Introduction to Panda Antivirus 6.0

Welcome to **Panda Antivirus 6.0 Home Edition / Platinum**. We have designed **Panda Antivirus 6.0 Home Edition / Platinum** to be easy and convenient to use. In this help you will find detailed explanations of all the operations you can perform with **Panda Antivirus 6.0 Home Edition / Platinum**. Consult this help whenever you have difficulty or do not know how to do something.

The main goal of **Panda Antivirus 6.0 Home Edition / Platinum** is to bring the most advanced antivirus technology closer to all users. The growing danger of computer viruses and the technological advances they show make a latest generation antivirus program incorporating leading edge technology an absolute must.

However, we at **Panda Software** do not forget that, in the final analysis, only people are important. That is why we put an exceptional suite of services at your disposal, whose aim is to help you whenever you have any sort of virus-related problem.

The combination of a product embodying state-of-the-art technology and near-at-hand services makes ours a complete, global solution against the danger of computer viruses.

New technology, new design

Panda Antivirus 6.0 Home Edition / Platinum offers a new technology which allows you to control the entire panoply of antivirus protection resources in a computer from a single program. In this way you can control the different protection strategies from the same point, making management easier and improving security.

The new design of **Panda Antivirus 6.0 Home Edition / Platinum** makes it a revolutionary product. Easy to use but offering all the power and scanning capability you require. Its new interface, with two operating modes (**only available in Panda Antivirus 6.0 Platinum**), adapts itself to your needs.

Protection strategies

Panda Antivirus 6.0 Home Edition / Platinum offers a complete set of protection strategies to keep all the entryways used by viruses to get into your computer protected.

Immediate scans: enable you to scan any part of the computer at any time in the simplest way.

Scheduled scans: allow you to scan any part of the computer automatically at the times you program in advance.

Startup scans: enable you to schedule an scan when the computer starts up so that it is protected from the very beginning of each work session.

Permanent scans: offer total, automatic protection at all times.

Special scans

Internet scans: antivirus protection against infecting your computer when you access the Internet.

E-mail and News scans: all messages sent and received using the MS-Outlook, MS-Exchange and MS-Outlook Express mail managers will be scanned.

Lotus Notes systems scans: Lotus Notes database systems will be scanned.

Note: some options are only available according to the specific product purchased (**Panda Antivirus 6.0 Home Edition** or **Panda Antivirus 6.0 Platinum**) and the configuration of your operating system. For more information, see Differences between versions

Services

Together with **Panda Antivirus 6.0 Home Edition / Platinum** you have acquired a complete suite of services to help you with everything related to viruses.

Technical support: 24 hours a day, 365 days a year, we have qualified technicians standing by to help you in person. To make it easy and convenient to contact us, we offer you all the means of communication: On-line (solutions to problems via e-mail), fax, regular mail, and our Web site electronic mail. In addition, **only with Panda Antivirus 6.0 Platinum** you will have access to phone-based personal technical support.

24-hour S.O.S. Virus: if you find a new virus, we will solve your problem in no more than 24 hours and will send you, within that time limit, an antivirus that will detect and disinfect the new virus.

Updates: DAILY updates from our Web site plus the possibility of receiving updates sent regularly to your office or home.

Note: the **12h S.O.S. Virus** and **Home-delivered Updates** services are available depending on the type of license purchased.

Upgrading the antivirus (Intelligent Upgrades)

In order to perform **Intelligent Upgrades**, it is necessary to have installed all of the antivirus components (by choosing **Complete Installation** at the time of installing). In addition, it will not be necessary to have an open Internet connection before beginning the *Upgrade* process. Once you have done this, the steps you must take to carry out an **Intelligent Upgrade** are as follows:

1. Select the **Intelligent Updates & Upgrades** option in the **Panda Antivirus 6.0** (**Home Edition** or **Platinum**) group under the **Programs** section in your **Start** menu.
2. The program will automatically check the update status of both the virus signature file and the antivirus itself. It will check to see if there exist more updated versions of the virus signature file and complete antivirus.
3. You will be offered the possibility of updating the virus signature file, the antivirus or both, depending on the results of the previously described checks. If you wish to go ahead with the update, you need only press the **Update** button.
4. When finished, you are given the optional choice of restarting your computer so that the changes made in the antivirus can take effect.

Updating the virus signature file (Intelligent Updates)

New viruses appear every day. In order to be fully protected, it is necessary to be permanently updated. **Panda Antivirus 6.0** can be updated quickly and efficiently by updating a single virus signature file.

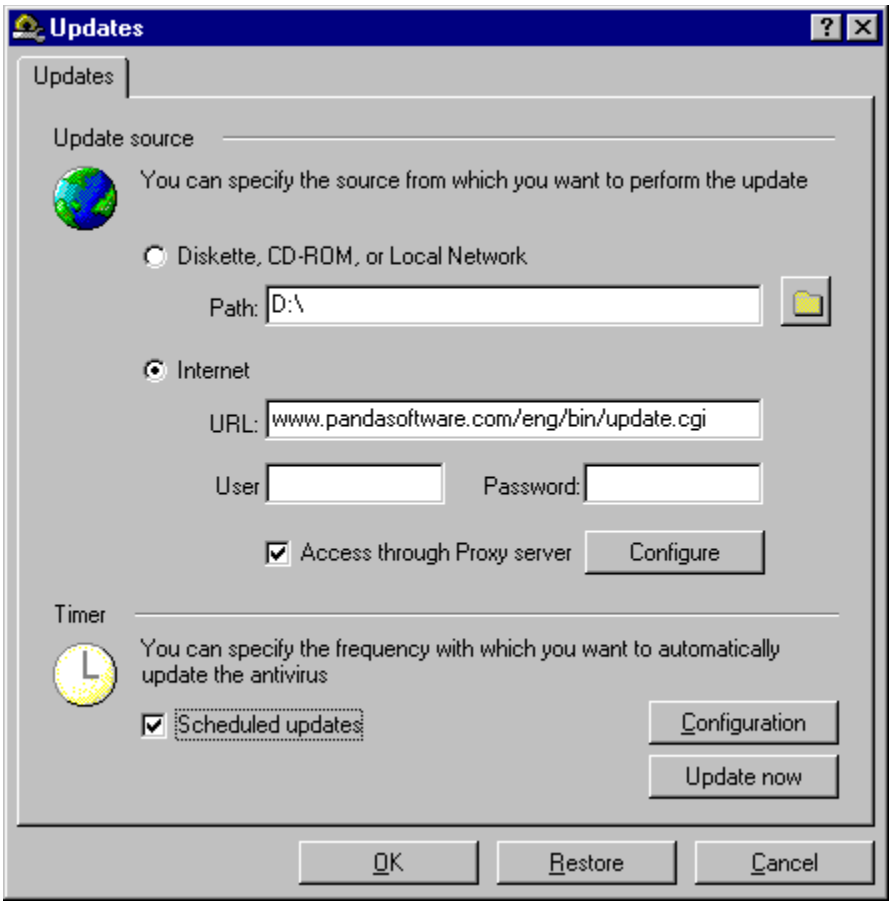
The updates of the virus signature file can be performed either from the program itself, by pressing the **Update** button, or from an external program created for this purpose.

To update the virus signature file from the **Panda Antivirus 6.0** program, you must first press the **Update** button. Once you have done this, a window will appear that will permit you to indicate the source of the update (diskettes, CD-ROM, network or Internet) as well as the necessary information to carry this out. It is important to point out that if the update is to be performed via Internet, it will not be necessary to have an open Internet connection, as **Panda Antivirus 6.0** (**Home Edition** or **Platinum**) will automatically open one for you.

If you wish to update the virus signature file without running **Panda Antivirus 6.0**, you must go to **Panda Antivirus 6.0** (**Platinum** or **Home Edition**) under the **Programs** section in your **Start** menu. Once there, run the **Intelligent Updates & Upgrades** program. This program will automatically detect if there exists a more updated version of the virus signature file than the one installed. It will inform you of the situation and will allow you to perform the update by clicking on the **Update** button.

Updating via CD-ROM or diskettes

If you wish to update your antivirus software via CD-ROM or diskettes, take the following steps:



1. Select the Diskette, CD-ROM or local network option.
2. Indicate the path from which the update will be taken. If it is to be done from a diskette, type in the disk drive. If the update source is a CD-ROM, key in the letter of the CD-ROM drive, and if a local area network is the source, indicate the network drive.
3. Press the **Update now** button.

Once you have completed the previous steps, the update process will begin.

Updating through the Internet

If you want to update the antivirus through the Internet, proceed as follows:

1. Choose the Internet option.
2. Indicate the Internet address (URL) from where you will obtain the update. Because the Internet-based updating service is exclusive to registered customers, you will also need to type in a user name (Login) and a Password for identification purposes.
3. If the connection to Internet is made through a *proxy*, you should check the **Access to Internet via Proxy**. Next, press the **Configure** button and then option and fill out the **IP Address** and **Port** fields. If you have any doubts concerning the correct IP address and/or port values, we recommend that you ask your network administrator. Here, you can also enter the **User name** and **Password** information needed to authenticate your connection to the proxy server.
4. Press the **Update now** button.

Once you have carried out the previous steps, the update process will begin.

Scheduled Updates

You can configure **Panda Antivirus 6.0** so that the updates are periodically performed in a totally automatic manner. This will allow you to be completely up-to-date in the easiest and most comfortable way possible.

The automatic updates of both the virus signature file and the entire antivirus will be performed via CD, diskettes or Internet, depending on what you have selected.

To indicate that you want your **Panda Antivirus 6.0** updated automatically, check the **Perform updates automatically** option.

You can configure when the antivirus will be updated to suit your specific needs. To configure the update calendar, press the **Configuration** button. A window will come up offering the following options:

Updates & Upgrades

- **Update the signature file (Update):** permits you to indicate that you wish to perform periodic updates of the virus signature file (*Intelligent Updates*).
- **Upgrade the entire antivirus (Upgrade):** permits you to indicate that you wish to perform periodic updates of the entire antivirus program.

Timing

- **Each time the antivirus is run:** permits you to indicate that you wish to check for *Updates* and *Upgrades* each time the antivirus is started.
- **Every:** allows you to indicate that the updates of the virus signature file are to be performed every x hours, days, weeks or months.
- **Update time:** if you have chosen to carry out the updates on a certain day of the week or every certain number of days, weeks or months, you will need to indicate the time you want the update process to begin.

Different types of updates

Panda Antivirus 6.0 offers two different types of update formats: **Intelligent Updates** and **Intelligent Upgrades**. **Intelligent Updates** renews the virus database so that the antivirus is capable of detecting and disinfecting all the latest viruses. **Intelligent Upgrades** renew the entire product in order to incorporate the latest improvements made to the antivirus.

To find out when you last updated your **Panda Antivirus 6.0**, the program displays a graph in the status bar located in the lower part of the antivirus' main window. This graph indicates the antiquity of the virus signature file in days. By double-clicking the graph, a window will appear showing information on the virus signature file. This information can also be accessed by pressing the **Version** button in the window that appears after clicking on the **Virus List** button in the application's main window. The information shown on the virus signature file is as follows:

- **No. of Known Viruses:** indicates the number of viruses detected by the virus signature file.
- **Virus File Version:** indicates the version of the virus signature file. The version refers to the different technologies implemented in the file. It is possible that the newest versions of the virus file will not work correctly with older versions of **Panda Antivirus 6.0**, and for that reason this information is shown.
- **Date Created:** this is the date that the virus signature file was generated.
- **Time Created:** this corresponds to the time the virus signature file was created.
- **Size:** indicates the size in bytes of the virus signature file.

Lastly, the information on both the version number installed and the date of the virus signature file with which the antivirus is working is shown in the About **Panda Antivirus 6.0** window, which can be accessed through the Help menu. These two pieces of information appear together in this window to facilitate their consultation.

Description of Panda Antivirus 6.0

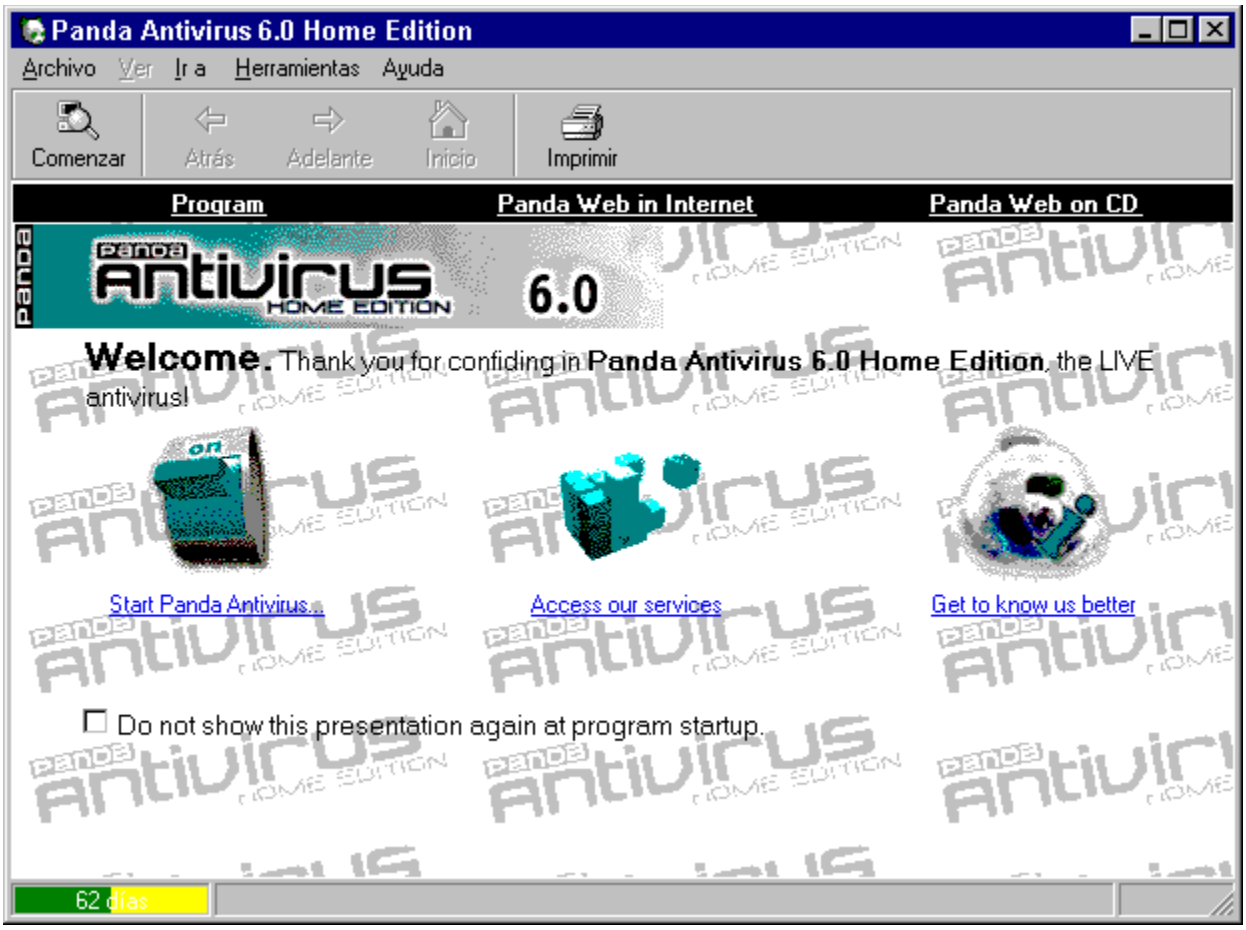
Panda Antivirus 6.0 Home Edition / Platinum displays a main window which is divided into the following parts:

1. **Menu bar**. This bar contains the main application menu which allows you to access all the program options.
2. **Standard button bar**. This bar contains the buttons which allow the user to access the most commonly used program options easily and quickly.
3. **Panda Antivirus 6.0 Home Edition / Platinum bar**. This is what we call the vertical button bar on the left-hand side of the window. It lets you go from one protection strategy to another; the antivirus program thus offers you a centralized control of all the different types of scan.
4. **Central area**. This is all the area of the main window located to the right of the **Panda Antivirus 6.0 Home Edition / Platinum bar**. In this central area you will see the different items required to create new scans or to monitor the status of others.
5. **Status bar**. A "thermometer" is shown in the status bar to indicate the antiquity of the virus file. As time goes by, an orange bar will progressively lengthen from right to left. After a certain time has passed, the color of this bar will change to red, which indicates that it is time for an antivirus update.

Furthermore, you can also select several items at the same time. This can be done two ways. You can select separate items that are not grouped together on the list (while pressing the CTRL key, click the items desired) or you can highlight items that are listed one after another (while pressing the SHIFT key, click the first and last item desired on the list. This will highlight a range of items).

In addition to these sections, the Panda bear icon will appear in the Windows taskbar, which will permit you to carry out various actions. If you right-click on the icon, you can choose any of the following menu options: **Unload** (removes the Sentinel, Internet and/or Lotus Notes permanent scan from memory), **Configure** (permits you to configure permanent scans), **Panda Antivirus 6.0 Home Edition / Platinum** (runs the antivirus) or **Close** (permits you to close the permanent protection). If you left-click the bear icon, you can directly access the permanent scan configuration screen.

Panda Antivirus 6.0 Home Edition



Panda Antivirus 6.0 Platinum


Panda Antivirus 6.0 Platinum
Archivo Ver Ir a Herramientas Ayuda
Comenzar
Atrás
Adelante
Inicio
Imprimir
Program
Panda Web in Internet
Panda Web on CD
Panda Antivirus PLATINUM 6.0
Welcome. Thank you for confiding in Panda Antivirus 6.0 Platinum, the LIVE antivirus!
Start Panda Antivirus...
Access our services
Get to know us better
Important: Panda Antivirus 6.0 Platinum adapts itself to both experienced users and beginners. It features two operating modes: basic and advanced. Both provide maximum protection, but the advanced mode permits you to make the most of the product's potential. [More information]. Start in [Basic Mode] [Advanced Mode]
Do not show this presentation again at program startup.
62 días
Buscando carpetas de correo...

Two modes: basic and advanced

Note: while **Panda Antivirus 6.0 Platinum** offers the possibility of working in either mode, **Panda Antivirus 6.0 Home Edition** only allows you to work in basic mode. For more information, we suggest you consult the section entitled Differences between versions.

To bring the operation of **Panda Antivirus 6.0 Platinum** closer to its users, we have given our antivirus two working modes: advanced and basic. The difference between the two is that, while guaranteeing the same levels of protection, the first allows you to configure all the scan options, whereas the second only lets you choose one of the predefined scans.

A button in the **Panda Antivirus 6.0 Platinum standard button bar** lets you easily change modes.

The following table details the differences between the two modes. The basic mode is recommended for less advanced users or users who have very concrete, specific needs. The advanced mode (only in **Panda Antivirus 6.0 Platinum**) is for experienced users, although the operation of the program can also be simplified in this mode by choosing only predetermined scans.

	Advanced mode	**Basic mode**
Immediate scan	Choose a predetermined scan OR Choose scan areas and options.	Choose a predetermined scan.
Scheduled scan	Choose a predetermined scan OR Choose scan areas, options and frequency.	Choose a predetermined scan.
Startup scan	Choose whether you wish to enable or disable. Choose optional areas and scan options also.	Choose whether you wish to enable or disable.
Permanent scan	Choose whether you wish to enable or disable, as well as permanent scan options.	Choose whether you wish to enable or disable.
Internet scan	Choose whether you wish to enable or disable, as well as Internet scan options.	Choose whether you wish to enable or disable.
Lotus Notes scan	Choose whether you wish to enable or disable, as well as Internet scan options.	Choose whether you wish to enable or disable.

Report

All the activity of the antivirus program is logged in the report. Its main function is to serve as an historical file of the operations carried out with the antivirus, as well as to record all virus incidents that have occurred.

To access the report's configuration options, you need to be in **Advanced** mode (Differences between versions). By pressing the **Configure** button, you can access a window that contains several tabs. The **Report** tab contains accessible configuration options. Each incident listed in the report presents a series of fields. These are the following:

Incident: indicates the action performed by the scan.

Job: this field indicates which type of scan has brought about the entry in the report.

Date and time: this field records the date and time the incident occurred.

Path: indicates the complete path together with the file name for all incidents in which this information makes sense.

Action: shows the action taken in response to the incident in question.

Use the button bar that appears at the top of the window to carry out any of the following actions with the report:

Print: permits you to print the report, for which you need to select the name of the printer, the page range and the number of copies desired.

Find: permits you to find items in the report. To begin the search, you first need to enter the word to find and where (report field or column) you wish to search in: **Incidents**, **Jobs**, **Paths** or **Actions**. You can select all of these.

File: thanks to this option, you can save the report as a text file (.TXT, in ASCII format). This enables you to save and subsequently consult or move the file to another computer. You need to indicate the name of the file, as well as the disk drive and directory where it will be saved.

Delete: allows you to permanently delete the report's contents. Once you have done this, the report window will close.

Filters: the purpose of this option is to present concise information. By means of the available filters, you can choose to display different information:

- **Type of scan:** with this drop-down list, you can display incidents according to the scans that were performed: **All**, **Immediate**, **Scheduled**, **Upon Startup**, **Permanent**.
- **Program:** this filter will only show the incidents that were produced in a determined program: **All**, **Platinum** or **Lotus Notes**.
- **Incidents:** in this case, the information is filtered according to the event or incident produced: **All, Detected**, **Suspicious**, **Infected and suspicious**, **Errors**, **Disinfected**, **Renamed**, **Deleted** or **Moved**.
- **Date:** this permits you to determine the comparison criteria (All, Before or equal to..., After or equal to..., Between) to use when filtering information according to date in the **Start** date and **End** date fields.

From the scan window, you can carry out another scan or action through the use of the right mouse button, which will display a pop-up menu that permits you to **Show information**, **Disinfect**, **Rename**, **Move**, **Delete** and **Select all**.

What is the startup scan?

The main purpose of the Startup Scan is to protect your computer from the moment it is switched on. **Panda Antivirus 6.0** offers three types of Startup Scans: at computer startup, at Windows startup or at Lotus Notes startup.

The three types of Startup Scans contain different configuration options. Please consult the corresponding section to obtain more detailed information on the configuration options.

If you are working in the advanced mode, you can choose the areas that will be scanned when the system is started up. The advanced mode also allows you to schedule the system startup scan so that it is only performed at certain times.

How to enable the startup scan (Advanced)

Note: certain options are only available depending on the product purchased and the operating system configuration. For more information, see Differences between versions.

The three types of Startup Scans (at computer startup, at Windows startup or at Lotus Notes startup) are enabled identically.

First, you will need to access the startup scan area by way of the **System startup** option in the **Go to** menu. You can also get there by using the **Panda Antivirus 6.0 Platinum bar**, which shows the main options of the program to make its handling easier.

In the Startup Scan menu, you can choose any of the following three options that appear: **Scan at computer startup**, **Windows Startup Scan** or **Lotus Notes Startup Scan**. You need only double-click on any of the desired options that you wish to enable, if they haven't already been checked. The three options can be enabled or disabled independently, for they are not related in any way.

Options in the computer startup scan (Advanced)

Note: certain options are only available depending on the product purchased and the operating system configuration. For more information, see Differences between versions.

The computer startup scan options enable you to configure how this scan will be performed. To access these options, press the **Configuration** button in the **Startup scan** section, bearing in mind the startup scan option you have selected (computer startup, Windows startup or Lotus Notes startup). All the scan options are grouped in a single window but separated into different tabs to make them easier to manage.

Select the section on which you want more information:

How to disable the startup scan (Advanced)

Note: certain options are only available depending on the product purchased and the operating system configuration. For more information, see Differences between versions.

Both the computer, Windows and Lotus Notes startup scans are disabled in the same way.

To disable either of them, go to the **System Startup** option via the **Go to** option in the main menu. You can also access this area by using the **Panda Antivirus 6.0 Platinum bar**, which offers the main program options to facilitate their handling. Once you are there, simply double click the **Computer startup scan** or the **Windows startup scan** or **Lotus Notes startup scan** option to disable them, assuming they are currently enabled.

How to enable the startup scan (Basic)

The three types of Startup Scans, at computer startup, at Windows startup or at Lotus Notes startup are enabled identically.

First, you will need to access the startup scan area by way of the **System startup** option in the **Go to** menu. You can also get there by using the **Panda Antivirus 6.0 bar**, which shows the main options of the program to make its handling easier.

In the Startup Scan menu, you can choose any of the following three options that appear: **Scan at computer startup**, **Windows Startup Scan** or **Lotus Notes Startup Scan**. You need only double-click on any of the desired options that you wish to enable, if they haven't already been checked. The three options can be enabled or disabled independently, for they are not related in any way.

How to disable the startup scan (Basic)

Both the startup scans, computer startup scans, Windows startup scans and Lotus Notes startup scans, are disabled in the same way.

To disable either of them, go to the **System Startup** option via the **Go to** option in the main menu. You can also access this area by using the **Panda Antivirus 6.0 bar**, which offers the main program options to facilitate their handling. Once you are there, simply double click the **PC startup scan**, **Windows startup scan** and/or the **Lotus Notes startup scan** option to disable them, assuming they are currently enabled.

What is an immediate scan?

Immediate scans let you scan any part of the computer in search of viruses any time you wish.

Immediate scans offer the possibility of choosing which area or areas you want scanned. The scan begins at the moment you order it. These characteristics make immediate scans especially apt for checking new files you may receive on any support medium, such as a diskette, e-mail or an Internet file download, to be sure they are free of viruses.

If you are in basic mode, an immediate scan is done by choosing one of the predetermined scans which come with the program. The objective of these predetermined scans is to provide users with the most common scans previously defined, so that their scanning work is made as easy as possible.

You can also select one or several areas of the section displaying items to be scanned and press the **Scan** button to start an immediate scan of the areas you have chosen.

If you are in advanced mode, a set of predetermined scans is also available to you. You can choose one of these or create a new scan according to your needs at the time. You can also modify the scan options. These options allow you to configure the scan to adapt it to your specific needs.

As in the basic mode, you can select one or several areas from the section offering items to be scanned and press the **Scan** button to start a scan on the spot.

Scan areas in an immediate scan (Advanced)

Note: certain options are only available depending on the product purchased and the operating system configuration. For more information, see Differences between versions.

In the advanced mode you can scan any part of the computer in search of viruses. To select the areas to be scanned you can work with the **Selection tree**. All the areas which can be scanned are shown in this tree. These areas are the memory, all assigned computer drives and, optionally, the e-mail folders of the **Microsoft Exchange**, **Microsoft Outlook** and **Microsoft Outlook Express** programs.

When you press the **Scan** button, the scan in search of virus will be carried out in all the areas in **Items to be scanned**. To determine which areas of the **Selection tree** will be included in **Items to be scanned**, there are three buttons between the two which have the following functions:

- **Add area:** if you select an area in the **Selection tree** and then press the **Add area** button, the selected area is added to **Items to be scanned**. You can achieve the same effect by dragging an area directly from the **Selection tree** to **Items to be scanned**.
- **Remove area:** if you select an area in **Items to be scanned** and press this button, the area you selected will be removed from **Items to be scanned**.
- **Clear:** when this button is pressed, all the items in **Items to be scanned** will be removed from the list.

If you attempt to add an area to **Items to be scanned** which is already there, the antivirus program will notify you of this and will cancel the operation. If you try to add an area to **Items to be scanned** which is included in another area which is already there, the antivirus program will advise you of this but will not cancel the operation.

It is also important to bear in mind that the different items to be scanned can be added with and without subdirectories. If you attempt to add an item with subdirectories and this item is already stripped of them, the antivirus program will ask if you want to remove the version without subdirectories and add the new one which includes them.

Finally, if an area is already in **Items to be scanned** and you attempt to add a higher area which includes it, you will be given the option of removing the repetitions automatically.

Panda Antivirus 6.0 Platinum is capable of scanning **Microsoft Exchange**, **Microsoft Outlook** and **Microsoft Outlook Express** folders. Any of the folders of these mail systems can be scanned in the same way the antivirus would scan any other area of the computer. It is also important to point out that **Panda Antivirus 6.0 Platinum** will scan for viruses any message database belonging to any of these systems which it may find during the scan, even when the message database in question is not defined as a folder.

Options in an immediate scan (Advanced)

The scan options allow you to configure how the scan in search of viruses will be performed. To access these options, press the **Configure Scan** button on the standard button bar. All the scan options are grouped in a single window, although they are separated into different tabs to make managing them easier. These tabs only appear in advanced configuration settings, which can only be accessed from **Panda Antivirus 6.0 Platinum**, but not from **Panda Antivirus 6.0 Home Edition**. For more information, consult the section entitled Differences between versions.

Click on the area on which you want more information:

Scan.
Actions.
Exclusions.
Report.
Warnings.

Predetermined scans in an immediate scan (Advanced)

Note: certain options are only available depending on the product purchased and the operating system configuration. For more information, see Differences between versions.

Predetermined scans offer the greatest ease in performing fast, simple scans.

A predetermined scan is a specific configuration of areas to be scanned and scan options. Predetermined scans are saved so that they can be reused as many times as needed, thus saving you an important amount of time and greatly simplifying your scan jobs.

The program comes equipped with a series of ready-configured predetermined scans. Among these already defined scans are the ones most frequently used when searching for viruses. If you wish to perform a different scan, you will be able to save the specified scan configuration (areas and scan options) to add a new predetermined scan to your list.

Adding a new predetermined scan. All you need to do is choose a set of areas to be scanned and establish the desired options. When you have done this, press the **Save** button in the standard program bar. The software will ask you for a name for the new predetermined scan. Once you have given it a name, the new scan will be available in the list of predetermined scans.

Removing a predetermined scan. To eliminate a previously created predetermined scan, simply right-click on the scan to be removed and choose the **Remove created scan** option. It must be borne in mind that only those predetermined scans that the user has created previously can be eliminated; those included with the program cannot be removed.

If you are going to scan the same areas on a regular basis, we recommend that you create a series of predetermined scans which will make the process much simpler and will avoid errors.

How to perform an immediate scan (Advanced)

Note: certain options are only available depending on the product purchased and the operating system configuration. For more information, see Differences between versions.

The immediate scan area is accessed through the **Immediate** option within the **Go to** menu. You can also get to this area by using the **Panda Antivirus 6.0 Platinum bar**, which shows the main options of the program in order to make its handling easier.

To perform an immediate scan, follow the steps below:

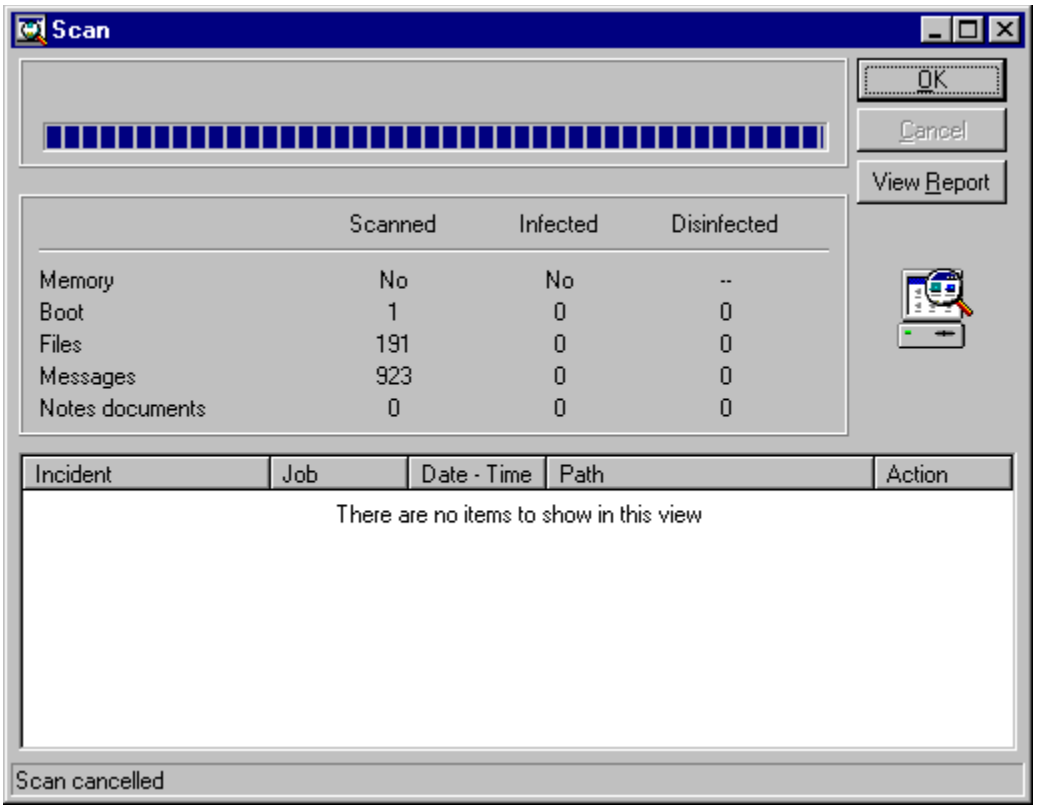
1. Add the areas which you want scanned in search of viruses to **Items to be scanned**. This can be done by dragging those areas from the **Selection tree** to **Items to be scanned** or by selecting each area and clicking on the **Add Items to be scanned** button.
2. Configure the scan options. For this purpose, press the **Configure Scan** button in the program's standard bar. This step is optional since there is a default set of scan options.
3. Press the **Scan** button. This will start the immediate scan. You will be able to view the progress of the scan in a window which is displayed for that purpose.

Except for in permanent scans, there exists another scanning possibility. You need only right-click the item(s) to scan. The first option displayed in the pop-up menu that appears next may read **Scan**, **Scan now**, or **Scan selected item(s)**, depending on the section from which you have enabled the pop-up menu. For more information, consult the Pop-up Menu section in this Help file.

Furthermore, you can also select several items at the same time. This can be done two ways. You can select separate items that are not grouped together on the list (while pressing the CTRL key, click the items desired) or you can highlight items that are listed one after another (while pressing the SHIFT key, click the first and last item desired on the list. This will highlight a range of items).

You may also wish to perform an immediate scan by using one of the predetermined scans. In that case, follow these steps:

1. Choose the predetermined scan you want to execute. The name of the predetermined scan indicates the areas it scans. You can consult exactly which areas the selected predetermined scan covers in the **Items to be scanned** area.
2. Press the **Scan** button. This will start the immediate scan. You will be able to view the progress of the scan in a window which is displayed for that purpose.



From the scan window, you can carry out another scan or action through the use of the right mouse button, which will display a pop-up menu that permits you to **Show information**, **Disinfect**, **Rename**, **Move**, **Delete** and **Select all**.

Options: scanning (Immediate / Scheduled / Windows Startup - Advanced)

Note: certain options are only available depending on the product purchased and the operating system configuration. For more information, see Differences between versions.

This tab contains diverse options which are grouped for greater convenience:

Scan

Compressed files: if this option is checked, all compressed files found will be scanned. These files will only be scanned if this option is checked; selecting all extensions will not be enough.

System files: indicates that the IO.SYS and MSDOS.SYS files or system files will be scanned. These files are only scanned if this option is checked; it is not enough to select all the extensions.

Electronic mail files: if this option is checked, the antivirus program will scan all e-mail files it finds, regardless of what may be indicated in the **Extensions** section. The antivirus is capable of scanning the e-mail files of the **MS-Exchange/Outlook** program (PST files). These files are only scanned if this option is checked; it is not enough to select all the extensions.

All files: selecting this option will ensure the scanning of all files, regardless of their extension, except for compressed files, system files and the electronic mail files of **Microsoft Outlook Express**, **Microsoft Exchange** and **Microsoft Outlook**, which must be separately checked in order to be scanned.

Only program files: if this option is selected, only files with EXE or COM extensions will be scanned.

Only my extensions: this option enables you to scan all the files whose extensions are included in a list. Pressing the **Extensions** button takes you to this list.

Additional

Enable sounds: if you check this option, you will enable the sounds in accordance with the configuration previously set in the corresponding section of general configuration.

Generate report: if this option is checked, the data relative to the scan in question will be logged in the report.

Multiple diskettes: enables you to indicate that you want to scan several diskettes consecutively. Thus, when the antivirus has scanned one disk, it will ask you to insert the next one.

Minimize while scanning: if you check this option, the antivirus will automatically minimize itself when it starts the scan.

Heuristic

Enable: if you check this option each file will be subjected to an additional scan in search of viruses. This second scan is performed using techniques designed to detect unknown viruses.

Configure: this button allows you to configure the heuristic scan. You can select one of three different levels of sensitivity and in what suspicious situations you want the antivirus to notify you.

Options: actions (Immediate / Scheduled / Windows Startup - Advanced)

Note: certain options are only available depending on the product purchased and the operating system configuration. For more information, see Differences between versions.

In this section you can indicate what action you want the antivirus program to take when it finds a virus. Depending on the action you choose, a series of options will be displayed to enable you to configure it. The different possibilities are:

Show information on the virus

This action makes the antivirus show a window containing information about the virus at the moment it is detected. However, no further action will be taken.

Ignore and continue scanning

Selecting this action will ensure that the antivirus program will perform no action when it detects a virus. It will continue the scan in the normal way.

Disinfect automatically

Choosing this action instructs the antivirus to automatically disinfect all infected files it detects. This option can be configured, since there may be occasions on which disinfection is not possible. The configuration options are:

Rename: if the infected file cannot be disinfected, this option tells the antivirus to rename it by changing its extension to VIR.

Delete: when disinfection is impossible and this option has been selected, the antivirus will delete the infected file.

Move: choosing this option instructs the antivirus to move an infected file to another location when it cannot be disinfected. To complete this option, you can indicate the destination to which these infected files will be moved.

Move – **path:** lets you indicate the directory to which infected files will be copied.

Move – **e-mail address:** allows you to indicate an e-mail address to which the infected file will be sent.

Rename the infected file

This option ensures that all infected files detected will be renamed.

Delete the infected file

When you choose this option, the antivirus will delete all the infected files it finds.

Move the infected file

If this option is selected, the antivirus will move all the infected files it detects.

Move – **path:** enables you to indicate the directory to which infected files will be copied.

Move – **e-mail address:** allows you to indicate an electronic mail address to which the infected file will be sent.

Ask what action to take

This option instructs the antivirus to ask for the action to be taken each time a virus is detected. This allows you to indicate different actions within the same scan. To make the configuration more flexible,

you can choose from among the options which are shown at the moment the virus is detected.

Move: this would correspond to the **Move** action described previously.
Delete: this would correspond to the **Delete** action described previously.
Disinfect: this would correspond to the **Disinfect** action described previously.
Show information: this would correspond to the **Show information** action described previously.
Rename: this would correspond to the **Rename** action described previously.

Suspend the scan and inform in case of any other incident
If you check this option, the scan will stop momentarily if some unexpected problem arises so that you can be informed of the incident. Once you accept the notification of the incident, the scan continues in the normal way.

Options: exclusions (Immediate / Scheduled / Windows Startup - Advanced)

Note: certain options are only available depending on the product purchased and the operating system configuration. For more information, see Differences between versions.

Exclusions allow you to indicate directories, files and/or extensions you do not want scanned.

Directories
As part of the exclusions you can indicate entire directories so that they will not be scanned. You can exclude a directory by itself or a directory together with all its subdirectories.

Add: pressing the **Add** button opens a window which enables you to indicate the directories you do not want scanned. A button bearing a file folder symbol allows you to indicate either that you wish to exclude all the subdirectories included in the directory which you have excluded from scanning, or that you are excluding only the files which depend directly on the directory in question.

Remove: pressing this button removes directories from the list of directories not to be scanned.

Clear: this button lets you quickly empty the list of directories which are not to be scanned.

Files

In the exclusions section you can also add files which you do not want scanned. You can indicate that a certain file is not to be scanned or that none of the occurrences of that file is to be scanned during the entire scanning operation. For example, if you have a file called EXAMPLE.EXE in several locations, you can either exclude one of those occurrences from scanning or all of them.

Add: pressing this button brings up a window which enables you to indicate the files you do not want scanned. A button bearing a file folder symbol allows you to indicate whether all occurrences of a certain file are to be excluded or only the one you have selected.

Remove: this button allows you to delete a file from the list of exclusions.

Clear: this button lets you easily empty the list of files which are not to be scanned.

Extensions

You can also exclude from scanning all files which have a certain extension. For this purpose, just as there is a list of extensions to be scanned, there is a list of extensions which are excluded from the scan.

Extension: you can use this edit box to indicate the extensions that you want to include in the excluded extensions list.

Add: when you click on this button, the extension indicated in the edit box provided is added to the list of extensions which will not be scanned.

Remove: removes the selected extensions from the list.

Options: report (Immediate / Scheduled / Startup / Permanent - Advanced)

Note: certain options are only available depending on the product purchased and the operating system configuration. For more information, see Differences between versions.

This tab is used to configure the general options governing the report on the activity of the antivirus. The configurable options are:

Level of detail
This option enables you to configure the level of detail you want in the report.

Simple: at this level of detail all virus-related incidents are recorded. The report will also register all errors which could affect the level of security (for example, the inability to disinfect a virus because a diskette is write-protected).

Medium: besides the data included on the simple level, all jobs are registered at both their start and finish. In addition, at this level the report includes all changes made in the antivirus that affect its level of protection (disabling of permanent protection, etc.).

Black box: this is a special mode intended to solve problems which may arise with the antivirus program. An exhaustive record is made aimed at providing the greatest possible quantity of information. We recommend against enabling this level if you have no problems.

Size of the report

Because the report is maintained between different antivirus sessions, if it is never erased it may reach an excessive size. This option allows you to consult the maximum size of the report.

Options: warnings (Immediate / Scheduled / Startup / Permanent - Advanced)

Note: certain options are only available depending on the product purchased and the operating system configuration. For more information, see Differences between versions.

Warnings are notifications the antivirus generates to indicate that it has detected a virus. Because of the importance of this type of notification, its configuration is flexible and powerful to ensure that the virus notification reaches the right person. In order to enable a specific warning system, just check the box that appears next to it. If you also want to control how these alerts should be produced, click on the **Configure** button. Alert options may vary from one scan type to another (e.g. only the **workstation** and **e-mail** options are available for the permanent Internet scan). The different alert types are as follows:

In the workstation (the Configuration button will not appear in the configuration section of Internet warnings)

This option enables you to choose how notification will be given of the detection of a virus in the computer in which it was found. If you indicate that you wish to see the warnings in the computer where the virus was found, a button allows you to configure the type of notification.

Audible warning: plays a sound at the time a virus is detected.

Audible warning – **beep:** if this option is chosen, a beep will be heard each time a virus is detected.

Audible warning – **WAV file:** if you select this option, each time a virus is detected a WAV type file will be played. You can indicate which WAV file you wish to hear.

Warning message: you may also choose a warning in the form of a displayed message.

Show next warning message: this is the message that will be shown each time a virus is detected.

Remove warning message after: in order not to stop the scan, you can indicate that you want the warning message to disappear after a certain number of seconds.

Via e-mail

This option instructs the antivirus to use electronic mail to notify of the detection of a virus in a computer.

Send warning messages to the following address: serves to indicate that you want an e-mail message to be sent each time a virus is detected. This is where you can enter the e-mail addresses of the recipients who should receive virus detection notifications.

Address: the e-mail address to which the virus detection messages will be sent.

Warn sender: the person who sent the infected message may also be warned.

Warn other recipients: other recipients of the infected message may also be warned.

Warning message: the message which will be shown each time a virus is detected.

Protocol: select the type of protocol through which you wish to send the warning message: MAPI or SMTP (outgoing mail).

Server: here is where you can enter the name of the server through which warning messages will be sent.

In the network

This option instructs the antivirus to communicate the detection of a virus in one computer to other computers connected in a network with the first one.

Send message to workstation: you can choose to send the virus detection message to a specific workstation in the network.

Workstation: enables you to indicate the workstation to which you wish to send the virus detection message.

Workstation warning message: the message which will be displayed each time a virus is detected.

Send message to domain: you can choose to send the virus detection message to all the workstations belonging to the same domain.

Domain: allows you to indicate the domain to which you wish to send the virus detection message.

Domain warning message: the message that will be displayed each time a virus is detected.

Server: here is where you can enter the name of the server through which warning messages will be sent.

In Lotus Notes

This option permits users to send alerts when a virus is detected in a Lotus Notes system. The warning may be sent to the document's author, to the person working with the infected file or to any other user.

Recipients: in this textbox, enter the name of the users that will receive the warning, separating each name with a coma.

Warn document's author: the creator of the infected document is notified of the detection.

Warn person using the document: the user working with the infected document is notified of the detection.

Warning message: this permits you to enter the message that will be sent as an alert on the detection.

In the lower part of the configuration screens, the following two buttons appear:

Restore: this enables you to select the type of configuration desired: *default* (configuration settings that the user defined as standard) or *manufacturer* (initial configuration settings defined by the antivirus program).

Predetermine: this enables the user to indicate that the configuration settings defined in that moment be used as the antivirus' default configuration values.

Scan areas in an immediate scan (Basic)

The purpose of the immediate scan is to check one or more parts of the computer in search of viruses.

To perform an immediate scan in the basic mode, just choose one of the predetermined scans which come with the program and press the **Scan** button.

There is an area called **Items to be scanned** in the immediate scan window which enables you to see which areas are going to be scanned in search of viruses. Each one of the predetermined scans which come with the program scans different areas of the computer. When you choose a predetermined scan, you can see the associated scanning areas in the **Items to be scanned** area. It is important to bear in mind that you will not be able to modify these areas when you are working in the basic mode.

Panda Antivirus 6.0 is capable of scanning **Microsoft Exchange**, **Microsoft Outlook** and **Microsoft Outlook Express** folders. Any of the folders belonging to these mail systems can be scanned in the same way as any other area of the computer. It should also be emphasized that **Panda Antivirus 6.0** will scan for viruses any message database belonging to any of these systems that it may find during the scan, even though the database has not been defined as a folder.

Predetermined scans in an immediate scan (Basic)

To perform an immediate scan in the basic mode, choose one of the predetermined scans available in the **Predetermined scans** area. When you have made your choice, you will see the scanning areas associated with the selected predetermined scan in the **Items to be scanned** area. The scan will begin when you press the **Scan** button.

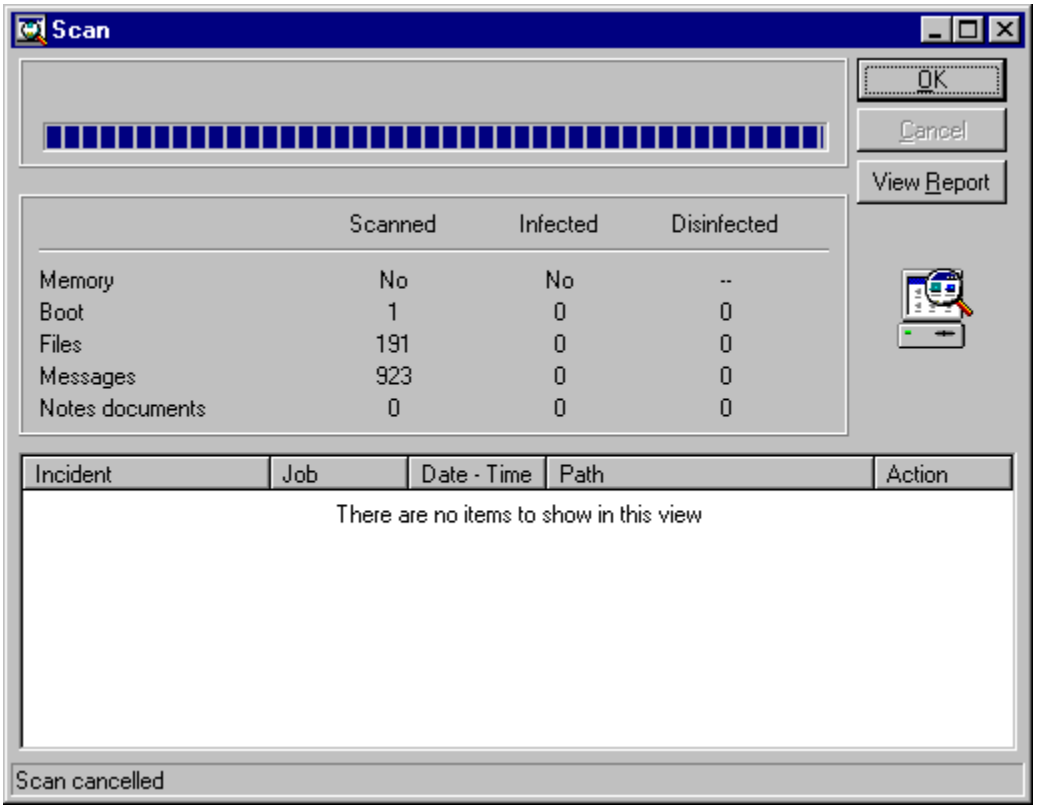
When you are working in the basic mode, you cannot add or remove predetermined scans. The predetermined scans which come with the program by default permit you to scan any of the areas of the computer prone to virus infection.

How to perform an immediate scan (Basic)

The immediate scan area is accessed through the **Immediate** option offered by the **Go to** menu. You can also access this area by exiting the antivirus presentation pages which are displayed when the program is started up, or by using the **Panda Antivirus 6.0 bar**, which shows the main options offered by the program to facilitate its use.

To perform an immediate scan in the basic mode, follow these steps:

1. Select the predetermined scan you wish. The name of the predetermined scan indicates what areas it scans. You can ascertain what specific areas are scanned by the predetermined scan you have selected by consulting the **Items to be scanned** area.
2. Press the **Scan** button to start the immediate scan. You can monitor its progress in a window that is displayed for that purpose.



Except for in permanent scans, there exists another scanning possibility. You need only right-click the item(s) to scan. The first option displayed in the pop-up menu that appears next may read **Scan**, **Scan now**, or **Scan selected item(s)**, depending on the section from which you have enabled the pop-up menu. For more information, consult the Pop-up Menu section in this Help file.

Furthermore, you can also select several items at the same time. This can be done two ways. You can select separate items that are not grouped together on the list (while pressing the CTRL key, click the items desired) or you can highlight items that are listed one after another (while pressing the SHIFT key, click the first and last item desired on the list. This will highlight a range of items).

If you wish to do an immediate scan which is different from the predetermined ones, or if you want to perform an immediate scan with options which are different from the default ones, you must be in the advanced mode.

From the scan window, you can carry out another scan or action through the use of the right mouse button, which will display a pop-up menu that permits you to **Show information**, **Disinfect**, **Rename**, **Move**, **Delete** and **Select all**.

Installing Panda Antivirus 6.0

To install **Panda Antivirus 6.0**, you will need a Win 95/98/NT-Ws 4.0 operating system, 486 or higher processor, 16 MB of RAM memory and 50 MB of free hard disk space.

Panda Antivirus 6.0 is available on CD-ROM and floppy disks. To install **Panda Antivirus 6.0**, you must insert the CD-ROM or the product's first floppy disk in the CD-ROM or disk drive.

If you are carrying out the installation from CD-ROM, an application will automatically be launched that will permit you to choose the **Panda Antivirus 6.0** (**Home Edition** or **Platinum**) version that you wish to install. Select the **Panda Antivirus 6.0 for Windows 95/98/NT** option. If the AutoPlay option is disabled on your computer, run the **CDMENU.EXE** program.

If you are carrying out the installation from floppy disk, there is first an added stage which will scan the computer's memory and hard drive in search of viruses. This pre-installation is in charge of executing the setup program once it has finished. The steps taken during the pre-installation process are as follows:

1. **Welcome:** the first window welcomes the user to the pre-installation process.
2. **Scanning of memory and hard disk:** this window allows you to choose whether you wish to scan the memory and/or hard disk in search of viruses, thereby assuring a safe installation. The areas that you have chosen will subsequently be scanned.
3. **Start file copy:** this window notifies you that the copying of files will begin. Once you accept to continue, the file copy process from the installer to the hard disk will begin.
4. **Installer:** once the pre-installation process has finished, the **Panda Antivirus 6.0** (**Home Edition** or **Platinum**) setup program will be executed.

The **Panda Antivirus 6.0** installation process is capable of determining whether the program is being installed for the first time or if it is an update of an older version. The procedure is similar for both cases. The following is a list of steps that will be taken during the installation:

1. **Language:** you will first be asked for the language you want the installation process to be performed in.
2. **Welcome:** the first window of the installer welcomes the user to **Panda Antivirus 6.0**.
3. **License agreement:** license agreement window. You can go back to the first step, accept the conditions (continues with the installation) or not accept them (cancels the installation).
4. **Scanning of memory and hard drive:** this window allows you to choose if you want to scan the memory and the hard drive in order to guarantee a virus-free installation.
5. **User's details:** you must type in your user name and company in order to register the product.
6. **Directory:** the program asks for the installation directory of the antivirus.
7. **Type of installation:** you may choose from one of the following: a **complete** installation, which will install all components, a **custom** installation, which allows you to choose which components to install or an **assisted installation (Wise Setup)** which, through a series of simple questions, offers the most suitable installation for each case.
8. **Program group:** allows you to choose the program group where the application's icons will be created.
9. **Summary:** once the initial phase of the gathering of installation information has concluded, a window displaying a summary of the data provided will be shown, and the program will begin to copy files.
10. **File copy:** in this section, the antivirus files will be copied onto your hard drive.

11. **Modification of the AUTOEXEC.BAT:** if the startup scan option was not disabled in step seven of the setup process (*Type of installation*), this is one of the components that will be installed by default. For this reason, you will be offered the possibility of automatically modifying the AUTOEXEC.BAT file, so that every time the computer is booted key components will be scanned. You can choose to have the installer make the changes automatically, or you can make them manually at another time.
12. **Safedisk:** permits you to execute the **Safedisk** program. The purpose of this utility is to generate emergency disks. One is used to boot the computer in a virus-free environment. The others are scan and disinfection disks. It is highly recommended that you create both of these diskettes, write-protect them, conveniently label them, and store them in a safe place.
13. **On-line registration:** thanks to this option you may register the product via Internet.
14. **End of installation:** the last step of the installation will recommend that you restart the computer if necessary in order to finish the installation.

Note: some options are only available according to the specific product purchased and the configuration of your operating system. For more information, see Differences between versions

Information on viruses

With the **Virus List** button in the standard **Panda Antivirus 6.0** button bar, you can access the list of viruses detected by **Panda Antivirus 6.0**. You can obtain detailed information on each virus in the list by selecting it.

In the drop-down **Show** list, you can choose to view **All Viruses**, only **Program Viruses**, **Boot Viruses**, **Macro Viruses** or a list of **Common Viruses**. Depending on the option you have selected, different viruses will be shown.

In the **Show** section you can choose among viewing all the viruses, viewing only those viruses which contaminate files, viewing those which infect the boot sector, the so-called macro viruses or a list of the most common viruses. Depending on the option you choose, you will see some or other viruses in the list.

You can indicate the name of a virus in **Search for viruses** to find a specific virus more easily. With this same purpose in mind, the virus list is shown in alphabetical order.

By selecting a virus from the list, you will see detailed information on it in the **Information on viruses** section. Among the information shown are the: **Name** and **Alias**, **Origin**, **Size** (of the virus), **Date** (the virus was detected), areas it **Infects** and whether or not it can be correctly disinfected, i.e. if it can be **Repaired**. As additional information, you will also be able to read whether the virus has specific characteristics, among which are included:

- **Permanent:** when the virus is executed, it reserves a small part of the memory and installs itself in it in order to contaminate your system progressively from there.
- **Stealth:** is a technique used by some permanent viruses. It consists of camouflaging the changes the virus makes in the files it infects. When a person tries to view one of the characteristics of the file modified by the virus, this one, which is permanent in memory, intercepts the consultation and offers the information previous to the modification.
- **Encrypted:** viruses that have this characteristic are capable of encrypting themselves in a different way each time they infect a file. This way, it is impossible to find the virus using a string search.
- **Overwrite:** Overwriting viruses, which may be permanent or non-permanent, overwrite the file they infect. This file then becomes useless. The size of the file does not change unless the size of the virus is greater than that of the file. The only way to remove these viruses is by deleting the infected file and putting an uninfected copy in its place.
- **Polymorphic:** Polymorphic viruses are advanced versions of encrypted viruses. They are capable of changing their method of encryption from one generation to the next. Thus, there is no part of the virus which remains unchanged.
- **Companion:** Companion viruses are those that, in order to contaminate an EXE file, create a COM file with the same name and with the hidden attribute enabled. The virus is permanent in the cited COM file. If there are two files with the same name and EXE and COM extensions, the MS-DOS operating system will first execute the one with the COM extension. This is how this type of virus propagates itself; when an attempt is made to run a program (an EXE file), what is really executed is the virus (COM file) that is then loaded in the memory, and which will typically execute the EXE file immediately afterward so that the user will not suspect anything.

The **Version** button brings up a window containing information on the virus file. The information it offers is:

- **Number of viruses:** indicates the number of viruses detected by the virus file.
- **Version:** indicates the version of the virus file. This version makes reference to the different technologies which are implemented in the file. It may be that very new releases of the virus file cannot operate properly with old versions of **Panda Antivirus 6.0**; that is why it is important to display this information.
- **Date:** the date on which the virus file was generated.
- **Time:** the time at which the virus file was generated.
- **Size:** indicates the size of the virus file.

The **Print** button will enable you to obtain a printed copy of the information on the virus whose information is being displayed.

What is a scheduled scan?

Scheduled scans make it possible to scan any part of the computer in search of viruses at certain times indicated beforehand.

The great usefulness of scheduled scans is the possibility of telling the program that it must activate itself and scan for viruses at a certain time on a certain date. This way, you can create a scan "calendar", which maximizes the ease with which the user can keep his/her computer free of viruses.

Scheduled scans work in the same way as immediate scans. You could say that a scheduled scan is, in fact, a set of immediate scans which are executed at specific times.

Because scheduled scans operate as immediate ones do, both have the same options and configuration possibilities. Scheduled scans offer the possibility of choosing the area(s) wished to be scanned. The scan is performed at the time indicated by the user. These characteristics make scheduled scans especially recommendable for scanning the computer in a regular manner and thus keeping it virus-free.

If you are in basic mode, in order to specify a scheduled scan you must choose one of the predetermined scheduled scans which come with the program. The object of these predetermined scans is to provide the most common scans in a predefined form in order to facilitate scan jobs as much as possible.

If you are in advanced mode (Differences between versions), you also have a series of predetermined scheduled scans at your disposal. You can choose any of these or create a new scan according to your specific needs. You also have the possibility of varying the scan options. These options allow you to configure the scan to adapt it to your needs.

Scan areas in a scheduled scan (Advanced)

Note: certain options are only available depending on the product purchased and the operating system configuration. For more information, see Differences between versions.

In the advanced mode you can define a scheduled scan capable of scanning any part of the computer in search of virus. To select the areas to be scanned, use the **Selection tree**, where you will find displayed all the areas which can be scanned. These areas are the memory, all the drives assigned in the computer and, optionally, the e-mail folders associated with the **Microsoft Exchange**, **Microsoft Outlook** and **Microsoft Outlook Express** programs.

To determine which areas from the **Selection tree** will become **Items to be scanned**, there are three buttons with the following functions:

- **Add area:** if you select an area in the **Selection tree** and then click on this button, the area in question is added to **Items to be scanned**. You can obtain this same effect by dragging an area directly from the **Selection tree** to **Items to be scanned**.
- **Remove area:** if you select an area in **Items to be scanned** and then press this button, the selected area will be removed from **Items to be scanned**.
- **Clear:** if you press this button, all the areas listed in the **Items to be scanned** list will disappear from said list.

If you try to add an area to **Items to be scanned** which is already there, the antivirus will notify you of this fact and will cancel the operation. If you try to add an area to the **Items to be scanned** list which is included within another area that is already on the list, the antivirus will let you know but will not cancel the operation.

It is also important to bear in mind that the different items to be scanned can be added with and without subdirectories. If you attempt to add an item with subdirectories and this item is already stripped of them, the antivirus program will ask if you want to remove the version without subdirectories and add the new one which includes them.

Finally, if an area is already in **Items to be scanned** and you attempt to add a higher area which includes it, you will be given the option of removing the redundancies automatically.

Panda Antivirus 6.0 Platinum is capable of scanning **Microsoft Exchange**, **Microsoft Outlook** and **Microsoft Outlook Express** folders. Any of the folders of these mail systems can be scanned in the same way the antivirus would scan any other area of the computer. It is also important to point out that **Panda Antivirus 6.0 Platinum** will scan for viruses in any message database belonging to any of these systems which it may find during the scan, even when the message database in question is not defined as a folder.

Options in a scheduled scan (Advanced)

The scan options enable you to configure how a scan in search of viruses will be carried out. To access these options, press the **Configure Scan** button in the standard button bar. All the scan options are grouped in a single window but separated into different tabs in order to make them easier to manage. These tabs only appear in advanced configuration settings, which can only be accessed from **Panda Antivirus 6.0 Platinum**, but not from **Panda Antivirus 6.0 Home Edition**. For more information, consult the section entitled Differences between versions.

Select the section you want more information on:

Predetermined scans in a scheduled scan (Advanced)

Note: certain options are only available depending on the product purchased and the operating system configuration. For more information, see Differences between versions.

Predetermined scheduled scans offer the greatest ease in creating a quick and simple scan "calendar".

A predetermined scan is a specific configuration of areas, frequencies and scan options. Predetermined scans are saved so that they can be reused as many times as needed, thus saving you an important amount of time and greatly simplifying your scanning jobs.

The program comes equipped with a series of predetermined scans. Among these predefined scans are the ones most frequently used when searching for viruses. If you wish to do a different scan, you will be able to save the specified scan configuration (areas, frequencies and scan options) to add a new predetermined scheduled scan to your list.

Adding a new predetermined scan. All you need to do is choose a set of scan areas and establish the scanning frequency and the desired options. When you have done this, press the *Save* button in the standard program bar. The software will ask you for a name for the new predetermined scan. Once you have given it a name, the new scan will be available in the list of predetermined scans.

Removing a predetermined scan. To remove a previously created predetermined scan, simply click on the scan to be removed with the right mouse button and choose the **Remove created scan** option. It is important to bear in mind that only those predetermined scans that the user has previously created can be removed; those included with the program cannot be removed.

How to perform a scheduled scan (Advanced)

Note: certain options are only available depending on the product purchased and the operating system configuration. For more information, see Differences between versions.

The scheduled scan area is accessed through the **Scheduled** option in the **Go to** menu. You can also get to this area by using the **Panda Antivirus 6.0 Platinum bar**, which shows the main options of the program in order to make its handling easier.

To perform a scheduled scan, follow these steps:

1. Add the areas you want scanned for viruses to **Items to be scanned**. This can be done by dragging these areas from the **Selection tree** to **Items to be scanned,** or by selecting each area and clicking on the **Add Items to be scanned** button.
2. Configure the scan options. To do this, press the **Configure Scan** button in the program's standard button bar. This step is optional since there is a default set of scan options.
3. Establish a scan calendar. The options for establishing the calendar are part of the configuration window. Therefore, you can also access them by clicking on the **Configure Scan** button in the standard button bar.
4. Double-click on the new scheduled scan you have defined. This will put it into the enabled state. You can also right-click on the scheduled scan you wish to enable and then choose the corresponding option.

You may also want to perform a scheduled scan by using one of the predetermined scans. In that case, the procedure to follow is:

1. Choose the predetermined scan you want to run. The name of the predetermined scan indicates the areas it scans. You can consult specifically which areas the selected predetermined scan covers in the **Items to be scanned** area.
2. Double-click on the new scheduled scan you have defined. This will put it into the enabled state. You can also right-click on the scheduled scan you wish to enable and then choose the corresponding option.

If you wish to do an immediate scan based on the selected scheduled scan, just press the **Scan** in the program's standard button bar.

Options: scheduler (Scheduled - Advanced)

Note: certain options are only available depending on the product purchased and the operating system configuration. For more information, see Differences between versions.

The scheduler's goal is to establish the periodicity with which a certain scheduled scan will be executed. You will need to indicate both the periodicity or frequency and the range of dates during which the scheduled scan in question will be enabled.

Frequency

In this section you can indicate when a scheduled scan will be executed. Scheduled scans can be executed one time only or every so many hours, days or weeks, and even on certain specific days of each month. Depending on the type of frequency chosen, the program will ask you for different types of data.

Schedule scan: this permits you to choose whether you want to scan just once, every certain number of hours, days or weeks, or even on a certain day of a month or year. Depending on the scan frequency selected (**Once**, **Hourly**, **Daily**, **Weekly**, **Monthly** or **Yearly**), different sections will be displayed in the central area of the screen:

- **Day scan will be performed:** by selecting the *Once* option from the **Schedule scan** list, you can select the desired launch date from a calendar.
- **Hourly Interval:** by selecting the *Hourly* option from the **Schedule scan** list, you can select every how many hours the scan should be performed.
- **Daily Interval:** by selecting the *Daily* option from the **Schedule scan** list, you can select the date and every how many days the scan should be performed.
- **Weekly Scheduling:** by selecting the *Weekly* option from the **Schedule scan** list, you can select every how many weeks and what day the scan should be performed.
- **Monthly Scheduling:** by selecting the *Monthly* option from the **Schedule scan** list, you can select the day of the month the scan should be performed (e.g. on the 17th of each month), or whether it should be carried out on the first, second, third, fourth or fifth day of the week of each month (e.g. the fourth Thursday of each month).
- **Day scan will be performed:** in this case, you can indicate the number of the day and month the scheduled scan should be performed.

Start time: allows you to indicate the time at which the scan will start.

Time limit: allows you to indicate the lastest time by which scanning must be completed. If it is not already finished by that time, it will be then be stopped.

Validity

You can indicate that a certain scheduled scan is valid only between two dates. Once these dates have passed, the scan will never be executed again because it will have exceeded its validity period.

Start date: indicates the beginning date of the validity period of a scheduled scan.

End date: indicates the date which ends the validity period of a scheduled scan. It is optional. If you prefer not to indicate a final date, the scheduled scan will never expire.

Enabled

You can use this option to enable or disable the scheduled scan in question.

Scan areas in a scheduled scan (Basic)

The mission of the scheduled scan is to scan one or several parts of the computer in search of viruses at a series of times which the user indicates beforehand.

To enable a scheduled scan in the basic mode, simply check one of the predetermined scans which are offered. You can check several predetermined scans to be executed simultaneously. You may also decide to carry out an immediate scan starting from a certain scheduled scan. To do this, just press the *Scan* button in the standard program button bar after selecting a predetermined scan.

There is an area called **Items to be scanned** in the scheduled scan window which enables you to display which areas are going to be scanned in search of viruses each time the scheduled scan is executed. Each one of the predetermined scans which come with the program scans different areas of the computer at different times. When you choose a predetermined scan, you can see the associated scan areas in the **Items to be scanned** area. It is important to bear in mind that you will not be able to modify these areas when you are working in the basic mode.

Panda Antivirus 6.0 is capable of scanning **Microsoft Exchange**, **Microsoft Outlook** and **Microsoft Outlook Express** folders. Any of the folders of these mail systems can be scanned in the same way the antivirus would scan any other area of the computer. It is also important to point out that **Panda Antivirus 6.0** will scan for viruses in any message database belonging to any of these systems which it may find during the scan, even when the message database in question is not defined as a folder.

Predetermined scans in a scheduled scan (Basic)

To enable a scheduled scan in the basic mode, simply select one of the predetermined scans which are offered in the **Predetermined scans** area. When you have done this, you will see the scan areas associated with the predetermined scan you selected in the **Items to be scanned** area. Once a scheduled scan has been enabled, it will be performed with the frequency you have indicated until it is disabled.

In the basic mode it is impossible to add or remove predetermined scans. The predetermined scans which come with the product by default allow the scanning of any of the areas of the computer which can possibly have viruses, and also take the most common frequencies into consideration.

How to perform a scheduled scan (Basic)

The scheduled scan area is accessed through the **Scheduled** option in the **Go to** menu. You can also access this area by using the **Panda Antivirus 6.0 bar** that shows the main options offered by the program to facilitate its use.

To perform a scheduled scan in the basic mode, follow these steps:

1. Select the predetermined scan you wish. The name of the predetermined scan indicates both the areas it will scan and the frequency with which it will scan. You can ascertain what specific areas the predetermined scan you have selected scans by consulting the **Items to be scanned** area.
2. Double-click on the predetermined scan you have selected in order to enable it. You can also right-click on the scheduled scan you wish to enable and choose the corresponding option.

If you want to perform an immediate scan based on the scheduled scan you have chosen, simply press the **Scan** button on the standard button bar.

If you wish to enable a scheduled scan which is different from any of the predetermined ones, or if you want to perform an immediate scan with options which are different from the default ones, you must be in the advanced mode.

What is the permanent scan?

Note: the Permanent File (Sentinel), Internet Scans and Lotus Notes Scans in Basic Mode will be available in **Panda Antivirus 6.0 Home Edition**. However, **Panda Antivirus 6.0 Platinum** will also include these scans in Advanced Mode. For more information, consult the section entitled Differences between versions.

The goal of the Permanent File/Internet/Lotus Notes Scan is to monitor any operation carried out on the computer in search of viruses. Thus, every time you attempt to execute, copy,…etc. a file, or access, send or download items from the Internet, or work with Lotus Notes items, the Permanent protection will carry out a scan to make sure the item being handled is clean.

XTherefore, the Permanent File/Internet/Lotus Notes Scan is responsible for giving a permanent protection in everything associated with the handling of files/Internet contents/ Lotus Notes items. This includes any copying of files to or from a networked computer, etc.

The Permanent File/Internet/Lotus Notes Scan has a minimal impact on the performance of the system, and offers the highest degrees of protection. Therefore, we always recommend that our users have it enabled. Once it has been enabled and until it is disabled, the Permanent File/Internet/Lotus Notes Scan will start up each time the computer is booted.

You can check whether the permanent scan is enabled by looking at the bottom of the screen (in the Windows taskbar), where you should see a bear icon. If you right-click it, you will be presented with these three options:

- **Unload:** removes the Sentinel, Internet and/or Lotus Notes permanent scan from memory.
- **Configure:** permits you to indicate the behavior of the permanent File, Internet and Lotus Notes database systems scans.
- **Panda Antivirus:** launches **Panda Antivirus 6.0** from the Windows Taskbar.
  Close: exits the permanent scan.

If you wish to obtain more information on each of the permanent scans that **Panda Antivirus 6.0 Home Edition / Platinum** supports, we recommend you read the following sections:

Permanent File Scan (Sentinel).
Permanent Internet Scan.
Permanent Lotus Notes Scan.

How to enable the permanent scan (Files / Internet / Lotus Notes - Advanced)

Note: certain options are only available depending on the product purchased and the operating system configuration. For more information, see Differences between versions.

The area scan by means of the file/Internet/Lotus Notes permanent is accessed through the **Permanent** option in the **Go to** menu. You can also access the area by using the **Panda Antivirus 6.0 Platinum bar**.

To enable the file/Internet/Lotus Notes permanent scan, check the **Enabled** option in the **Permanent status** section. From that moment on, the file/Internet/Lotus Notes permanent will monitor all the file-related operations which are performed in the computer, thus preventing it from being infected.

In the **Permanent** section, the report on the activity of the file permanent is displayed. All the events which are related to the work of the permanent will be progressively recorded in this file.

To complete this information, the **Permanent status** section offers additional information regarding the activity of the permanent:

In the Sentinel (Permanent File Scan) tab:

- **Files checked:** number of files the permanent has scanned for viruses from the beginning of its activity (normally since the booting of the computer).
- **Viruses found:** number of viruses detected by the permanent.
- **Total scan time:** total time invested by the permanent in the scanning of files.

In the Permanent Internet Scan tab:

- **No. of files scanned:** this indicates the number of files the permanent protector has scanned in search of viruses since you first connected to the Internet.
- **No. of files infected:** this indicates the number of files in which the permanent protector has detected a virus.
- **No. of files disinfected:** this indicates the number of files in which the permanent protector has detected a virus and subsequently disinfected.
- **No. of Websites visited:** this indicates the number of sites visited since you first connected to the Internet.
- **Last Website visited:** this indicates the address/name of the last site you visited via Internet.
- **Last file scanned:** this indicates the name of the last file the permanent Internet protector scanned.

In the Permanent Lotus Notes Scan tab:

- **Scanned:** this indicates the number of Lotus Notes items the permanent protector has scanned.
- **Infected:** this indicates the number of infected Lotus Notes items the permanent protector has detected.
- **Disinfected:** this indicates the number of infected Lotus Notes items the permanent protector has disinfected.

Permanent scan options (Advanced)

Note: certain options are only available depending on the product purchased and the operating system configuration. For more information, see Differences between versions.

The file permanent scan options allow you to configure the way in which this type of scan is performed. To access these options, press the **Configuration** button in the **permanent status** section. All the scanning options are grouped in a single window but are separated into different tabs to make managing them easier.

Choose the section on which you want more information:

How to disable the permanent scan (Files / Internet / Lotus Notes - Advanced)

Note: certain options are only available depending on the product purchased and the operating system configuration. For more information, see Differences between versions.

First, access the file/Internet/Lotus Notes permanent scan area through the **Permanent** option in the **Go to** menu, or by using the **Panda Antivirus 6.0 Platinum** bar.

To disable the permanent file/Internet/Lotus Notes protection, uncheck the **Enabled** option in the **Permanent status** section. It is important to bear in mind that, from the moment the file/Internet/Lotus Notes permanent is disabled, the computer will be without permanent protection, and will thus be vulnerable to contamination by viruses.

Disabling the scan by the file/Internet/Lotus Notes permanent means that the files the system accesses will not be scanned. However, the file/Internet/Lotus Notes permanent will still be loaded in memory despite not being enabled. Moreover, the permanent will continue to be loaded in memory each time the computer is booted, regardless of the fact that it is not enabled.

Unload: the advanced mode includes an additional option which makes it possible to unload the permanent module from memory. When this is done, the file permanent will not be loaded when the computer is booted.

Options: scan (Permanent - Advanced)

Note: certain options are only available depending on the product purchased and the operating system configuration. For more information, see Differences between versions.

This tab contains two groups of options:

What operations must be scanned
Opening: all accesses to a file (to open it, execute it, etc.) entail opening it. If this option is checked, all the files the operating system attempts to open will be scanned.

Closing: just as all accesses to a file require its opening, a subsequent closing of the file will be necessary. Checking this option will ensure the scanning of all files when they are closed. The advantage of scanning files as they are closed lies in the fact that, sometimes, the file can be clean when opened, but be contaminated before it is closed.

Move / Rename: this option orders the file permanent to scan all file copying, moving and renaming operations.

Compressed files: if this option is checked, all the compressed files found will be scanned.

Save results: if you check this option, the information relative to the scan in question will be logged in the report.

What files must be scanned

All files: selecting this option will ensure the scanning of all files, regardless of their extension.

Only Program files: if this option is selected, only files ending in the extension EXE or COM will be scanned.

Only my extensions: this option enables you to scan all the files whose extensions are on a list. This list is accessed by pressing the *Extensions* button.

Options: actions (Permanent - Advanced)

Note: certain options are only available depending on the product purchased and the operating system configuration. For more information, see Differences between versions.

In this section you can indicate what action you want the antivirus program to take when it finds a virus. Depending on the action you choose, a series of options will be displayed to enable you to configure it. The different possibilities are:

Show information on the virus

This action causes the antivirus to show a window containing information about the virus in the moment it is detected. However, no further action will be taken.

Ignore and continue scanning

Selecting this action will ensure that the antivirus program will perform no action when it detects a virus. It will continue the scan in the normal way.

Disinfect automatically

Choosing this action orders the antivirus to automatically disinfect all the infected files it detects. This option can be configured, since there may be occasions on which disinfection is not possible. The configuration options are:

Rename: if the infected file cannot be disinfected, this option tells the antivirus to rename it by changing its extension to VIR.

Delete: when disinfection is impossible and this option has been selected, the antivirus will remove the infected file.

Move: choosing this option orders the antivirus to move an infected file to another location when it cannot be disinfected To complete this option, you can indicate the destination to which these infected files will be moved.

Move – **path:** lets you indicate the directory to which infected files will be copied.

Move – **e-mail address:** allows you to indicate an e-mail address to which the infected file will be sent.

Rename the infected file

This option ensures that all infected files detected will be renamed.

Delete the infected file

When you choose this option, the antivirus will delete all the infected files it finds.

Move the infected file

If this option is selected, the antivirus will move all the infected files it detects.

Move – **path:** enables you to indicate the directory to which infected files will be copied.

Move – **e-mail address:** allows you to indicate an electronic mail address to which the infected file will be sent.

Ask what action to take

This option tells the antivirus to ask for the action to be taken each time a virus is detected. This allows you to indicate different actions within the same scan. To make the configuration more flexible,

you can choose from among the options which are shown at the moment the virus is detected.

Move: this would correspond to the **Move** action described previously.
Delete: this would correspond to the **Delete** action described previously.
Disinfect: this would correspond to the **Disinfect** action described previously.
Show information: this would correspond to the **Show information** action described previously.
Rename: this would correspond to the **Rename** action described previously.

Note: some options are only available according to the specific product purchased and the configuration of your operating system. For more information, see Differences between versions

Options: exclusions (Permanent - Advanced)

Note: certain options are only available depending on the product purchased and the operating system configuration. For more information, see Differences between versions.

Exclusions allow you to indicate directories, files and/or extensions you do not want scanned.

Directories
As part of the exclusions you can indicate entire directories so that they will not be scanned. You can exclude a directory by itself or a directory together with all its subdirectories.

Add: pressing the **Add** button opens a window which enables you to indicate the directories you do not want scanned. A button bearing a file folder symbol allows you to indicate either that you wish to exclude all the subdirectories included in the directory which you have excluded from scanning, or that you are excluding only the files which depend directly on the directory in question.

Remove: pressing this button removes directories from the list of directories not to be scanned.

Clear: this button lets you quickly empty the list of directories which are not to be scanned.

Files

In the exclusions section you can also add files which you do not want scanned. You can indicate that a certain file is not to be scanned or that none of the occurrences of that file is to be scanned during the entire scanning operation. For example, if you have a file called EXAMPLE.EXE in several locations, you can either exclude one of those occurrences from scanning or all of them.

Add: pressing this button brings up a window which enables you to indicate the files you do not want scanned. A button bearing a file folder symbol allows you to indicate whether all occurrences of a certain file are to be excluded or only the one you have selected.

Remove: this button allows you to delete a file from the list of exclusions.

Clear: this button lets you easily empty the list of files which are not to be scanned.

Extensions

You can also exclude from scanning all files that have a certain extension. For this purpose, just as there is a list of extensions to be scanned, there is a list of extensions which are excluded from the scan.

Extension: you can use this edit box to indicate the extensions that you want included in the excluded extensions list.

Add: when you click on this button, the extension indicated in the edit box provided is added to the list of extensions which will not be scanned.

Remove: removes the selected extensions from the list.

Options: report (Permanent - Advanced)

Note: certain options are only available depending on the product purchased and the operating system configuration. For more information, see Differences between versions.

This tab is used to configure the general options governing the report on the activity of the antivirus. The configurable options are as follows:

Level of detail
This option enables you to configure the level of detail you want in the report.

Simple: at this level of detail all virus-related incidents are recorded. The report will also register all the errors which could affect the level of security (for example, the inability to disinfect a virus because a diskette is write-protected).

Medium: besides the data included on the simple level, all jobs are registered at both their start and finish. In addition, at this level the report includes all the changes which are made in the antivirus software which affect its level of protection (disabling of permanent protection, etc.).

Black box: this is a special mode intended to solve problems which may arise with the antivirus program. An exhaustive record is made aimed at providing the greatest possible quantity of information. We recommend against enabling this level if you have no problems.

Size of the report

Because the report is maintained between different antivirus sessions, if it is never erased it may reach an excessive size. This option allows you to consult the maximum size of the report.

Options: warnings (Permanent - Advanced)

Note: certain options are only available depending on the product purchased and the operating system configuration. For more information, see Differences between versions.

Warnings are notifications the antivirus generates to indicate that it has detected a virus. Because of the importance of this type of notification, its configuration is flexible and powerful to ensure that the virus notification reaches the right person. The configuration options are as follows:

In the workstation

This option enables you to choose how notification will be given of the detection of a virus in the computer in which it was detected. If you indicate that you wish to see the warnings in the computer where the virus was found, a button allows you to configure the type of notification.

Audible warning: plays a sound the moment a virus is detected.

Audible warning – **beep:** if this option is chosen, a beep will be heard each time a virus is detected.

Audible warning – **WAV file:** if you select this option, each time a virus is detected a WAV type file will be played. You can indicate which WAV file you wish to hear.

Show warning message: you may also choose a warning in the form of a displayed message.

Warning message: this is the message that will be shown each time a virus is detected.

Remove warning message: in order not to stop the scan, you can indicate that you want the warning message to disappear after a certain number of seconds.

In the network

This option instructs the antivirus to communicate the detection of a virus in one computer to other computers that are connected in a network with the first one.

Send message to workstation: you can choose to send the virus detection message to a specific workstation in the network.

Workstation: enables you to indicate the workstation to which you wish to send the virus detection message.

Message: the message which will be displayed each time a virus is displayed.

Send message to domain: you can choose to send the virus detection message to all the workstations belonging to the same domain.

Domain: allows you to indicate the domain to which you wish to send the virus detection message.

Message: the message that will be displayed each time a virus is detected.

Server: here is where you can enter the name of the server through which warning messages will be sent.

Via e-mail

This option instructs the antivirus to use electronic mail to notify the detection of a virus in a computer.

Send message to address: serves to indicate that you want an e-mail message to be sent each time a virus is detected.

Address: the e-mail address to which the virus detection messages will be sent.

Message: the message which will be shown each time a virus is detected.

In messages containing viruses

This option makes it possible to notify the detection of a virus in an e-mail message. The notification can be addressed to the sender or to the rest of the recipients, or the warning message can be directly inserted into the infected message.

Insert warning in the message: inserts a virus warning message into the same e-mail message which contains the infected file.

Warning in the infected message: this is the text of the notification which will be inserted into the message.

Send warning to sender: sends an e-mail message to the sender advising them of the detection of the virus in the message they have sent.

Warning for the sender: the text of the notification which will be transmitted to the sender.

Send warning to the other recipients: sends an e-mail message to each of the remaining recipients of the infected message, if there are additional recipients.

Warning for other recipients: the text of the warning message which will be sent to the other recipients of an infected e-mail message.

Note: some options are only available according to the specific product purchased and the configuration of your operating system. For more information, see Differences between versions

How to enable the permanent scan (Files / Internet / Lotus Notes - Basic)

The area pertaining to scanning by the file/Internet permanent is accessed through the **Permanent** option in the **Go to** menu. You can also access the area by using the **Panda Antivirus 6.0 bar**.

To enable the file/Internet permanent, check the **Enabled** option in the **Permanent status** section. From that moment on, the file/Internet permanent will monitor all the file-related operations which are performed in the computer, thus preventing it from being infected.

In the **Permanent** section the report on the activity of the file permanent is displayed. All the events which are related to the work of the permanent will be progressively recorded in this file.

To complete this information, the **permanent status** section offers some additional data regarding the activity of the permanent:

In the Sentinel (Permanent File Scan) tab:

- **Files checked:** number of files the permanent has scanned for viruses from the beginning of its activity (normally since the booting of the computer).
- **Viruses found:** number of viruses detected by the permanent.
- **Total scan time:** total time taken by the permanent in the scanning of files.

In the Permanent Internet Scan tab:

- **No. of files scanned:** this indicates the number of files the permanent protector has scanned in search of viruses since you first connected to the Internet.
- **No. of files infected:** this indicates the number of files in which the permanent protector has detected a virus.
- **No. of files disinfected:** this indicates the number of files in which the permanent protector has detected a virus and subsequently disinfected.
- **No. of Websites visited:** this indicates the number of sites visited since you first connected to the Internet.
- **Last Website visited:** this indicates the address/name of the last site you visited via Internet.
- **Last file scanned:** this indicates the name of the last file the permanent Internet protector scanned.

In the Permanent Lotus Notes Scan tab:

- **Scanned:** this indicates the number of Lotus Notes items the permanent protector has scanned.
- **Infected:** this indicates the number of infected Lotus Notes items the permanent protector has detected.
- **Disinfected:** this indicates the number of infected Lotus Notes items the permanent protector has disinfected.

How to disable the permanent scan (Files / Internet /Lotus Notes - Basic)

First, access the file/Internet permanent scan area through the **Permanent** option in the **Go to** menu, or by using the **Panda Antivirus 6.0 bar**, which displays the main options of the program in order to facilitate its use.

To disable the file/Internet permanent, uncheck the **Enabled** option in the **Permanent status** section. It is important to bear in mind that, from the moment the file permanent is disabled, the computer will be without permanent protection, and will thus be vulnerable to virus infection.

What is the Internet scan?

The Internet is a worldwide network made up of interconnected computers. By means of the access offered by an Internet service provider, the users of this international network can connect to it and use its services. The Internet offers different types of services. The best known among them are:

- **Web pages:** one of the best known Internet services. Web pages are pages of text and graphics in a format called HTML. Anyone can create his or her own Web pages and "publish" them (leave them in any Web page server) so that they are accessible to all Internet users. One of the most important characteristics of Web pages are their hyperlinks. A hyperlink is a connecting device joining two pages which can be in different servers located anywhere in the world. Thus, the mass of existing Web pages constitute a gigantic book containing subjects to please every taste, and offering the possibility of jumping from one "chapter" to another by clicking on a hyperlink. To display Web pages, you need a program known as a navigator or Internet browser.
- **Electronic mail (e-mail):** this is the other "basic" Internet service. It operates in a way that is similar to regular mail. Any user with access to an e-mail server can send and receive messages to and from any part of the world. The messages that are sent will go to the recipient's e-mail server, not directly to their computer. Thus, there is no need for them to have their computer connected to the server (nor even turned on) in order to receive incoming mail. In addition to text, the messages that are sent can include files of all types that the senders may attach to them. To send and receive electronic mail, an e-mail program is required.
- **File transfer:** through this service, better known as FTP, Internet users can download files left in file servers. One way to describe this is to say that the FTP programs enable any user to connect to a file server connected to the Internet and to view its directories and files as if they were in your own computer. If you want to work with those files, the FTP program allows you to download them onto your computer. It is well worth noting that files can also be downloaded from Web pages.
- **News (NNTP):** through this service, you can access newsgroups being discussed or that are placed in certain servers for consultation and subsequent discussion. You can also subscribe in order to periodically receive e-mails containing the latest news, although these may be infected. You can scan all the news received from **Exchange/Outlook** and **Outlook Express**.

The four services described above are the most important and widely used of all those offered by the Internet. Each of them uses a different protocol to operate. The question is: what is a protocol? A protocol is a means of exchanging information. The protocol enables the Internet server and the computer which connects to it to understand each other. Thus a protocol is the "language" which must be spoken to ensure communication between the two.

The protocol used to work with Web pages is called **HTTP**, the one used for sending e-mail is **SMTP** and the one used to receive it is **POP3**. The protocol used for transferring files in the Internet is called **FTP**. Lastly, the protocol used for news services is **NNTP**.

The Internet scan keeps watch on all the operations which are carried out with the protocols mentioned above (**HTTP**, **SMTP**, **POP3**, **FTP** and **NNTP**). Therefore, everything that comes into the computer via any of these pathways will be intercepted by the Internet scan, which will take care of checking it for viruses. If an e-mail message is received or sent, the Internet scan will make sure that it is free of viruses. Likewise, it will examine all files which are downloaded using the **FTP** or **HTTP** protocols, through any of the following programs: MS Internet Explorer, Netscape, Opera, WS_FTP95, CuteFTP, GetRight and Gozilla. Finally, all the contents that may be associated with a Web or **HTML** page will be also be scanned for viruses while they are being received by means of the **HTTP** protocol.

As you can see, the Internet scan is responsible for providing permanent protection against possible

viruses in all contents received from the Internet, thus relieving the user of this burden and offering the highest levels of security since, for example, in the case of e-mail, it not only scans the incoming mail but also the outgoing messages, thus ensuring that viruses will not be distributed. Due to the high levels of protection offered by the Internet scan, we recommend having it always enabled.

How to enable the Internet scan (Advanced)

Note: certain options are only available depending on the product purchased and the operating system configuration. For more information, see Differences between versions

The Internet scan area is accessed through the **Internet** option in the **Go to** menu. You can also access the area by using the **Panda Antivirus 6.0 Platinum bar**.

To enable the Internet scan, check the **Internet enabled** option in the **Internet status** section. From that moment on, the Internet scan will monitor all the Internet-related operations which are performed on the computer, thus preventing infection.

The report on the activity of the file permanent is displayed in the **Internet** section. All the events which are related to the operation of the Internet scan will be progressively recorded in this file.

To complete this information, the **Internet status** section offers some additional data regarding the activity of the Internet scan:

- **Files checked:** number of files the Internet scan has checked for viruses from the beginning of its activity (normally from the time the computer is booted).
- **Viruses found:** number of viruses detected by the Internet scan.
- **Total scan time:** total time taken by the Internet scan in the scanning of files.

Options in the Internet scan (Advanced)

Note: certain options are only available depending on the product purchased and the operating system configuration. For more information, see Differences between versions

The Internet scan options enable you to configure how this scan will be performed. To access these options, press the **Configuration** button in **Internet status**. All the scan options are grouped in a single window but separated into different tabs to make them easier to manage.

Select the section on which you want more information:

How to disable the Internet scan (Advanced)

First, access the Internet scan area through the **Internet** option in the **Go to** menu, or by using the **Panda Antivirus 6.0 Platinum** bar.

To disable the Internet scan, uncheck the **Internet enabled** option in the **Internet status** section. It is important to bear in mind that, from the moment the Internet scan is disabled, the computer will be without protection against possible viruses in the incoming Internet contents, and will thus be vulnerable to infection.

Disabling the Internet scan means that the Internet contents that are accessed will not be scanned. However, the Internet scan will still be loaded in memory despite not being enabled. Moreover, the Internet scan will continue to be loaded in memory each time the computer is booted, regardless of the fact that it is not enabled.

Unload: the advanced mode includes an additional option which makes it possible to unload the Internet scan module from memory. When this is done, the Internet scan will not be loaded when the computer is booted.

How to enable the Internet scan (Basic)

The Internet scan area is accessed through the **Internet** option in the **Go to** menu. You can also access the area by using the **Panda Antivirus 6.0 bar**, which shows the main options offered by the program in order to make using it easier.

To enable the Internet scan, check the **Internet enabled** option in the **Internet status** section. From that moment on, the Internet scan will monitor all the Internet-related operations which are performed on the computer, thus preventing infection.

The report on the activity of the file permanent is displayed in the **Internet** section. All the events which are related to the operation of the Internet scan will be progressively recorded in this file.

To complete this information, the **Internet status** section offers some additional data regarding the activity of the Internet scan:

- **Files checked:** number of files the Internet scan has checked for viruses from the beginning of its activity (normally from the time the computer is booted).
- **Viruses found:** number of viruses detected by the Internet scan.
- **Total scan time:** total time taken by the Internet scan in the scanning of files.

How to disable the Internet scan (Files/Intener - Basic)

First, access the Internet scan area through the **Internet** option in the **Go to** menu, or by using the **Panda Antivirus 6.0 bar**, which displays the main options offered by the program in order to make it easier to handle.

To disable the Internet scan, uncheck the **Internet enabled** option in the **Internet status** section. It is important to bear in mind that, from the moment the Internet scan is disabled, the computer will be not be protected against possible viruses in the incoming Internet contents, and will thus be vulnerable to infection.

Computer viruses

One of the best defenses against viruses is understanding them. By knowing how the different kinds of viruses operate, what parts of the computer they affect and how they behave, you will be better able to defend yourself against them.

Basically, we can mention three types of viruses:

Boot viruses.

File viruses.

Macro viruses.

In the following paragraphs we will explain some of the techniques used by the different types of viruses:

Techniques used by viruses.

How to prevent infections

Below is some advice about how to prevent virus infections. Remember that prevention is one of the most efficient tools for combating computer viruses.

Backup copies: make a habit of regularly copying your most important data on backup copies. This is one of the most common pieces of advice in the computer world, but one that is rarely followed. Regular backup copies do not only solve the problem of viruses, but also get round any problem arising in the computer. If backup copies are only made of important data, then your copies will be quick and easy to make. A backup copy should be made at least once every month.

Scan everything you receive: this is one of the most important bases for prevention. Scan any programs or files that you are going to introduce or have introduced in your computer before you run or open them. This will allow you to detect possible viruses before they have time to infect any of your files.

Use permanent active protection: permanent protections constantly check all operations carried out in the computer that might be infected by a virus. If you possess a reliable permanent protection such as that included in **Panda Antivirus 6.0**, the risk of infection is minimal and work with your computer is greatly facilitated, as you no longer have to remember to scan everything you receive. Your permanent protection takes care of it automatically.

Periodic scanning: scan your entire computer periodically. With **Panda Antivirus 6.0** it is easy to carry out periodic scans at times when you are not working with the computer. This type of periodic scanning will prevent any virus that has entered your computer from spreading too far. It is best to scan the whole system at least once a week, although this will depend on how much you use your computer.

Keep up-to-date: given the number of new viruses that are detected every month – some 300 – it is essential that you have an update service to keep your antivirus up-to-date. Otherwise your computer will be at the mercy of the new, dangerous viruses that continuously appear.

Clean boot disk: to prevent future problems, always keep a virus-free boot disk at hand. This will make it easier to clean your computer in case it becomes contaminated by a virus. Although you can create this disk yourself, the **Safedisk** utility shipped with **Panda Antivirus 6.0** creates several disks. The first of these is a boot disk, whereas the others are used for disinfection purposes. These disks constitute an essential tool when it comes to ridding a computer of viruses.

Boot and Emergency Disks (Safedisk Process)

The **Safedisk** process permits you to create several disks that will make it possible to boot, scan and disinfect a computer in a virus-free environment. When we speak of a virus-free environment, we refer to a computer that has no viruses permanently lodged in memory that could interfere with the scanning and disinfection procedures.

Panda Antivirus 6.0 incorporates a utility called **Safedisk**, whose mission it is to automatically create boot and emergency disks. **Safedisk** creates a disk that allows you to boot the computer in such a way that you are assured that no virus will be loaded during the startup process (providing the floppy disk used is virus-free), as well as other disks that allow you to scan and disinfect the computer using the command-line version of our antivirus (PAVCL).

It is essential that the **Safedisk** utility be run on a virus-free machine, as this is the only way to guarantee that the disks that are created are also free from the effects of viruses. Otherwise, the disks you create would be of no use, as they would not guarantee the virus-free booting of the computer.

To create these disks, proceed as follows:

1. Run the **Safedisk** utility. You will be offered this possibility during the **Panda Antivirus 6.0** setup process, although you will also be able to do so at a later stage through the corresponding menu option in **Panda Antivirus 6.0**.
2. The first **Safedisk** window informs you of the purpose of this utility. You should have several empty 3½ inch high-density floppy disks ready so that **Safedisk** can create the boot and disinfection disks. If you wish, you can exit the program through the **Cancel** button.
3. If you choose to continue, the first of the floppy disks will be formatted and **Safedisk** will then begin to copy the files that are needed to convert it into a boot disk.
4. When **Safedisk** has finished creating the first disk (boot disk), you will be asked to insert disk number 2 (first Emergency disk).
5. The disk will be formatted and **Safedisk** will begin to copy the necessary **Pavcl** files.
6. You will then be asked to insert another floppy disk (second Emergency disk).
7. The floppy will be formatted and **Safedisk** will continue to copy the necessary **Pavcl** files.
8. When the entire process has finished, a window will appear featuring a number of recommendations. Write-protect the disks you have created. This way, you will prevent them from being accidentally deleted or infected should they be used on an infected computer. Then, label them accordingly (Safedisk1 for the boot disk and Safedisk 2 and Safedisk 3 for Emergency disks 2 and 3) for future reference and store them in a safe place.
9. Lastly, click **Finish** to exit the **Safedisk** utility.
10. Remember that to scan in a clean environment, you should first boot the computer with a boot disk and then insert the first Emergency disk (Safedisk 2). You can then run **Pavcl**. By using the following command, all the drives on your computer will be scanned in search of viruses and all those found will be disinfected: **`PAVCL /ALL /CLV`**.

The term Emergency Disks refers to the 3½ inch floppy disks created to enable you to scan and disinfect your system through the command-line version of our antivirus, PAVCL. You should understand the difference between the Boot Disk and the Emergency Disks. While the former enables you to boot the system from the disk drive, the latter disks allow you to scan and disinfect your computer using the command-line antivirus, PAVCL.

The Emergency Disks are provided with the **Panda Antivirus 6.0 Platinum** and **Home Edition** programs, although you will also be able to create them during the antivirus setup process (Installing Panda Antivirus 6.0). You are recommended to carry out this process in order to create all the aforementioned disks (both Boot and Emergency). The Boot Disk does not form part of the **Panda Antivirus 6.0 Platinum/Home Edition** packages, which means that users will have to create it manually or through the **Safedisk** process.

After creating these disks, remember to label them accordingly, write-protect them by adjusting the disk tab and store them in a safe place.

The first disk created is a boot (system) disk and contains the following files: AUTOEXEC.BAT, MSDOS.SYS, KEYBOARD.SYS, IO.SYS, HIMEM.SYS, CONFIG.SYS, DRVSPACE.BIN, KEYB.COM, FORMAT.COM, EDIT.COM, DOSKEY.COM, COMMAND.COM, SMARTDRV.EXE, REGEDIT.EXE and FDISK.EXE.

The second disk (the first emergency disk) contains the following files: COMMAND.COM, PANDA.CHP, PAVCL.EXE (the command-line version of the antivirus), PAVCL.MSG and PAVCLSD.BAT.

The third disk (the second emergency disk) created during this process contains the following files: GLOBAL.MSG and PAVSIG.CMP

Characteristics of Panda Antivirus 6.0

The following are some of the characteristics of **Panda Antivirus 6.0**.

Centralized management: in order to guarantee maximum protection, various scan types are necessary. Some of them are for providing permanent protection and others for protecting new entryways for viruses such as e-mail or Internet. **Panda Antivirus 6.0** incorporates all sorts of scans for protection against any eventuality, but comes with an interesting new feature: centralized management. All the scans (including permanent protection) are managed from a single program. This makes it easier for the user to handle and provides a greater level of security.

Two operating modes: ease of use is one of the most highly-appreciated characteristics of a program. However, difficulties often arise with respect to power and the program's potential as flexibility and the fact that the program offers many options generally complicate its operation, especially for less experienced users. With this in mind, **Panda Antivirus 6.0 Platinum** offers two operating modes: advanced and basic (depending on the version used). Both offer the same protection against viruses. The difference between them is that the basic mode offers the greatest possible ease of use in performing scans, whereas the advanced mode offers everything that an antivirus product can offer without neglecting ease of handling.

Report: all operations carried out by the antivirus as well as incidents detected can be logged in a report for subsequent consultation. The degree of detail included in the report can be configured (only available in advanced mode for the **Panda Antivirus 6.0 Platinum** version). All the information is kept between different sessions of the antivirus so that the data can be consulted whenever necessary.

Warnings: a complete warning system warns of the presence of a virus detected in the computer via the network (if connected to one) or by sending an e-mail message. Only available in advanced mode for the **Panda Antivirus 6.0 Platinum** version.

Updates: the antivirus updates itself either via CD-ROM or diskettes or through the Internet. In addition, updates can be scheduled to take place periodically without user intervention.

Predetermined scans: predetermined scans are one of the most important characteristics of **Panda Antivirus 6.0**. These predefined scans allow for scanning at the touch of a single button. All you need to do is choose the scan you want from the list of predefined scans and click the **Scan** button.

Scanning from the File Explorer: by offering a high degree of integration with the operating system, **Panda Antivirus 6.0** allows you to carry out immediate scans from the Windows File Explorer at the touch of a button and without previously having to open the antivirus. Through the Windows Explorer you can select any file you wish. By right-clicking on the file(s) you can call up a contextual menu, in which the **Panda Antivirus** option is displayed. This option enables you to scan the file(s) in question in search of viruses.

Integration with the Maintenance Wizard: the Maintenance Wizard is one of the new characteristics of Windows 98. **Panda Antivirus 6.0** integrates with the wizard to facilitate the execution of the antivirus at the most convenient times.

Note: some options are only available depending on the product purchased and the configuration of the operating system. For further information, consult Differences between versions

Detection of a virus: what to do

Any of the various scans that are possible in **Panda Antivirus 6.0** are capable of detecting viruses and act accordingly. Disinfection is one of the possible actions. There is no specific section for disinfection in the program as this is considered as just another action that can be taken upon the detection of a virus.

Panda Antivirus 6.0 respects and maintains the information in files and in e-mails as it allows for disinfection in both cases. Other antiviruses limit themselves to deleting any infected e-mail messages that are detected. In the same way that this is not considered acceptable in the case of files, it should not be done with e-mail messages. By disinfecting infected files attached to an e-mail message, **Panda Antivirus 6.0** respects the information it contains and saves the effort of requesting that the message be sent again, this time free of infection. This total protection of information is possible thanks to the fact that **Panda Antivirus 6.0** is also capable of detecting and disinfecting viruses in e-mail messages that are sent, not just in those that are received.

In addition, it is important to note that the disinfection of an infected file attached to an e-mail message is carried out in memory, since such disinfection should not be carried out on the hard drive because of possible interference from other antiviruses or even from another program. Not all antiviruses carry out disinfection with the guarantee of non-interference from other programs.

Through the Windows Explorer you can select any file you wish. By right-clicking on the file(s) you can call up a contextual menu, in which the **Panda Antivirus** option is displayed? This option enables you to scan the file(s) in question in search of viruses.

- **Show information on the virus:** will display detailed information on the virus without taking any further action.
- **Ignore and continue scanning:** no action will be carried out and the scan will continue normally.
- **Disinfect automatically:** will disinfect the infected file returning it to its original condition.
- **Rename the infected file:** will rename the infected file by changing its extension.
- **Delete the infected file:** will delete the infected file.
- **Move the infected file:** will move the infected file to a specified location. This allows you to create a space to keep viruses ‘‘in quarantine’’.
- **Ask what action to take:** in the event of a virus being detected, the user will be prompted for the action to be taken (Move, Delete, Disinfect, Show Information or Rename).
- **Block access to file:** after detection, this option makes it impossible to use the infected file.

Virus detected in memory

If you suspect there may be a virus in the memory, switch off the computer, insert a boot disk that you are sure is virus-free (if you are going to carry out the disinfection from CD-ROM, the diskette should load the CD drivers), and reset the computer.

If you used the **Safedisk** program during installation or at any other time, use disk number 1 generated by this utility as a boot disk. Disk number 2 contains our command-line version of the antivirus, **Pavcl**.

Once you have started, run our command-line antivirus (PAVCL) as follows:

- If you want to run **Pavcl** from a floppy disk, insert the first **Panda Antivirus** for DOS/Windows 3.x emergency disk (the second floppy disk created by **Safedisk** - not the boot disk) and enter the following:

  ```
  PAVCL /ALL /CLV /AEX /AUT
  ```

  If a message is displayed requesting that the disk containing the PAVSIG.CMP file be inserted, insert the last (# 3) of the floppy disks, as the file in question is saved here (for more information, consult the **Boot and Emergency Disks** section).

- If you wish to execute **Pavcl** from our CD-ROM, insert it in the drive, go to the DOSWIN3X directory and the desired language and enter the following:

  ```
  PAVCL /ALL /CLV /AEX /AUT
  ```

The above-mentioned command will carry out a scan of all system drives searching for viruses in all files and trying to disinfect all viruses found without requesting user intervention. **Pavcl** is the command-line version of **Panda Antivirus 6.0** and detects and removes the same viruses as any version of **Panda Antivirus 6.0**.

Virus detected in a file

If you have detected a virus in one or more files, proceed as follows:

1. Go to **Immediate scan** (if you have **Panda Antivirus 6.0 Platinum**, it is recommended that you select Advanced mode).
2. Choose the predetermined scan **Hard disk scan**.
3. Click on the **Configure** button in the toolbar.
4. Within the **Scan** section, enable the **Compressed files**, **E-mail files** and **Generate report** options. Choose **All Files**.
5. In the **If a virus is found** section (within the **Actions** tab if you have **Panda Antivirus 6.0 Platinum** installed and are in Advanced mode), unfold the list and choose **Disinfect automatically**.
6. Only if **Panda Antivirus 6.0 Platinum** is installed (and you are in Advanced mode) make sure that in the **Exclusions** section there are no exclusions specified to be sure that all files on all hard drives are scanned.
7. Accept the changes made in the scan configuration window.
8. Press the **Scan** button on the standard button bar.

The above-mentioned procedure will scan and disinfect all the files on your hard drives leaving the system free of viruses, Once the process has concluded, a report will be displayed featuring information on the viruses detected and the files they were found in.

Virus detected in the boot

To disinfect a boot virus, several floppy disks will be necessary: one boot disk to guarantee virus-free system startups, and others for disinfection purposes.

It is possible to create a boot disk using the **Safedisk** utility included with **Panda Antivirus 6.0** or using the procedure described below.

The **Safedisk** tool will create several floppy disks. The first of these is a boot disk, whereas the others are used for disinfection purposes. Otherwise, you have all the necessary tools for disinfection in the DOSWIN3X directory on the **Panda Antivirus 6.0** CD-ROM.

The procedure is as follows:

1. Switch off your computer. Insert a virus-free boot disk (if you are going to carry out disinfection from the CD-ROM, the diskette should load the CD drivers), and reset your computer.
2. Once you have started the computer, Insert the first disk. If you are going to carry out disinfection from the CD, insert the **Panda Antivirus 6.0** CD-ROM and go to the DOSWIN3X directory.
3. Then execute our command-line antivirus (PAVCL) by typing the following: **`PAVCL /ALL /CLV /AEX`**. If you are asked to insert the disk containing the PAVSIG.CMP file, insert the last of the floppy disks shipped with **Panda Antivirus** or which you generated through the **Safedisk** utility.
4. If a virus is detected in memory once, you should continue. When the virus is found on the hard drive, press **S** to disinfect.

Creating a boot disk without using the Safedisk process

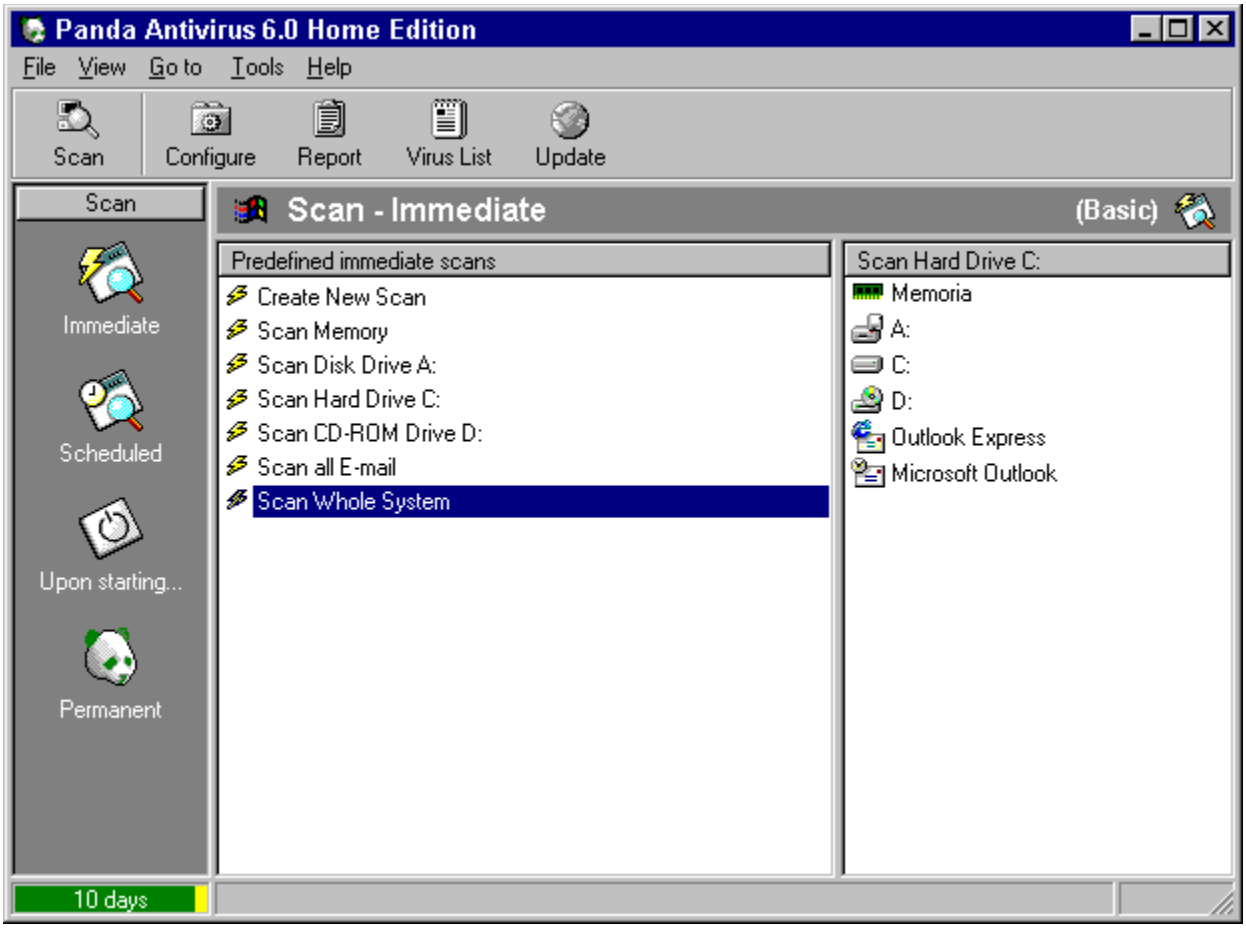
To generate a virus-free boot disk, it is necessary for such a disk to be created on a virus-free computer. The **Safedisk** utility is designed to create both a boot disk and emergency disks, which can be used for disinfection purposes.

If you created the above-mentioned diskettes with the **Safedisk** utility before virus infection, use the first diskette as the boot disk. If you did not already create these disks, go to a virus-free computer and follow these steps:

1. Insert an empty disk and type **`FORMAT A: /S`**.
2. Go to the DOS directory using the command **`CD DOS`**.
3. Copy the HIMEM.SYS and SMARTDRV.EXE files on the diskette by typing **`COPY HIMEM.SYS A:`** followed by **`COPY SMARTDRV.EXE A:`**.
4. Edit the CONFIG.SYS file in drive A using the following command: **`EDIT A:\CONFIG.SYS`**.
5. On the editor that appears, type the following two lines: **`DEVICE=HIMEM.SYS`** and **`DOS=HIGH`**.
6. Choose the **Save** option in the **File** menu then the **Exit** option in the same menu..
7. Edit the AUTOEXEC.BAT file in drive A using the following command: **`EDIT A:\AUTOEXEC.BAT`**.
8. On the editor that appears, type the following line: **`SMARTDRV.EXE`**.
9. Choose the **Save** option in the **File** then the **Exit** option within the same menu.

Immediate scan (Basic)

Two mouse clicks are all that are needed to run an immediate scan in basic mode. The function of this scan is to guarantee maximum security with minimum complexity of use.



Basically, running an immediate scan in basic mode consists of selecting one of the predetermined scans and clicking on the **Scan** button. When a predetermined scan is selected, the areas to be scanned will be shown so that the user will know exactly what the scan consists of.

It is also possible to select one or more areas of the items to be scanned section and click on the **Scan** button to immediately start a scan of the chosen areas.

For more information on any aspect of an immediate scan, click on one of the following subjects:

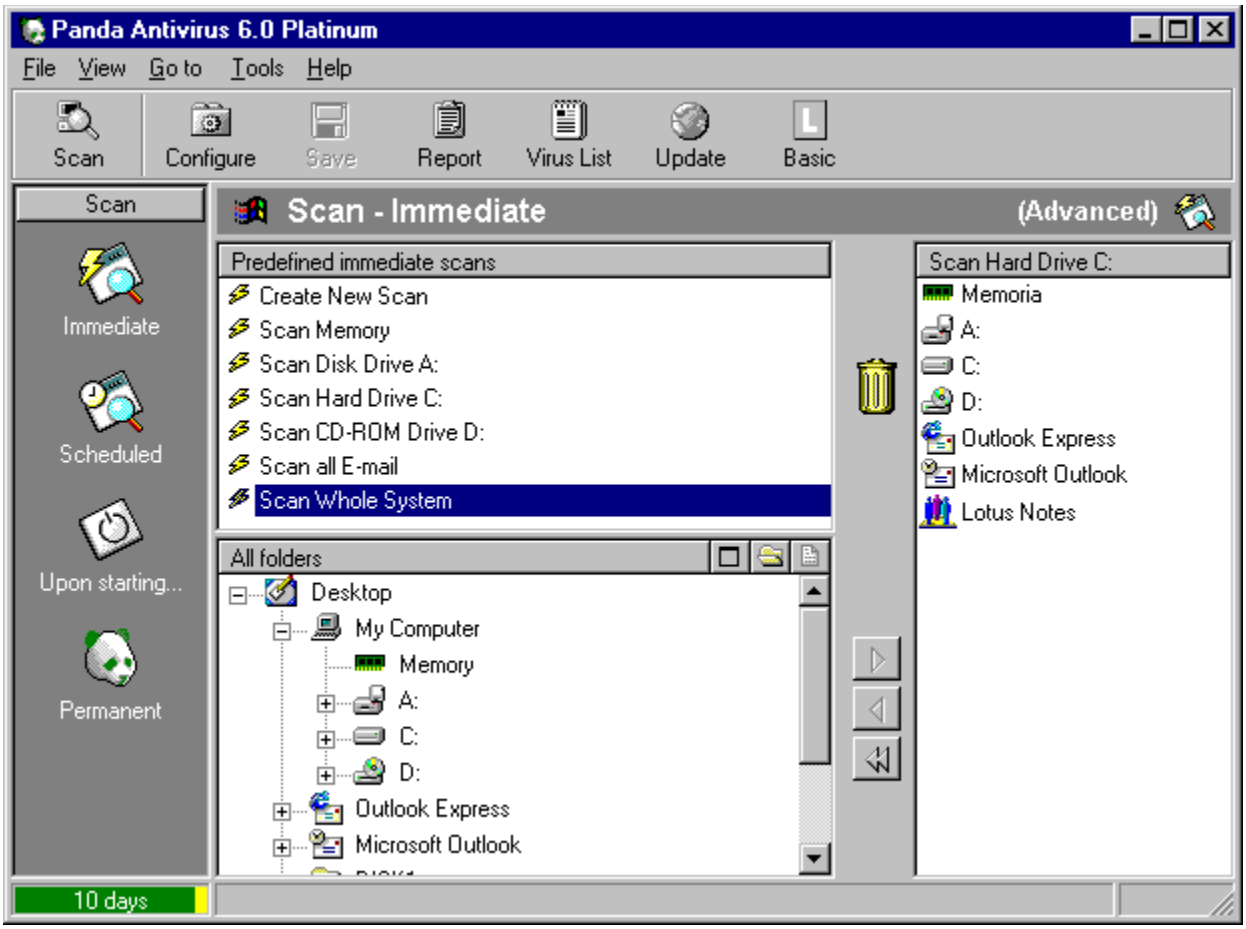
How to perform an immediate scan.
Scan areas in an immediate scan.
Immediate scan options.
Predetermined immediate scans.

Scanning from the File Explorer.

Immediate scan (Advanced)

Note: certain options are only available depending on the product purchased and the operating system configuration. For more information, see Differences between versions.

Immediate scans are a fundamental part of **Panda Antivirus 6.0 Platinum**. These permit you to scan any area of the computer (memory, hard drive, floppy drives, network drives, etc.) at any given time.



To scan even more quickly and easily, you can select one or several areas in the items to be scanned section, then click on the **Scan** button to start an immediate scan of the selected areas.

In the advanced mode, immediate scans can be totally configured. Areas and scan options are user selectable. In keeping with the **Panda Antivirus 6.0 Platinum** motto of maximum security with minimum complexity of use, a series of predetermined scans are available in advanced mode immediate scans which facilitate the scanning process.

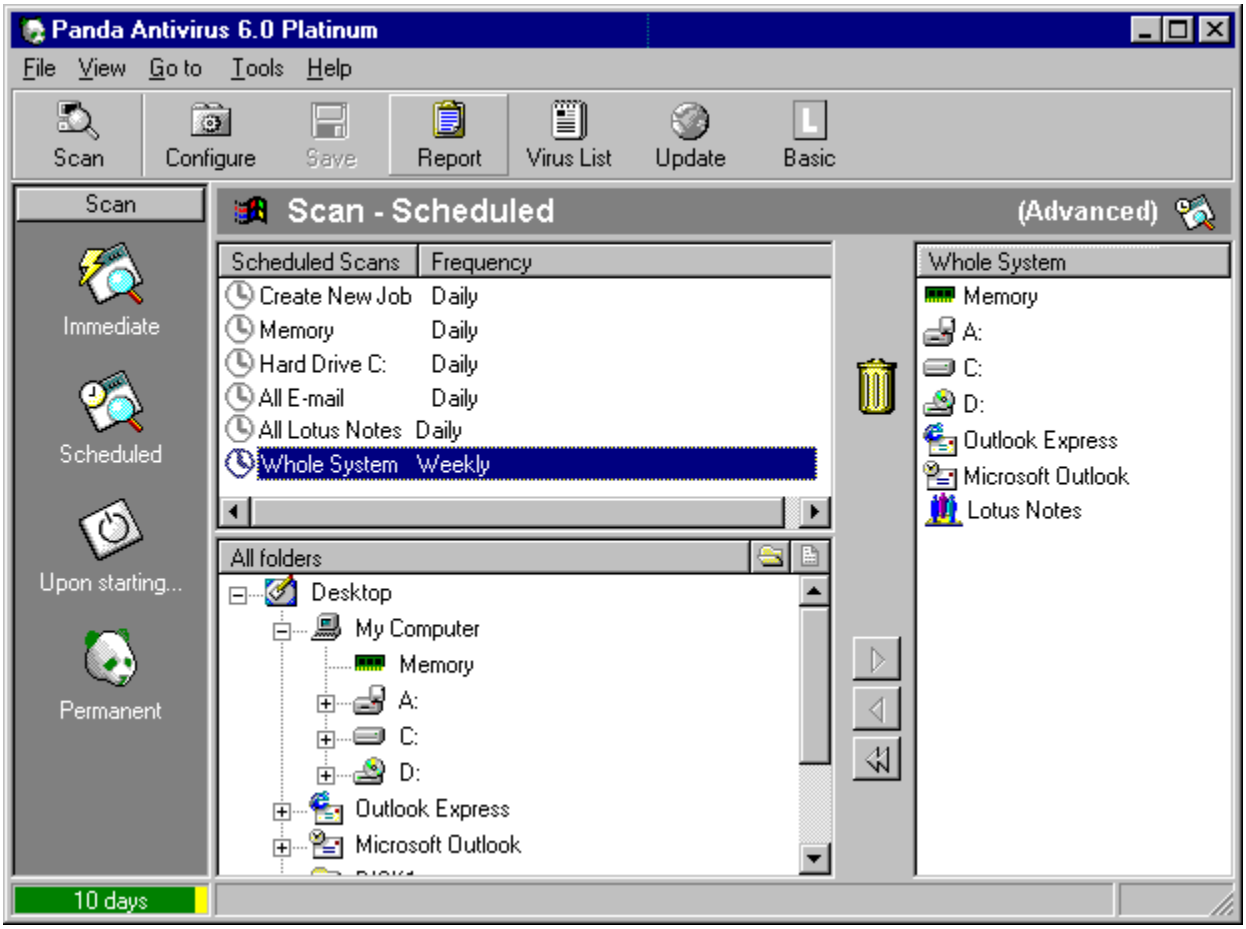
The configuration possibilities, as well as the capacity to create new predetermined scans that will be available both in the advanced and basic modes, are the strengths of the advanced mode. These newly-created predetermined scans are saved and available to be used until removed by the user.

For more detailed information on each of the above-mentioned points, click on the following subjects:

Scheduled scan (Advanced)

Note: certain options are only available depending on the product purchased and the operating system configuration. For more information, see Differences between versions.

Scheduled scans are immediate scans that are performed periodically in accordance with a determined schedule. Therefore, scheduled scans function in the same way as immediate scans. A series of predetermined scans offering maximum simplicity in program handling is also available for scheduled scans.



To set up a scheduled scan, just enable any of the predetermined scheduled scans provided. Any number of these scans may be enabled simultaneously, and in the advanced mode new scheduled scans may be created.

In the advanced mode, the following may be selected for each scheduled scan defined: areas to be scanned, scan options to be included, and the frequency with which the scans will be performed.

For more information on the above-mentioned aspects of the program, click on any of the following subjects:

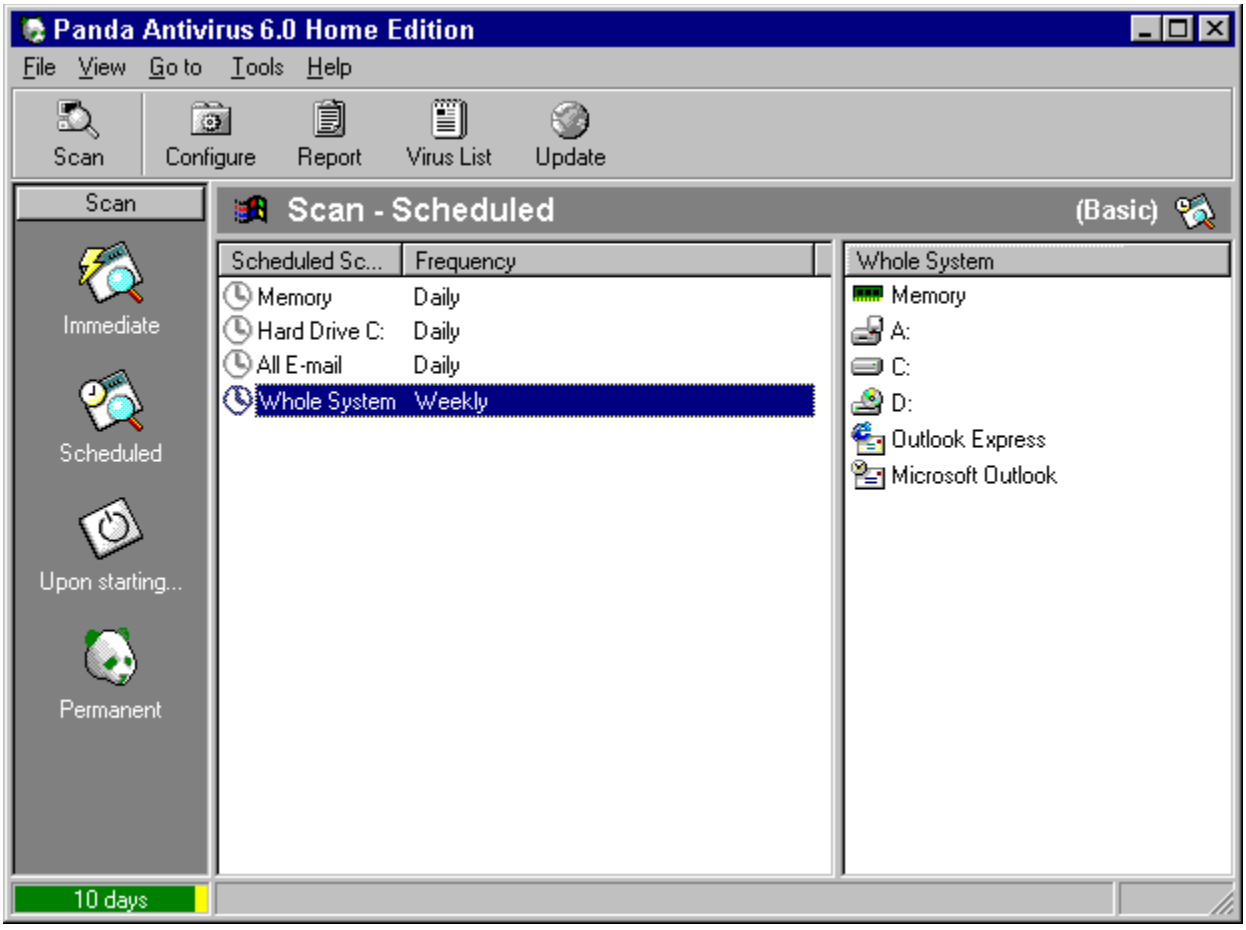
How to perform a scheduled scan.
Scan areas in a scheduled scan.

Scheduled scan options.
Predetermined scans in a scheduled scan.

Maintenance Wizard.

Scheduled scan (Basic)

Scheduled scans are immediate scans which are carried out periodically in accordance with a determined schedule.



Therefore, scheduled scans work in the same way as immediate scans. A series of predetermined scans offering maximum simplicity in program handling is also available for scheduled scans.

To set up a scheduled scan, just enable any of the predetermined scheduled scans provided. You may activate as many as you wish.

For more information on the above-mentioned aspects, click on any of the following subjects.

How to perform a scheduled scan.
Scan areas in a scheduled scan.
Scheduled scan options.
Predetermined scans in a scheduled scan.

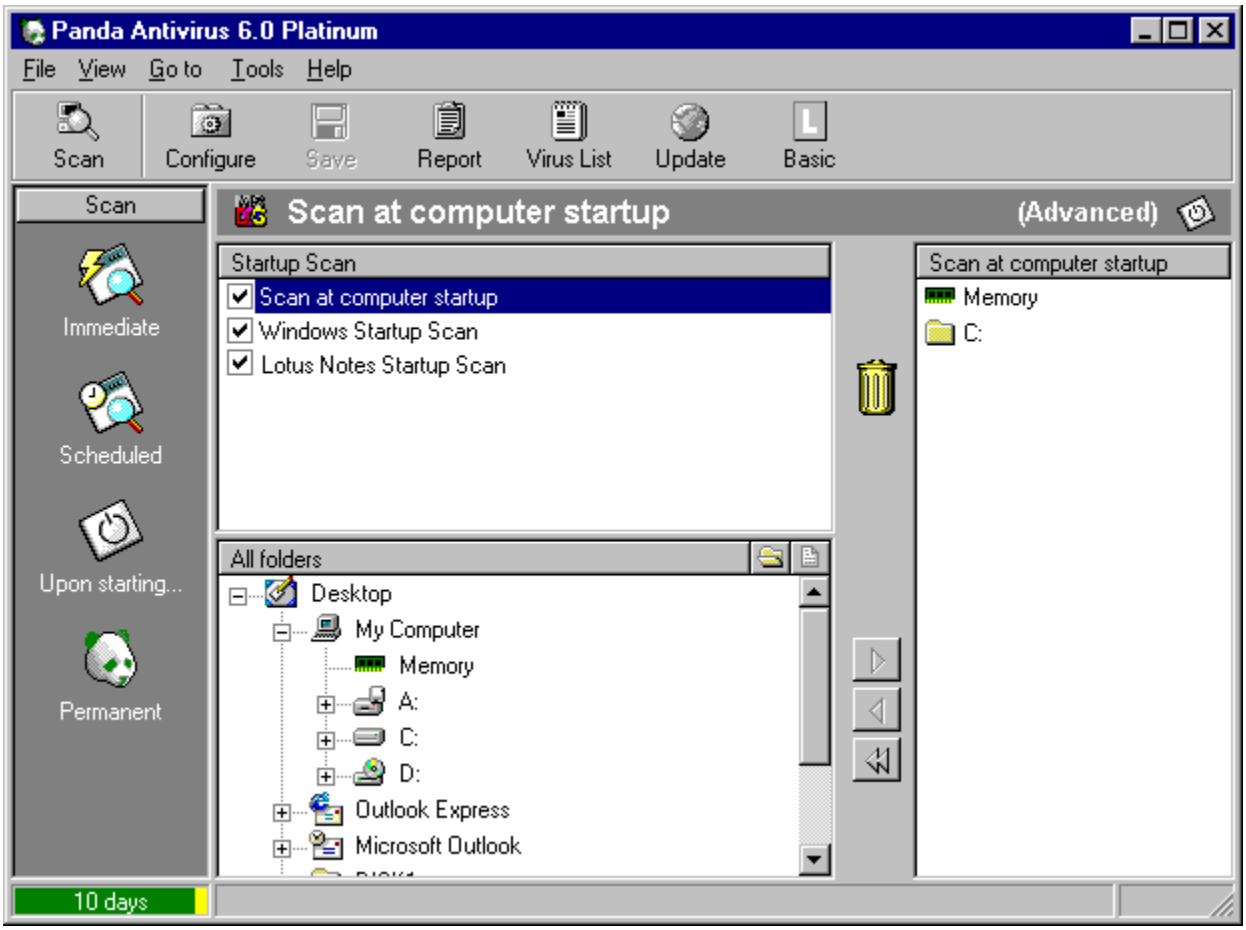
Maintenance Wizard.

Computer startup scan (Advanced)

Note: certain options are only available depending on the product purchased and the operating system configuration. For more information, see Differences between versions.

A startup scan is a scan that is carried out when the computer is booted. The advantage of this type of scan is that it allows the user to scan the most important files on the hard drive as well as in memory, and the boot sector before the computer finishes the booting process. In this way any possible virus is detected at the earliest possible occasion.

> **Note:** you cannot choose to automatically carry out a Startup Scan in the Windows NT antivirus version.



In the advanced mode, the user is able to configure the startup scan with two important options: the ability to add additional areas to be scanned at computer startup and the possibility to program the scan so that it is run at certain times.

Since the startup scan is run each time the computer is booted up, it is preferable not to scan very large areas as that will slow down the booting process.

> Scheduling the computer startup scan permits you to configure the scan with greater precision. This way, maximum protection can be combined with complete efficiency by performing the scan only at

certain times.

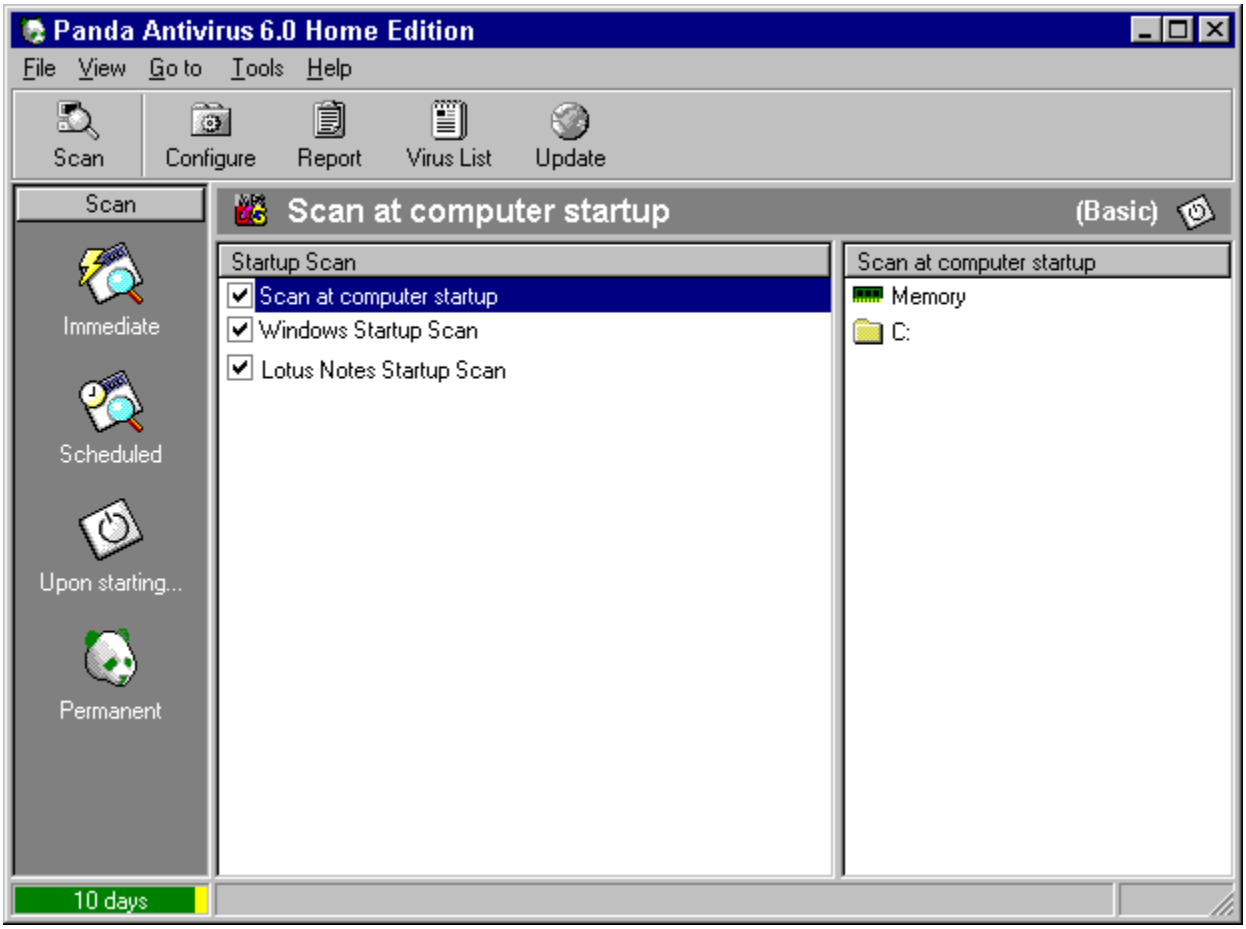
Click on any of the following options for more information on the subjects referred to above.

How to enable the startup scan.
Startup scan options.
How to disable the startup scan.

Computer startup scan (Basic)

A startup scan is a scan that is carried out when the computer is booted. The advantage of this type of scan is that it allows the user to scan the most important files on the hard drive as well as in memory and the boot sector before the computer finishes the booting process. In this way any possible virus is detected at the earliest possible occasion.

Note: you cannot choose to automatically carry out a Startup Scan in the Windows NT antivirus version.



The startup scan therefore provides protection right from the time the computer is booted.

In basic mode you can specify whether or not you want to run this scan at computer startup. Information is also available on the areas that will be scanned when this option is selected.

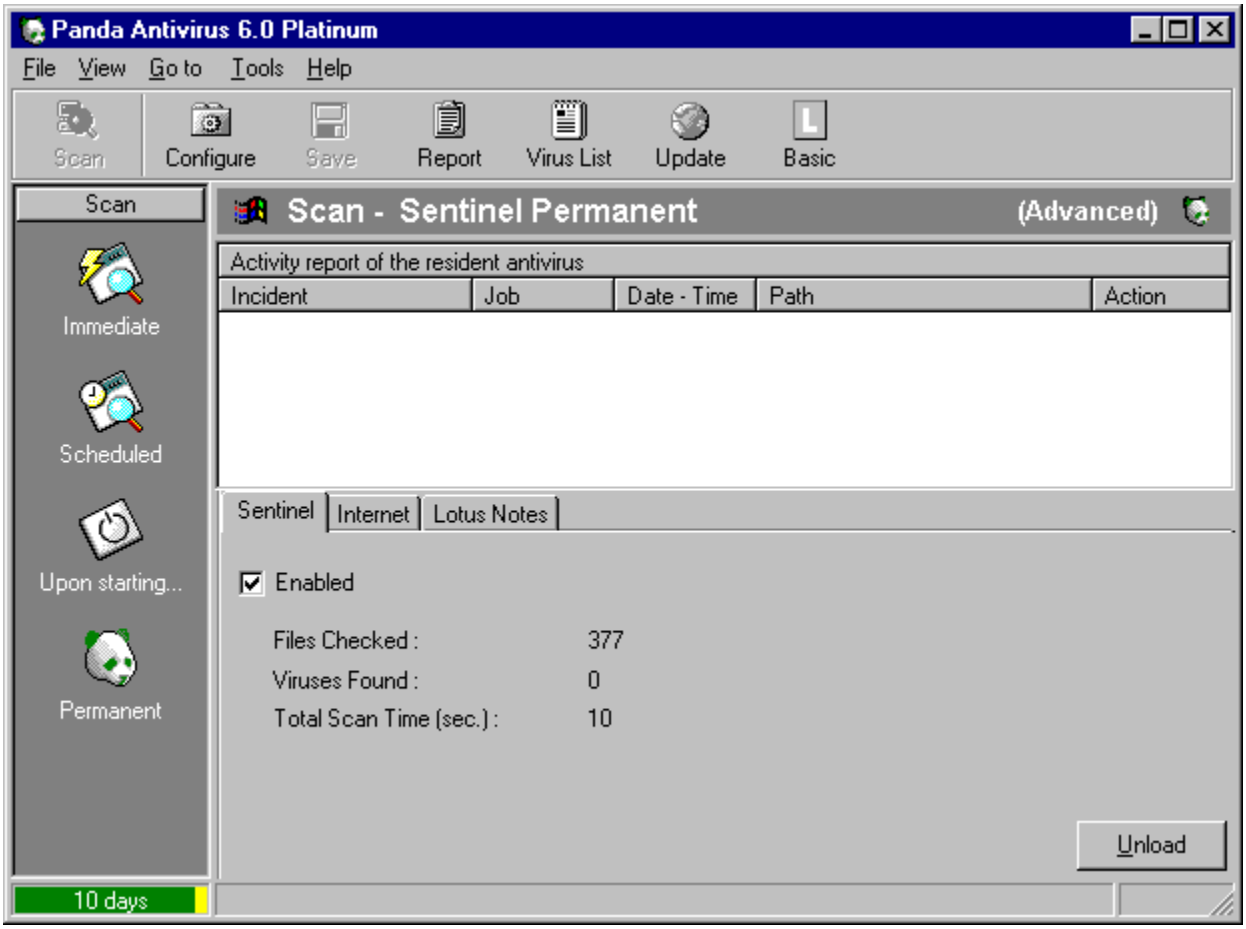
For more information on enabling or disabling the startup scan, the following subjects are available for consultation.

How to enable the computer startup scan.
Computer startup scan options.
How to disable the computer startup scan.

Permanent File scan (Advanced)

Note: certain options are only available depending on the product purchased and the operating system configuration. For more information, see Differences between versions.

The permanent scan offers one of the most important functions of **Panda Antivirus 6.0 Platinum**: that of providing permanent protection against viruses. The permanent protection starts working as soon as the operating system is started up. From that moment on, its job is to monitor all operations carried out on the computer that may be susceptible to virus infection.



This way, the permanent scan ensures that your computer remains virus-free in a totally automatic way.

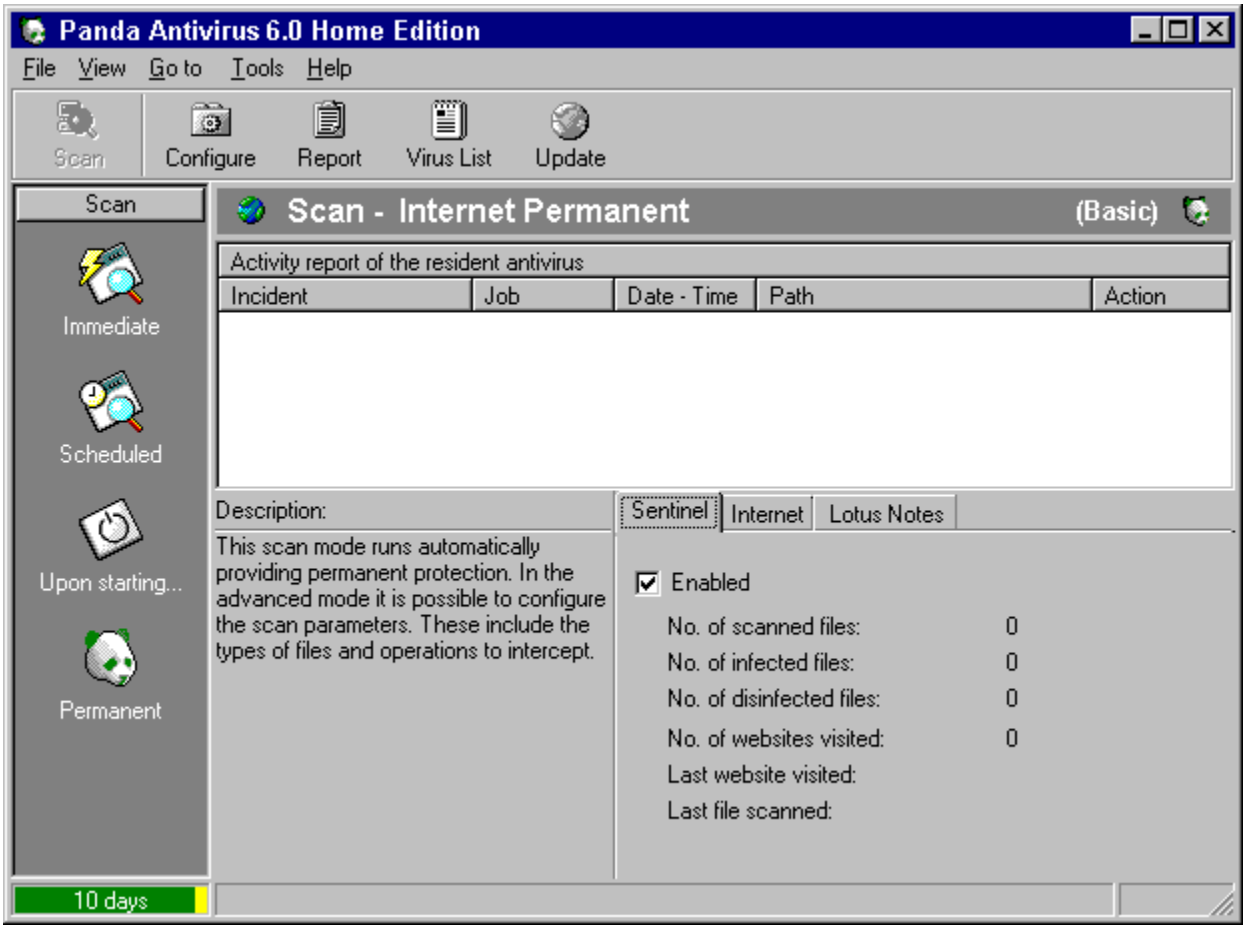
In the **permanent scan** section, you can see an activity report of the permanent scan, a summary of the number of files scanned and the number of viruses detected, as well as the possibility of enabling or disabling this type of scan.

In addition, in advanced mode you also have the possibility of configuring the permanent program scan to indicate the options with which you want to perform the scan, and the option of unloading the permanent scan.

For more information on these subjects, see the following sections.

Permanent File scan (Basic)

The permanent scan offers one of the most important functions of **Panda Antivirus 6.0**: that of providing permanent protection against viruses. The permanent protection starts working as soon as the operating system is started up. From that moment on, its job is to monitor all operations carried out on the computer that may be susceptible to virus infection.



This way, the permanent scan ensures that your computer remains virus-free in a totally automatic way.

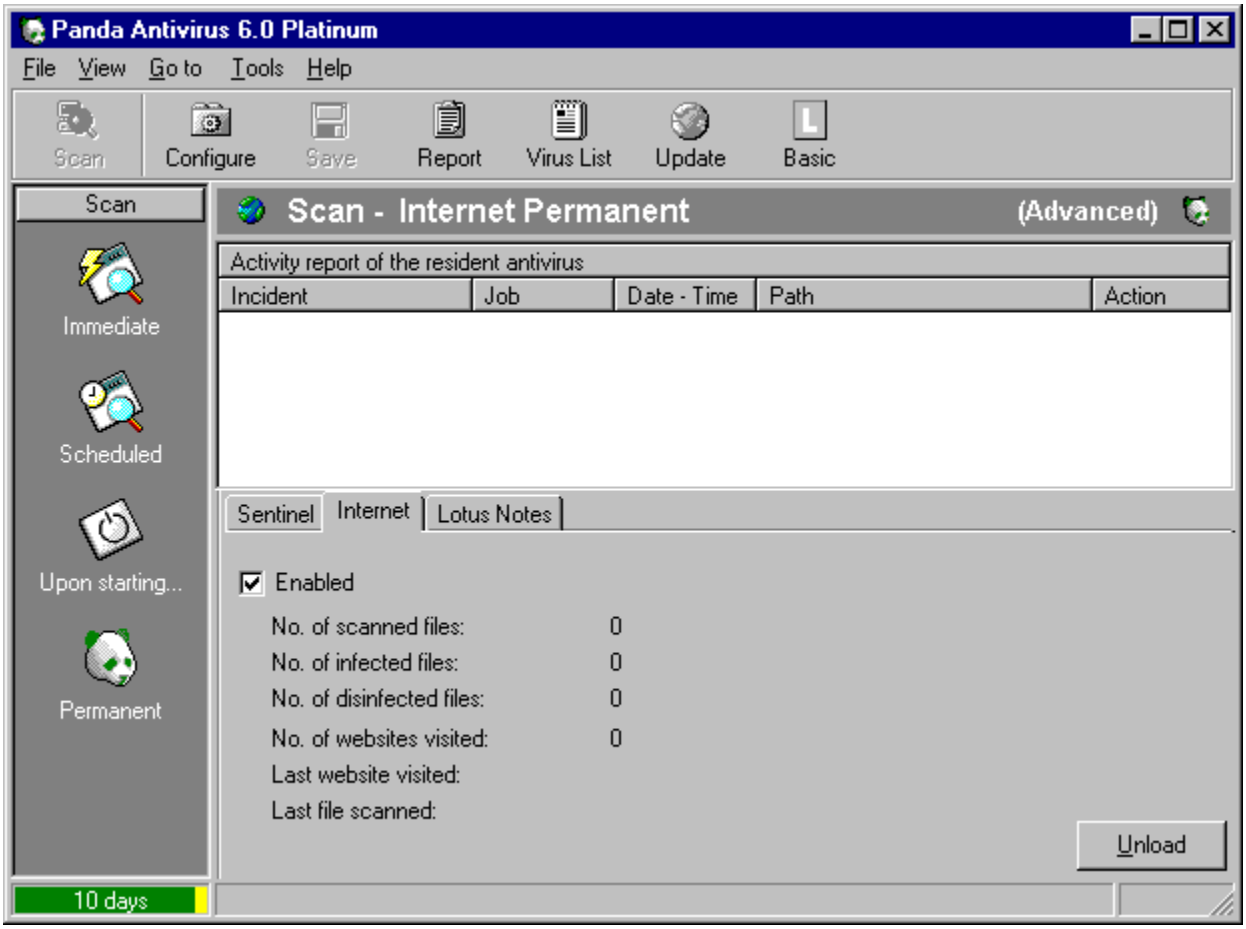
In the **permanent scan** section you can see an activity report of this scan, as well as a brief summary of the files scanned and the possible viruses found. This scan can be easily enabled or disabled. For more information, please consult the following subjects.

How to enable the permanent scan.
Permanent scan options.
How to disable the permanent scan.

Permanent Internet scan (Advanced)

Note: certain options are only available depending on the product purchased and the operating system configuration. For more information, see Differences between versions

The Internet scan offers a singular function: permanent protection against viruses that can come in through the Internet. This permanent protection against Internet viruses starts working from the startup of the operating system. From that moment on, the scan is responsible for monitoring all Internet related operations carried out on the computer.



This way, by means of a totally automatic process, the Internet scan takes care of keeping your computer free from viruses originating from the Internet.

In the **Internet scan** section you can see an activity report of this scan, as well as a brief summary of the files scanned and the possible viruses found. This scan can be easily enabled or disabled.

In addition, in advanced mode you also have the possibility of configuring the Internet scan to indicate the options with which you want to perform the scan, and the option of unloading the Internet scan.

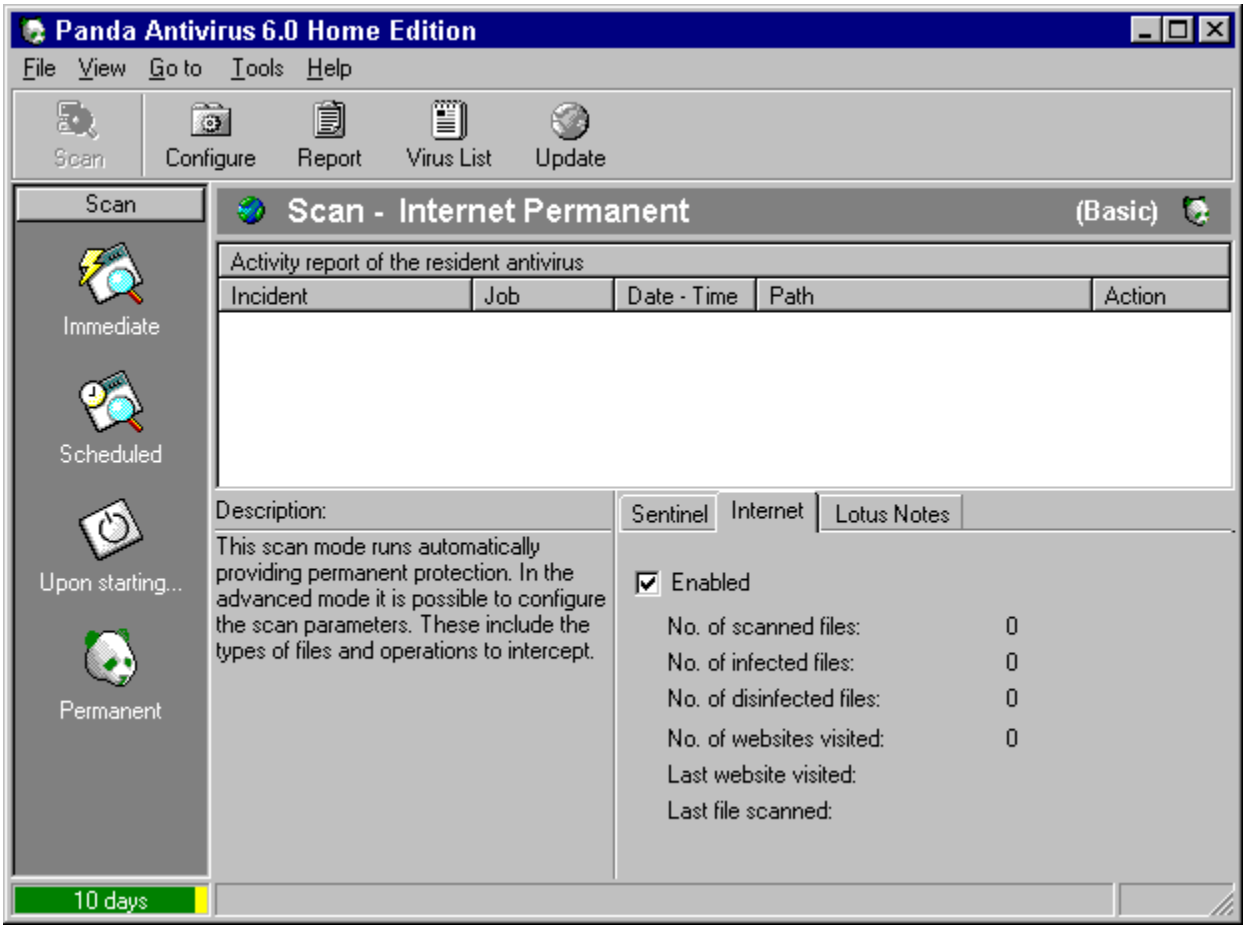
For more information on these subjects, see the following sections.

How to enable the Internet permanent scan.

How to configure the Internet permanent scan.
How to disable the Internet permanent scan.

Permanent Internet scan (Basic)

The Internet scan offers a singular function: permanent protection against viruses that can come in through the Internet. This permanent protection against Internet viruses starts working from the startup of the operating system. From that moment on, the scan is responsible for monitoring all Internet related operations carried out on the computer.



This way, by means of a totally automatic process, the Internet scan takes care of keeping your computer free from viruses originating from the Internet.

In the **Internet scan** section you can see an activity report of this scan, as well as a brief summary of the files scanned and the possible viruses found. This scan can be easily enabled or disabled.

For more information on these subjects, please consult the following sections.

How to enable the Internet scan.
Internet scan options.
How to disable the Internet scan.

Uninstalling Panda Antivirus 6.0

To uninstall **Panda Antivirus 6.0** (**Home Edition** or **Platinum**), go to **Control Panel**, select the **Add/Remove programs** option and choose **Panda Antivirus 6.0** (**Home Edition** or **Platinum**) from the list. Click on the **Add/Remove** button. The software will be uninstalled in a matter of moments. Uninstallation should never be attempted by deleting the version from the directory in which it was installed. Always follow the described procedure to uninstall the antivirus.

Boot viruses

What is the boot sector?

The boot sector is a very important area of a diskette or hard disk, as it contains information on the type of disk in question. In addition, this sector contains a program that is run when the computer is started up, and whose function is to determine if there is an operating system present and if there is, to execute it.

Therefore, when a computer is booted up, it first tries to load the program located in the boot sector, so that it executes the operating system. Once the operating system is run, the computer is said to be booted up and the user can begin to work with it.

What does a boot virus infect?

A boot virus infects the program located in the boot sector. This way, the virus is loaded each time the computer is started up, whether from a diskette or the hard disk.

It is important to keep in mind that there are viruses that belong to several categories, and which are therefore capable of infecting both boot sectors and files.

How can a computer be infected by a boot virus?

In order to become infected with a boot virus, you must start or try to start up the computer from an infected diskette. It is very important to note that, although a disk may NOT be a boot disk, it can still produce a boot virus infection since the attempt to boot up the computer alone is enough to produce the infection.

How does a boot virus “work”?

When you boot or attempt to boot your computer from an infected diskette, what actually happens is that the virus is executed. The virus then reserves a space in the computer’s memory and “installs” itself there. Once in place, the virus runs the original boot-sector program. This way, everything appears as normal and the user remains unaware of the presence of the virus.

From this moment on, all access to a hard disk or diskette will be intercepted by the virus. It will check to see whether the disk in question is infected or not, and if it is not, the virus will infect it. This means that if the computer was booted up or an attempt was made to boot it using an infected diskette, as soon as the hard disk is accessed it will be infected. Therefore, all subsequent boots performed from the hard disk will execute the virus, thus infecting more diskettes and ensuring the propagation of the virus.

How to prevent a boot virus infection

The best form of protection is to always have a properly updated antivirus installed. If a permanent protection system is in place and you scan every diskette prior to use, it will be very difficult for a boot virus to enter your computer.

There exists a very simple method of providing an additional guarantee against accidentally booting up a computer with a diskette unknowingly left in the disk drive. It consists of placing the boot sequence in the BIOS in such a way that the computer always attempts to boot first from the hard drive and then from the disk drive.

File viruses

What does a file virus infect?

As its name indicates, a file virus infects files contained on any physical support that is not write-protected. A file virus can therefore infect files on a diskette or an entire hard drive.

It is important to keep in mind that there are viruses that belong to several categories, and which are therefore capable of infecting both boot sectors and files.

How can a computer be infected by a file virus?

A file virus is ‘‘contracted’’ by executing a previously infected file. Therefore, viruses normally only infect executable files. Macro viruses are an exception to this rule as they infect non-executable files such as documents.

How does a file virus “work”?

The file virus works in a much wider variety of ways than a boot sector virus.

Permanent file viruses: first of all, these viruses check that the necessary conditions are in place for them to ‘‘attack’’. If that is the case, the virus will trigger its destructive action. If the conditions are not right, the virus reserves a space in the computer’s memory and continues the normal execution of the file so that its presence goes unnoticed. From that point on, all operations involving files will be intercepted by the virus, which will infect all files not previously infected.

Direct-action file viruses: these viruses also check that the necessary conditions exist for them to carry out their destructive action. If that is not the case, the virus will then infect new files. The virus generally infects files in the current directory and directories referenced by the PATH variable. Lastly, the virus continues with the normal execution of the file so that its presence remains undetected. As we have already seen, these viruses do not remain in memory but instead infect at the time they are executed.

Companion viruses: these viruses may be permanent or direct-action. What differentiates them from the others is that the companion viruses take advantage of a peculiarity of the MS-DOS operating system. In this system, if two files are named identically but with different extensions, namely COM and EXE, the file with the COM extension will be executed first. For this reason, a companion virus does not infect an EXE file, but creates a COM file containing the virus (with the stealth attribute to conceal its presence). Each attempt to run the EXE file actually executes the COM file first. The virus is thus free to carry out its work, and only then is the EXE file executed so that the virus presence is not detected.

Overwrite viruses: in all the above-mentioned cases, the virus infects files without changing any of their original contents. It simply limits itself to adding data. Overwrite viruses, however, infect files by partially writing over the information contained within. The results are twofold: infected files can no longer function correctly and they cannot be disinfected since part of the original data has been lost.

How to protect yourself against file viruses

First and foremost, it is very important to always have a permanent protection enabled. The function of a permanent protection is to monitor all operating system operations involving files in order to scan the ones to be used.

With a good permanent protection you can be sure of being protected against file viruses. In addition,

several measures are strongly recommended. They are as follows:

- Scan all incoming files prior to using them, regardless of how you receive them: via diskette, network, e-mail, Internet, etc.
- Use only software that is original and from a reliable source.
- Scan the hard drive periodically to make sure that no virus has managed to infect it.

It is always absolutely essential to have an adequately updated antivirus installed.

Macro viruses

What does a macro virus infect?

Since a virus is nothing more than a program, for it to do anything it must be loaded by the operating system. This is the reason why viruses only infect executable files. No matter how much a virus infects a text file, as this file is not executable, the virus can never take over control of the computer and therefore cannot be activated.

Macro viruses have changed all that. The ever growing capacity of some applications such as word processors, spreadsheets, etc. have led their developers to incorporate an interesting function: macros. A macro is a sequence of instructions that the program in question (word processor or spreadsheet, for example) can interpret and execute.

Therefore, If virus code is introduced into one of these macros, this code will be executed by the program, thereby giving the virus access to the control of the computer.

What this means is that files handled by such programs (documents, spreadsheets, etc.) are capable of containing viruses and infecting other similar files.

An additional risk from this type of virus is that, given their character, they are run "inside" a program. This means that if the program in question is multiplatform (that is, it can be run on different operating systems), then the virus will also be multiplatform, thus increasing the range of files it can infect.

How does a macro virus infect?

Macro viruses take advantage of a normal characteristic of programs in which macros are used. The MS-Word program presents a clear example of this. This program basically handles two file types: documents and templates. Templates are used to define generic documents and so simplify work with documents, as it is then not always necessary to start from the very beginning with similar documents.

In MS-Word, it is the templates that can contain macros. The problem lies in the fact that, by default, all documents are based on a template called NORMAL.DOT. This template contains a macro which is executed automatically as soon as it is opened.

Virus creators take advantage of this characteristic. By infecting the macro that is executed automatically, the propagation of the virus is ensured, as it will infect every document that is opened.

How does a macro virus work?

As explained above, viral macros are executed and infect all documents opened. It is then the documents that take up the job of transmitting the "infection".

One of the most dangerous characteristics of macro viruses is their great speed of propagation. For example, an infected document on a company network to which different people have access, can infect all of the company's documents in an extremely short space of time.

As this type of file is exchanged very frequently by electronic mail, these viruses can spread to anywhere in the world at astonishing speeds.

It is important to note that, although they are not generally believed to be harmful, these viruses can

cause a lot of damage, as much as that caused by any boot or file virus.

How to protect yourself against macro viruses

The best defense against a macro virus is to have a permanent protection system installed. This way, each time an attempt is made to open an infected document, the permanent protection warns the user and cancels the operation, eliminating all risk of infection.

Given the ease with which this type of virus can spread by e-mail, it is also recommended to install an antivirus capable of scanning incoming e-mail upon reception prior to opening the message.

Techniques used by viruses

To avoid detection by antiviruses, virus creators have developed a series of specialized and complex techniques. Antiviruses have had to adapt to these new techniques in order to detect these increasingly complex and perfected viruses.

The following are some of the most common techniques used by viruses:

Stealth: this is a technique used by permanent file viruses. The infection of a file makes it necessary to modify the original file. It is therefore possible to see that a virus has manipulated the file. To avoid this, permanent viruses can be made to monitor all operations designed to obtain virus information and intercept them. It then presents pre-infection data in the place of virus detection information. This way, the infection goes undetected.

Tunneling: viruses and antiviruses work using similar techniques. Viruses intercept all operating system operations involving files in order to infect all files accessed. On the other hand, permanent antivirus protection systems also intercept file operations in order to verify that the files being accessed are not infected. Using the tunneling technique, a virus is capable of finding the services intercepted by the permanent protection and use them directly without the permanent protection being aware of it.

Self-encryption: the main goal of a virus is to replicate. Antiviruses detect infections by searching for a particular string (also called signature) which is identical in all of the copies of a virus. To avoid detection by this virus search mechanism (the most common type), some viruses are able to encrypt themselves to change each time they infect a file. This way, the virus never replicates in exactly the same way, and the traditional detection method fails. However, the encryption routine used is always the same and can therefore be used by antiviruses to detect this type of virus.

Polymorphism: in this case, not only do viruses encrypt themselves in a different way for each infection, but they also change the encryption routine. This way, there are no identical copies of one virus as all of its parts differ. To detect this type of virus, decryption simulation techniques are used, which force the virus to ‘‘show itself’’.

Scanning from the File Explorer

Panda Antivirus 6.0 becomes an integral part of the operating system on which it is installed. This makes the handling of the antivirus even easier.

To be precise, **Panda Antivirus 6.0** offers the possibility of starting a virus scan from the Windows File Explorer.

To start a scan from the File Explorer, proceed as follows:

1. Select the area or areas to be scanned. Any area in the File Explorer may be selected.
2. Right-click any part of the selection. In the contextual menu that appears, choose the **Panda Antivirus** option.
3. Once you have done this, the same scan progress window that appears when a **Panda Antivirus 6.0** immediate scan is run will appear on the screen.

Scanning from the File Explorer facilitates the use of the antivirus as it permits you to scan the desired areas without even having to open the antivirus.

Maintenance Wizard

The **Maintenance Wizard** is a new feature available with Windows 98. With this feature periodical maintenance jobs are carried out automatically, freeing the user from having to carry out these jobs manually. The **Maintenance Wizard** is accessed by clicking on the *Start* button in Windows and then selecting the following options in this order: *Programs - Accessories - System Tools - **Maintenance Wizard***.

With **Panda Antivirus 6.0**, scheduled scans can be created to accomplish the same objective. However, in order to offer maximum integration with the operating system, **Panda Antivirus 6.0** also offers the possibility of integration with the **Maintenance Wizard.**

The **Maintenance Wizard** starts by offering the possibility of executing all jobs active at that moment or configuring the defined jobs. If you choose to execute jobs, the one corresponding to **Panda Antivirus 6.0** will be executed first. Subsequently, all other active jobs defined in the **Maintenance Wizard** will be executed.

If you decide to configure the different **Maintenance Wizard** jobs, the option to configure the **Panda Antivirus 6.0** task will be presented first. The configuration options are as follows:

- **Search for viruses regularly:** this option permits you to enable the job.
- **Mornings - 00:00 to 03:00:** if this option is checked, the job will start at midnight every day.
- **Days - 12:00 to 15:00:** if this option is checked, the job will start at 12 noon every day.
- **Afternoons - 20:00 to 23:00:** if this option is checked, the job will start at 8 p.m. every day.
- **Customized - Uses the current configuration:** if this option is checked, the defined frequency will be used.
- **Reprogram:** by clicking on this button a window is displayed allowing you to specify the times for starting an automatic scan job.
- **No, do not search for viruses:** this option disables the job.

Note: some options are only available depending on the product purchased and the operating system configuration. For more information, see Differences between versions

Options: e-mail (Internet - Advanced)

Note: certain options are only available depending on the product purchased and the operating system configuration. For more information, see Differences between versions

This section includes the e-mail scan options.

Scan
Incoming messages: indicates that all incoming e-mail (messages received) will be scanned.
Outgoing messages: indicates that all outgoing e-mail (messages sent) will be scanned.
Compressed files: indicates that all compressed files associated with a message will be scanned.

Nested messages: indicates that all messages found inside other messages will be scanned.

Generate results: if this option is checked, all data relative to the scan in question will be logged in the report.

All files: if this option is selected, all files regardless of their extension will be scanned.

Only Program files: if this option is selected, only files with EXE or COM extensions will be scanned.

Only my extensions: this option permits you to indicate that all files with extensions indicated on a list are to be scanned. This list can be accessed by means of the **Extensions** button.

MIME

MIME is a file-coding format for sending files. Through this option you can instruct the antivirus to scan all MIME files associated with any message. For more flexibility, the types of MIME files to be scanned or not may be indicated. This also permits you to speed up the process as it avoids the scanning of large image or video files. The types of message files that will be scanned may be any of the following: **Applications**, **Images**, **Video**, **Audio**, **Text**, **HTML** and **Others**.

Options: Internet (Internet - Advanced)

Note: certain options are only available depending on the product purchased and the operating system configuration. For more information, see Differences between versions

Included in this section are the scan options for contents downloaded from the Internet.

Scan
Enabled: this enables the scanning of files received from the Internet (Web pages, file transferring, e-mail, newsgroups).
Compressed files: indicates that all compressed files included in data sent or received via Internet will be scanned.

Save results: if this option is checked, all data relative to the scan in question will be logged in the report.

All files: if this option is selected, all files regardless of their extension will be scanned.

Only program files: if this option is selected, only files with EXE or COM extensions will be scanned.

Only my extensions: this option indicates that only the files with extensions indicated on a list are to be scanned. This list can be accessed using the **Extensions** button.

Additional protection

ActiveX Controls: if this option is checked, all *ActiveX Controls* found in Web pages accessed will be scanned for viruses.

Java Applets: when this option is checked, all *Java Applets* found in Web pages visited will be scanned.

Options: actions (Internet - Advanced)

Note: certain options are only available depending on the product purchased and the operating system configuration. For more information, see Differences between versions

In this section you can specify the action to be taken by the antivirus when a virus is found. Depending on the action chosen, a series of options for configuring the selected option will appear on screen. The different possibilities are as follows:

Ignore and continue scanning

This instructs the antivirus not to take any action when a virus is detected. Scanning will continue as usual.

Disinfect automatically

Through this option you can instruct the antivirus to automatically disinfect all infected files found. This option may be configured, as there will be times when disinfection will not be possible. The configuration options are the following:

Delete the file: when disinfection is not possible and this option is checked, the infected file will be deleted.

Move the file: with this option, a file which cannot be disinfected will be moved to another location. To complete this option, you can specify the destination infected files will be moved to.

Move the file – **path:** permits you to indicate the directory to which infected files will be copied.

Move the file – **E-mail:** permits you to indicate the e-mail address to which an infected file is to be sent.

Delete the infected file

By indicating this option, all infected files found will be deleted.

Move the infected file

If this option is checked, all infected files found will be moved.

Move the infected file – **path:** used to indicate the directory to which infected files will be copied.

Move the infected file – **e-mail address:** used to indicate the e-mail address to which an infected file is to be sent.

Ask what action to take

This option indicates that the antivirus should ask what action is to be taken each time a virus is detected. This permits you to indicate different actions during a single scan. In order to make the configuration more flexible, the options that will be displayed when a virus is detected may also be chosen.

Move: refers to the **Move** action described above.

Delete: refers to the **Delete** action described above.

Disinfect: refers to the **Disinfect** action described above.

Show information: refers to the **Show information** action described above.

Rename: refers to the **Rename** action described above.

Options: ports (Internet - Advanced)

Note: certain options are only available depending on the product purchased and the operating system configuration. For more information, see Differences between versions

This section permits you to indicate the ports through which communications will be made.

Ports
SMTP: permits you to indicate the port for outgoing mail communication (messages sent).
POP3: permits you to indicate the port for incoming mail communication (messages received).
FTP: permits you to indicate the port through which file transfers will be made.
HTTP: permits you to indicate the port through which World Wide Web HTML pages will be received.
NNTP: permits you to indicate the port through which News will be received.

Virus entry points

For several years now, the trend is towards more connectivity between computers. More and more each day, the computer is less of an isolated item with only one input point. Although this has been beneficial for users and PC's in general, it has also multiplied the number of available entry points for viruses.

For these reasons, it is important to know which are the entry points that a virus can use to access a computer, and understand how an antivirus must protect all entry points.

In addition to having multiplied the possible entry points for viruses, new types of viruses and new forms of transmitting these viruses have also appeared.

Last but not least, the importance of monitoring all outgoing items must be stressed. This is not usually taken into consideration, since it is considered that "there is no entry of viruses". It should not be forgotten, however, that most infections occur without malicious intentions. Thus, a user may send an infected file or diskette without realizing that he is also sending a virus. If every user carefully monitors their outgoing messages as well as the incoming ones, the rapid diffusion of viruses as occurs today could be avoided. A user who sends a virus could find him/herself in trouble under such circumstances.

Diskettes and CD-ROMs

In the past, these were the only entry points to a PC (if it was not connected to a network). Viruses can be carried in files that are saved on either of these two mediums or can reside in the boot sector of a diskette. Given that both mediums can contain files susceptible of having a macro virus, the three most common types of viruses (boot, file and macro) may enter a computer by these mediums.

The **Panda Software** response to this entry point is two-fold. On one hand, it contains a permanent program that offers permanent protection. This way, all access to any file contained on diskette or CD-ROM will trigger a permanent protection scan. And, on the other hand, it offers the possibility of carrying out an immediate scan (on-demand scan) of the diskette or CD-ROM inserted in the computer to verify that it is virus-free.

Therefore, with adequate permanent protection, an antivirus can efficiently resolve the danger that this entry point poses.

Network

This entry point has been around for a long time, but has become very wide spread in the last few years. Today, in almost all stations where there are several computers, there is a network that connects them. The basic objective of a network is the sharing of information and thus the sharing of files. Since many types of files are shared on a network, this medium can be a point of transmission of file and macro viruses.

The **Panda Software** response to this entry point is also two-fold. On one hand, the key protection is still via a permanent program offering permanent protection. It is the same one that monitors the access to files mentioned above. Each time that a user tries to send or receive an infected file on the network, the permanent program will scan the file and display a warning. As in the previous case, this response also offers the possibility of carrying out an immediate scan (on-demand scan) to check any drive on the network. However, given the shared character of a network, new files can be added constantly making it difficult to ensure that a network station is virus-free.

As with the previous case, and even more importantly, having adequate permanent protection is the best guarantee of protection against viruses for this entry point.

Internet

Although Internet has existed for years, it has only recently become a massive means of communication. It is more and more present every day in every field. The primary function of Internet is to facilitate, and in many cases make possible, the exchange of information. Thus, Internet also facilitates the exchange of files which, as already stated, are a "vehicle" for transmitting viruses. However, Internet presents a situation slightly more complicated than a network for the following reasons:

Internet provides different services, including for example: Web pages, electronic mail, etc. Each of these services uses a particular protocol (language); thus it is necessary to know these languages in order to correctly perform virus scans of this entry point. For example, an e-mail message may contain an attached file that is infected. Since the file is not in its normal format, a conventional antivirus cannot detect it. For this reason, an antivirus must be specially developed to understand the format used to receive e-mail messages in order to detect the virus.

The following are entry points of viruses transmitted via Internet:

- **Electronic mail:** viruses may be hidden in files attached to e-mail messages. They can never be found in the e-mail message itself. In other words, an e-mail message that does not have an attachment or embedded object cannot contain a virus. It is important to note that two protocols are used for electronic mail on the Internet. One is **POP3**, used for incoming mail (messages received) and the other is **SMTP**, used for outgoing mail (messages sent).
- **News (NNTP):** through this service, you can access newsgroups being discussed or that are placed in certain servers for consultation and subsequent discussion. You can also subscribe in order to periodically receive e-mails containing the latest news, although these may be infected. You can scan all the news received from **Exchange/Outlook** and **Outlook Express**.
- **Downloading files (FTP):** files can be downloaded from the Internet using this service. These files may be virus-infected.
- **Web pages (HTTP):** principally, Web pages (HTML pages) are only text and graphics that do not present any virus threats. More and more, however, Web pages contain other components such as *Java applets* or *ActiveX controls*. These types of components can be virus-infected and affect a computer for the sole reason of having accessed a Web page.

To correct such a potentially serious problem, **Panda Software** offers a series of solutions. These are the following:

- **Electronic mail:** A *special* permanent program scans all outgoing messages (SMTP protocol) and incoming messages (POP3 protocol) for viruses. Thus, an e-mail message containing a virus-infected file cannot be sent or received. Other antiviruses scan only incoming mail. This is very dangerous since it is possible to send a virus, with all the consequences this can cause the sender. Electronic mail antivirus protection provided by **Panda Antivirus 6.0** is independent from the e-mail program being used, and operates with all types of such programs.

  There is an added danger with electronic mail. All outgoing and incoming messages are stored in a message database. The message database format is not recognized by conventional antiviruses, so a normal antivirus will not be able to scan all outgoing and incoming messages for viruses prior to the installation of the program. For some reason, they also cannot scan those messages that were not scanned at the time they were received. To solve this problem, **Panda Antivirus 6.0** is able to recognize the format of the message database of **Microsoft Outlook**

Express (including Internet Explorer 4), **Microsoft Exchange** and **Microsoft Outlook** programs. This way, **Panda Antivirus 6.0** allows the user to scan any message, any time he/she wishes from a message database, thus offering the guarantee of virus-free electronic mail.

- **News (NNTP):** all possibly-infected contents (related documents) located in a server that provides a news service will be scanned by the *special* permanent protector responsible for monitoring the connection with that server. This guarantees the safe consultation of information regardless of the news program used.

- **Downloading files (FTP):** a *special* permanent program, in charge of monitoring the Internet connection, will scan all FTP downloaded files. This prevents the downloading of an infected file. All files previously downloaded could be scanned with an antivirus file, thus avoiding the problem mentioned above with e-mail messages. The virus protection is independent from the FTP program being used.

- **Web pages (HTTP):** All Web page or HTML page contents (*Java applets, ActiveX, etc.*) that may be virus-infected will be scanned by a *special* permanent program in charge of monitoring the Internet connection. This guarantees secure Website browsal, regardless of the search engine used while visiting the Websites.

In summary, it can be said that **Panda Antivirus 6.0** offers the best protection against possible viruses coming in through the Internet. On one hand, all the data is scanned as it enters the computer, to verify that no virus is being carried with the message. On the other hand, it is possible to scan all electronic mail handled by the user, that is all incoming and outgoing messages, guaranteeing a virus-free connection to the Internet.

Why not all antiviruses are the same

When all is said and done, all antiviruses are frequently considered to be the same. Perhaps the most generalized idea is that the only difference between one antivirus and another is the number of viruses that each is capable of detecting.

However, this is not the case. The real difference between antiviruses is the protection that each one is able to provide. An antivirus must be able to provide the following:

- **Protection of all entry points:** the fundamental characteristic of an antivirus is the ability to protect all points through which a virus may infect a computer.
- **Constant updates:** for its own sake, an antivirus must be updated constantly since new viruses appear every day. Without a constant update service, an antivirus becomes obsolete and is no longer useful.
- **Technical Support:** unfortunately, the situations in which viruses are detected are usually the source of conflicts. At times, the virus is detected too late if the user does not have antivirus protection or has not kept it updated. Other times, the virus is detected on time, but the fear of the damage a virus can do causes the user great consternation. Finally, the third point for solving virus problems is having efficient technical support capable of responding to all virus-related problems. This support must be easily accessible around-the-clock in order to accomplish its goal: to help all those who, unfortunately, have encountered a virus.

Protection of all entry points

On this point, **Panda Antivirus 6.0** offers the following:

- **Permanent scan** by means of a permanent program of all files which are accessed by the computer. This is an automatic and simple way to avoid the entry of infected files into the computer. It also avoids all operations using infected files, which for one reason or another, are already in the computer. This permanent scan also protects the computer against all possible viruses transmitted through a network.
- **On-demand scan** (at any time) of any area of the computer. Using this scan, any area of the computer may be scanned for viruses. It may seem unnecessary if permanent protection is also provided, but that is not the case. If, for whatever reason, the computer is infected, there must be a simple way to completely disinfect the system. The permanent protection program does not allow this, given that it would have to try to access every infected file. The on-demand scan also allows the scanning of all network drives.
- **Permanent scan** of the contents coming in via Internet (in SMTP, POP3, HTTP, FTP and NNTP protocols). This means that all incoming and outgoing e-mail messages will be automatically scanned regardless of the e-mail program being used. All files downloaded using HTTP and FTP protocols, as well as *Java applets* and *ActiveX controls* that may arrive with the HTTP protocol will also be scanned. Also in these cases, the scan will be independent of the search engine or FTP program being used. Lastly, it should be mentioned that all data sent to or received from newsgroups will be scanned in search of viruses.
- **Permanent scan** of all e-mail messages received through the **Microsoft Outlook** and **Microsoft Exchange** programs. This feature is presented apart from the permanent scan of electronic mail received from Internet, due to the fact that these two programs can receive e-mail from an Exchange server using different protocols. However, **Panda Antivirus 6.0** is capable of carrying out permanent scans of all incoming or outgoing messages in these programs, regardless of the protocol.
- **On-demand scan** of any of the folders (where messages are stored) in the **Microsoft Outlook Express**, **Microsoft Exchange** and **Microsoft Outlook** programs. This allows you to scan all

messages received or sent, even if they are prior to the installation of the antivirus.

- **Permanent scan** of all elements that form a part of a **Lotus Notes** system. This way, you will always be protected against potentially infected files included in databases or attached to mail messages, etc. This is just one of the permanent scan options offered by **Panda Antivirus 6.0**.

Constant update

On this point, **Panda Antivirus 6.0** offers the following:

- **24-hour S.O.S. Virus service:** with this service, **Panda Software** promises to provide a solution within 24 hours to any new virus not detected by even our latest antivirus.
- **Daily updates via Internet:** everyday, an updated version of our file of virus-detected identifiers is available on Internet. This file is updated with new viruses every day.
- **A complete updated version of the antivirus via Internet:** a complete version of the antivirus updated monthly is also available via Internet.
- **Updates with home delivery:** a completely updated version of the antivirus is sent to your home regularly, depending on the service chosen.

Technical support

One of the fundamental services offered by **Panda Software** is the technical support. It features the following characteristics:

- Available 24 hours a day, 365 days a year. The user can call at any time (only if you have **Panda Antivirus 6.0 Platinum**, as **Panda Antivirus 6.0 Home Edition** only comes with on-line support via e-mail) and have a highly qualified technician on the other end of the line ready to solve any virus-related problem.
- The technical support service can be contacted by telephone (only if you have **Panda Antivirus 6.0 Platinum**, as **Panda Antivirus 6.0 Home Edition** only comes with on-line support via e-mail), fax, e-mail, regular mail, or through our Web page.

Note: the **12h S.O.S. Virus** and **Home-delivered Updates** services are available depending on the type of license purchased.

Where to find viruses

It is important to know where a virus can be ‘‘hidden". The first thing that must be clear is that in order to carry out its work of infecting, or totally or partially damaging computer data, a virus must be executed. Thus, viruses will only insert themselves in areas where they can be executed:

- **Executable files:** viruses insert themselves in executable files in order to be able to control the computer.
- **Documents of any program able to manage macros:** traditionally, non-executable files could not contain viruses (or at least there wasn't a reason for them to contain viruses), since a virus in a non-executable file cannot do any work. However, due to the latest technical advances, certain programs such as the Microsoft Office suite have endowed non-executable files such as documents or spreadsheets with *macros*. A macro is a combination of instructions that can be executed by a certain program. In other words, a Microsoft Word document can contain a combination of instructions that Word itself will run. This has widened the possibility for viruses to infect files, which, despite being non-executable, contain macros.
- **Files attached to e-mail messages:** any type of file (executable or not) may be attached to an e-mail message. All e-mail messages, together with their corresponding attached files, are usually stored in one file. Since the structure of this file is not standard, nor does it have to be known, an antivirus may see such a message base as just another file and not find any viruses contained in it.
- **Boot sector:** the boot sector is an area in a diskette or hard disk containing important information on the type of disk. The boot sector also stores a program that is run when the disk in question is used for booting. Given that the program stored in the boot sector is able to run itself, it is also susceptible to being infected by a virus. You must bear in mind that a boot sector virus is also executed if an attempt to boot the computer from a diskette is made, whether or not it is a boot disk.
- **Java Applets:** before, Internet pages, or Websites (HTML pages), could only contain text or graphics. This has changed with the need to be able to create more complicated Web pages. Today, Web pages can also contain small programs called *Java applets.* When a browser downloads a Web page with some of these small programs, it makes sure to execute them. It works in a similar way as a macro document. For this reason, *Java applets* are also susceptible to being infected by viruses.
- **ActiveX Controls:** ActiveX controls have the same function as *Java applets*. For this reason and given that they are also executable, they are susceptible to being infected by viruses.

Panda Antivirus 6.0 is capable of scanning for viruses in any of the areas mentioned above, thus offering the highest levels of protection.

If disinfection is not possible...

There could be cases where, despite having selected the disinfection option, a particular virus cannot be removed.

Of these, the most frequent is the detection of a file virus found in a compressed file. In order to disinfect this virus, the following steps are necessary:

1. Decompress the compressed file in an empty directory. There is no risk in doing this, even if one of the files in the compressed file is infected.
2. Scan the directory containing the decompressed files, checking the disinfection option.
3. With the first two steps, the infected file will be disinfected. If desired, the files may be compressed again to return them to their original state but without any virus-infected files.

Differences between versions

This Help file applies to 2 different products: **Panda Antivirus 6.0 Home Edition for Windows 95/98/NT WS 4.0** and **Panda Antivirus 6.0 Platinum for Windows 95/98/NT WS 4.0**.

Depending on the product installed on the user's computer, some of the listed features may not apply to the application being used.

In addition, some features of both products apply only to Windows 98 and therefore will only be available for that operating system.

Although both versions of the antivirus are equipped with excellent scanning and disinfection capacity, there is a difference between them as far as the operating mode and configuration possibilities are concerned and the services that ship with the product:

- **Panda Antivirus 6.0 Home Edition** this version allows you to work with and configure the antivirus in ***basic mode*** (but not in advanced mode), which makes it extremely easy to use. This makes it ideal for users with no special needs, who will have not have to worry about having to deal with complex technical configurations.

- **Panda Antivirus 6.0 Platinum** allows you to configure and work with the antivirus in ***basic*** and ***advanced modes***. This enables you to carry out any type of configuration, thereby enhancing the power of the antivirus.

	Pav. 6.0 Home Edition	**Pav. 6.0 Platinum**
Basic mode	**Yes**	**Yes**
Advanced mode	**No**	**Yes**
Internet scan	**Yes**	**Yes**
Electronic mail scan	**Yes**	**Yes**
Lotus Notes scan Windows 85/98 and Windows NT WS 4.0	**Yes**	**Yes**

For more information on the basic and advanced modes, we suggest you consult the section entitled Two modes: basic and advanced.

Note: the **12h S.O.S. Virus** and **Home-delivered Updates** services are available depending on the type of license purchased.

Antivirus configuration

The antivirus configuration section allows the user to centralize the configuration of its different operation options.

Using this section, a combination of general options, update options and e-mail profiles can be configured. In addition, the sounds presented by the antivirus and the access password for the program's options can also be configured.

For more information on any aspect of the antivirus configuration, consult the following topics:

Mail Profile
General
Update
Sounds
Password

Configuration: mail profile

Panda Antivirus 6.0 is capable of displaying folders that contain e-mail messages in the **Microsoft Exchange**, **Microsoft Outlook** and **Microsoft Outlook Express** programs, allowing them to be selected for scanning. Since both programs allow several profiles to be defined, each one with its own features, a section has been set up to configure which profile will be chosen by the antivirus.

Default profile

This option indicates that a default profile in accordance with the e-mail program (**Microsoft Exchange**, **Microsoft Outlook**, or **Microsoft Outlook Express**) will be opened.

Ask upon entering

This option causes the antivirus to ask for the profile that it must open by offering a list of all defined profiles in the e-mail program (**Microsoft Exchange**, **Microsoft Outlook** or **Microsoft Outlook Express**).

Specified profile

Thanks to this option, a specific profile can be indicated, so that the antivirus can always work with it.

Profile: if the user has chosen to always work with a specific profile, that profile can be indicated here.

Configuration: general

The section on general configuration allows the user to indicate which items among those listed below he/she wishes to present in the selection tree of items to be scanned. This option will affect those parts of the program having present possible scan areas.

CD-ROM drives
Indicates if CD-ROM drives should be displayed or hidden.

Network drives
Indicates whether or not network drives should be displayed.

Electronic mail folders
Indicates whether or not e-mail folders (**Microsoft Exchange**, **Microsoft Outlook** and/or **Microsoft Outlook Express**) should be shown.

Lotus Notes databases
Indicates that Lotus Notes databases should be shown as scannable areas in the diverse scans.

Report size
Since the report is kept in between different antivirus sessions, if it is never deleted, it may become excessively large after a certain amount of time. With this option, the user may control the size of the report so that it does not exceed a determined size.

Limit the report size to: allows the user to indicate the report size in kilobytes. When the indicated size is reached, the oldest incidents will be deleted in order to save the newer ones.

Boot Scanning
The Boot sectors of floppy disks that are left in the disk drive when the computer is restarted or turned off will automatically be scanned when this option is checked. If you do not want floppy disks to be scanned in these situations, just uncheck this box.

Note: some options are only available according to the specific product purchased and the configuration of your operating system. For more information, see Differences between versions

Configuration: updates

For more information, consult any of the following sections:

Different types of updates.
Updating the virus signature file (Intelligent Updates).
Upgrading the antivirus (Intelligent Upgrades).

Configuration: sounds

The purpose of the sound section is to allow the user to choose which antivirus incidents will be accompanied by sound schemes. A sound can be selected for each incident, which will be heard when the corresponding incident occurs. In addition, and to complete the functionality of this section, a button allows the user to hear each sound so that he can select the ones he desires.

The options are:

Select the sounds you wish to play in each case: the incidents shown in this list can be associated to a sound. This way, with each particular incident, the indicated sound will be heard. If the user wishes to associate a particular incident to a sound, the incident must then be checked. If he/she does not wish to make the association, the incident must be left unchecked.

Name: this is the name of the sound file that is to be associated to a particular incident.

Browse: this button displays the standard file selection window to facilitate the choice of the sound file to be associated to a particular incident.

Test: press this button to preview the chosen sound. This avoids having to provoke the incident associated to it in order to test the action.

Configuration: password

This section allows the user to protect the access to specific sections of the antivirus by means of a password. This guarantees that those sections will not be altered by anyone without permission.

Items to be protected

Shows the different sections of the antivirus that will be protected by a particular password.

Panda Antivirus: by ticking this checkbox, you can block the use of the **Panda Antivirus 6.0 Home Edition/Platinum** antivirus.

Scheduled: with the protection offered by this section, unauthorized manipulation of scheduled scans can be avoided.

Startup: startup scan protection avoids the making of any changes to the configuration or the disabling of this scan.

Permanent: by protecting this section, unauthorized changes to the configuration or even the disabling of the Permanent protection can be avoided.

Updates: access to this part of the antivirus can be blocked so that nobody alters necessary data inputs for updating.

Password

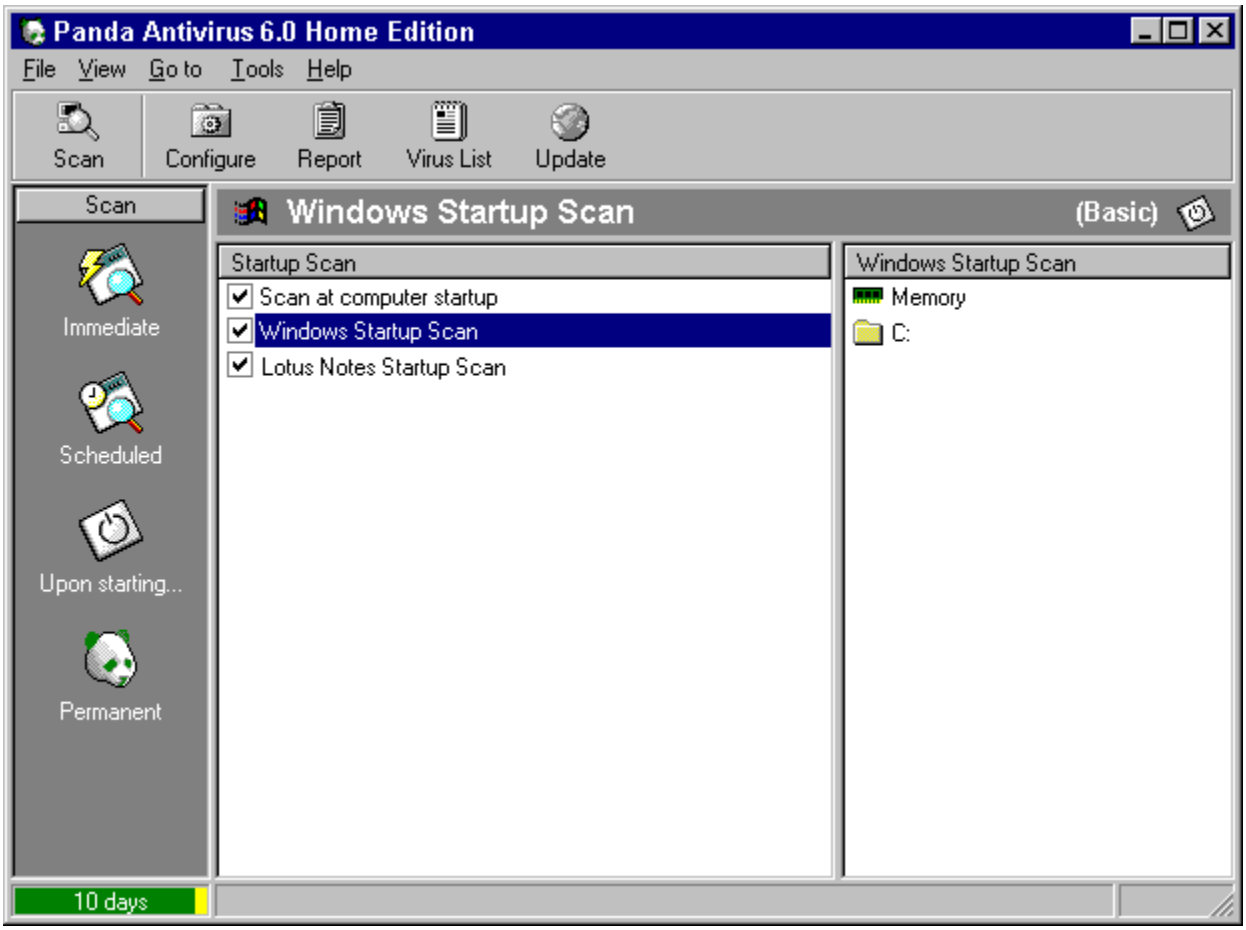
Allows the user to type in a password in order to protect those items that have been selected. A previously indicated password can also be changed.

Enter your password: a password chosen to protect the access to certain parts of the antivirus must be inserted here.

Change password: to change a password already introduced, select this option.

Windows Startup Scan (Basic)

A Windows startup scan is run during the booting of the Windows operating system. Thanks to this type of scan, it is possible to run a scan of any area of the computer as the first job after loading the operating system.



In basic mode, the user can indicate whether or not he wishes to run this Windows startup scan. Information is also available about the areas to be scanned with this option.

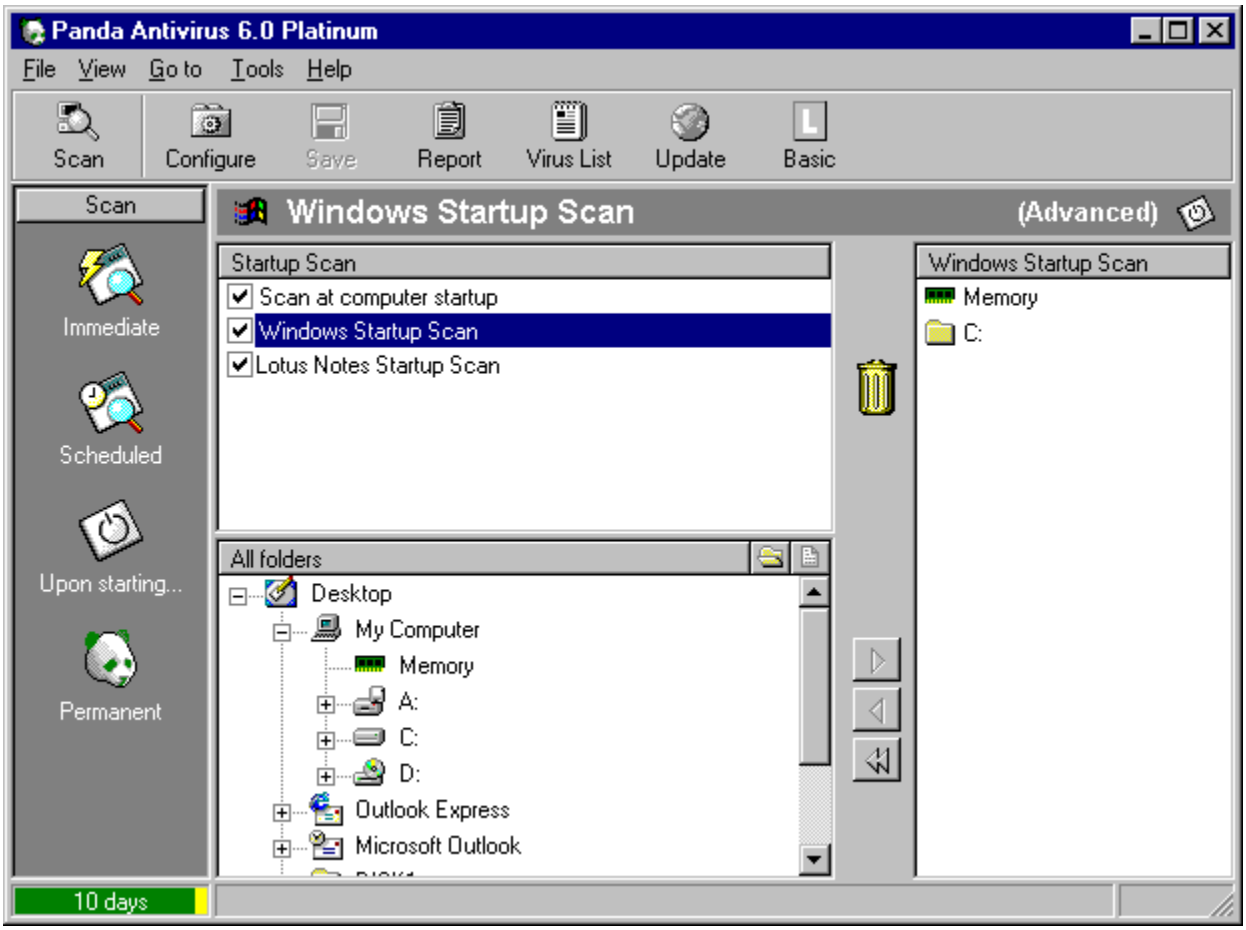
For more information on enabling or disabling the Windows startup scan, consult the following subjects:

How to enable the Windows startup scan.
Windows startup scan options.
How to disable the Windows startup scan.

Windows Startup Scan (Advanced)

Note: certain options are only available depending on the product purchased and the operating system configuration. For more information, see Differences between versions.

A Windows startup scan is a scan run during the booting of the Windows operating system. Thanks to this type of scan, it is possible to run a scan of any area of the computer as the first job after loading the operating system.



In the advanced mode, the Windows startup scan can be configured with two interesting options: the ability to add additional areas to be scanned when the computer starts, and the possibility to schedule the scan to be run only on determined occasions.

The scheduling of the Windows startup scan allows you to indicate if the mentioned scan should be run only when Windows starts after rebooting the computer or, on the contrary, if it should be run each time that Windows is started up (that is, at the beginning of each Windows session).

Since the Windows startup scan is run each time that the operating system is booted up, it is not convenient to scan very large areas.

More information is available on the above-mentioned subjects. Just click on any of the options below:

Options: scan (Startup - Advanced)

Note: certain options are only available depending on the product purchased and the operating system configuration. For more information, see Differences between versions.

There are several options grouped under this section for a maximum ease of use.

Scan

Compressed files: if this option is checked, all compressed files found will be scanned. These files will only be scanned if this option is checked. Selecting all the extensions is not enough.

All files: by selecting this option, all files will be scanned regardless of their extension, except for compressed files, system files, **Microsoft Outlook Express**, **Microsoft Exchange** and **Microsoft Outlook** e-mail files. These must be checked separately in order for them to be scanned.

Only Program files: if this option is selected, only files with EXE or COM extensions will be scanned.

Additional. This section only appear during the configuration of Lotus Notes Startup Scans, and not during the configuration of Permanent Lotus Notes Scans.

Enable sounds: if this option is checked, the sounds configured in the corresponding section of the general configuration will be enabled.

Save report: if this option is checked, all data concerning the scan in question will be saved in the report.

Heuristic

Enable: if this option is checked, an additional virus scan will be run on each file. This second scan will be run based on techniques designed for detecting unknown viruses

Configure: A heuristic scan can be configured using this button. The user can choose between three different sensitivity levels and which suspicious situations will give rise to a warning from the antivirus.

Options: actions (Computer startup - Advanced)

Note: certain options are only available depending on the product purchased and the operating system configuration. For more information, see Differences between versions.

In this section, the user can indicate which action the antivirus should carry out when a virus is detected. The different possibilities are:

Ignore and continue scanning
The antivirus does not carry out any action when a virus is detected. Normal scanning is continued.

Disinfect automatically
Using this option, the user can have the antivirus automatically disinfect all files found containing viruses.

Suspend scanning and report in the case of another incident
If this option is checked, scanning will be momentarily stopped if any unexpected problem occurs during the process. The incident will be immediately reported. Once the warning is accepted, scanning will continue normally.

Options: scheduler (Computer startup / Windows startup - Advanced)

Note: certain options are only available depending on the product purchased and the operating system configuration. For more information, see Differences between versions.

A startup scan may be scheduled in this section. In this case, this scan will be run only under certain circumstances. The available options are:

- **Always:** the startup scan will be run each time the computer is started up.
- **Every x startups:** the startup scan will be run in a regular manner after the indicated number of startups.
- **Every x days:** the startup scan will be run periodically as every x days as indicated.
- **Every "day of the week":** the startup scan will be run only on the indicated day of the week.

Enabled
With this option, the scheduled scan can be enabled or disabled.

Windows Startup Scan Options (Advanced)

Note: certain options are only available depending on the product purchased and the operating system configuration. For more information, see Differences between versions.

The Windows startup scan options allow the user to configure how the scan will be performed. To access these options, click on the **Configuration** button in the **Startup scan** section, taking into consideration the startup scan option selected (computer, Windows or Lotus Notes startup). All scan options are grouped in the same window, though separated by different tabs for a maximum ease of use.

For more information select the appropriate section:

Scan.
Actions.
Exclusions.
Report.
Warnings.
Scheduler.

Options: configuration in basic mode

In the basic mode, the different protection strategies (immediate, scheduled, startup, permanent and Internet scans) all have the same window configuration. This window includes the main scan options, which are the following:

Scan

Compressed files: if this option is checked, all compressed files found will be scanned. These files will only be scanned if this option is checked. Selecting all the extensions is not enough.

Electronic mail files: if this option is checked, the antivirus will scan all e-mail files regardless of the indication in the **Extensions** section. The antivirus is capable of scanning **MS-Exchange/Outlook** (PST files) e-mail files. These files will only be scanned if this option is checked. Selecting all the extensions is not enough. Disabled for Computer Startup Scans. Disabled for Computer Startup Scans.

Generate report: if this option is checked, the information concerning the scan in question will be logged in the report.

All files: by selecting this option, all files will be scanned regardless of their extensions. The exceptions are compressed files, system files, **Microsoft Outlook Express**, **Microsoft Exchange** and **Microsoft Outlook** e-mail files, which must be marked separately in order for them to be scanned.

Only program files: if this option is selected, only files with EXE or COM extensions will be scanned.

Only my extensions: this option permits you to indicate that all files with extensions indicated on a list are to be scanned. This list can be accessed by means of the **Extensions** button. Disabled for Computer Startup Scans.

Action

Show information on the virus: this causes the antivirus to display a window with information on the virus when it is detected. No other action will be taken.

Ignore and continue scan: the antivirus takes no action when a virus is detected. Scanning will then continue normally.

Disinfect automatically: here, you can indicate the automatic action the antivirus should take if a file is infected: rename, delete or move the file in question.

Rename the infected file: permits you to rename a selected scan.

Delete infected files: by indicating this option, all infected files found will be deleted.

Move the infected file: if this option is indicated, all infected files found will be moved.

Ask what action to take: with this option, the antivirus can be advised to ask what action to take each time a virus is found. The user can indicate different actions during the same scan.

For most of the different scan types, the same set of options are presented for when a virus is found. However, there are scans that may not offer all of them or which even display entirely new ones. For instance, the startup scan configuration only offers two options: **Ignore and continue scanning** and **Disinfect**. Likewise, the permanent scan (Sentinel) features an option that generally does not appear in the list of possible actions: **Block access to file**.

In the lower part of the configuration screens, the following two buttons appear:

Restore: this enables you to select the type of configuration desired: *default* (configuration settings that the user defined as standard) or *manufacturer* (initial configuration settings defined by the antivirus program).

Predetermine: this enables the user to indicate that the configuration settings defined in that moment be used as the antivirus' default configuration values.

Automatic configuration of the antivirus (Wise Setup)

Wise Setup is a tool that is specially designed to facilitate the installation and configuration of **Panda Antivirus 6.0**. Through an exhaustive analysis of the hardware and software installed on the computer and a simple questionnaire, **Wise Setup** optimally configures **Panda Antivirus 6.0** in order to achieve the best possible results.

The different steps that make up **Wise Setup** start by welcoming the user to the process and offering a brief explanation of how it works:

1. An analysis of installed hardware and software is carried out. Once finished, and after clicking on the **Continue** button, a summary of the hardware and software components found is displayed.
2. A questionnaire is presented, in which you are asked to answer a number of simple questions concerning the work performed on the computer. Answers to these questions are already offered thanks to the hardware and software analysis carried out previously.
3. Lastly, a summary report displays the configuration options offered by **Wise Setup**. If you proceed with the installation, these will be used as the configuration options for **Panda Antivirus 6.0** (**Home Edition or Platinum**).

What is the integrated MS-Exchange/Outlook scan?

Panda Antivirus 6.0 includes a module especially designed to be completely integrated with **MS-Exchange/Outlook**. Therefore, all antivirus management for **MS-Exchange/Outlook** can be done using this e-mail program.

The antivirus integration in **MS-Exchange/Outlook** offers various advantages. Two of the most important are:

- **Scanning of all messages:** the Internet scan checks all e-mail messages coming in from Internet. It does not, however, scan those messages that **MS Exchange/Outlook** receives from an **MS-Exchange Server** in case it is connected to it. Nevertheless, the scan integrated with **MS-Exchange/Outlook** guarantees a scan of all messages received using this e-mail program, regardless of their origin.
- **Scanning of all operations carried out with a message:** the Internet scan checks messages the moment they are received and sent. However, the scan integrated with **MS-Exchange/Outlook** scans all messages subject to being used to carry out an operation, for example the opening, modification or moving files from one folder to another.

Panda Antivirus 6.0 has added four buttons to the standard **MS-Exchange/Outlook** button bar. These four buttons are:

Scan: this button starts a scan of the folder or messages selected when the scan begins. All sub-folders found in the indicated folder will also be scanned. A window allows the user to follow the process, displaying the group of folders to be scanned, the folder being scanned in each moment and a progress bar.

Results report: this button displays a report of incidents found by the antivirus. This report is kept from one session to another until deleted by the user.

Enable or disable the antivirus: using this button, the **Panda Antivirus 6.0** permanent protection can be enabled or disabled. If this protection is disabled, **Panda Antivirus 6.0** does not scan new incoming or outgoing messages for viruses, nor does it scan any messages upon opening for reading. However, it can scan at any time a particular folder or message using the **Scan** button. The **Exchange/Outlook** startup scan will be performed even though the permanent protection has been disabled.

Configure: this button displays the **Panda Antivirus 6.0** configuration window. In this window, you can configure the general functioning of the antivirus, its execution upon the start up of the mail program, as well as its behavior as a permanent and on-demand protection.

How to scan from MS-Exchange/Outlook

To scan a particular folder, select it. If the selected folder contains other folders (a mailbox, for example), all of the interrelated folders will be scanned. Once the folder has been selected, click on the **Scan** button of the standard **MS-Exchange/Outlook** button bar, or select the **Scan** option to search for viruses within the **Tools** option in the **MS-Exchange/Outlook** main menu.

Once the scan has finished, you will be able to see the results detailing any incidents encountered during the scan.

Panda Antivirus 6.0 allows you to scan one or more messages. In order to do this, select the message or messages you wish to scan. Once they have been selected, click on the **Scan** button to start the scan.

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

Options: blocking (Internet - Advanced)

Note: certain options are only available depending on the product purchased and the operating system configuration. For more information, see Differences between versions

In this section, you can specify the Internet addresses you wish to restrict access to in order to prevent the possible infections caused by accessing unreliable addresses or services. It is made up of the following two sections:

Blocking addresses: when you mark the check box, the configuration button will be enabled. If pressed, a dialog box will display the following sections:

- **Add this address:** in this section, you need to enter the Web address to which you wish to block access.
- **Add:** pressing this button will add the new address, written in the box at the top, to the list of addresses.
- **Remove:** if you press this button after selecting an address from the list on the left, it will be deleted from the list.
- **Clear list:** if this button is pressed, all addresses will be removed from the list.
- **Ask for the action to be taken in case of blocking:** if checked, you will be asked before an address is blocked.

Blocking services: when you mark the check box, the configuration button will be enabled. If pressed, a dialog box will display the following sections:

- **List:** a list appears detailing all the services that can be blocked. To block a specific service, click on the box that appears to its left.
- **Ask for the action to be taken in case of blocking:** if checked, you will be asked before a service is blocked.

Lotus Notes system scans

In addition to performing the aforementioned scan types, **Panda Antivirus 6.0 Home Edition / Platinum** is capable of scanning Lotus Notes databases. It integrates with this database management program by adding menu options to its interface, thereby facilitating the detection tasks carried out on the information contained in the database.

Its ability to scan Lotus Notes databases permits **Panda Antivirus 6.0 Home Edition / Platinum** to perform immediate scans of selected databases, schedule scans jobs and automatically run them at a given time, scan upon starting up the Lotus Notes database or carry out permanent scans that constantly check all information managed.

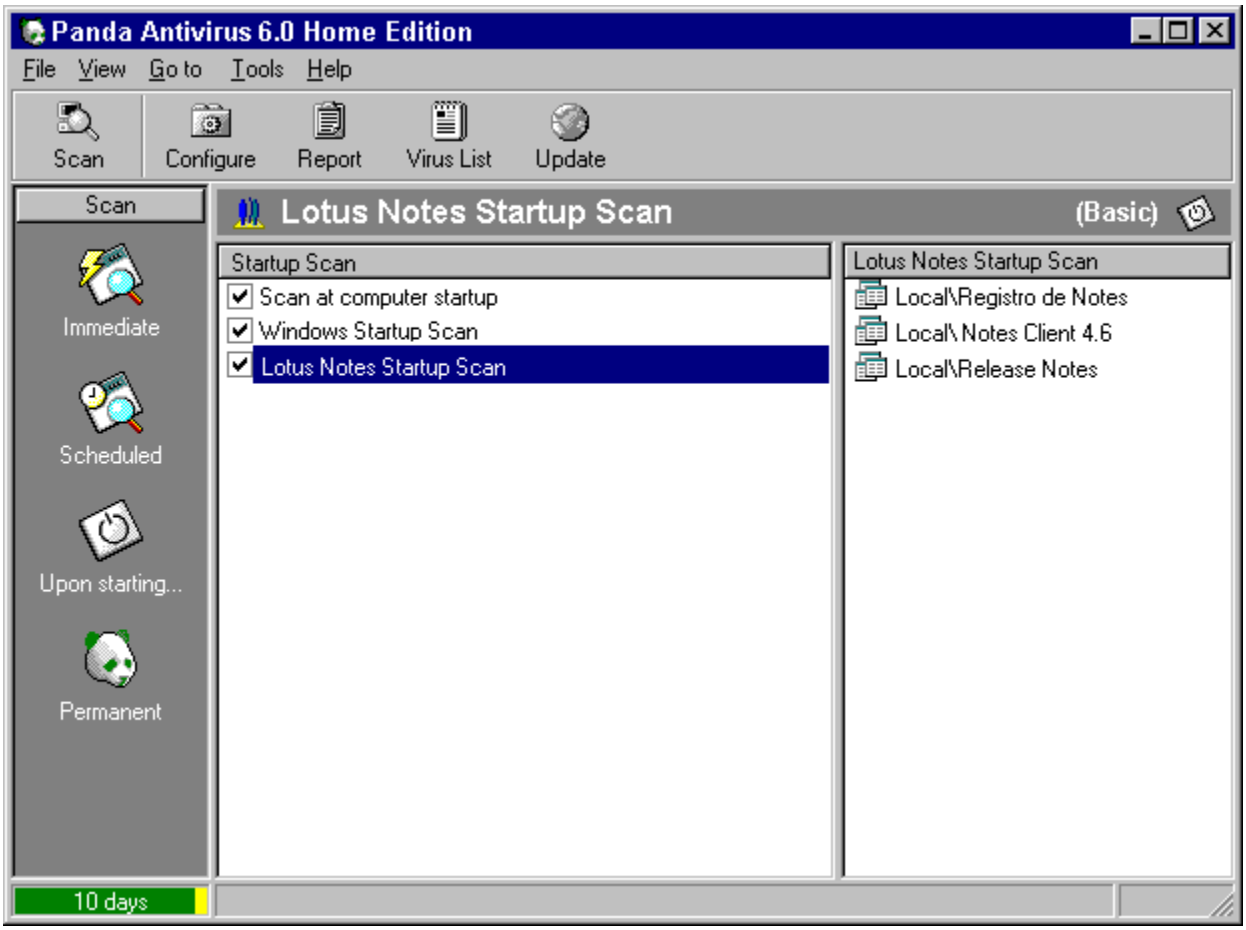
In addition to performing the different scan types, **Panda Antivirus 6.0 Home Edition / Platinum** lets you configure each type of scan, the actions to take if an infection occurs, the characteristics with which the report should be generated and the alerts that can be sent to warn of virus detection.

Lotus Notes database scans can be carried out from the antivirus program or from the Lotus Notes database program. This means that **Panda Antivirus 6.0 Home Edition / Platinum** fully integrates in Lotus Notes in order to provide greater ease of use. The advantage of this is that you will not have to execute the antivirus program to scan a database document, for you can perform said scan from the Lotus Notes program itself. You need only select the **Actions** option form the main menu.

Lotus Notes databases may be selected from the antivirus item tree for scanning. **Panda Antivirus 6.0 Home Edition / Platinum** will scan entire Lotus Notes databases. If you need to scan individual documents contained within a database, but do not want to scan the entire database, you will have to open that database from Lotus Notes. Once you have done this, select the database documents you want to scan. These can then be scanned by means of the corresponding option in the **Actions** menu.

Lotus Notes startup scan (Basic)

The Lotus Notes Startup Scan is that which is carried out when the Lotus Notes database application is executed or loaded. Thanks to this type of scan, you can analyze any database used on this system, as well as the documents they contain.



In Basic Mode, you can indicate whether or not you want to scan upon executing the Lotus Notes database system. Through this option, you can also obtain information on the files that are scanned.

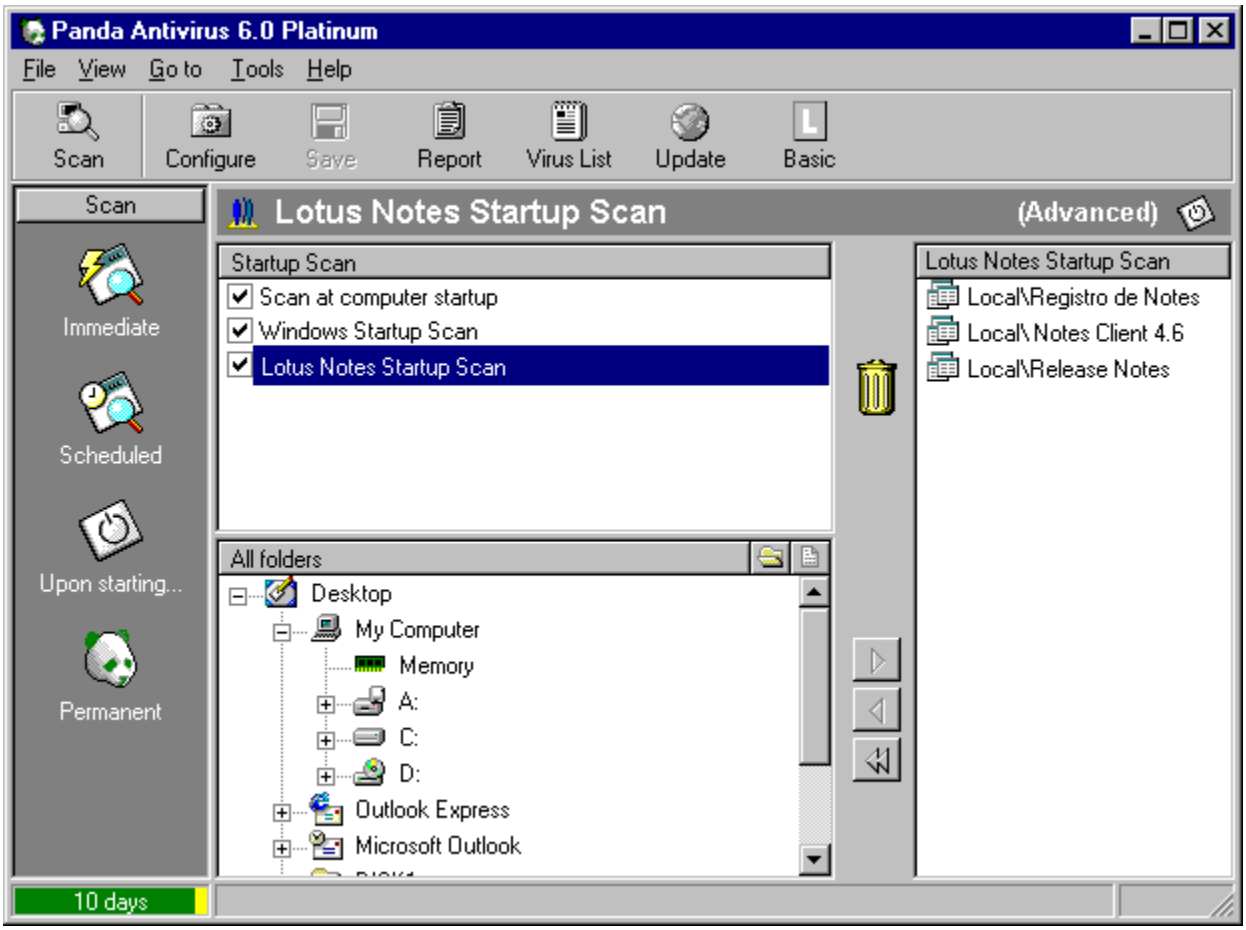
To obtain more information on how to enable or disable the Lotus Notes Startup Scan, you can consult the sections that follow.

How to enable the Lotus Notes startup scan.
Options in Lotus Notes startup scan.
How to disable the Lotus Notes startup scan.

Lotus Notes startup scan (Advanced)

Note: certain options are only available depending on the product purchased and the operating system configuration. For more information, see Differences between versions.

The Lotus Notes Startup Scan is that which is carried out when the Lotus Notes database application is executed or loaded. Thanks to this type of scan, you can analyze any database used on this system, as well as the documents they contain.



In Advanced Mode, you are offered the possibility of configuring the Lotus Notes Startup Scan through five tabs that will permit you to independently work on each of the possibilities and to specify what you want to scan and when.

The Scheduler of the Lotus Notes Startup Scan permits you to indicate whether you just want to perform said scan every time the database system is started or, on the contrary, if you want to carry it out every certain number of startups, every certain number of days or every certain day of the week.

To obtain more information on how to enable or disable the Lotus Notes Startup Scan, you can consult the sections that follow.

How to enable the Lotus Notes startup scan.

Options in the Lotus Notes startup scan.
How to disable teh Lotus Notes startup scan.

Options: scan (Startup/Lotus Notes Permanent - Advanced)

Note: certain options are only available depending on the product purchased and the operating system configuration. For more information, see Differences between versions.

There are several options grouped under this section for a maximum ease of use.

Scan
Compressed files: if this option is checked, all compressed files found will be scanned. These files will only be scanned if this option is checked. Selecting all the extensions is not enough.

Nested documents: by selecting this option, all documents within other documents will be scanned.

Generate report: if this option is checked, the data relative to the scan in question will be logged in the report.

All files: selecting this option will ensure the scanning of all files, regardless of their extension, except for compressed files, system files and the electronic mail files of **Microsoft Outlook Express**, **Microsoft Exchange** and **Microsoft Outlook**, which must be separately checked in order to be scanned.

Only program files: if this option is selected, only files with EXE or COM extensions will be scanned.

Only my extensions: this option enables you to scan all the files whose extensions are included in a list. Pressing the **Extensions** button takes you to this list.

Additional. This section only appear during the configuration of Lotus Notes Startup Scans, and not during the configuration of Permanent Lotus Notes Scans.

Enable sounds: if you check this option, you will enable the sounds in accordance with the configuration previously set in the corresponding section of general configuration.

Generate report: if this option is checked, the data relative to the scan in question will be logged in the report.

Minimize while scanning: if you check this option, the antivirus will automatically minimize itself when it starts the scan.

In the lower part of the configuration screens, the following two buttons appear:

Restore: this enables you to select the type of configuration desired: *default* (configuration settings that the user defined as standard) or *manufacturer* (initial configuration settings defined by the antivirus program).

Predetermine: this enables the user to indicate that the configuration settings defined in that moment be used as the antivirus' default configuration values.

Options in the Lotus Notes scan (Starting/Permanent - Advanced)

Note: certain options are only available depending on the product purchased and the operating system configuration. For more information, see Differences between versions.

The Lotus Notes startup scan options enable you to configure how this scan will be performed. To access these options, press the **Configuration** button in the **Startup scan** section, bearing in mind the startup scan option you have selected (computer startup, Windows startup or Lotus Notes startup). All the scan options are grouped in a single window but separated into different tabs to make them easier to manage.

Select the section on which you want more information:

Options: actions (Startup/Lotus Notes Permanent - Advanced)

Note: certain options are only available depending on the product purchased and the operating system configuration. For more information, see Differences between versions.

In this section you can indicate what action you want the antivirus program to take when it finds a virus. Depending on the action you choose, a series of options will be displayed to enable you to configure it. The different possibilities are:

Ignore and continue scanning

Selecting this action will ensure that the antivirus program will perform no action when it detects a virus. It will continue the scan in the normal way.

Disinfect automatically

Choosing this action instructs the antivirus to automatically disinfect all infected files it detects. This option can be configured, since there may be occasions on which disinfection is not possible.

Suspend the scan and inform in case of any other incident

If you check this option, the scan will stop momentarily if some unexpected problem arises so that you can be informed of the incident. Once you accept the notification of the incident, the scan continues in the normal way.

Options: scheduler (Starting Lotus Notes - Advanced)

Note: certain options are only available depending on the product purchased and the operating system configuration. For more information, see Differences between versions.

This configuration tab is only available in scheduled Lotus Notes Startup Scans, but NOT in the configuration of Permanent Lotus Notes Scans.

The Scheduler Scan permits you to indicate whether you just want to perform said scan every time the database system is started or, on the contrary, if you want to carry it out every certain number of startups, every certain number of days or every certain day of the week.

Always: if you select this option, the Lotus Notes database will be scanned each time the database management system is started.

Every certain number of startups: if you select this option, the Lotus Notes Startup Scans will be carried out every certain number of startups of the Lotus Notes database system.

Every certain number of days: if you select this option, the Lotus Notes Startup Scan will not be performed at every startup, but rather after certain number of days.

Every certain day of the week: if you select this option, the Lotus Notes Startup Scan will be performed only on the day that you have chosen from the drop-down menu.

Enabled

With this option, the scheduled scan can be enabled or disabled.

Options: warnings (Lotus Notes Startup - Advanced)

Note: certain options are only available depending on the product purchased and the operating system configuration. For more information, see Differences between versions

Warnings are notifications the antivirus generates to indicate that it has detected a virus. Because of the importance of this type of notification, its configuration is flexible and powerful to ensure that the virus notification reaches the right person. The configuration options are as follows:

In the workstation (the Configuration button will not appear in the configuration section of Internet warnings)

This option enables you to choose how notification will be given of the detection of a virus in the computer in which it was found. If you indicate that you wish to see the warnings in the computer where the virus was found, a button allows you to configure the type of notification.

Audible warning: plays a sound at the time a virus is detected.

Audible warning – **beep:** if this option is chosen, a beep will be heard each time a virus is detected.

Audible warning – **WAV file:** if you select this option, each time a virus is detected a WAV type file will be played. You can indicate which WAV file you wish to hear.

Show warning message: you may also choose a warning in the form of a displayed message.

Warning message: this is the message that will be shown each time a virus is detected.

Remove warning message: in order not to stop the scan, you can indicate that you want the warning message to disappear after a certain number of seconds.

Via e-mail

This option instructs the antivirus to use electronic mail to notify of the detection of a virus in a computer.

Send message to address: serves to indicate that you want an e-mail message to be sent each time a virus is detected.

Address: the e-mail address to which the virus detection messages will be sent.

Warn sender: the person who sent the infected message may also be warned.

Warn other recipients: other recipients of the infected message may also be warned.

Message: the message which will be shown each time a virus is detected.

Protocol: select the type of protocol through which you wish to send the warning message: MAPI or SMTP (outgoing mail).

Server: here is where you can enter the name of the server through which warning messages will be sent.

In the network

This option instructs the antivirus to communicate the detection of a virus in one computer to other computers connected in a network with the first one.

Send message to workstation: you can choose to send the virus detection message to a specific workstation in the network.

Workstation: enables you to indicate the workstation to which you wish to send the virus detection message.

Message: the message which will be displayed each time a virus is detected.

Send message to domain: you can choose to send the virus detection message to all the

workstations belonging to the same domain.

Domain: allows you to indicate the domain to which you wish to send the virus detection message.

Message: the message that will be displayed each time a virus is detected.

Server: here is where you can enter the name of the server through which warning messages will be sent.

In Lotus Notes

This option permits users to send alerts when a virus is detected in a Lotus Notes system. The warning may be sent to the document's author, to the person working with the infected file or to any other user.

Recipients: in this textbox, enter the name of the users that will receive the warning, separating each name with a coma.

Warn document's author: the creator of the infected document is notified of the detection.

Warn person using the document: the user working with the infected document is notified of the detection.

Warning message: this permits you to enter the message that will be sent as an alert on the detection.

In the lower part of the configuration screens, the following two buttons appear:

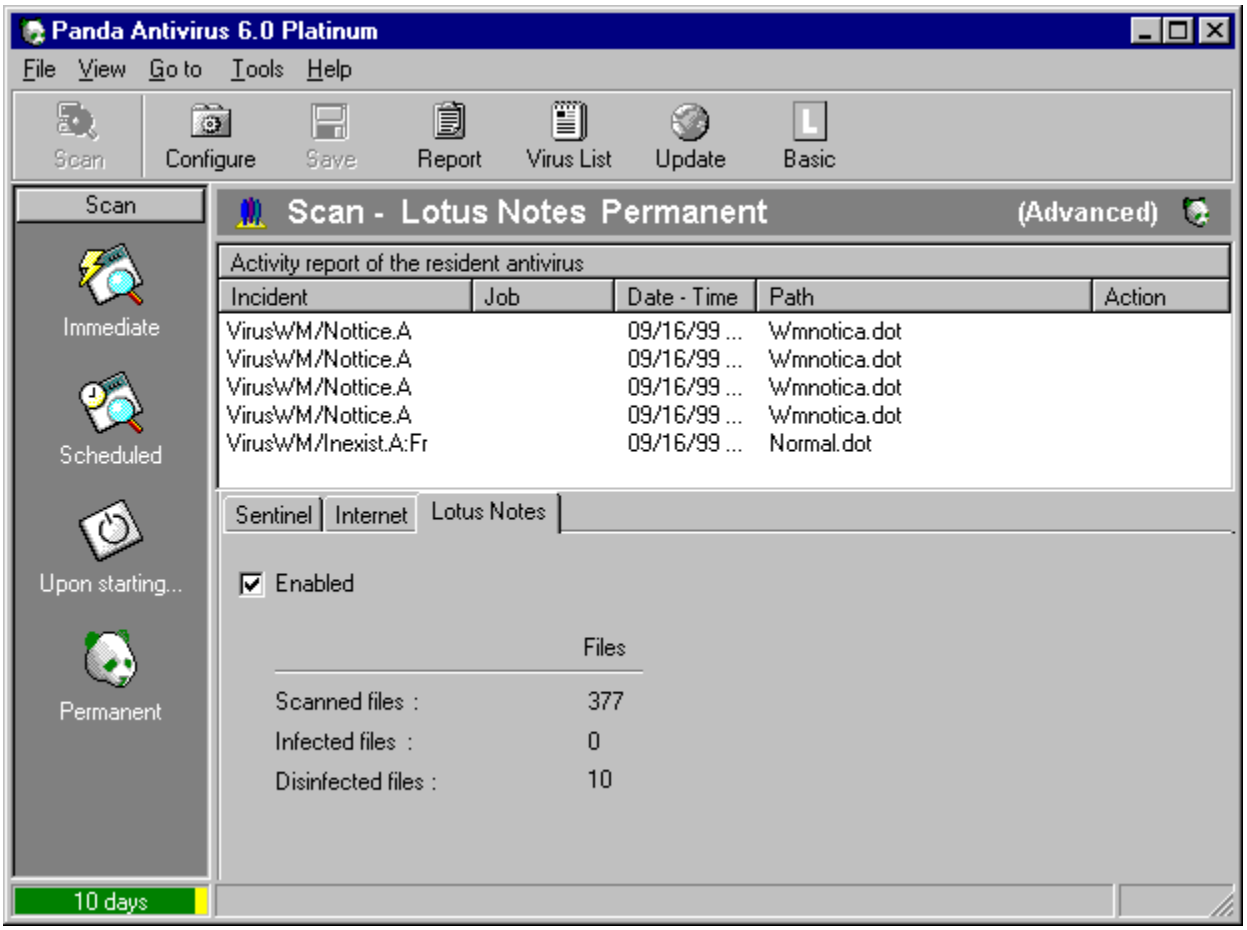
Restore: this enables you to select the type of configuration desired: *default* (configuration settings that the user defined as standard) or *manufacturer* (initial configuration settings defined by the antivirus program).

Predetermine: this enables the user to indicate that the configuration settings defined in that moment be used as the antivirus' default configuration values.

Permanent Lotus Notes scan (Advanced)

Note: certain options are only available depending on the product purchased and the operating system configuration. For more information, see Differences between versions.

By Permanent Lotus Notes Scan, we refer to a background scan that is constantly being carried out on Lotus Notes databases. Thanks to this type of scan, you can scan any database, as well as the documents contained within.



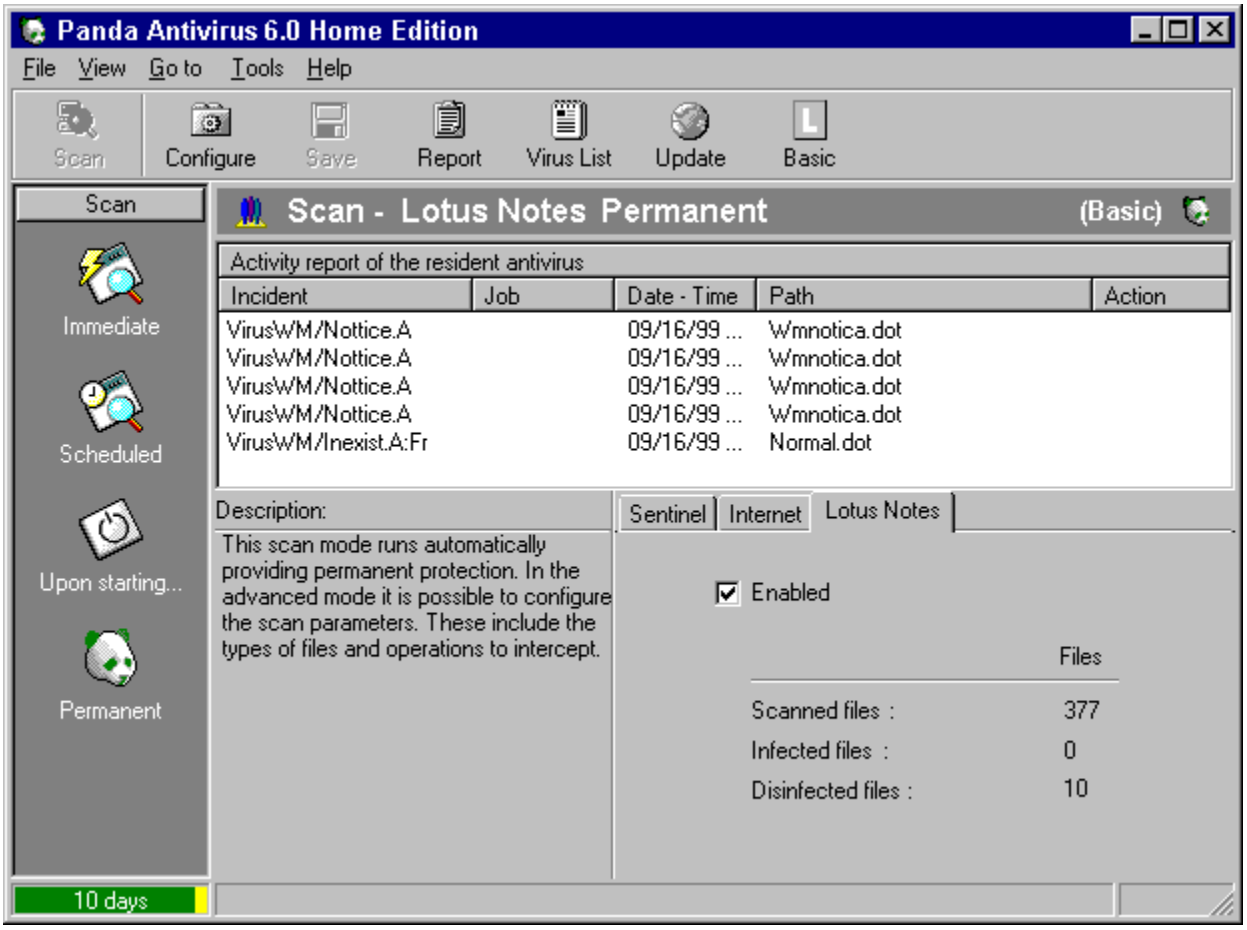
The application enables you to configure the Permanent Lotus Notes Scan in Advanced Mode through the use of four separate tabs, where you can specify what and when you wish to scan.

For additional information on the aforementioned topic, click on any of the options that follow:

How to enable the Permanent Lotus Notes Scan.
Permanent Lotus Notes Scan options.
How to disable the Lotus Notes Permanent Scan.

Permanent Lotus Notes scan (Basic)

The Permanent Lotus Notes scan offers a singular function: permanent protection against viruses that can come in through the Lotus Notes. This permanent protection against Lotus Notes viruses starts working from the startup of the application. From that moment on, the scan is responsible for monitoring all Lotus Notes related operations carried out on the computer.



This way, by means of a totally automatic process, the Lotus Notes scan takes care of keeping your computer free from viruses originating from the Lotus Notes.

In the **Lotus Notes scan** section you can see an activity report of this scan, as well as a brief summary of the files scanned and the possible viruses found. This scan can be easily enabled or disabled.

For more information on these subjects, please consult the following sections.

How to enable the permanent Lotus scan.
Permanent Lotus Notes scan options.
How to disable the permanent Lotus Notes scan.

Options: permanent configuration (Actions - Sentinel)

Pop-Up Menus

When working with **Panda Antivirus 6.0**, in addition to using toolbar menu options and buttons, you may also enable pop-up menus. For this, you need only right-click on any item. These menus are available in the following sections.

Pop-Up Menus: in the main window.
Pop-Up Menus: in the reports
Pop-Up Menus: in the scan window

Pop-Up Menus: in the main window

By main window, we refer to the default window that appears when **Panda Antivirus 6.0 Home Edition / Platinum** is loaded. There, you will see several sections, for which different pop-up menus may appear.

Toolbar: this is a section that contains certain buttons (Scan, Configure,...etc). The actions you are allowed to perform through their pop-menus can also be accessed in the **View** – **Toolbar** menu. This menu will present the following options:

- **Standard:** if this is selected, the normal toolbar will be displayed.
- **Additional:** if you enable this option, a new toolbar will appear in the lower left-hand side of the window with the following buttons: **Enable/Disable sounds**, **Scan compressed files**, **Scan e-mail files**, **If a virus is found, ignore and continue**, **Generate scan report** and **Heuristic scan**.
- **Labels:** this option allows you to choose whether or not you wish to display the names of the standard toolbar's buttons.

Predetermined scans: this section displays the predetermined scans that correspond to the section you are in. You cannot choose to perform several scans at once. Some options only appear for certain types of scans, and not for all of them.

- **Enable/Disable:** permits you to enable/disable the selected scan. This option is not available in Immediate Scans.
- **Scan** or **Scan now:** permits you to perform the predetermined scan selected.
- **Configure scan:** permits you to modify the characteristics of the predetermined scan selected.
- **Save created scan:** permits you to save the information on the new scan.
- **Delete created scan:** permits you to delete a selected scan.
- **Change name:** permits you to rename a selected scan.

All folders: this section displays a tree of possible items to scan, allowing you to select one or more items. This only appears in Advanced mode (see Differences between versions). Some options only appear for certain types of scans, and not for all of them.

- **Scan selected item:** when this option is selected, the item(s) marked will be scanned.
- **Configure default options:** permits access to the configuration settings of the current scan.
- **Add selected item:** the tree's item(s) selected will be added to the list of items to scan.

Selected items: these are the items selected for scanning. You can choose to scan one or more at the same time. The following describes the options that are available:

- **Scan selected item:** when this option is selected, the item(s) that is/are marked will be scanned.
- **Configure scan:** permits access to the configuration settings of the current scan.
- **Remove selected item:** any selected item will be removed from the list.
- **Remove all items:** all items will be removed from the list.

Pop-Up Menus: in reports

From the report window, you can highlight as many lines as you wish in order to carry out certain actions with them. If you enable a pop-up menu by right-clicking a selected line, the following options will appear:

Scan: this is only enabled if a virus has been detected. Permits you to scan the same incident again. You can also repeat a scan by double-clicking the incident.

Show information: this is only enabled if a virus has been detected. It provides more detailed information on the incident.

Disinfect: this is only enabled if a virus has been detected. Permits you to disinfect the affected item.

Rename: this is only enabled if a virus has been detected. Permits you to rename the infected file.

Delete: this is only enabled if a virus has been detected. Permits you to delete the infected file.

Move: this is only enabled if a virus has been detected. Permits you move the infected file to another location.

Select all: all the items on the list will be selected, regardless of whether they have been infected.

Pop-Up Menus: in the scan window

In the scan window, you will see a list that summarizes incidents detected during scanning. You can work with the items that such list displays.

Should an item appear on the list at any given moment, warning about the detection of a virus and notifying of the actions that have been taken, you may choose to scan the infected item again. To do this, enable the pop-up menu by right-clicking the desired item. This action will display a list, where you need to choose the **Scan** option.

How to configure the permanent scan (Sentinel/Internet/Lotus Notes - Advanced)

Note: certain options are only available depending on the product purchased and the operating system configuration. For more information, see Differences between versions.

Permanent scan configuration: Sentinel (basic and advanced).
Permanent scan configuration: Internet (advanced).
Permanent scan configuration: Lotus Notes (advanced).