Scans all compressed files found during the scan.

Scans system files every time you scan, regardless of the areas chosen.

Scans all Microsoft Outlook Express, Microsoft Exchange or Microsoft Outlook e-mail files found during scanning.

Scans all files regardless of their extension.

Only scans files that have COM and EXE extensions.

Scans all files whose extension coincides with those present in the list of extensions.

This allows you to change the personal list of extensions.

Records the results of the scan in a report for subsequent consultation.

After scanning one diskette it will ask you to insert another, so that several can be scanned easily.

When a scan starts, the window showing its progress will be minimized.

It carries out a second scan in each file in search of generic virus characteristics in order to identify unknown viruses.

Configures the behavior of the heuristic scan.

List of extensions. Shows the extensions that will be scanned if the **My extensions** option is selected.

Enter a new extension here to add it to the list.

Adds the new extension indicated to the list of extensions.

Removes the selected extension from the list.

Removes all the extensions from the list.

Restores the list so that it only contains the original extensions.

Configures the heuristic scan to make it work faster. In this mode, the heuristic scan will only detect files that are very likely to be infected by unknown viruses.

Configures the heuristic scan so that it scans quickly while checking all files that are quite likely to be infected by a new virus.

Configures the heuristic scan so that it warns of any files that may be infected by a new virus. Even at this level, it is very unlikely that the antivirus will produce a false alarm.

Gives warning of any files containing an incorrect date or time.

Gives warning of any compressed files found.

Gives warning of any vaccinated files found.

Enables the sounds for the scan being configured according to the values introduced in the sound tab during the general configuration of the antivirus.

Allows you to choose the action to be taken if a virus is detected.

If this option is checked and a virus is detected, the contaminated file will be renamed.

If this option is checked and a virus is detected, the contaminated file will be deleted.

If this option is checked and a virus is detected, the contaminated file will be moved to the specified location.

Allows you to indicate the directory to which any infected files that are detected will be moved.

Allows you to indicate an e-mail address to which any contaminated files that are detected will be sent.

Allows you to indicate the directory to which any infected files that are detected will be moved.

Allows you to indicate an e-mail address to which any contaminated files that are detected will be sent.

If you check this option when asked what should be done with a virus-infected file, the move action will become available.

If you check this option when asked what should be done with a virus-infected file, the delete action will become available.

If you check this option when asked what should be done with a virus-infected file, the disinfect action will become available.

If you check this option when asked what should be done with a virus-infected file, the display information action will become available

If you check this option when asked what should be done with a virus-infected file, the rename action will become available.

If you check this option, the scan will pause momentarily to report on any problem found. The scan process will then continue normally.

This list shows the directories that will be excluded from the scan.

This button allows you to add directories to the list of directories that will be excluded from the scan.

This button allows you to remove directories from the list of directories that will be excluded from the scan.

This button allows you to completely empty the list of directories that will be excluded from the scan.

This list shows the files that will be excluded from the scan.

This button allows you to add files to the list of files that will be excluded from the scan.

This button allows you to remove files from the list of files that will be excluded from the scan.

This button allows you to completely empty the list of files that will be excluded from the scan.

This list shows the extensions that will be excluded from the scan.

Insert in this box any new extensions to be added to the list of extensions to be excluded from the scan.

This button allows you to add the extension entered in the box provided to the list of extensions to be excluded from the scan.

This button allows you to remove extensions from the list of extensions to be excluded from the scan.

If this option is checked, only virus incidents as well as any error events that might affect security will be recorded in the report.

If this option is checked, virus incidents, any error events and changes in the configuration that might affect security will be recorded in the report, as well as the start and finish times of the diverse scans performed.

If this option is checked, warnings will be sent to the workstation when a virus is detected.

This button allows you to configure the warnings to be sent to the workstation.

This allows you to indicate that a sound should be made when a virus is detected. This sound may range from a simple beep to the reproduction of any WAV file you possess.

This allows you to indicate that a message should be displayed when a virus is detected. This message may be customized and even configured to disappear automatically after a few seconds.

If this option is checked, warnings will be sent via the network when a virus is detected.

This button allows you to configure the warnings to be sent via the network.

This allows you to indicate that a warning message should be sent to a specific workstation in the network. This message can be configured.

This allows you to indicate that a warning message should be sent to a network domain. This message can be configured.

If this option is checked, warnings will be sent by e-mail when a virus is detected.

This button allows you to configure the warnings to be sent by e-mail.

This allows you to indicate that a warning message should be sent by e-mail to a specific address. The message can be configured.

This allows you to indicate the protocol to be used for sending an e-mail message with the warning.

If this option is checked, warnings will be sent when viruses are detected in e-mail messages.

This button allows you to configure the warnings to be sent when viruses are detected in e-mail messages.

This allows you to indicate that a warning message should be sent to the sender of the virus-infected message.

This allows you to indicate that a warning message should be sent to the other recipients of a virus-infected message.

This allows you to indicate that a warning message should be inserted in the infected message itself.

Scans according to the selected scan areas or the chosen scan job.

Allows scan to be configured.

Allows any new scan jobs created to be saved.

Shows the incident report drawn up by the antivirus.

Shows the list of viruses with important information on some of the viruses detected by the program.

Shows the window that permits the configuration of the antivirus updates.

Allows you to switch the application over to basic mode. This mode offers maximum ease of use while concealing most of the many scan options of the antivirus.

Allows you to switch the application over to advanced mode. This mode allows you to configure the various scan options of the antivirus while offering maximum flexibility.

Goes to the immediate scans, which allow any area of the computer to be scanned instantly.

Goes to the scheduled scans, which allow you to program scans to be carried out periodically and at the most convenient times.

Goes to the startup scans, which allow you to configure scans both at computer startup and during Windows startup.

Goes to the configuration of the resident scan, which offers permanent automatic protection.

Goes to the configuration of the Internet scan, which carries out constant automatic checks on all items coming from the Internet.

Shows the antiquity of the file with the virus identifiers.

Shows the list of predefined scans.

Shows the different scan areas found in the computer.

Shows the areas to be scanned according to the predefined scan selected.

Shows the two different startup scans offered by the antivirus..

To make a scan area disappear from the list of areas to be scanned, just drag the area over to the trash can.

Allows you to add an area selected from the tree to the list of areas to be scanned.

Allows you to remove an area from the list of areas to be scanned.

Allows you to completely empty the list of areas to be scanned.

Presents a report on the activity of the resident scan.

Shows the status of the resident scan and a summary of its activity.

Unloads the resident scan from memory.

Presents a report on the activity of the Internet scan.

Shows the status of the Internet scan and a summary of its activity.

Unloads the Internet scan from memory.

Allows you to indicate the frequency with which the scans will be performed: once, hourly, daily, weekly, monthly, or yearly.

Allows you to indicate the time at which the scan will start.

Allows to you indicate the latest time by which scanning must be completed. If it is not already finished by that time, it will be then be stopped.

Together with the option that permits you to indicate whether you want weekly, monthly, etc. scans, this allows you to define the frequency of the scans.

Indicates the date on which the validity of the scheduled scan begins.

Indicates the date on which the validity of the scheduled scan ends.

Allows you to enable or disable a scheduled scan.

Has the scan carried out whenever the computer is started up.

Has the scan carried out every certain number of computer startups, the number of which can be varied.

Has the scan carried out every certain number of days, the number of which can be specified.

Has the scan carried out only on certain days of the week.

Allows you to enable or disable a scan at computer startup.

If this option is enabled, the scan will be carried out only when Windows is started up.

If this option is enabled, the scan will be carried out whenever a Windows session is started.

Scans all files to which access is attempted.

Scans all files which are no longer going to be used and you therefore attempt to close.

Scans all files which you attempt to move or rename.

Scans all compressed files to which access is attempted.

Logs in the antivirus report all operations and incidents related to the resident scan.

Scans e-mail messages received from Internet.

Scans e-mail messages sent to Internet.

Scans compressed files found in any e-mail message received or sent.

Scans e-mail messages inside other mail messages regardless of the degree of nesting.

Logs operations and incidents produced during the Internet scan in the antivirus report.

Indicates that MIME encoded files found attached to e-mail messages should be scanned.

Scans all files received from Internet via HTTP (Web pages) or FTP (file transfer) protocols.

Scans all files sent to the Internet.

Scans all compressed files received or sent.

Scans all ActiveX controls or Java Applets contained in Web pages accessed.

Allows you to indicate the port used by the SMTP protocol, which is responsible for sending e-mail messages.

Allows you to indicate the port used by the POP3 protocol, which is responsible for receiving e-mail messages.

Allows you to indicate the port used by the FTP protocol, which is responsible for transferring files.

Allows you to indicate the port used by the HTTP protocol, which gives access to Web pages.

Indicates that the default profile configured in the Control Panel should always be used to show your mail in the antivirus and allow it to be scanned.

Whenever the antivirus is opened, you will be asked what mail profile you want to use.

Allows you to indicate a specific mail profile so that it is always used in the antivirus.

Indicates that e-mail folders should be shown as scannable areas in the diverse scans.

Indicates that network drives should be shown as scannable areas in the diverse scans.

Indicates that CD-ROM drives should be shown as scannable areas in the diverse scans.

Allows you to indicate the maximum size of the report recording antivirus activity to prevent it from growing excessively.

Indicates that the update is located on diskette, a CD-ROM, or a local network drive. It also permits you to indicate the specific location of the update.

Indicates that the update is to be carried out from the Internet. The address as well as a user name (login) and password should be provided for proper identification.

Allows the update to be configured so that the antivirus updates itself automatically and regularly.

Allows you to configure the frequency with which the automatic updates will be carried out.

Causes the update to be carried out at the time specified.

Shows the list of events to which a sound can be associated.

Allows you to indicate a specific sound to be associated to an event. The Browse button allows you to easily choose any sound file you possess.

This button reproduces the specified sound, allowing you to check that it is correct.

List of the different parts of the program that may be protected if a password is set.

Here you should enter the password you want for the selected areas.

Allows you to change the password.

Allows you to indicate the port used by the NNTP protocol, which manages the newsgroups.

If checked, the blocking of Internet addresses will be enabled in order to prevent access.

Clicking here takes you to the list where you can insert and remove the Internet addresses to be blocked.

If checked, you will be asked before an address is blocked.

Enter the address to block.

List of addresses to be blocked.

The last address to be entered will be added to the list.

Removes the selected address from the list.

Leaves the entire address list blank.

Clicking here takes you to the list where you can select the Internet services you wish to block.

If checked, the blocking of Internet services will be enabled in order to prevent their use.

List of services to be blocked. To select a service, click on the box that appears to its left.

If checked, you will be asked before a service is blocked.

Allows you to send a message to a selected workstation.

Enter the message that will be sent to the workstation.

Enter the name of the workstation that will receive the message.

Allows you to send a message to a selected domain.

Enter the name of the domain that will receive the message.

Enter the message that will be sent to the domain.

Enter the name of the server through which warning messages will be sent.

If checked, the database of detectable viruses will be updated.

Specify the time that should elapse between one update and the next.

Choose the day the update should be performed.

Enter the hour, minutes and seconds the update will be performed.

If selected, both the updates of the virus database and the antivirus components will be checked.

If selected, a check of both Updates and Upgrades will be carried out upon running the antivirus.

Restores the default values.

Restores the initial configuration values of the antivirus, regardless of the changes that have been made.

This button permits you to configure immediate scans.

If checked, the selected items will be scanned when the program is started.

Permits you to configure the characteristics of the scan that will be carried out when the program is started.

If checked, the permanent scanning feature will be enabled.

This button permits you to configure the actions to take with permanent scans.

This button permits you to configure when the update will be performed and from where.

If checked, the permanent file scan will be enabled.

This button permits you to configure the behavior of the permanent file scan.

If checked, the permanent Internet scan will be enabled.

This button permits you to configure the behavior of the permanent Internet scan.

If checked, the permanent Lotus Notes database system scan will be enabled.

This button permits you to configure the behavior of the permanent Lotus Notes database system scan.

Scans Lotus Notes documents that are found within other documents.

The scan will be paused if an unexpected error is produced. By accepting the warning, you can continue scanning.

Warns other networked computers if a virus is detected.

After a certain period of time, the warning message produced will be deleted.

Time that should elapse between receiving the warning message and deleting it.

Type of protocol used to send warning messages: MAPI or SMTP (outgoing mail).

The names of the users that should receive the warning message are entered, separating each name with a comma.

The user that created the infected document is warned about the detection.

The user working with the infected document is warned about the detection.

Message text that will be sent to warn about the detection.

Enables the sending of messages in Lotus Notes systems when a virus is detected.

This button permits you to configure the warnings that will be sent in Lotus Notes systems.

The report will only display the incidents that coincide with the type of scan selected from the list.

The report will only display the incidents that have occurred in the program selected from the list.

The report will only display the incidents (events, situations or actions) that coincide with those selected from the list.

Permits you to determine the criteria used for comparison, when filtering by date, between the Start Date and End Date fields.

This value will be the only date used for comparison or as the first in a range of dates, depending on the criteria selected in the Date list.

This value will be the last in a range of dates when "Between" is selected from the Date list.

If a proxy server is used to connect to the Internet, this allows you to determine the characteristics of the proxy used, as well as the user's details.

The proxy's IP address used to connect to the Internet.

Number of the proxy's communications port used to connect to the Internet.

User name that will be authenticated before connecting to the Internet via a proxy server.

User password that will be authenticated before connecting to the Internet via a proxy server.

Permits you to enable the time (weeks, days, hours) that should elapse between scheduled tasks.

This number indicates every how many hours, days or weeks the scheduled update should be performed.

Specifies that Lotus Notes databases be displayed as scannable items when performing different scans.

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.

Path through which updates should be carried out. By default, the CD-ROM root directory (D:\).

Internet address where the update files are located.

Identifier or username assigned to each user so that he/she can update through the Internet.

By enabling this option you will be able to configure the Internet connection through the proxy server.

By checking this option, files with no extensions will also be scanned.

This allows you to specify the start date for a scheduled task.

This allows you to specify the end date for a scheduled task.

Lists the types of virus which will be shown (All types. Program, Boot, Macro, and Common).

Select a virus from the list to see its characteristics.

Type in the name of a virus which you would like more information about.

A resident virus infects the memory of the computer. From there it continually checks the operations carried out with the files which it should infect. If one of these files is executed the virus infects it.

Concealment. Stealth viruses try to get by unnoticed. They avoid showing their effects in the infected files.

Encrypted viruses (or encoded viruses) infect in a different way, modifying its signature (identifiers used by the antivirus) every time. This makes it difficult to detect.

This type of virus does not respect the data in the files it infects. It loses the information (overwrites it) thereby corrupting these files.

As well as encrypting its signature in all infections, this virus also modifies the mode of infection (routine or algorithm) every time. By doing this it creates different versions of itself.

If there is a progam with an EXE extension, the virus copies it with the same name and the extension COM. When the file (with the same name) is executed, the operating system executes the file with the extension COM (the virus).

When you click on this button the information about the virus selected from the list will be printed.

When you click on this button all the antivirus information about the virus identification file (virus signature file) will be displayed.

When you click on close you will go back to the antivirus main screen.