: These commands start with a number sign (#) and have the following structure: #Variable = value. They are used to assign a certain value to a variable. The different variables available in script (SCR) files are detailed below.

Variable name	**Description**
Win3xDir	Windows 3.1x directory
Win95Dir	Windows 95 directory
WinNTDir	Windows NT directory
BaseSourcePath	Base source directory
BaseTargetPath	Base target directory
RelSourcePath	Relative source directory
RelTargetPath	Relative target directory
SourcePath	BaseSourcePath + RelSourcePath

TargetPath — BaseTargetPath + RelTargetPath

CopyMode — Indicates the file copying conditions. It can take three values. COPY indicates that files will only be copied if they do not exist in the target directory. UPDATE indicates that files will only be copied if the version to copy is more recent that the existing file in the target directory. OVERWRITE indicates that files will always be copied. ONCHANGE indicates that a copy will be made only if the source file is different from the destination file regardless of whether it is dated earlier or later.

ErrorMode — Indicates if error messages should be displayed or not. It can be assigned the value 0 (messages will not be displayed) or the value 1 (messages will be displayed).

3. **Functions:** these commands also start with a number sign (#), and are used to perform certain operations. Its syntax is as follows: #Function parameter1, parameter2, etc. The different functions available are:

AddProfileEntry

This function adds an entry to a section of an INI file. It takes 4 parameters:

Parameter 1: indicates the section in which to create the entry.
Parameter 2: indicates the field (the 1st part of the entry).
Parameter 3: indicates the value (the 2nd part of the entry).
Parameter 4: indicates the path to the INI file.

Example:

```
#AddProfileEntry Windows, Load,
f:\pavfn\winkir.exe, c:\windows\win.ini
```

AppendLine

This function adds a line to a text file. It takes 3 parameters:

Parameter 1: indicates the path to the text file.
Parameter 2: indicates the text line to add.
Parameter 3: LITERAL (optional). When this parameter is specified, you are assured that the text line appears exactly as written, eliminating any possible modifications.

Example:

```
#AppendLine c:\autoexec.bat,
c:\pavfn\sentinel.com
```

AppendLineBefore

This function adds a line to a text file, but always before another specified line. It takes 4 parameters:

Parameter 1: indicates the path to the text file.

Parameter 2: indicates the text line to add.
Parameter 3: indicates the text line before which the new line is to be inserted.
Parameter 4: LITERAL (optional). When this parameter is specified, you are assured that the text line appears exactly as written, eliminating any possible modifications.

Example:

```
#AppendLineBefore c:\autoexec.bat,
c:\pavfn\sentinel.com, win, LITERAL
```

DeleteLine
This function deletes a line from a text file. It takes 2 parameters:

Parameter 1: indicates the path to the text file.
Parameter 2: indicates the line of text to delete.

Example:

```
#DeleteLine c:\autoexec.bat,
c:\pavfn\sentinel.com
```

InsertLine
This function inserts a line at the beginning of a text file. It takes 3 parameters:

Parameter 1: indicates the path to the text file.
Parameter 2: indicates the text line to insert.
Parameter 3: LITERAL (optional). When this parameter is specified, you are assured that the text line appears exactly as written, eliminating any possible modifications.

Example:

```
#InsertLine c:\autoexec.bat,
c:\pavfn\sentinel.com
```

MakeDir
This function creates a directory. It takes one parameter:

Parameter 1: indicates the path to the directory to create.

Example:

```
#MakeDir c:\pavfn
```

NoWinLoad
The WIN.INI file contains a [Windows] section, which has an entry called Load. This command loads a series of programs when starting Windows. More than one program can be specified in the same Load command. The NoWinLoad command removes the selected program from the Load command. It takes one parameter:

Parameter 1: indicates the program not to load.

Example:

```
#NoWinLoad c:\pavfn\winkir.exe
```

ReplaceLine
This function replaces a line in a text file. It takes 3 parameters:

Parameter 1: indicates the path to the text file.
Parameter 2: indicates the text line to replace.
Parameter 3: indicates the new text line.

Example:

```
#ReplaceLine c:\autoexec.bat,
«TargetPath»SENTINEL.COM,
«TargetPath»SENTINEL.COM /OE
```

SetProfileEntry
This function assigns a value to an entry in a specified section of an INI file. The function tries to find the specified section. If found, a value is assigned. If not, it creates the entry and assigns the value. If the section does not exist, it is also created. It takes 4 parameters:

Parameter 1: indicates the section of the INI file
Parameter 2: indicates the field (the 1st part of the entry)
Parameter 3: indicates the value (the 2nd part of the entry)
Parameter 4: indicates the path to the INI file.

Example:

```
#SetProfileEntry Windows, Load,
c:\pavfn\winkir.exe, c:\windows\win.ini
```

WinLoad
The WIN.INI file contains a [Windows] section, which has an entry called Load. This command loads a series of programs when starting Windows. More than one program can be specified in the same Load command. The WinLoad command adds the specified program to the Load command. It takes one parameter:

Parameter 1: indicates the program to load.

Example:

```
#WinLoad c:\pavfn\winkir.exe
```

AdminRequired

This function indicates that from this moment onwards and until the line with the function EndAdminRequired appears, it will be necessary to have administrator privileges in order to execute all the command block (ones that are found between #AdminRequired and #EndAdminRequired). The function is only in effect when Rinstall is executed with the /Local parameter. This function does not admit parameters.

Example:

```
#AdminRequired
```

EndAdminRequired

The appearance of this function indicates that all the commands following it can be executed without needing to have administrator privileges. This function is only in effect when Rinstall is executed with the /Local parameter. This function does not admit parameters.

Example:

```
#EndAdminRequired
```

ResetMode

This indicates whether the equipment will be restarted at that very moment or whenever necessary. The 0 value means that it will not be restarted, whereas 1 indicates that it should be restarted at that very moment. In either of the two cases a warning will be displayed.

CheckSpace

This command checks the space (in Mb) existing in the destination. If it is not found, a warning will be displayed and the files will not be copied.

Parameter 1: indicates the size needed in Mb.

Example:

```
#CheckSpace 8
```

CopyFileAs

Copies the file from its source to its destination indicating the mode of copying and makes it possible for the file name to be changed in the said destination. It admits 3 parameters:

Parameter 1: indicates the original route of the file.

Parameter 1: indicates destination of the destination file.

Parameter 1: indicates the copying mode through the following possibilities: COPY (the file will only be copied if it does not already exist in the destination), UPDATE (the file will only be copied if the version to be copied is more recent than the one existing in the destination), OVERWRITE (the file will always be copied even if the source and destination are the same) and ONCHANGE (it will always be copied whenever the source and destination files are different).

DeteleDirDelayed

When Rinstall is executed (after the #Run command), this command deletes a complete directory, including the subdirectories.

Parameter 1: indicates the directory to be deleted.

Example:

```
#DeleteDirDelayed c:\pavfn
```

ExchangeRequired
This command indicates the necessity of having an Exchange/Outlook client installed in order to continue processing the section where it happens to be. It does not admit any parameter.

Example:

```
#ExchangeRequired
```

EndExchangeRequired
This command indicates that it is no longer necessary to have an Exchange/Outlook client installed in order to continue processing the section where it happens to be. It does not admit any parameter.

Example:

```
#EndExchangeRequired
```