Introduction

Panda Antivirus

Panda Antivirus is a complete and effective solution for keeping your computer protected against all types of viruses. Versions of the Antivirus for Windows 95, Windows NT Workstation, Windows 3.1x, DOS and OS/2 are included to offer you protection no matter what your operating system is. This Help corresponds to **Panda Antivirus** for Windows NT Workstation.

Protection Strategies

Panda Antivirus incorporates various types of protection against viruses:

- **Permanent protection:** the permanent protection is responsible for protecting your computer at all times and does not require user intervention. The great advantage of this protection strategy is that it permits you to protect your computer in a completely automatic way.
- **On-demand scan:** the on-demand scan permits you to scan any area of the computer at any given time. Just choose the area you want to scan and the program will immediately begin to scan the selected area in search of viruses.
- **Disinfection:** when a virus is found, there are several possible actions you can take. One of these is disinfection, which consists of removing the virus from the file and leaving it exactly as it was before the infection took place.
- **Heuristic scan:** the heuristic scan method is an alternative scanning technique to those already mentioned. Heuristic scanning works upon user demand. Users must indicate what area of the computer they want to scan using this method at the time in question. This scanning technique is designed to find unknown viruses.
- **String search:** as with heuristic scanning, this is an alternative scanning technique that also functions upon user demand. It is used to search for new viruses in accordance with the data provided by the Panda Software technical support service.
- **Other options:** under this heading are grouped certain features of the antivirus designed to provide information or to facilitate the handling of the application. For example, there is a results report in which you can view the different virus incidents and operations performed using the antivirus.

Panda Software Antivirus Solutions

Panda Software offers you the following antivirus solutions:

- **24h-365d® Antivirus Insurance® for Individual PCs.** Licenses.
- **24h-365d® Antivirus Insurance® for Networked PCs** (automatic distribution from servers).
- **24h-365d® Antivirus Insurance® for Network Servers** (Novell NetWare and Windows NT servers*).*
- **24h-365d® Antivirus Insurance® for Local Area Networks.**
- **24h-365d® Antivirus Insurance® for E-mail and Groupware Clients.**
- **24h-365d® Antivirus Insurance® for E-mail and Groupware Servers.**
- **24h-365d® Antivirus Insurance® for SMTP Mail Servers.**
- **24h-365d® Antivirus Insurance® for PCs connected to Internet.**
- **24h-365d® Antivirus Insurance® for Internet Servers** (SMTP, FTP and HTTP).

- **24h-365d® Antivirus Insurance® for Proxy Servers.**

What is 24h-365d® Panda Software Antivirus Insurance®?

24h-365d® Panda Software Antivirus Insurance® is a new and revolutionary antivirus protection concept that offers you the maximum possible security. **24h-365d® Panda Software Antivirus Insurance®** is an extraordinary combination of products and services that offers the highest levels of protection against viruses. **24h-365d® Panda Software Antivirus Insurance®** can be purchased with different insurance coverage periods and update frequencies.

The product name is **Panda Antivirus**, an antivirus that has obtained the most demanding antivirus detection certifications, including:

- **ICSA Certification:** granted by the prestigious American ICSA (International Computer Security Association) to antivirus products that periodically detect 100% of *In the Wild* viruses (the most frequently found viruses at any given moment) and more than 90% of the *Zoo Collection* (collection of thousands of lesser-known viruses).

- **CheckMark Certification:** granted by the British computer security magazine *Secure Computing*.

If you do not already have **24h-365d® Panda Software Antivirus Insurance®**, you can acquire it using the order form included on the registration card. The services offered by **24h-365d® Panda Software Antivirus Insurance®** are the following:

- **Hot-Line:** for ONE year, we will solve your virus problems by phone, fax, the Internet or e-mail. Whenever you call, at any time of the day or night, you will find the most highly qualified personnel at your disposal, 24 hours a day, 365 days a year. This is an exclusive **Panda Software** service.

- **S.O.S. Virus:** if you find a virus that **Panda Antivirus** does not detect or remove, we will send you a courier (or we will collect the suspicious sample by the quickest available means) and in less than 24 hours we will develop a new version capable of detecting and removing the new virus. We will then send you this new version completely free of charge.

- **Update Service with home delivery:** your antivirus will always be updated. You will receive at your mailing address monthly or quarterly updates on CD-ROM or floppy disks if you purchased our **24h-365d® Panda Software Antivirus Insurance®** solution. You can also update the product through our WEB site as often as you wish for the period of one year, with the guarantee of at least one new update every day.

- **WEB Service:** virus information and answers to your most frequently asked questions.

Installation

System Requirements

To install **Panda Antivirus** for Windows NT Workstation, you require the following elements:

- IBM compatible computer with a 486 or superior processor.
- 16 MB RAM.
- 4 MB hard disk space.
- Windows NT 3.51 or higher operating system.
- CD-ROM drive.
- Mouse.

Installation Procedure

There are two versions of **Panda Antivirus** for Windows NT Workstation. One corresponds to the 3.51 version of this operating system and the other to the 4.0 version. You must make sure to install the corresponding version for each operating system.

Both versions can only be installed from the CD-ROM that accompanies the product. To install either version, run the CDMENU.COM program. This program offers you a simple options menu. You must first select the desired language and then the version you wish to install. In this case select one of the two **Panda Antivirus** for Windows NT versions, 3.51 or 4.0, depending on the operating system you have installed.

To install the **Panda Antivirus** for Windows NT Workstation version you must have administrator privileges on your computer. This is due to the privileges required to install the driver responsible for the permanent protection.

The installation procedure consists of the following steps:

1. First a presentation screen is displayed.
2. The user is then asked for his/her personal details.
3. You are asked for the directory in which you want to install the application.
4. You are then asked for the program group in which the access icons for the antivirus will be created.
5. You will be given the choice to install the permanent protection (**Sentinel** driver) or not.
6. The copying of files to the hard disk will begin.
7. Once the copying of files has concluded, you are advised to reset the computer for the permanent protection to take effect.

Updating the Antivirus

To update the current version with the update you receive, just install the new version over the old one.

Uninstallation

The uninstallation of the **Panda Antivirus** for Windows NT 3.51 version is performed by the UNINST program located in the application's program group.

In Windows NT 4.0, **Panda Antivirus** is uninstalled using the *Add/Remove Programs* option in the *Control Panel*. Just select **Panda Antivirus Windows NT W/S 4.0** from the list that is displayed and press the *Add/Remove* button. To complete the uninstallation it is necessary to reset the computer.

Do not try to uninstall by deleting the folder where the antivirus was installed. Always uninstall the program following the indicated procedure.

What is permanent protection?

Permanent protection is a program that, from the moment the computer is started up, intercepts all operations that carry risk of infection in order to verify that no virus enters the system.

The permanent protection is totally automatic and requires no user intervention. Despite this constant monitoring, system performance is not affected. The installation of the permanent protection is therefore always advisable as it greatly enhances your level of protection.

How to use the permanent protection

Permanent protection is one of the installation options. If you choose to install this protection, as soon as the computer is booted the permanent protection (**Sentinel**) will be brought into operation.

In the Windows NT Workstation 3.51 operating system, **Sentinel** appears as a minimized icon on the Windows desktop. If you have a Windows NT Workstation 4.0 operating system, **Sentinel** appears as an icon next to the clock in the taskbar.

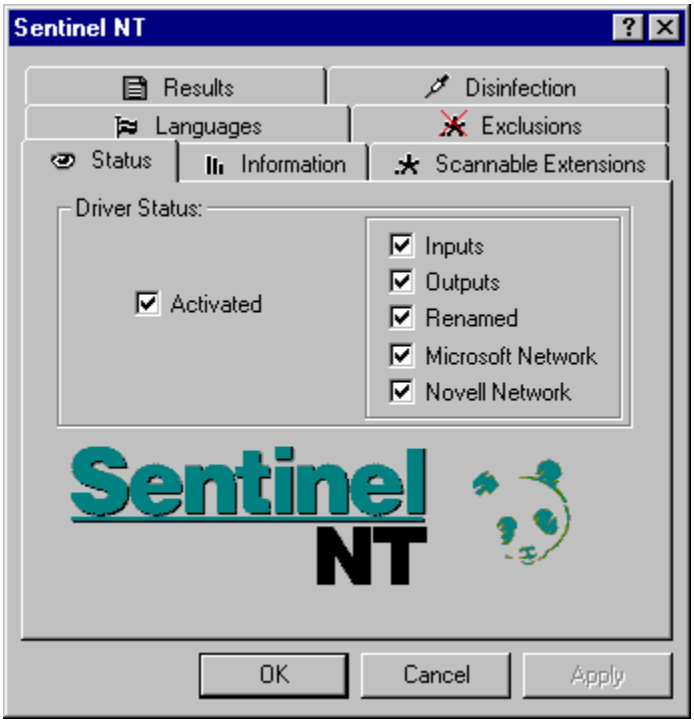
The permanent protection works in a totally automatic way. If a virus is detected during any computer operation, **Sentinel** will warn you of this circumstance and will carry out the appropriate action.

How to configure the permanent protection

The permanent protection can be configured to adapt to the needs of each user. By double-clicking the **Sentinel** icon, a window containing several tabs will appear. Each tab refers to a different aspect of the **Sentinel** configuration. The configuration options are as follows:

Status

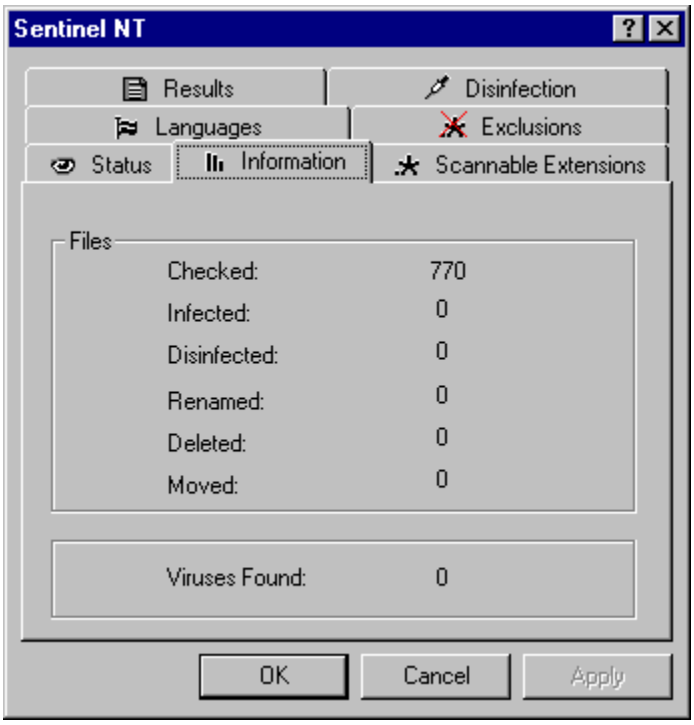
This tab defines the status of the permanent protection.



- **Enabled:** this option permits you to enable or disable the permanent protection. Keep in mind that if you disable the permanent protection, the computer will be left unprotected against viruses.
- **Incoming files:** when the permanent protection is enabled, this option indicates that all files entering the computer should be scanned. All files that are created or modified will also be scanned.
- **Outgoing files:** when the permanent protection is enabled, this option indicates that all files leaving the computer should be scanned. All files opened or executed will also be scanned.
- **Renamed:** when the permanent protection is enabled, this option indicates that all file rename operations should be scanned in search of viruses.
- **Microsoft network:** if the permanent protection is enabled, this option indicates that a remote scan should be performed on all Microsoft network operations.
- **Novell network:** if the permanent protection is enabled, this option indicates that a remote scan should be performed on all Novell network operations.

Information

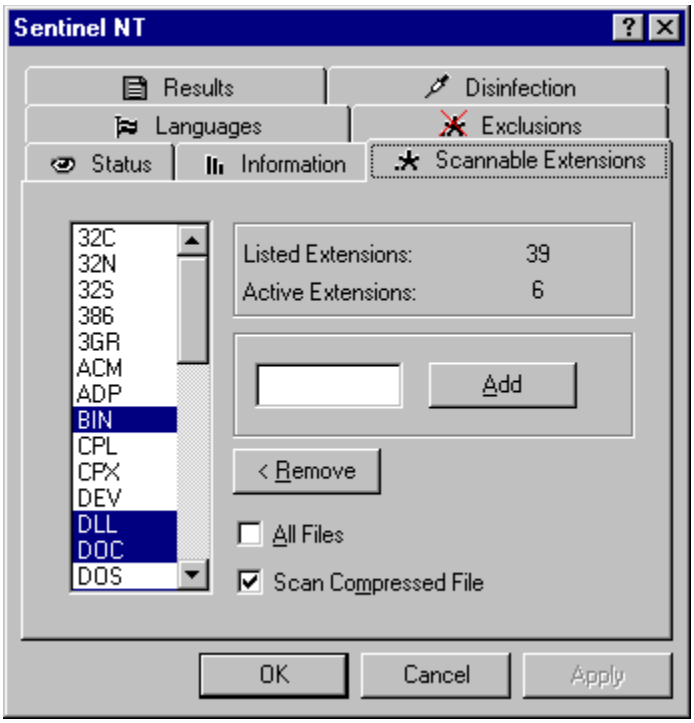
This tab shows diverse information about the activity of the permanent protection.



- **Checked:** this shows the number of files checked by the permanent protection since system startup.
- **Infected:** this shows the number of infected files that were found.
- **Disinfected:** this is the number of files disinfected by the permanent protection.
- **Renamed:** this is the number of files that were renamed by the permanent protection.
- **Deleted:** this indicates the number of files deleted by the permanent protection because of virus infection.
- **Moved:** this indicates the number of files moved by the permanent protection because of virus infection.
- **Viruses found:** lastly, this shows the number of viruses that were found.

Scannable extensions

This section permits you to configure the extensions that the permanent protection should scan.



- **List of extensions:** in the list of extensions you can mark as many extensions as you wish to scan. The permanent protection always intercepts all files that are accessed but will only scan those files whose extensions are marked. Regardless of the extensions that are selected, COM and EXE files are always scanned.
- **Listed extensions:** this figure indicates the number of extensions currently in the list.
- **Active extensions:** this shows the number of extensions in the list that have been marked for scanning.
- **Add extension:** to add an extension to the list, enter the extension name in the space provided and press the *Add* button.
- **Remove extension:** to remove an extension from the list, select the extension and press the *Remove* button.
- **All files:** if this option is checked, all files will be scanned regardless of what extensions are marked.
- **Scan compressed files:** if this option is checked, all compressed files that are accessed will be scanned.

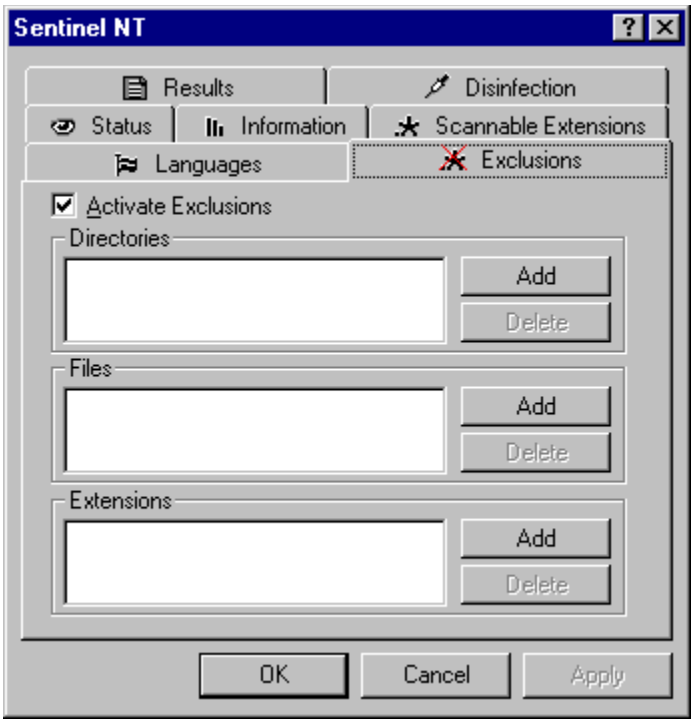
Languages

You can consult what language the permanent protection is currently in and also choose another language from the list of available languages.

- **Available languages:** a list is displayed containing the different languages available for the permanent protection. To change language, just select the language you want and press the *OK* or *Apply* buttons.
- **Current language:** this shows the language the permanent protection is currently in.

Exclusions

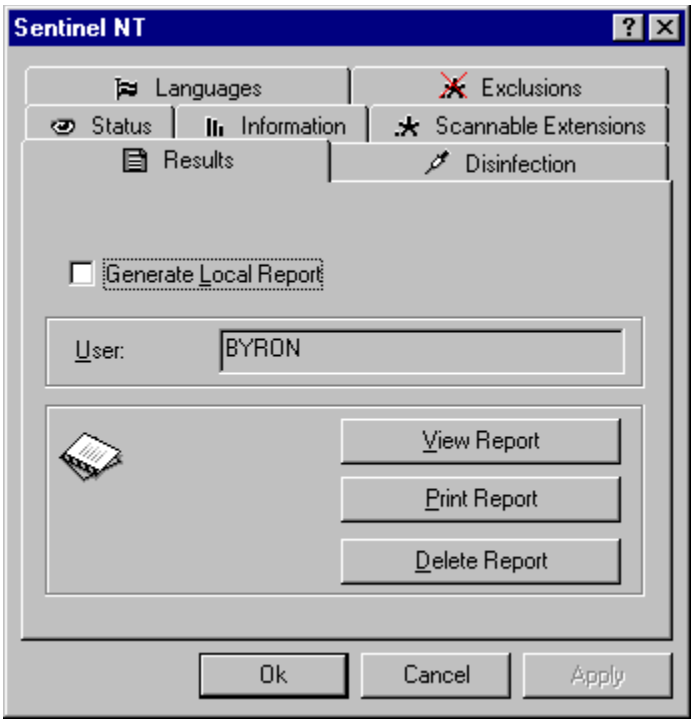
This tab permits you to indicate what areas, files or extensions you do not want to scan. Regardless of what is indicated in *Extensions*, all areas, files or extensions marked here **will not be scanned**.



- **Enable exclusions:** if this option is checked, the exclusion feature will be enabled according to the data you have indicated.
- **Directory:** this section displays a list of the directories that you do not want to scan.
- **Add directory:** this option permits you to add directories to the list of directories that will not be scanned.
- **Remove directory:** this option permits you to remove directories from the list of directories that will not be scanned.
- **File:** this section displays a list of the files that you do not want to be scanned.
- **Add file:** this option permits you to add files to the list of files that will not be scanned.
- **Remove file:** this option permits you to remove files from the list of files that will not be scanned.
- **Extensions:** this section displays a list of the extensions that you do not want to be scanned. Even if some of these extensions appear in the list of extensions to be scanned, they will not be scanned.
- **Add extension:** this option permits you to add extensions to the list of extensions that will not be scanned.
- **Remove extension:** this option permits you to remove extensions from the list of extensions that will not be scanned.

Results

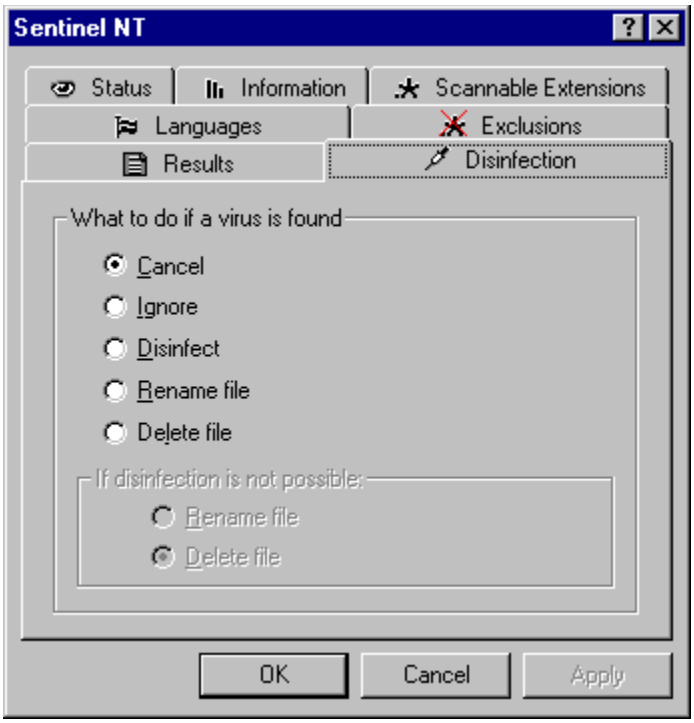
This is where you can configure the behavior of the system of incident reports generated by the permanent protection.



- **Generate local report:** if this option is checked, a report will be created with the different incidents detected by the permanent protection.
- **User:** The computer user's name is displayed here.
- **View report:** this buttons displays the report containing the incidents found so far.
- **Print report:** this button permits you to print the incidents report.
- **Delete report:** this button permits you to delete the incidents report.

Disinfection

This tab permits you to configure the behavior of the disinfection of virus-infected files detected by the permanent protection.

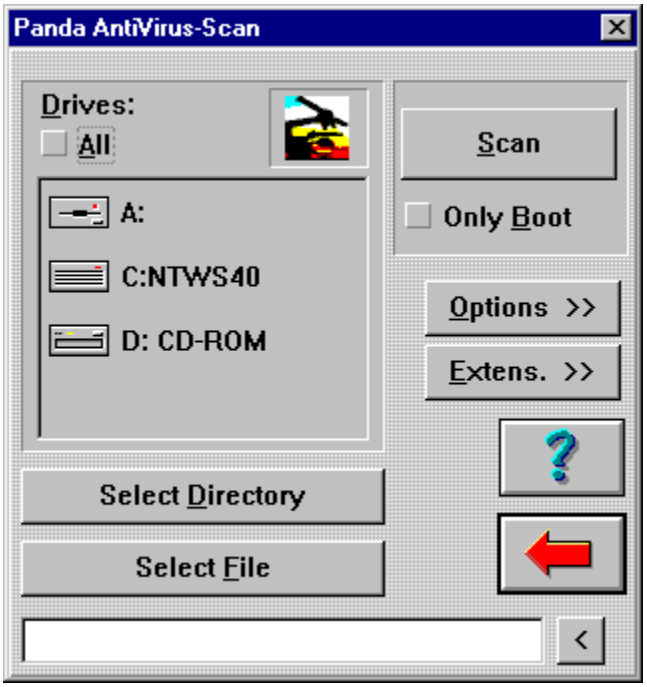


- **Cancel:** if you select this option, the operation in which the virus was detected will be cancelled. For example, if a virus is found in a file that you tried to execute, the execution of this file will be cancelled.
- **Ignore:** if this option is selected, even if a virus is detected it will be ignored.
- **Disinfect:** if this option is selected and the permanent protection detects a virus, it will proceed to disinfect the contaminated file, leaving it as it was before the infection took place.
- **Rename file:** if this option is selected and a virus is detected, **Sentinel** will rename the file by giving it a VIR extension.
- **Delete file:** if this option is selected and **Sentinel** detects a virus in a file, this file will be deleted.
- **If disinfection is not possible, rename file:** if this option is active and **Sentinel** detects a virus but cannot disinfect it successfully, the file will be renamed.
- **If disinfection is not possible, delete file:** if this option is active and **Sentinel** detects a virus but cannot disinfect it successfully, the file will be deleted.

What is the on-demand scan?

The on-demand scan permits you to scan any area of your computer whenever you choose. All scans performed can be configured through a series of simple options.

How to use the on-demand scan



To perform an on-demand scan, proceed as follows:

1. **Run the antivirus:** to run the antivirus, go to the program group containing the icons that permit its execution. Double-click the *Panda Antivirus* icon.
2. **Go to the scan section:** to access this section, press the *Scan* button in the application's button bar. A window will appear in which you can specify what should be scanned and how.
3. **Select the area to be scanned:** you must choose what area you want to scan. The different drives recognized by the system are displayed in a list. You can also select a particular directory or file by using the buttons designed for this purpose.
4. **Configure extensions:** this step is optional. The program saves the configuration of the extensions you want to scan. Therefore, once configured, there is no need to repeat this step for each scan.
5. **Configure scan options:** this step is also optional. The program saves the configuration of the scan options. Therefore, once you have configured the scan there is no need to repeat it each time you scan. The configuration only needs to be changed if you want to select a different series of options. There is a more detailed explanation of the scan options in this documentation in the configuration section.
6. **Indicate if you only want to scan the boot sector:** this step is optional. If you check this option, only the boot sector and not the files of the selected drives will be scanned. If the option is not checked, both the boot sector and the files of all selected drives will be scanned.
7. **Start scan:** the *Scan* button begins a scan of the selected drives in search of viruses in accordance with the options you have chosen.

How to configure the on-demand scan

As already explained, the following data must be provided for the scan:

- What area you want to scan.
- What extensions are to be scanned.
- How the scan is to be performed.

The configuration of a scan takes into account the choice of extensions that are to be scanned and the scan options.

Extensions

By pressing the *Extensions* button, a window appears in which you can indicate what extensions you want to scan.

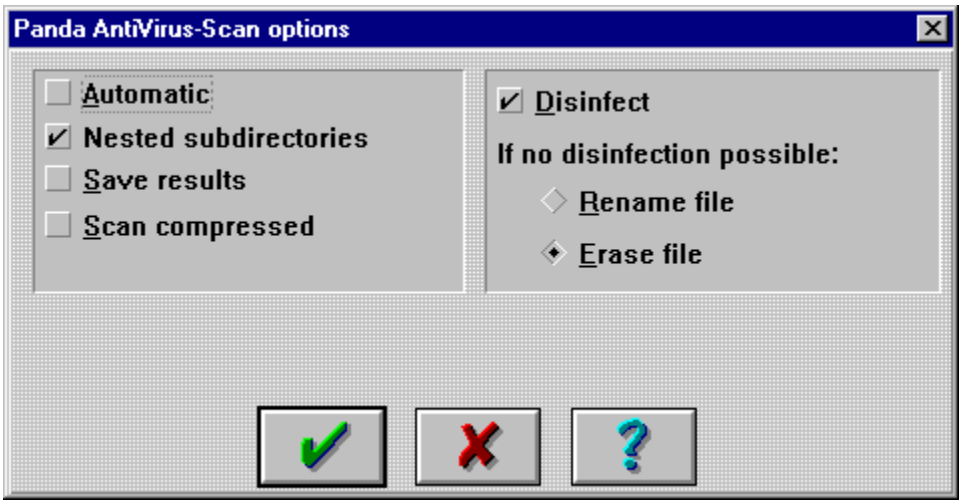
The *All* option above the list of extensions indicates that all files will be scanned regardless of their extension. If this option is not checked, only those extensions that are marked in the list will be scanned.

Two buttons permit you to add or remove extensions from the list. By default, a list of the most common file extensions is provided as well as a selection of extensions that commonly carry viruses.

Regardless of the extensions that are selected, COM and EXE files are always scanned.

Scan options

By pressing the *Options* button, a window appears which permits you to choose from the following scan options:



- **Automatic:** if this option is checked, the scanning process will be completely automatic. If viruses

are found, you will be warned of the incident but the process will continue without interruption. This is especially useful if the computer contains many infected files to be disinfected.

- **Nested subdirectories:** if this option is checked, all subdirectories found in the selected drives will be scanned. If you do not check this option, nested subdirectories will not be scanned. Therefore, if you choose to scan a drive and this option is not checked, the antivirus will only scan the root directory of the selected drive.
- **Save results:** if this option is checked, the data relative to the scan in question will be recorded in the results file.
- **Scan compressed files:** if this option is checked, all compressed files that are found will be scanned.
- **Disinfect:** if this option is checked and a virus is found, the antivirus will try to disinfect it.
- **If disinfection is not possible, rename:** if this option is checked and a virus is found that the antivirus cannot disinfect, the file in question will be renamed.
- **If disinfection is not possible, delete:** if this option is checked and a virus is found that the antivirus cannot disinfect, the file in question will be deleted.

What is a heuristic scan?

Heuristic scanning is an additional scanning technique specifically designed to detect unknown viruses.

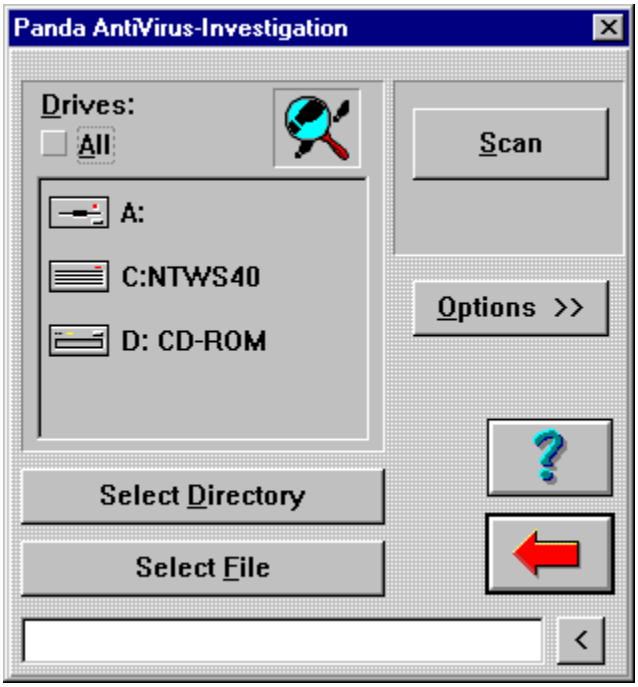
As with on-demand scans, the heuristic scan is immediate and is performed upon user request. The scanning method on which the heuristic scan is based is completely different to the method used for the on-demand scan. The latter tries to find a virus known to the antivirus, whereas the heuristic scan tries to determine if a virus exists based on general characteristics common to most viruses.

As the heuristic scan can only determine that a file is suspected of being virus-infected, but does not possess enough information on the supposed virus, it is not possible to disinfect the suspected viruses detected by the heuristic scan.

It is important to realize that the heuristic scan serves to complement the on-demand scan.

The working of the heuristic scan is similar to that of the on-demand scan.

How to use the heuristic scan



To perform a heuristic scan, proceed as follows:

1. **Run the antivirus:** to run the antivirus, go to the program group containing the icons that permit its execution. Double-click the *Panda Antivirus* icon.
2. **Go to the heuristic scan section:** to access this section, press the *Investigate* button in the application's button bar. A window will appear in which you can specify what should be scanned using the heuristic method and how the scan should be performed.
3. **Select the area to be scanned:** you must choose what area you want to scan. The different drives recognized by the system are displayed in a list. You can also select a particular directory or file by using the buttons designed for this purpose.
4. **Configure heuristic scan options:** this step is optional. The program saves the configuration of the heuristic scan options. Therefore, once you have configured the heuristic scan there is no need to repeat it each time you perform this type of scan. The configuration only needs to be changed if you want to select a different series of options. There is a more detailed explanation of the heuristic scan options in this documentation in the configuration section.
5. **Start scan:** the *Scan* button begins a heuristic scan of the selected drives in search of viruses in accordance with the options you have chosen.

How to configure the heuristic scan

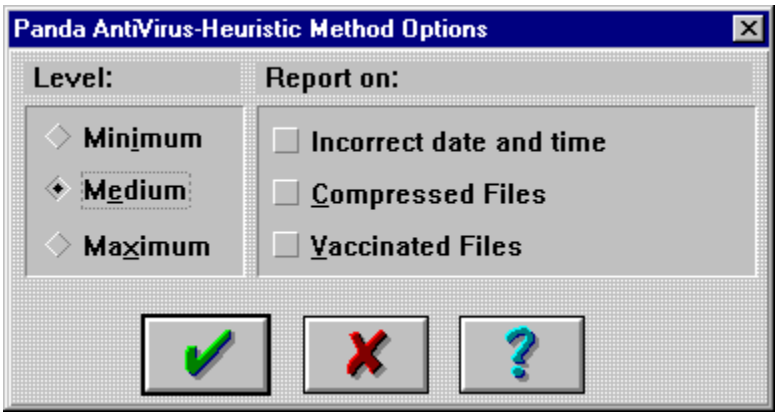
As already explained, the following data must be provided for the heuristic scan:

- What area you want to scan using this method.
- How the scan is to be performed.

The configuration of a heuristic scan takes into account the options for this scan type.

Scan options

By pressing the *Options* button, a window appears which permits you to choose from the following heuristic scan options:



- **Minimum sensitivity:** if this option is selected, the sensitivity of the heuristic scan will be low, meaning that only highly suspicious files will be indicated as being possible virus carriers.
- **Medium sensitivity:** if this option is selected, the heuristic scan will be performed with a medium level of sensitivity. In this way, only those files that are quite likely to be infected will be considered suspicious.
- **Maximum sensitivity:** if this option is selected, the sensitivity of the heuristic scan will be at its maximum level, meaning that all files in which it detects possible virus presence will be considered suspicious. However, even at this level of sensitivity the possibility of an uninfected file being considered suspicious is minimal.
- **Inform of incorrect date and time:** if this option is checked, you will be warned each time a file with an incorrect date or time is found.
- **Inform of compressed files:** if this option is checked, you will be notified of each compressed file found.
- **Inform of vaccinated files:** if this option is checked, you will be notified of each vaccinated file found.

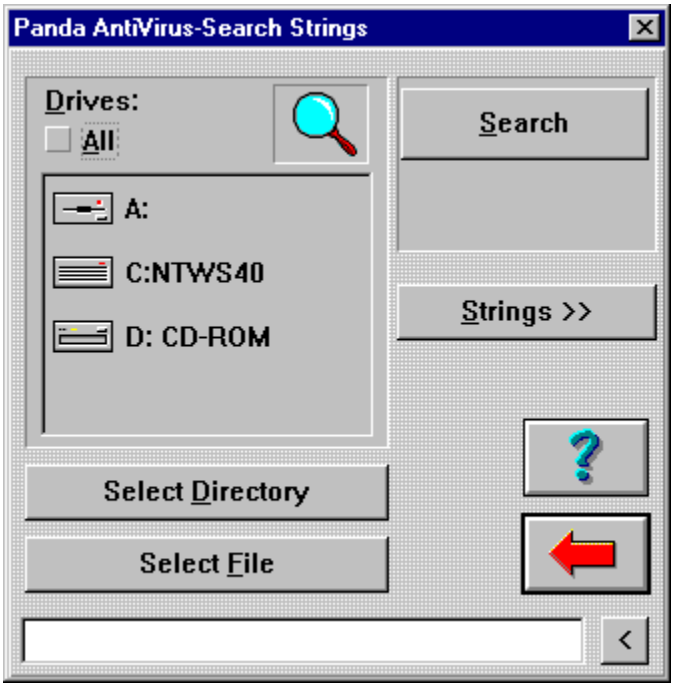
What is the string search?

The on-demand scan searches files for parts of viruses that the antivirus recognizes. Due to the fact that new viruses appear every day, the on-demand scan method is gradually becoming outdated.

String searching uses the same method as the on-demand scan but permits you to indicate a particular string (part of a virus) to be searched for. In this way, **Panda Software**'s technical support service can provide you with a string that corresponds to a new virus, thereby enabling the antivirus to detect it even though it does not contain any information on this new virus.

As with the on-demand scan, the string search is immediate and is performed upon user request.

How to use the string search



To perform a string search, proceed as follows:

1. **Run the antivirus:** to run the antivirus, go to the program group containing the icons that permit its execution. Double-click the *Panda Antivirus* icon.
2. **Go to the string search section:** to access this section, press the *Search* button in the application's button bar. A window will appear in which you can specify what should be scanned using the string search method and how the scan should be performed.
3. **Select the area to be searched:** you must choose what area you want to search. The different drives recognized by the system are displayed in a list. You can also select a particular directory or file by using the buttons designed for this purpose.
4. **Indicate what strings should be searched for:** enter the strings the antivirus is to search for or select existing strings from a list. As the program saves the strings that were entered on other occasions, there is no need to repeat this step unless you want to add a new string.
5. **Start search:** the *Search* button starts the search for the specified strings in the chosen areas.

How to configure the string search

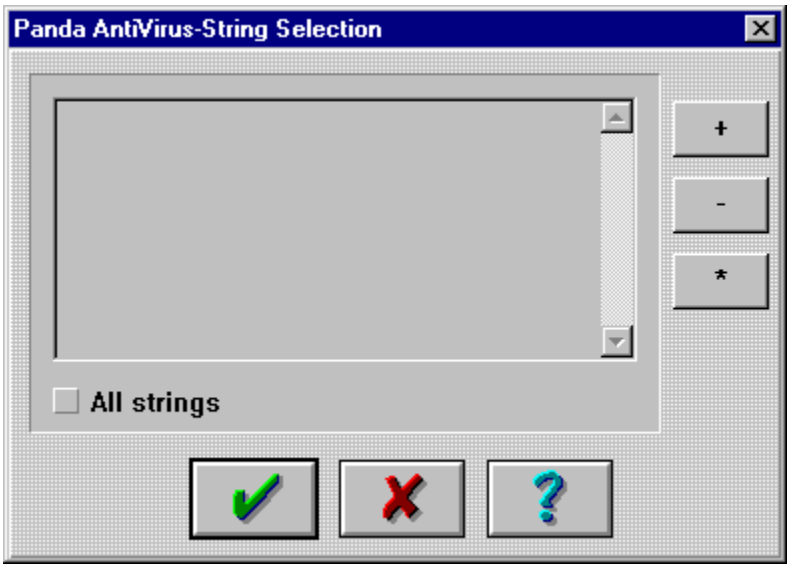
As already explained, the following data must be provided for the string search:

- What area you want to scan using this method.
- What strings should be searched for.

The configuration of a string search consists of specifying the strings to be searched for.

Strings

By pressing the *Strings* button, a window appears in which you can select the strings you want to search for.



This window displays a list of strings that have been entered. By means of the buttons provided, you can add a string to the list, modify an existing string or remove a string from the list.

Not all the strings in the list will be searched for unless the *All strings* option is checked. If this option is not checked, only those strings selected in the list will be searched for.

How to disinfect using Panda Antivirus

Panda Antivirus does not contain a specific disinfection section. Disinfection is associated with the on-demand scan or the permanent protection. If the on-demand scan or permanent protection detect a virus, they will try to disinfect it (if the options in these two sections have been configured to do so).

The configuration options permit you to indicate that all infected files that cannot be disinfected should be deleted or renamed.

Viruses may be found in the boot sector of a disk or in files. For each case, you must proceed in a slightly different manner. Consult the corresponding sections to obtain detailed information on the disinfection procedures.

Disinfection of a boot virus

FAT partition

To disinfect a boot virus from drive C, proceed as follows:

1. Switch off your computer. Insert a virus-free boot disk (if you are going to carry out the disinfection from CD-ROM, the disk must load the CD drivers) and restart the computer.
2. Once the computer has rebooted, run the command-line version of the antivirus (PAVCL) following the instructions below:

    - If you want to run **Pavcl** from floppy disk, insert disk 1 of **Panda Antivirus** for DOS/Windows 3.1x and enter the following:

      ```
      PAVCL C: /CLV
      ```

    - If you want to run **Pavcl** from the CD-ROM, insert it in the CD drive, go to the DOSWIN3X directory and the required language and enter the following:

      ```
      PAVCL C: /CLV
      ```

      If in either of these two situations a message appears indicating that the selected drive is not valid, enter the following:

      ```
      PAVCL /HD0 /CLV
      ```

NTFS partition

If you have an NTFS partition, in order to disinfect a boot virus it is important to know whether the virus affects the master boot record, the boot sector or both. If the virus only affects the master boot record, the procedure indicated for FAT partitions is equally valid in this case.

If the virus affects the boot sector, the way to remove the virus is to replace the boot sector with a generic boot by means of one of the tools provided by Windows NT for this purpose.

Disinfection of viruses found in files

If viruses were found in your files, proceed to clean your system by configuring the antivirus as follows:

- In *Scan Options* enable *All extensions, Disinfect* and *Automatic Scan*.
- Go to the scan section and select the option to scan the whole system (all drives). While the scan is being carried out, infected files will be cleaned.

Disinfection through the permanent protection

Sentinel is capable of disinfecting the viruses it detects. If **Sentinel** detects a virus and is configured to disinfect it, it will proceed to disinfect it before the current operation is performed. Once disinfected, the operation in which the virus was detected will continue. **Sentinel** always displays a window indicating the detection of a virus.

Command line scan

Panda Antivirus possesses a program called **Pavcl** which is run from the MS-DOS command line. Our command line scanner detects and disinfects the same viruses as any other version of **Panda Antivirus**.

Pavcl is a fast scanner that takes up very little memory, although a certain knowledge of the parameters it admits is required to manage it. **Pavcl** can be found on disk number 1 of the DOS/Windows 3.1x version or in the corresponding language directory within the DOSWIN3X directory on the CD-ROM.

Pavcl Parameters

Tasks

`/NOM` Do not scan memory.

`/NOB` Do not scan BOOT sectors.

`/NOF` Do not scan files.

`/ALL` Scan all system drives.

`/INVx` Investigate drive "x" for unknown viruses.
Example: `/INVa` investigates drive A.

`/CLV` Remove detected viruses.

`/LIS` List the viruses that are detected in this version.

`/HEU` Enable Heuristic detection method.

`/CMP` Scan compressed files.

`/CDR` Display **Pavcl** return codes.

`/SAV` Save current parameters to a file. On the next program runs, these parameters will be added to those specified in each session.

`/IB+` Add Internal vaccine to the BOOT.
`/IB-` Remove Internal vaccine from the BOOT.
`/IB*` Verify Internal vaccine of the BOOT.

`/EB+` Add External vaccine to the BOOT.

`/EB-` Remove External vaccine from the BOOT.
`/EB*` Verify External vaccine of the BOOT.

`/IF+` Add Internal vaccine to a file.
`/IF-` Remove Internal vaccine from a file.
`/IF*` Verify Internal vaccine of a file.

`/EF+` Add External vaccine to a file.
`/EF-` Remove External vaccine from a file.
`/EF*` Verify External vaccine of a file.

`/B+` Add Internal and External vaccines to the BOOT.
`/B-` Remove Internal and External vaccines from the BOOT.
`/B*` Verify Internal and External vaccines of the BOOT.

`/F+` Add Internal and External vaccines to a file.
`/F-` Remove Internal and External vaccines from a file.
`/F*` Verify Internal and External vaccines of a file.

Options

`/NSB` Do not scan nested subdirectories.

`/PTH` Scan directories contained in the DOS PATH variable.

`/ISO` Activate isolation mode.

`/NOS` Disable sound.

`/AEX` Scan all files, regardless of their extension.

`/AUT` Scan without user intervention.

`/OVR` Overwrite before deleting.

`/NOR` Do not generate results file.

`/DEL` Delete infected files even if they can be disinfected.

`/LOC` Scan all local drives.

`/NBR` Do not allow cancelling of scanning process.

`/ITW` **Pavcl** will only scan in search of *In The Wild* viruses. This parameter must only be used in

special circumstances.

You can also avail of the "/?" switch, standardized in DOS, to access a list of all available parameters. This also includes the switches for the languages supported by this version of **Pavcl**.

The default tasks are:

- Scan Memory.
- Scan Boot.
- Scan Files.

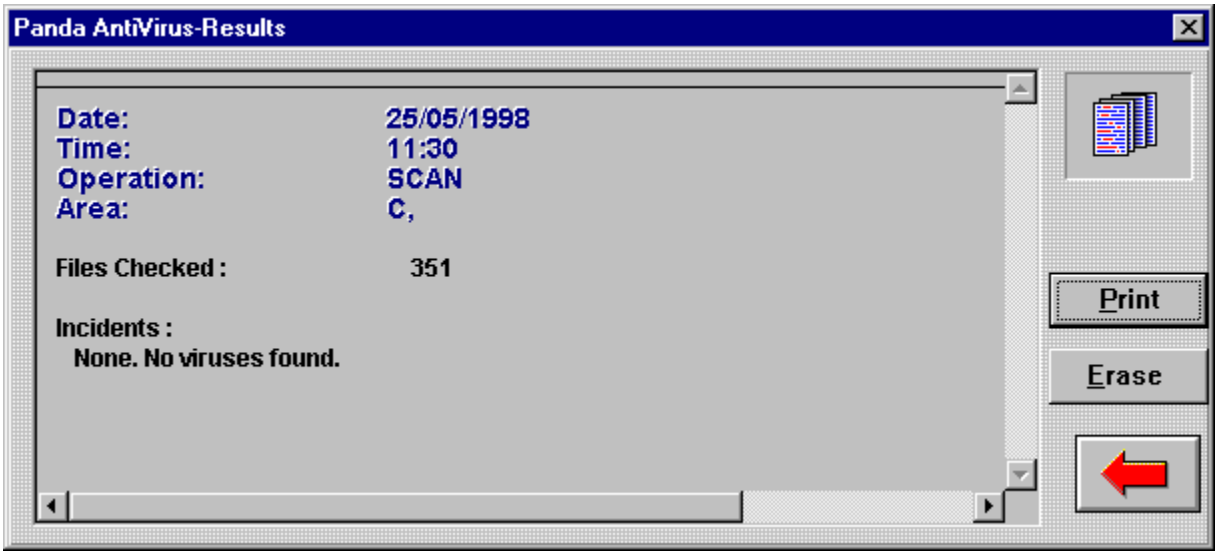
And the default options are:

- Scan subdirectories.
- Do not disinfect.
- Enable sound effects.
- Scan only executable file extensions.
- Generate results file.

The switches /?, /LIS and /INVx are exclusive; i.e. when they are used no other action is performed. After finishing the selected task, the program returns to DOS. The path or paths to be scanned are specified as usual in DOS:

```
[Drive:][Path][FileName]
```

Results report



The results report records the different operations that are performed using the antivirus as well as all incidents produced.

The information contained in the results report is saved from session to session. It can therefore be used to consult at any time all operations performed using the antivirus.

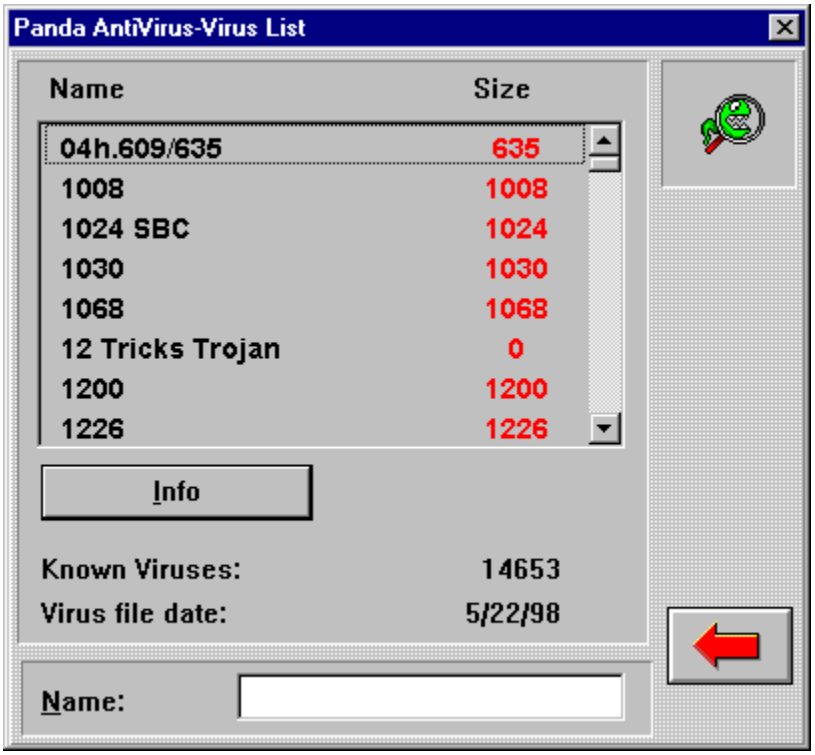
For every antivirus operation performed, the following data is recorded:

- Date and time.
- Type of operation.
- Area in which the operation was performed.
- Number of files checked.
- All virus-related incidents.

To record this information in the results report, it is necessary to check the *Save results* option in the *Scan Options* window.

The contents of the results report can be printed to make it easier to consult. It is also possible to delete the contents of the results report at any time in order to prevent it from becoming too big.

Virus list



The virus list presents a list of the most common viruses that **Panda Antivirus** is capable of detecting. The name and size of each virus are displayed in the list.

The number of viruses recognized by this version of **Panda Antivirus** is indicated below the list. The virus file creation date is also displayed so that you can know the update situation of the antivirus.

You can enter the name of a virus in the space provided to help you find a specific virus more quickly and easily. For this same reason the virus list appears in alphabetic order.

Once you have selected a virus, press the *Info* button to display a window containing information of interest, including the following:

- Name.
- Origin.
- Size.
- Alias.
- Date it was first detected.
- If it is possible to disinfect.
- Areas of the computer that may be affected by the virus.
- Behavioral characteristics of the virus.

Below is an explanation of the different characteristics that may be attributed to a virus:

- **Resident:** when the virus is executed it reserves a small part of memory in which it installs itself and from where it can spread.
- **Stealth:** this is a technique used by some resident viruses. It consists of concealing the changes the virus makes to the files it infects. When the user tries to view the characteristics of the file that the virus has modified, the virus, which is resident in memory, intercepts the request and provides information prior to the modification.
- **Encrypted:** viruses that possess this characteristic are capable of encrypting themselves in a different manner each time they infect a file. Therefore, it is not possible to search for the virus by means of a string.
- **Overwrite:** overwrite viruses, which may be resident or not, overwrite the files they infect. Infected files are therefore rendered useless. The file size does not vary unless the virus is bigger than the file. The only way to remove these viruses is by deleting the infected file and replacing it with an uninfected copy.
- **Polymorphic:** polymorphic viruses are advanced versions of encrypted viruses. Polymorphic viruses are capable of changing their encryption method from generation to generation. In this way, no part of the virus remains unaltered.

General functioning

Panda Antivirus for Windows NT presents an easy to use interface. In the main program window, the most common options are available through the use of large-sized buttons.

By pressing these buttons you can access the different parts of the program. Refer to the corresponding section to obtain a detailed explanation of its functioning.