

Help/About AntiVir

{button ,AL('rtoHelp',0,'')} Related topics

This windows provides details of the version number and copyright, the name of the license holder, the serial number and the H+BEDV Datentechnik GmbH hotlines.

Hotline / further product information

If you require technical support, product information or other information, you can reach us at one of the addresses given in this section:

General information

H+BEDV Datentechnik GmbH
Lindauer Straße 21
88069 Tettnang
Germany

Telephone: +49 (0) 7542 - 500 0
Fax: +49 (0) 7542 - 525 10

Internet: <http://www.hbedv.com>
Email: info@hbedv.com

Technical support

Internet: <http://www.hbedv.com/support/support.htm>
Email: support@hbedv.com

Suspicious files

Unknown new Malware so as suspicious files can be sent as an encrypted archive (ZIP, RAR etc.) in the attachment of an email to the following addresses:

virus@hbedv.com
dialer@hbedv.com
heuristic@hbedv.com

Please don't forget thereby to send the password for the archive and a small description of the file or of the appeared phenomena.

To the AntiVir Personal Edition Users:

Technical inquiries via Phone/Fax/Letter and e-mail can not be answered!

In order to facilitate your inquiries to the technical support, we have created an Internet Support Forum for you.

You find the AntiVir Support Forum on the internet at: <http://www.free-av.de/forum>.

You will find the frequently asked questions about AntiVir Personal Edition and you will have the possibility to submit technical questions to all other forum members and our moderators. Additionally, you can discuss with other users of AntiVir and share your own experiences and hints.

Options/Action after search

(AntiVir Professional only)

{button ,AL('toOptions',0,'')} Related topics

In this index card, you can specify the name and command line parameters of any program you want AntiVir to start automatically on detecting a virus or unwanted program.

Program name (Alt+P)

Enter the full name of the program you want to start after a scan here (drive, path filename and extension). This program will only be started if at least one virus or unwanted program is detected. Using the folder button, you can scroll through the directories in the usual way and select your target folder and program.

Arguments (Alt+A)

You can enter any command line parameters for the program you want to start here.

This dialog window contains the following buttons:

{button OK.}

Transfers the data from the 'Action after search' window and then closes it.

{button Cancel.}

Closes the dialog window without transferring the new settings.

{button Help.}

Displays this help text.

Backup

And now to one of our perennial topics: backups.

Comprehensive backups can mean the difference between half a day's work and a major disaster. The operating system and programs are the lesser evil, however, as these can all be re-installed from the original data carriers. Far more important are your own files, as these will be irrecoverable without a backup.

Please don't forget: **AntiVir can 'only' remove viruses/unwanted programs: it cannot rectify the damage caused by harmful programs.** This is your own responsibility. Think about it honestly: when did you last do a backup and what would you do if your hard disk gave up the ghost right now?

Data **must** be saved regularly and you **must** make sure your sequence of backups is complete. Vital data such as databases or important texts should be saved twice: after all, without backups, there is no way of restoring irreplaceable data.

BIOS

Basic Input/Output System. This term is generally used to refer to the operating system routines in the ROM. These are the core routines of the operating system, which are adapted to the installed hardware modules. The BIOS is responsible for carrying out the memory test, initialising the ports and keyboard and booting the operating system from the floppy or hard disk, for example.

Boot Record

This is the first record of the operating system to be loaded from a floppy or hard disk and executed. The program code of this record is responsible for loading the operating system.

Boot Record Virus

This type of virus attacks the boot record.

As a rule, boot record viruses only infect floppy disks: in the case of hard disks, it is normally the master boot record which is infected. Boot record viruses are transmitted by booting with an infected disk in drive A: or by starting a dropper or a program infected with a multipartite virus. If the virus is active, any inserted non write-protected disk will be infected on entry of a `DIR A:-` or `DIR B:` command!

In most cases, the boot record virus moves the original boot record to a backup area before writing its own program code in the boot record. This means that, when you start up the computer, the code of the boot record virus will be activated first, which in turn loads and executes the program code of the original boot record. Boot record viruses are normally identified from a reduction of the main memory, i.e. the computer only appears to have 638 or 639 KB of DOS memory left instead of 640 KB (655,360 bytes).

Scan/Boot Records

{button ,AL(`rtoScan',0,'')} Related topics

The selection window 'Drives' allows you to select the drives whose boot record you wish to test. The boot records of the highlighted drives will then be scanned for viruses when you click on the 'Scan' button. If one of the highlighted drives is a hard disk, the master boot records of all hard disks will also be scanned in addition.

The 'Boot Record Test' dialog window contains the following buttons:

{button Scan,}

This button is active when at least one drive is highlighted. Clicking on this button will trigger an immediate scan for boot record viruses in the highlighted drives.

{button Close,}

Closes this window and transfers the entries.

{button Report,}

Clicking on this button enables you to view the report file on the last scan started from this window. This option is only activated once a scan has been initiated.

{button Help,}

Displays this help text.

Display Recognition List

This shows you a list of the viruses and unwanted programs detected by AntiVir.

Help

Display this help.

Internet Update

This is where the AntiVir Internet Updater is started.

With this program, you can load new updates from the Internet.

You find assistance for configuration under [Options/Internet Updater](#).

Report

Opens the main window of AntiVir Report containing the last report file created.

[Further information about report.](#)

Scan Options

Here you can select the options to be used by AntiVir for the scan. Further information on the wide range of possible configurations can be obtained by calling the help function of the relevant index cards via the 'Options' window.

Start Scan

If you click on this button,
AntiVir will start a scan.

This button is only active once you
have selected a drive, directory or
file.

Start Scheduler

This is where the AntiVir Scheduler is started. With this program, you can specify the times when you want AntiVir to start an automatic scan.
For further information, call the Scheduler help function.

Command Line

AntiVir offers you several command line parameters which can be useful in certain situations, e.g. for adapting the software to your computer environment or overcoming problems with particularly stubborn viruses.

You can change these parameters by clicking the AntiVir icon on the desktop. Now press the right mouse key and select 'Properties' from the Context menu. Then select the 'Link' index card and enter the desired parameters in the 'Target' box after the program name.

Alternatively, you can start AntiVir together with the desired command line parameters from a DOS box: simply switch to the installation directory of AntiVir and enter the program name and parameters `ANTIVIR /<PARAMETER>`.

Description of command line parameters

/AF

Highlights all floppy disk drives in the drive list. The drive settings in the `AVWIN.INI` file are ignored.

/AH

Highlights all hard disk drives in the drive list. The drive settings in the `AVWIN.INI` file are ignored.

/AN

Highlights all network drives in the drive list. The drive settings in the `AVWIN.INI` file are ignored.

/B

The automatic batch mode is only terminated if viruses/unwanted programs are found in the memory or if a boot record or master boot record is infected. Otherwise, this mode will operate just as if you had selected "Record in Report File Only" under Options/Repair. You should always specify a name for the report file, however.

/BASK

Automatic batch mode which takes into account the settings of AntiVir. If you have specified, for example, that all detected viruses/unwanted programs should be repaired automatically, this will be carried out accordingly.

If you select this parameter together with the parameter `/B`, the latter will be ignored.

/BASK+

This parameter is identical to `/BASK` except that in this case statistical information is displayed at the end of the scan.

/CLA

Closes the report file after every write access.

This parameter is solely for support purposes; you should only use it if instructed to by `H+BEDV`, as the constant opening and closing of the report file impairs the performance of the software.

/DY

This parameter is only effective in batch mode, i.e. one of the parameters `/B`, `/BASK` or `/BASK+` has to be set in addition. If no viruses/unwanted programs were found and the scan was terminated normally (i.e. not aborted), AntiVir will save the current date in a date log file (`AVWIN95.DLG`). If

AntiVir is then started again on the same day with the same parameters, only the self-test will be carried out. On the following day, the scan will be repeated in all cases according to the specified parameters the first time you start AntiVir.

/DYNoMsg

This parameter is identical to /DY, except that no message is generated on termination after the self-test.

/FF

Indicates a full scan of the relevant files.

/IM

This parameter allows you to specify under 'Options/Miscellaneous' whether you want reported files to be moved to the INFECTED directory of AntiVir before being repaired. If you started AntiVir without this parameter, the relevant settings will not be available.

/NB

This parameter prevents searching the bootsectors of your system. This parameter should only be used, if there are problems with any bootsector.

/NOCOPYVIR

By default, AntiVir will suggest that you copy certain viruses/unwanted programs to a floppy disk and send them in to us for quality assurance purposes. If you want to suppress this message, you should set this parameter.

/NOESC

Prevents a scan from being stopped by deactivating the 'Stop' button in Luke Filewalker. This parameter has the same function as the setting 'Stop Scan' in Options /Miscellaneous.

/NONETDRV

No network drives are displayed in the drive list of AntiVir.

/NOUMB

Deactivates the memory test in the UMA (between 640K and 1MB).

/NOHMA

Deactivates the memory test in the HMA (between 1024K and 1088K).

/NS

Suppresses the opening screen when you start AntiVir.

/R0

Prevents a report file from being generated. This parameter is only effective in conjunction with the parameter /B, and should only be used for test purposes.

X:

Stands for a drive letter. In this case, the settings for the drives in the AVWIN.INI file are ignored and only the drives specified in the command line are scanned. A maximum of 26 entries are possible here.

Contents

[About AntiVir](#)
[Action after search](#)
[Backup](#)
[BIOS](#)
[Boot Record](#)
[Boot Record Virus](#)
[Boot Records](#)
[Button Display Recognition List](#)
[Button Help](#)
[Button Internet Update](#)
[Button Report](#)
[Button Scan Options](#)
[Button Start Scan](#)
[Button Start Scheduler](#)
[Command Line](#)
[CRC](#)
[CRC Definition](#)
[CRC/CRC Files](#)
[CRC/CRC Files/Insert](#)
[Delete Summary Report](#)
[Demo Version](#)
[Dialer Found](#)
[Display Summary Report](#)
[Download](#)
[Drag&Drop](#)
[Exit AntiVir](#)
[Extensions](#)
[Extensions/Insert](#)
[FAQ](#)
[File Viruses](#)
[Game detected](#)
[Help \(Contents\)](#)
[Heuristic](#)
[Important Notes](#)
[Internet Updater](#)
[Intranet Update](#)
[Keyboard Commands](#)
[License File](#)
[Load License File](#)
[Luke Filewalker](#)
[Main Window](#)
[Master Boot Record](#)
[Master Boot Record Virus](#)
[Miscellaneous](#)
[Multiple Licence](#)
[Network Warnings](#)
[Network Warnings \(XP\)](#)
[Options \(Contents\)](#)
[Partition Table Discrepancy](#)
[Password](#)
[Profiles](#)
[Profiles \(Contents\)](#)
[Profiles tab](#)

[ReadMe](#)
[Recognition List](#)
[Repair](#)
[Report](#)
[Report \(Contents\)](#)
[Report Delete](#)
[Report Display](#)
[Report Print](#)
[Report/Summary Report](#)
[Report/Warnings](#)
[Save Settings](#)
[Save Settings on Exit](#)
[Save System Files](#)
[Scan \(Contents\)](#)
[Scheduler](#)
[Search](#)
[Search/Archives](#)
[Search/Boot Records](#)
[Search/Omit Files](#)
[Start scan](#)
[Status](#)
[Tools \(Contents\)](#)
[Unwanted Programs](#)
[Unwanted Programs \(Selection\)](#)
[Update Drive List](#)
[UpdateWizard](#)
[Verifiably Clean DOS Disk](#)
[Virus Found](#)
[Virus Information](#)
[Viruses and other malware](#)

Options/CRC

(AntiVir Professional only)

{button ,AL('toOptions',0,'')} Related topics

This index card allows you to define the mode for the CRC calculation. Inputs are only accepted if the 'Calculate Checksums' box is activated.

During the CRC test, only files are accepted in the CRC database, in which no viruses as well as no unwanted programs were found!. If AntiVir detects an concerning file which has NOT been repaired, no CRC sum will be calculated for that file.

Whenever it has to calculate the CRC sum, AntiVir creates a CRC database in the root directory of each drive (using the filename entered under 'Database Name' or found automatically by AntiVir).

Calculate checksum (Alt+C)

This option activates the function 'Calculate CRC Sums', assuming you have specified a valid database name for the CRC file. If you have confirmed this option with (OK) without entering the name of a database, AntiVir will remind you to do so and display the CRC index card again.

Database name (Alt+D)

This is for entering the filename under which the CRC calculation data are to be stored. A default name is not provided for this file, as it could be manipulated e.g. by viruses. A CRC file with this name is stored in the root directory of each drive.

Since the database format is compatible with AntiVir for DOS, you can still use the old CRC database.

If no database name exists, AntiVir will search all available hard disks for a CRC database when the program is started. If a valid database is found (this includes databases generated under AntiVir for DOS), the name of this file will be used as the database name.

Confirm changes (Alt+O)

In this mode, every change to the CRC sum is reported with one exception: if the box 'Record in Report File Only' is activated in the dialog window Options/Repair, any change to the CRC sum will merely be recorded in the report file. You can tell when this is the case because the 'Confirm Changes' box is deactivated.

Mode

There are two modes available for calculating the CRC sum: In 'Turbo mode' (Alt+T), only part of the file in question is used to calculate the CRC sum. If 'Whole file' (Alt+H) is selected, the CRC sum will be calculated for the entire file.

The 'Turbo Mode' is sufficient in most cases, and is much quicker than calculating a CRC sum for an entire file. If a new entry is added to the CRC database, however, this setting won't make any difference, as both CRC values will then have to be calculated.

This dialog window contains the following buttons:

{button CRC files,JI('','OPTIONEN_CRC_FILES')}

If the 'Calculate Checksums' box is activated, this button can be used to open a window in which to specify the files to be included in the CRC calculation.

{button OK,}

Closes the dialog window and transfers the current entries. If 'Calculate Checksums' is activated, a

database name must be entered, otherwise an error message will appear reminding you to do so.

`{button Cancel.}`

Closes the dialog window without transferring the new settings.

`{button Help.}`

Displays this help text.

CRC

(AntiVir Professional only)

CRC (Cyclic Redundancy Check) is a method of calculating checksums. By generating a checksum and storing it in a database on a virus-free computer, AntiVir is able to compare it with a subsequently generated checksum. If the computer is infected with an unknown virus, for example, this will be revealed by the checksum comparison.

In the menu Options/CRC, you can choose whether, how and for which files you wish to use the CRC method.

Options/CRC/CRC Files

(AntiVir Professional only)

{button ,AL('toOptions',0,'')} Related topics

This index card allows you to define the settings for the CRC files.

You can choose whether to subject all files to a CRC test or only program files.

If you have selected 'All Files', you will find that AntiVir reports changes to the CRC sum more frequently because you are working continuously on your computer and probably changing your text files, for example. If there are no suspected viruses/unwanted programs, you should update the CRC sum whenever a change is reported.

If you have selected 'Program Files', AntiVir will suggest a list of the most common extensions. You can of course also adapt these extension to your own file system as described later on. If a CRC change is reported in this mode, you should consider whether or not you have modified the relevant file (e.g. by updating your development environment, in which executable files are often recompiled). If not, compare the relevant file with the original (on disk or CD). If you find a discrepancy here, e.g. in the length of some executable file, this could be due to a virus or unwanted program.

In the 'CRC Files' window, you can enter the names of files you wish to exclude from the CRC calculation in the group box 'Omitted Files'. This is advisable in the case of files which are frequently modified (e.g. in the development/design sector). To add a file to this list, click on the 'Insert' or 'Browse' button. To delete a file, highlight the file and click on the 'Delete' button.

If you have entered a filename together with its full path, only this particular file will be omitted from the CRC test; if you enter a filename without a path, all files with this name (regardless of path and drive) will be omitted.

This dialog window contains the following buttons:

{button Extensions,}

This button opens a dialog window in the 'Files' group box containing all file extensions to be scanned during the CRC calculation in the 'Program files' mode.

{button Insert,JI('','OPTIONEN_CRC_INSERT')}

If you click on this button, a dialog window will appear in which to enter the name of the files you want to omit.

If you only enter one filename, AntiVir will exclude *all* files with this name from the CRC calculation, whether on drive C:, D: or A:. If you only want one *specific* file with this name to be omitted from the CRC calculation, you must enter its complete path.

{button Browse,}

If you select this function, a dialog window will appear to help you search a data medium for the files you want to omit. Use this button if you don't know the exact path or name of the file you want to omit.

{button Delete,}

Deletes the highlighted entry from the list of files to be omitted. This button is only active if an entry is highlighted.

{button OK,}

Closes the dialog window and transfers the current entries. If 'Calculate Checksums' is active, you

must enter a database name, otherwise an error message will appear reminding you to do so.

`{button Cancel,}`

Closes the 'CRC files' window without transferring the new settings.

`{button Help,}`

Displays this help text.

Options/CRC/CRC Files/Insert

(AntiVir Professional only)

{button ,AL('toOptions',0,'')} Related topics

If you click the button 'CRC files', a dialog window will appear in which to enter the names of the files you want to omit.

If you only enter one filename, AntiVir will exclude *all* files with this name from the CRC calculation, whether on drive C:, D: or A:. If you only want one *specific* file with this name to be omitted from the CRC calculation, you must enter its full path and name.

This dialog window contains the following buttons:

{button OK.}

Transfers the data from the 'Enter files to be omitted' window and then closes it.

{button Cancel.}

Closes the dialog window without transferring the new settings.

{button Help.}

Displays this help text.

Report/Delete Summary Report

{button ,AL(`rtoReport',0,`,`')} Related topics

Deletes the file containing the summary report information. If you select this menu option, a dialog window will appear asking you whether you really want to delete the summary report. This function is only active provided such a file is available.

Caution: The entire list is erased in all cases: this method cannot be used to delete individual entries from the list!

Demo Version

If you have installed AntiVir as a demo version (i.e. without a valid license file), the program will be subject to the following restrictions:

- * AntiVir only scans the first directory branch
- * AntiVir only repairs files in the directory 'AVTest', which has to be created in the AntiVir directory by the user himself
- * AntiVir does **not** repair boot records
- * All network options are deactivated

Dialer Found

AntiVir has found a dialer.

Unlike computer viruses, dialers are not normally capable of damaging or modifying files. As a rule, they cannot enter data in the registry either. They usually copy themselves in the form of an .EXE file to C:\Windows, C:\Windows\System\ or the desktop, thereby (with some exceptions) creating a link to the start menu. In some cases, entries may be made in the start menu itself (Start - Programs - Autostart).

If you have activated the option Dialers under Unwanted programs in the configuration menu of AntiVir, you will receive a warning whenever AntiVir detects the item.

Report/Display Summary Report

{button ,AL('rtoReport',0,'')} Related topics

This window tells you when your computer was scanned by AntiVir and what the results were. If a scan was aborted by the user, this is indicated by a (*) at the end of the line. If an entry is marked ✓, this means that AntiVir was unable to find a virus or unwanted program in this scan. An entry marked → on the other hand means that a virus or unwanted program was detected. To obtain further information on a particular entry, simply double-click on the entry.

This dialog window contains the following buttons:

{button Close,}

Closes the window 'Summary report' without transferring the changes.

{button Delete,}

Deletes all entries in the summary report without any further prompting.

{button Help,}

Displays this help text.

In the dialog window Options/Summary Report, you can also specify how many entries are to be stored. If the maximum number of entries is exceeded, the corresponding number of entries are deleted from the top of the list. Under 'Output File', you can specify the name of a file in which to store the summary report data. By default, AntiVir will suggest the name AVWIN.ACT.

Download

Obtaining files from the internet or from mailboxes and storing them locally on your computer.

Options/Drag&Drop

{button ,AL('toOptions',0,'')} Related topics

In this index card, you can define the settings for the drag&drop and profile features. The drag&drop feature enables you to move files and directories to the main window of AntiVir.

If you want to scan individual directories or files on a regular basis, you can create a profile for this purpose.

Scan subdirectories (Alt+S)

If this function is selected, all subdirectories will be scanned whenever you move one or more folders from Windows Explorer to the main window of AntiVir. If this option is not activated, the folders will only be scanned on the directory level which you have dragged and dropped to the main window of AntiVir.

Files

(AntiVir Professional only)

All files (Alt+D)

By default, AntiVir looks for executable files only. If this menu option is selected, all files in the folder you have dragged and dropped to the main window of AntiVir will be scanned, including non-executable files.

AntiVir takes longer for this type of scan, as there are far more files to get through. When 'All Files' is active, the 'Extension' button cannot be selected.

Files listed in 'Options/Search/Files/Extensions' (Alt+O)

This function is used to scan only the files you have previously set in the menu Options/Scan/Files/Extensions.

Program and macro files (Alt+G)

If this function is selected, AntiVir will only scan the relevant folder for files with specified extensions (e.g. *.BIN, *.COM, *.EXE, etc.). Default values are given for these extensions, and can be changed in a window opened via the 'Extensions' button.

If this option is activated and you have deleted all entries from the file extension list, the words 'NO EXTENSIONS' will appear below the Extensions button.

This dialog window contains the following buttons:

{button Extensions,JI('','OPTIONS_SCANNER_EXTENSIONS')}

(AntiVir Professional only)

If the function 'Program Files' is activated, this button can be selected. The dialog window File Extensions will then appear, in which you can enter the extensions of the files to be scanned directly.

{button OK,}

Transfers the data from the 'Drag&Drop' window and then closes it.

{button Cancel,}

Closes the dialog window without transferring the new settings.

{button Help,}

Displays this help text.

Scan/Exit AntiVir

{button ,AL(`rtoScan',0,'','')} Related topics

To exit AntiVir, you can either select 'Exit AntiVir' under the menu option 'Scan', click the H+BEDV Datentechnik GmbH symbol in the top left-hand corner and scroll to the 'Close' command, or use the usual key combination 'Close' (Alt+F4).

If the menu item Options/Save Settings on Exit is activated, all settings will automatically be saved in the AVWIN.INI file. If this item is not active and settings have been changed, AntiVir will ask you whether you want to save these changes before exiting.

Extensions

{button ,AL('rtoOptions',0,'')} Related topics

By default, AntiVir scans program files only. The extensions of the program files are displayed in the 'File Extensions' window. The list in this window contains the extensions of the most common program files and documents which may contain macros. If you have installed program files or documents with different extensions on your computer, add these extension to the list (click Insert button).

Please do not enter the extensions of any non-executable files, as this will impair the scanning performance of AntiVir.

The 'File Extensions' window contains the following buttons:

{button OK.}

Transfers the data from the 'File extensions' window and then closes it.

{button Cancel.}

Closes the window without transferring the current settings.

{button Insert,JI('','OPTIONS_SCAN_INSERT_EXT')}

Inserts a new file extension. See under Insert.

{button Delete.}

Deletes the highlighted file extensions.

{button Default.}

If you press this button, the existing entries are deleted and the most common extensions are inserted in the file extension list (default setting).

{button Help.}

Displays this help text.

Extensions/Insert

{button ,AL('rtoOptions',0,'')} Related topics

If you select the 'Insert' button, a dialog window will appear in which to enter file extensions for the AntiVir scan. You can enter a maximum of 255 characters here, remembering to leave out the dot. Illegal characters are not accepted.

You may add extensions to the list of existing extensions. After confirming the changes by clicking OK, the changes are taken into effect for the next scan.

This dialog window contains the following buttons:

{button OK.}

Transfers the data from the 'Insert extensions' window and then closes it.

{button Cancel.}

Closes the dialog window without transferring the new settings.

{button Help.}

Displays this help text.

FAQ

[When should I carry out virus scans?](#)

[How do I remove viruses?](#)

[AntiVir cannot remove the Form virus from the hard disk](#)

[AntiVir is unable to repair certain files](#)

[AntiVir is unable to create certain files](#)

[I keep getting warnings when working in a network!](#)

[AntiVir has found viruses in the Windows swap file](#)

[Virus in the memory, but not after booting from a floppy disk](#)

[Virus in the memory even after booting from a floppy disk](#)

[AntiVir and network card drivers](#)

When should I carry out virus scans?

Always. Think of it like a car: This too is monitored in various ways - oil change, inspection and MOT, plus the occasional check-up on the indicators and lights. Similarly, you should run a standard scan on the hard disk every day. This will check executable program files (.COM, .EXE etc.) in turbo mode, and is roughly equivalent to the oil change in your car. The weekly scan of all executable program files can be likened to the inspection. Finally, there is the monthly MOT, when all files should be checked (select parameter 'All Files'). And don't forget to check all floppy disks for viruses, of course. By the way, if you always perform the light and indicator test before starting the software, you can get AntiVir to scan your DOS file with the command line parameter /B.

How do I remove viruses?

Easy: with AntiVir. Joking apart, please always boot your computer system before a possible decontamination from your good old 'verifiably clean DOS disk'. Start Windows using the 'verifiably clean Windows disk'. Then reinstall AntiVir and run it over the data medium in question. In the case of a boot record or master boot record virus, you can carry out repairs directly with AntiVir (except Form on the hard disk; for this, please use the command 'SYS C:'). In the case of a file virus, scan and repair the entire hard disk using the default options of AntiVir (program files only). Now repeat the process in scan mode only (without repairs) using the parameter 'All Files'. If AntiVir still encounters any anomalies, these could be viruses but are not necessarily. AntiVir only distinguishes internally between .EXE and non-.EXE files, and overlays with unusual filename extensions might also be infected. Please check this before repairing. The third step is the most tricky, and requires you to run AntiVir in enhanced scanning mode (/FF) over the data medium in question. In this mode, many of the security prompts are deactivated. This can lead to false alarms (unlikely, but possible). AntiVir now searches for corrupt files and mutations. Corrupt files are particularly important. Many viruses are so badly programmed that they don't even infect the file properly in all cases. Sometimes only part of the virus is copied to the file, sometimes only the first 10 bytes are modified, sometimes the virus overwrites bits of the file randomly with itself, sometimes it only modifies the program entry without copying itself to it - the list is endless, and provides another challenge for AntiVir. IF AntiVir reports anything abnormal in this mode, check these files particularly carefully and compare the reported program files with the originals.

AntiVir cannot remove the Form virus from the hard disk

Yes - AntiVir refrains from repairing the boot record (but not the master boot record) of a hard disk to be on the safe side. This is because you can also get rid of this virus yourself. Boot from a clean DOS disk containing the same operating system as that installed on your hard disk (very important!). This disk should also contain the file SYS.COM or SYS.EXE. After booting from this disk, please enter the command 'SYS x:', whereby 'x' stands for the drive letter of your hard disk. Since this is presumably 'C', the command should read: 'SYS C:'. The SYS command now transfers both system files (IBMBIO.COM and IBMDOS.COM or IO.SYS and MSDOS.SYS) to the hard disk and creates a new boot record (not a master boot record!). This overwrites the old, infected boot record and that's

all there is to it.

AntiVir is unable to repair certain files

This probably also depends on the setting 'Path for Temporary Files'.

AntiVir creates a copy of the reported file prior a repair, and repairs this file - the original is never repaired, because a file that has been affected by viruses or unwanted programs several times, later, it could turn out that the file is not repairable. Or there might be a power failure while the FATs or directories are being updated, in which case there might be nothing left at all. Only after a successful repair is the repaired, temporary copy copied back again, thus overwriting the previously concerning file. For this temporary copy, the path indicated under 'Options/Miscellaneous' is used. If you booted your computer system from a 'verifiably clean DOS disk' prior to a repair routine, the 'Path for Temporary Files' should point to 'A:\'. If you change the path to an existing, empty folder (e.g. C:\TEMP), the prompt will be suppressed.

AntiVir is unable to create certain files

This probably depends on the archive files .ZIP, .PAK or .ARJ. AntiVir cannot unpack the files contained in the archive files into the memory. They are therefore physically unpacked into the path indicated under 'Options/Miscellaneous', 'Temporary Path'. If this path is non-existent or invalid, AntiVir will abort the unpacking procedure for this file, so please set the temporary path to a valid (preferably empty) folder. Attention: this setting is stored in the file AntiVir.INI.

I keep getting warnings when working in a network!

This is probably due to files which AntiVir is not allowed to access because they have been barred by the network software itself. As a result, neither AntiVir nor a virus can get to these files. Printer queues are another example of this.

AntiVir finds viruses in the Windows swap file

It is possible for viruses to be found in the Windows swap file. In this case, however, the problem is usually due to other relocated antivirus programs whose unencrypted search strings have now turned up in this file. Remedy: change swap file to a temporary file, close the relevant programs prior to scanning and create a new swap file after running a defragmenter (with the option Clear Free Clusters if necessary).

Virus in the memory, but not after booting from a floppy disk

AntiVir finds a virus in the memory after booting from the hard disk but a scan conducted after rebooting from a 'verifiably clean DOS disk' yields no results. In this case, try to find out which program call prompts AVScan to report the virus by 'REM'ing or working through CONFIG.SYS or AUTOEXEC.BAT line by line. If this fails, check WIN.INI as well, as well as any programs registered in the Windows autostart program group. These are usually other antivirus programs or resident virus guards. Sometimes it helps to optimise or compress the hard disk. From DOS 6.0 upwards, you can at least work through the entries of CONFIG.SYS step by step instead of line-by-line 'REM'ing. For this purpose, press the key F8 when booting the computer system, then select the 'Individual Confirmation' mode. DOS 6.20 also allows line-by-line processing of AUTOEXEC.BAT.

Virus in the memory even after booting from a floppy disk

You are informed of a virus in the memory despite having booted from a 'verifiably clean DOS disk' in conjunction with a 'verifiably clean Windows disk'. Let's ignore for the moment the possibility that these system disks might be infected. AntiVir can only find what's actually in the memory, and if a signature is found, that means it really is there. The big question is how it got there in the first place. After a clean start from the emergency disks, you would assume no viruses to be active. This is in fact the case, but the infected master boot record of the hard disk has already been read into the memory (buffers, SmartDrive) by DOS. In other words, DOS only interprets the read-in data: this

doesn't mean the virus is active. AntiVir makes no distinction here, however - a signature is a signature. As to the question of how the master boot record of the hard disk came to be in the memory, there are two possible explanations: firstly, drive 'C:' was accessed during the booting procedure while processing the file CONFIG.SYS or AUTOEXEC.BAT. This access could have been a DIR C: or the action of loading a program from the hard disk. Please check the start files and make sure no access to C: occurs. Secondly: your hard disk is normally stacked, double-spaced or compressed in some other way. Please press the left shift key when you start up your computer system: this will prevent the compression driver from being loaded and CONFIG.SYS or AUTOEXEC.BAT from being processed.

AntiVir and network card drivers

In the resident state, some network card drivers often call the interrupt 03 without cause, which is an absolute NO-NO. This probably means that the debugging routines have been omitted from these drivers, which not only makes them larger than necessary but also causes AntiVir to crash. This may be due to the hardware-emulating driver. We have heard from one customer who eliminated the problem by replacing the installed DLLNDIS.EXE of the Developer CD from Novell with the retail version.

File Viruses

These attack files. Depending on the option you have selected, AntiVir will offer to restore the infected file (if it is capable of repair) or delete it. If a file is irreparable, AntiVir will automatically offer to delete it.

Game detected

AntiVir has detected a game.

Computer games are intended for purposes of entertainment. They do not cause harm to files, nor are they designed to undermine the operability of computer systems. However, their presence is not always welcome: indeed, it may be undesirable if they take up valuable runtime and computer resources.

AntiVir is able to detect computer games. If you have activated the "Games" option under Unwanted Programs in the configuration menu, you will receive a warning whenever AntiVir finds one. In this case the game is literally up, giving you the chance to delete it if necessary.

Help (Contents)

{button ,AL(`rtoHelp',0,`,`')} Related topics

To obtain help on a particular topic, select one of the following options from the 'Help' menu:

Read Me (Alt+R)

This displays the current Read Me file, in which you will find important information on each new version of AntiVir. If you have any problems or queries regarding AntiVir, please consult this file. You should find the solution to your problem here in the vast majority of cases.

Context (F1)

'Contents' allows you to display the list of contents for the help file, and has the same function as the 'Help' button. The help function of AntiVir operates on the same principle as any other Windows tool.

Using Help (Alt+U)

This shows you a list of ways of using the Windows Help functions. You can obtain information on individual keywords by double-clicking the relevant entries.

About AntiVir

Under this menu option, you will find details of the version number and copyright, the name of the license holder, the serial number and the hotline numbers.

Options/Heuristic

{button ,AL('toOptions',0,'')} Related topics

This property tab contains the settings for the AntiVir virus heuristic.

Macro virus heuristic

AntiVir contains a very powerful macro virus heuristic, which is able to detect even unknown viruses, worms and trojans. This is done by analyzing the macro virus code and searching for typical virus actions and code fragments. If a macro fits into this pattern, it will be marked as suspicious.

If the repair is disabled, suspicious documents will be reported only. This means that AntiVir will not try to repair them. If repair is enabled, all macros are deleted.

Win32 file heuristic

AntiVir contains a very powerful heuristic for Windows executables, which may detect even unknown viruses, worms and trojans. If activated, you can decide which level of detection capabilities AntiVir should use.

Detection level low

With this setting, AntiVir false positives are minimized,

Detection level medium

This is the default setting.

Detection level high

Using this level, AntiVir detects almost all unknown viruses. There might be some false positives, however.

This dialog window contains the following buttons:

{button OK.}

Transfers the data from the 'Heuristik' window and then closes it.


{button Cancel.}


Closes the dialog window without transferring the new settings.


{button Help.}


Displays this help text.


Important Notes


 To create a verifiably clean DOS disk, format a new floppy disk on a guaranteed virus-free computer with the command '`format a: /s /u`'. Then copy all the important programs you need from '`FORMAT.EXE`' to '`KEYB.COM`'. Finally, write-protect the disk and keep it somewhere safe.


 The AntiVir CD-ROM is now bootable as from the beginning of 1999. This means that, in most cases, the 'verifiably clean DOS disk' is no longer necessary for restarting in a guaranteed virus-free environment. This is what the bootable CD-ROM is for:

 If the boot and master boot records on FAT16 or FAT32 drives are infected by a virus, it may no longer be possible to start the operating system. With the aid of the bootable CD-ROM from H+BEDV Datentechnik GmbH, these infected records can be repaired without using an external operating system.

 Beside repairing boot records, it is also possible to scan all file areas on FAT16 or FAT32 drives from the AntiVir CD-ROM immediately after booting.

 As a read-only medium, this CD-ROM also allows scanning in a guaranteed virus-free environment. Up to now, this has always required a 'verifiably clean DOS disk'. In many cases, however, this disk was either not generated on a guaranteed virus-free system or not readily locatable. Thanks to the self-booting AntiVir CD-ROM developed by H+BEDV Datentechnik GmbH, you now no longer have this problem.

 Since the CD-ROM also contains the AntiVir programs, you can now repair the infected operating system with AntiVir. In other words, you no longer have to go through the time-consuming process of reloading programs from floppy disks.

 Thanks to a boot manager on the CD-ROM, it is possible to boot on standard systems either from the CD-ROM or in the customary way from the hard disk without having to remove the CD-ROM from the drive.

For further information, please consult the page [Frequently Asked Questions](#).

Options/Internet Updater

{button ,AL('toOptions',0,'')} Related topics

The **Internet Updater** ensures that you always have the latest version of your AntiVir program at your disposal. With the Scheduler, you can specify whether and how often you want AntiVir to dial up to the internet in order to compare versions. You can define a set time or rota for this; otherwise, the Internet Updater can be started manually at any time. If an updated version or a new virus definition file of AntiVir is available, an update is performed automatically.

N.B.: The Internet Updater can be used at any time with an AntiVir **single license**. If you have a **multiple license** (for three or more users), the Internet Updater will need to be configured accordingly.

Installing the Internet Updater

Select the 'Configuration menu' under 'Options' in the AntiVir menu window. There you will find the menu item Options/Miscellaneous. If you click on this, some options including 'Use Internet Updater (plugin)' will appear in the dialogue window.

Use Internet Updater (plugin)

If you have activated this setting, you must restart AntiVir (for the first time only). Once you have done this, the new menu item 'Internet Updater' will subsequently appear in the 'Options' under 'Configuration menu'. The 'Internet Updater' symbol has now been added to the tool bar of the AntiVir main menu window:

If you press this button in the AntiVir main window, the Internet Updater will be activated. This enables you to update your AntiVir version or virus definition file automatically or manually at any time.

Internet connection and proxy server

This dialogue window contains information on the type of internet connection you are using.

Network- or modem connection established by Windows (Alt+N)

This setting is displayed if your internet connection takes place via a modem. The information window indicates that no remote data connections have been found.

The internet update program establishes the default connection (Alt+D)

This setting is displayed if your internet connection takes place via a suitably configured standard.

The internet update program establishes the following connection (Alt+F)

This setting is displayed if your internet connection is defined individually by you.

Connection via proxy server (Alt+X)

If your internet connection takes place via a proxy server, you can enter the relevant address path, port, login name and login password here (login name and login password - AntiVir Professional only)

Test the settings for internet connection and proxy server (Alt+T)

This function enables you to check whether the internet connection to the update server has been successfully established and the version information transferred from the server without error. If so, a dialogue window appears telling you that you can use the current settings for the internet update.

Allow automatic internet update downloads (Alt+U)

If you have selected this function, you can activate two different options under {button Settings,}:

Settings for automatic internet updates (Alt+S)

If you activate the option 'Allow automatic internet update downloads', you can enter other configurations via the dialogue box under {button Settings,}: you can 'Create desktop link to installation file ' and/or 'Terminate remote data connection after internet update'. And now you can also carry out a fully automatic update (e.g. as an entry in the Scheduler).

Create a link on the desktop for the downloaded installaton file (Alt+D)

If you have activated this function, you will be notified of a successfully completed full update on the desktop.

Hangup a dialup connection which was opened for the internet update (Alt+U)

If you have activated this function, the remote data connection established for the internet update is automatically interrupted again as soon as the download is completed.

Install automatic after download (Alt+I)

If you have activated this function, the setup will be established automatic after a successfull download.

Additionally this dialog window contains the following buttons:

{button OK,}

Transfers the data from the 'Internet Updater' window and then closes it.

{button Cancel,}

Closes the dialog window without transferring the new settings.

{button Help,}

Displays this help text.

Options/Intranet Update

(AntiVir Professional only)

{button ,AL('toOptions',0,'')} Related topics

In this index card, you can specify whether AntiVir is to be updated via the internet and if so how frequently.

For this purpose, AntiVir starts the Update Wizard; this now checks the path in which the current program files are centrally located on the server and copies any new source files to the AntiVir target directory on your workstation.

This function is only available with a multiple AntiVir license (for 3 or more users).

Intranet Update

Do not perform automatic update (Alt+D)

If this function is selected, AntiVir will not perform an automatic update.

Only search for new files every 'xxx' days (Alt+N)

If you only want AntiVir to search for new files every xth day, select this entry and enter the appropriate number of days in the input box.

Search for new files every 'monday, tuesday, ...' (Alt+F)

If you only want AntiVir to search for new files on a certain day of the week, select this option box and enter the chosen day.

Search for new files each system start

If you would like AntiVir to look for new files on each system start, select this option field.

Path containing source files (Alt+P)

Enter the path containing the current AntiVir files on the server here. If the data structure was retained on transferring the current files to the server, the current AntiVir files will be located in the folder Disk_1.

This source path might look like this, for example: \\SERVERNAME\VOLUME\UPDATES\AVWIN9x\DISK_1

If the directory structure of the AntiVir source files remains unchanged, the parallel folders, e.g. Disk_2, Disk_3, Admin, etc. will also be searched. In order to ensure a successful intranet update, it is essential to specify the update path Disk_1 correctly.

Path Containing license file

Here you can specify the path to a directory on the server via which to distribute new license files. For example, if the Update Wizard finds a new license file (internal generation date) in the specified directory, this will be installed automatically first and then used for the rest of the update procedure.

Hide copy dialog of update application (Alt+H)

If the Update Wizard is started from AntiVir, it will begin immediately by checking the source files. If you don't want the user to follow the progress of the update routine, you should select this setting.

This dialog window contains the following buttons:

{button More Help,}

Detailed information on how to install the Intranet Update Wizard can be found on the H+BEDV Datentechnik GmbH CD-ROM in the directory [\\[language\]\products\windows\workstat\setup\disk_1\admin.htm](#), which can be opened using this button.

{button OK.}

Transfers the data from the 'Intranet Update' window and then closes it.

{button Cancel.}

Closes the dialog window without transferring the new settings.

{button Help.}

Displays this help text.

Keyboard Commands

The following keyboard command and key combinations are used to activate the corresponding AntiVir functions:

| | |
|---------------|--------------------------|
| F1 | Call Help |
| F2 | Start Scan |
| F5 | Update Drives |
| ESC | Close Dialog Window |
| Alt+F4 | Exit AntiVir for Windows |

License File

On purchasing AntiVir, we will send you a license key - depending on the license model - in the form of the file HBEDV.KEY on disk or by email. This file tells AntiVir whether you are a registered user of the relevant product.

Full, unrestricted operation of this product is only possible once you have been registered.

The license file 'HBEDV.KEY' must be located in the same directory as your corresponding AntiVir program package. This file is either transferred to the correct directory at the appropriate point during the setup routine or by selecting the option 'Copy License File' in the 'Tools' menu afterwards.

If AntiVir is still started as a demo version after you have copied the license file, please check whether the correct version of AntiVir for your operating system is enabled. With your license key, you will also find a file called LIC_INFO.TXT which contains the following information on your license:

| | |
|----------------------|---|
| Product name | The full designation of the AntiVir package enabled by the license file. |
| Serial number | Indicates your serial number. |
| License type | Tells you which type of license is enabled. |
| Updates | Tells you which version number your license starts from and when it is due to expire. |
| License | The name of the user with whom the license agreement was made. |

Tools/Load License File

{button ,AL(`rtoTools',0,'')} Related topics

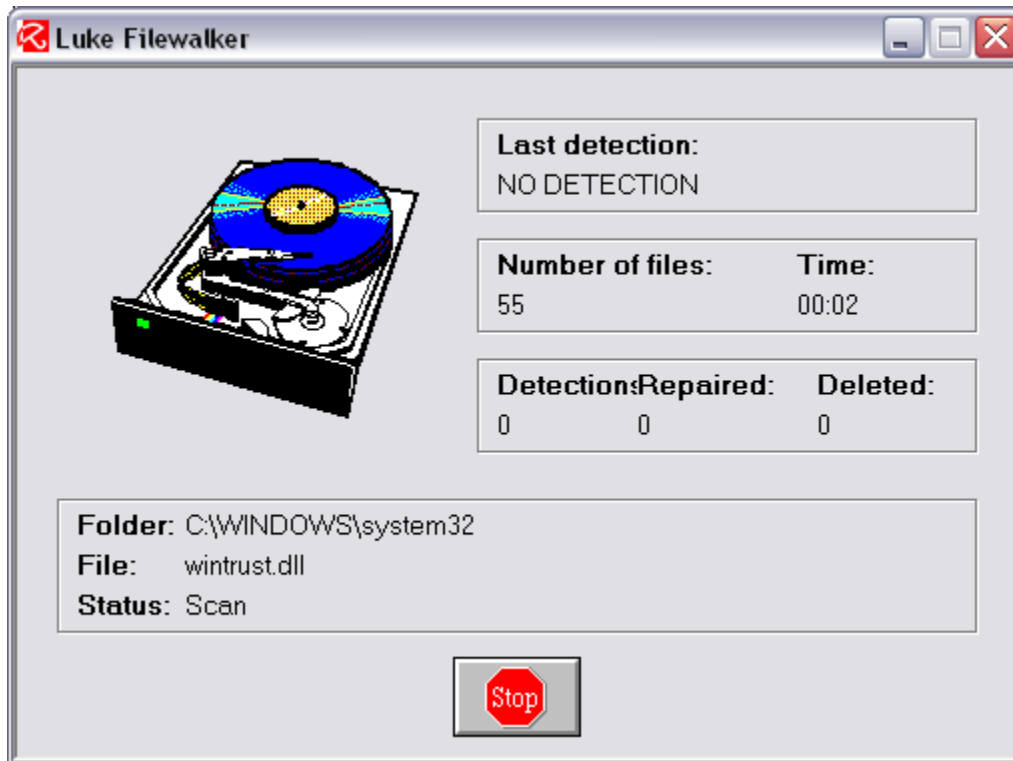
This menu option can be used to read the license file HBEDV.KEY. AntiVir can transfer this license file from all data media, e.g. floppy disks, CD-ROMs, hard disks, network drives, etc. If no license file is transferred, AntiVir will only run as a restricted demo version.

If you scroll to this menu option, the standard file selection window is opened. Select the license file from the selection box or enter the drive, path and name of the license (DRIVE:\PATH\HBEDV.KEY) directly in the 'Filename' box.

If the license file is not found in the specified location, check to make sure it is in the right folder and correct your inputs in the 'Open' window if necessary.

Luke Filewalker

Luke Filewalker is the scanner screen of AntiVir. It tells you what AntiVir is currently scanning and which tasks it has already completed.



Last detection

With any luck, this should say 'NO DETECTION'; if not, the name of the last detected virus or unwanted program appears in red.

Number of files

This tells you which file AntiVir has got to so far.

Time

Indicates the scanning time in mm:ss.

Detections

Indicates the number of viruses/unwanted programs found.

Repaired

Indicates the number of viruses/unwanted programs repaired.

Deleted

Indicates the number of viruses/unwanted programs deleted.

Folder

Tells you the name of the folder currently being scanned.

File

Tells you the name of the file currently being scanned.

Status

This line tells you what AntiVir is doing at the moment. There are three different possibilities: Scanning, Repairing and Unpacking.

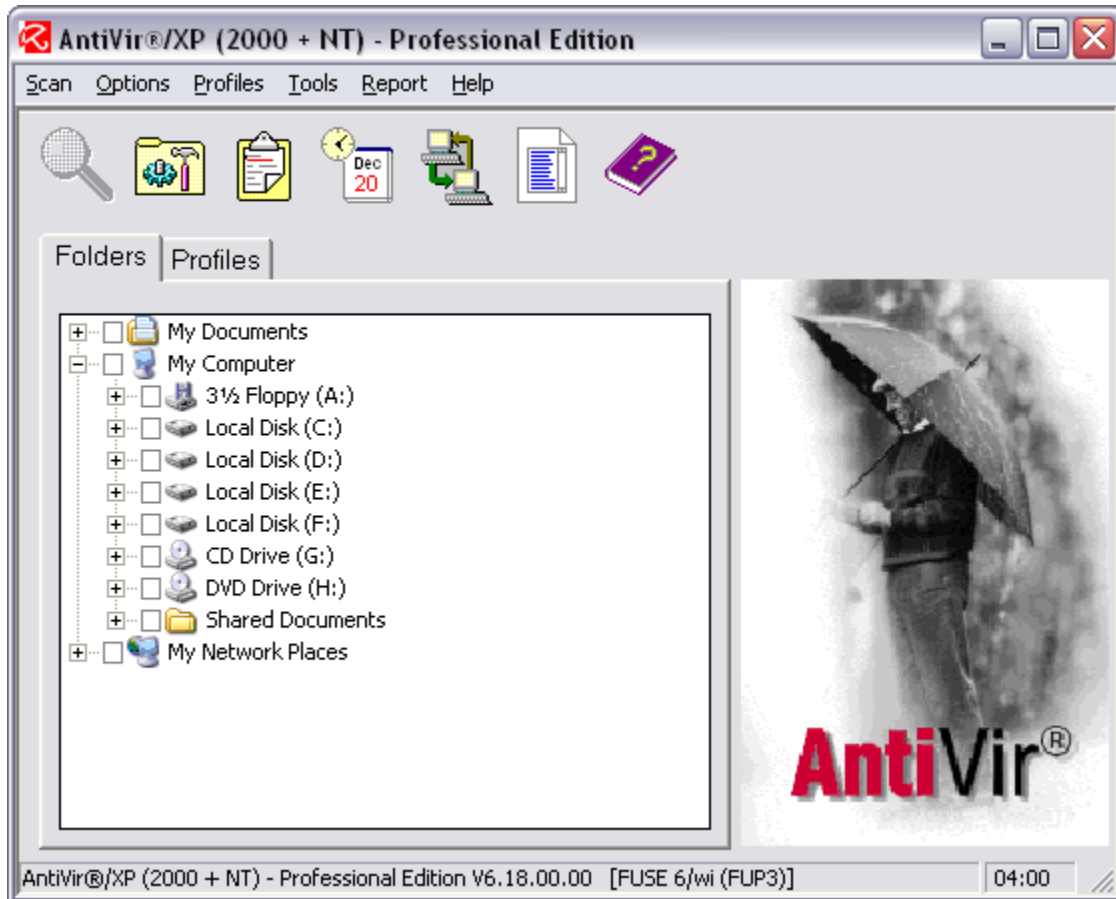
STOP

This button stops the scan instantly.

If this button is greyed out, the scan cannot be interrupted. In this case, the option 'Allow Stopping' is not selected in the group box 'Stop Scan' under Options/Miscellaneous.

Main Window

Here you see the main window of AntiVir for Windows (Professional Edition):



'Folders' tab

(AntiVir Professional only)

In the tab, you can select individual drives and directories for scanning.

You can select the desired drives and directories in the selection box. The display corresponds to that of the Windows Explorer:

- To change directories, double-click on the desired directory.
- To change drives, double-click on the desired drive.
- To select folders and drives, you can also click on the + sign in front of a folder or drive symbol.
- To navigate your way through the menu structure, use the scroll bar and arrows.

The scan can then be started with your chosen settings by clicking the 'Scan' button or the 'F2' key.

Selected drives are shown with check in the small box before their name.

Note: Depending upon the option, AntiVir can remember what was selected.

'Profiles' tab

(AntiVir Professional only)

This tab enables you to group files, folders and drives into profiles and then save them in a list. These profiles can then be used for quicker, more specific scans, without having to go through all the other drives. [Further information about the 'Profiles' tab.](#)

Master Boot Record

This is the first physical sector of a hard disk and only occurs in hard disk drives. It has a double function: firstly, it contains the partition table indicating which locations have been reserved for which operating system and how, and which partition is identified as active. The other part of the program code checks the validity of the partition table, selects the active partition and loads the first record of this active partition into the memory. This record is the boot record of a hard disk.

Master Boot Record Virus

This replaces the program code of the master boot record with its virus code after placing the original master boot record in temporary storage (in most cases). In this way, the master boot record virus is the first program to gain control over the entire system after the BIOS.

Options/Miscellaneous

{button ,AL('toOptions',0,'')} Related topics

Stop scan

Interruption allowed (Alt+I)

If this checkbox is highlighted, the scan can be stopped at any time with the 'Stop' button. If you have deactivated this setting, the 'Stop' button in the Luke Filewalker window will be greyed out, in which case you can no longer abort the scan, but must wait patiently until AntiVir has completed it's task.

Temporary Path

Temporary path (Alt+T)

Enter the temporary path to be used by AntiVir in this line.

The temporary path is used in order to

- unpack and scan compressed executable files
- carry out repairs
- unpack archives

If the path for temporary files no longer exists or if there is less than 1 MB of free storage space available on this drive, you will be asked which path you want AntiVir to use.

Many programs (including Microsoft Windows) use the environment variable 'TEMP' in order to determine the path for swap files. This path often points to a RAM disk or other fast medium, and is thus ideal for AntiVir. This means that you can set the environment variable 'TEMP' or 'TMP' in your `AUTOEXEC.BAT` (`SET TMP=C:\RAMDISK`).

Within AntiVir, you can also use the wildcard `%TEMP%` for the environment variable.

If there is no entry in the `AVWIN.INI` file, AntiVir will search for the environment variable 'TEMP' first, and then 'TMP'. If no entry exists in either case, the start directory of AntiVir will be used by default.

Additionally this dialog window contains the following options:

Overwrite deleted files (Alt+O)

If this checkbox is activated, the data of the files in question are overwritten first and then deleted. This setting should be permanently activated, as it prevents any concerning files from being recovered (e.g. with UNERASE).

Exit AntiVir if system was booted via the shell extension (Alt+X)

If this entry is highlighted, AntiVir will be terminated again after a scan in which it was started via the shell extension. If you don't want this to happen, you should deactivate this setting.

This option is only effective if AntiVir is started via the shell extension; if AntiVir is active and a scan is started via the shell extension, it will have no effect.

Do not scan files or pathes on network drives (Alt+N)

If this option is highlighted, no drives accessible via a network will be scanned. This is useful if the server or other workstations are protected by antivirus software (preferably a suitable version of the

AntiVir program).

Load Guard at system start (Alt+L)

If this option is activated, AVGuard will be loaded automatically when you start the system. If you want to suppress the automatic start, you should deactivate this entry. This option does not take effect until you restart the system.

Load guard via the control programm (Alt+V)

(AntiVir Professional for Win 9x, ME only)

If this option is highlighted, AVGuard can only be activated via the control program, i.e. this no longer happens automatically when you start the program. This option does not take effect until the system is rebooted.

Use Internet Updater (plugin)

(AntiVir Professional only)

If you have activated this setting, you must restart AntiVir (only the first time round). Once you have done this, the new menu option 'Internet Updater' will always appear in the 'Options' under 'Configuration menu'. You will also notice that the 'Internet Updater' symbol has been added to the tool bar of the AntiVir main menu window.

Check for old virus definition files (Alt+C)

If you have activated this setting, the age of the virus definition file will be checked during the startup of AntiVir.

This dialog window contains the following buttons:

{button OK.}

Transfers the data from the 'Miscellaneous' window and then closes it.

{button Cancel.}

Closes the dialog window without transferring the new settings.

{button Help.}

Displays this help text.

Multiple license

With a multiple license - from three users upwards - you can also use AntiVir on several platforms according to the number of users.

There are also additional network options available such as network warnings.

In a network, the [Intranet Update Wizard](#) provides an easy way of updating AntiVir. Further information on this can be found [here](#).

Options/Network Warnings

(AntiVir Professional only)

{button ,AL('toOptions',0,'')} Related topics

This function is only available if you have a multiple license for AntiVir and you are working within a Novell NetWare network with a installed NetWare-Client.

In this index card, you can select the names of the network users who are to receive a warning automatically via the network following the detection of a virus or unwanted program. It is always advisable to notify the supervisor in the event of a virus or unwanted program, as concerning files can spread very quickly via the network.

If the user at the receiving end has switched off the NetWare Broadcast Messages via the 'CASTOFF' command, for example, the message will be sent to him but not displayed.

Warning message

Here you can enter the text of the warning message you want AntiVir to send should a virus or an unwanted program be detected. This message may contain the wildcards %NAME% and %VIRUS%. AntiVir replaces %NAME% with the name of the user on whose workstation the virus/unwanted program was found, and %VIRUS% with the name of the last detected virus or unwanted program. This warning message is sent at the end of each scan leading to the detection of a virus or unwanted program, and may contain a maximum of 58 characters: anything over this is curtailed.

Warnings to

In the '**Type**' list box, you can choose whether to send the warnings messages to a group or individual users.

The selection window '**Group**' or '**User**' contains a list of the groups or users with access authorisation to the server you are currently logged into. You can use the checkbox here to specify whom you wish to send the message to. Once you have confirmed the entries with 'OK', each user in the right-hand list will be sent the message entered above whenever a virus or unwanted program is detected.

Additionally this dialog window contains the following buttons:

{button OK.}

Transfers the data from the 'Network Warnings' window and then closes it.

{button Cancel.}

Closes the dialog window without transferring the new settings.

{button Help.}

Displays this help text.

Options/Network Warnings (XP)

(AntiVir Professional only)

{button ,AL('rtoOptions',0,'')} Related topics

Activate network warnings

This menu option must be activated in order to send network warnings within a LAN.

Warning message

Here you can enter the text of the warning message you want AntiVir to send should a virus or an unwanted program be detected.

This message may contain the wildcards %NAME% and %VIRUS%. AntiVir replaces %NAME% with the name of the user on whose workstation the virus/unwanted program was found, and %VIRUS% with the name of the last detected virus/unwanted program. This warning message is sent at the end of each scan leading to the detection of a virus or unwanted program, and may contain a maximum of 58 characters: anything over this is curtailed.


If you click on the {button Standard,} button, the standard message is entered and the old message deleted.

Send warning message to

This field contains a list of all computers which are to receive this warning. These warnings are only received by XP computers, however. Workstations can be added and removed from the list using the Add and Delete buttons respectively.

Add network computer

This window allows you to add a workstation to the list of computers which are to receive a warning message. You can now enter the name of the workstation directly in the field provided. Using the

button , you can also open a selection menu of available computers from which to select the desired computer.

Additionally this dialog window contains the following buttons:

{button OK,}

Transfers the data from the 'Network Warnings (XP)' window and then closes it.

{button Cancel,}

Closes the dialog window without transferring the new settings.

{button Help,}

Displays this help text.

Options (Contents)

{button ,AL('rtOptions',0,'')} Related topics

In this window, you can select the following index cards in order to set the options for the relevant areas:

Search

Here you can specify when and how you want AntiVir to scan for viruses and unwanted programs.

Repair

Here you can select the settings for repairing reported files.

Unwanted Programs (Selection)

AntiVir protects you against computer viruses.

In addition, it will also scan selectively for dialers, backdoor control software (BDC), games, jokes and possible malicious software (PMS).

Heuristic

Settings for the AntiVir virus heuristic.

Drag&Drop

Here you can specify whether you want to scan the subdirectories of folders dragged and dropped to the main window of AntiVir, and which file formats you want to include.

Report

Here you can specify which information you want to include in the report.

Action after search

(AntiVir Professional only)

Here you can enter the name and command line parameter of any program to be started after the scan.

Password

(AntiVir Professional only)

Here you enter a password in order to restrict access to the options of AntiVir.

Intranet Update

(AntiVir Professional only)

This feature allows a simple automatic update in a network (enabled for 3-user licenses and upwards).

Internet Updater

The Internet Updater ensures that you always have the latest version of your AntiVir program at your disposal.

Profiles

(AntiVir Professional only)

You can specify whether subdirectories are to be included in profile scans and which file types you want AntiVir to include when scanning a profile.

CRC

(AntiVir Professional only)

Here you can specify whether you want to use the CRC method, and if so how and for which files.

Network Warnings

Network Warnings (XP)

(AntiVir Professional only)

If you are connected to a network, you can specify here which users you want to warn in the event of a virus/unwanted program.

Miscellaneous

Here you can enter the temporary path, whether you want to allow interruption of scanning for viruses/unwanted programs and whether you want to overwrite deleted files.

If you select the options via the menu bar of the main window, you will also find these two entries at the bottom:

Save Settings

Saves the settings of AntiVir immediately.

Save Settings on Exit

Automatically saves all settings of AntiVir on closing the program.

Partition Table Discrepancy

The partition table has been modified by a virus. As AntiVir cannot restore the partition table, you are invited here to create a new one.

Caution: You may lose data during this process, so whatever you do, make a backup first!

Options/Password

(AntiVir Professional only)

`{button ,AL('toOptions',0,'')} Related topics`

You can protect access to the options of AntiVir by means of password. Once you have entered a password, you will be asked for this password whenever you wish to open the 'Options' dialog window.

Please enter your password (Alt+P)

Enter the password of your choice here.

Important: This input is case-sensitive!

Please confirm your password (Alt+L)

Enter your password again in the second input box by way of confirmation.

Next time you start AntiVir, a dialog window will appear as soon as the Options menu is selected in which to enter the password.

This dialog window contains the following buttons:

{button OK.}

Transfers the data from the 'Password' window and then closes it.

{button Cancel.}

Closes the dialog window without transferring the new settings.

{button Help.}

Displays this help text.

Options/Profiles

(AntiVir Professional only)

{button ,AL('toOptions',0,'')} Related topics

In this index card, you can specify whether subdirectories are to be included in profile scans and which file types you want AntiVir to include when scanning a profile.

Scan subdirectories (Alt+S)

If this option is activated, all subdirectories will be scanned in profiles containing one or more directories. If this option is not activated, only directories grouped together directly in the profile will be scanned.

Files

All files (Alt+A)

By default, AntiVir only searches for executable files. If this menu option is selected, all files in the relevant directory will be incorporated in the profile scan, including executable files. The scan for viruses and unwanted programs takes longer on this setting as there are far more files to get through. When 'All Files' is activated, the 'Extensions' button cannot be selected.

Files according to the list in 'Options/Search/Files/Extensions' (Alt+O)

On this setting, only files previously selected in the menu Options/Scan/Files/Extensions are scanned.

Program and macro files (Alt+P)

(AntiVir Professional only)

If this option is selected, AntiVir will only search within the profile for files with specified extensions (e.g. *.BIN, *.COM, *.EXE, etc.). Default extensions are already given, and can be changed using the {button Extensions,JI('','OPTIONS_SCANNER_EXTENSIONS')} button. If this option is active and you have deleted all the entries from the list of file extensions, you will see the words 'NO EXTENSIONS' below the 'Extensions' button.

Additionally this dialog window contains the following buttons:

{button OK.}

Transfers the data from the 'Profiles' window and then closes it.

{button Cancel.}

Closes the dialog window without transferring the new settings.

{button Help.}

Displays this help text.

Profiles (Contents)

{button ,AL(`rtoProfiles',0,','')} Related topics

AntiVir offers the following possibilities in this menu:

Save profile as default...

This menu option or the button 'Save as default profile' opens a window in which to save a new profile as the default profile.

When you restart AntiVir, this default profile will be loaded into the index card automatically.

Save profile as...

This menu option or the button 'Save profile' opens a window in which to save a new or edited profile.

Profile files can be identified from the extension * .PRO.

Load profile...

If you want to scan one of the existing profiles for viruses/unwanted programs, all you have to do is open the list of profiles with this menu option or the button 'Load Profile' and double-click on the relevant profile in the list (or highlight it and click on the 'Open' button).

The selection window is then closed and you can start a scan with the 'Scan' button or the 'F2' key.

Create a new profile

Opens the profiles tab.

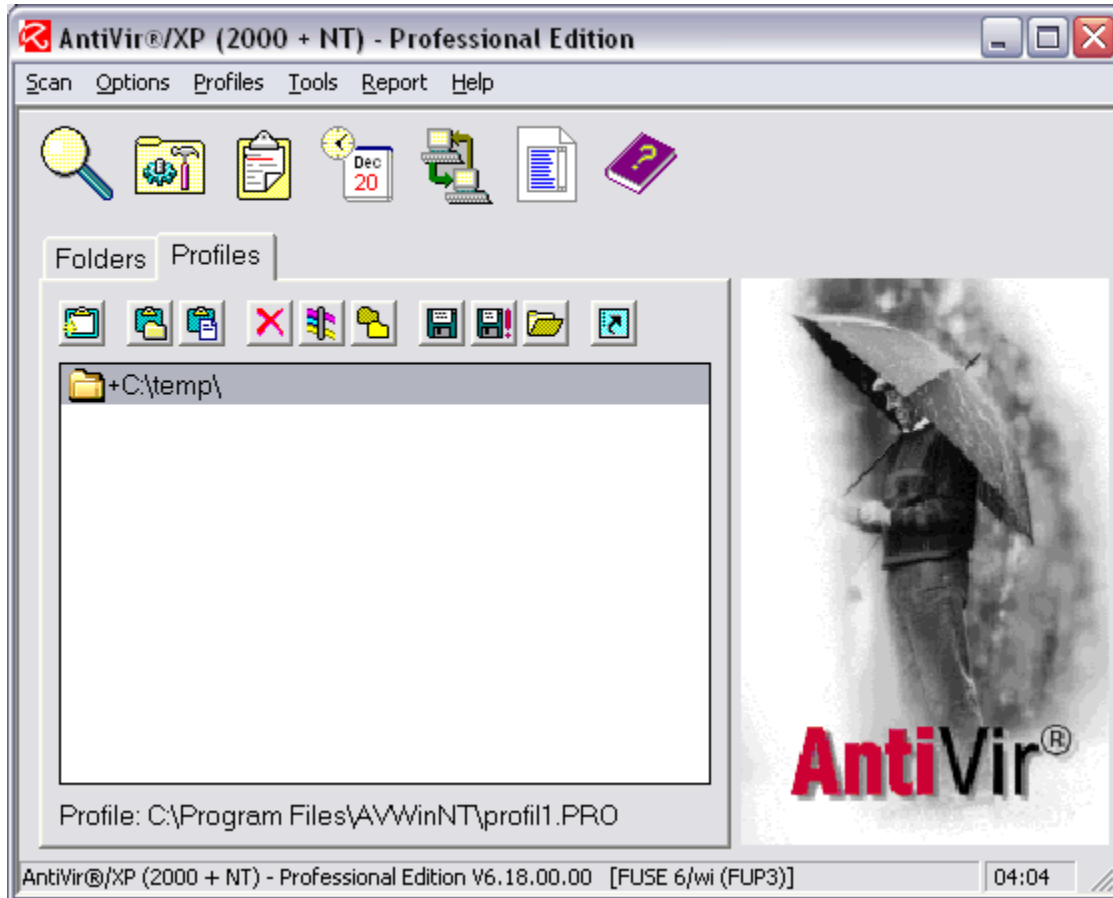
Profiles


(AntiVir Professional only)


{button ,AL('toProfiles',0,'')} [_Related topics](#)


This tab enables you to group files, folders and drives into profiles and then save them in a list. These profiles can then be used for quicker, more specific scan for viruses/unwanted programs, without having to go through all the other drives.


As soon as you select the 'Profiles' tab, this function switches to edit mode.



 If you want to scan one of the existing profiles for viruses/unwanted programs, all you have to do is open the list of profiles with the button 'Load Profile' and double-click on the relevant profile in the list (or highlight it and click on the 'Open' button). The selection window is then closed and you can start a scan with the 'Scan' button or the 'F2' key.

 Once you are in the list of existing profiles, you can switch to edit mode via this button and then create a new profile as described above.

 You can now open a window via the button 'Insert Folder' in which to select the folder you wish to insert in the profile. By default, AntiVir will scan all subdirectories of the selected folder.

 This button can be used in the same way to insert individual files in the current profile.



This button can be used to delete highlighted folders or files from the 'Profiles' tab. You can also highlight the relevant entries and delete them from the list with the 'Del' key.



This button can be used to open a window which enables you to specify which file types you want to include in a scan.

Scan according to this scan mask (Alt+M)

Here you can enter the extensions of the file types you wish to scan. For a specific scan of all .EXE files for example, enter * .EXE.

TIP: To scan .DOC **and** .DOT documents, simply enter * .do?.

Scan according to the default profile settings (Alt+D)

In this case, only the file types selected in the menu Options/Profiles are scanned.

Scan all files in this path (Alt+A)

All files are scanned.



This button enables you to specify whether you also want to scan the subdirectories of the selected folder.

If you click on this button, the + next to the highlighted folder is replaced by a -

+ means: scan subdirectories

- means: don't scan subdirectories

By default, AntiVir scans all subdirectories of the selected folder.



This button opens a window in which to save a new or edited profile.

Profile files can be identified from the extension * .PRO.

If you have made any changes in the 'Profiles' Tab since the last save, you will be asked whether you wish to save them before closing the profile in question. Answer this query accordingly with 'Yes' or 'No'.



This button opens a window in which to save a new profile as the default profile. When you restart AntiVir, this default profile will be loaded into the index card automatically.



The button 'Create Link' enables you to create a desktop link for a particular profile called 'AntiVir <Profilename>'..

Whenever you click this link on the desktop, AntiVir will start up and scan all files and folders of this profile.

Help/Read Me

{button ,AL(`rtoHelp',0,`,`')} Related topics

In this file, you will find important information on each new version of AntiVir.

Due to the short intervals between updates, we are unfortunately unable to include all new features in the manual: these are therefore described in the READ.ME file. Should you have any problems or questions concerning AntiVir which the manual cannot answer, have a look in this file: in the majority of cases you will find the solution to your problem here.

Tools/Recognition List

{button ,AL('rtoTools',0,'')} Related topics

This function is used to list the names of all viruses and unwanted programs known to AntiVir, and has a convenient integrated search function for virus and unwanted program names.

Search for a substring in the names (Alt+S)

Here you can enter a consecutive string of letters or characters via the keyboard. The cursor will then jump to the first place in the name list where this sequence of characters occurs (e.g.: 'raxa' will find 'Abraxas').

Search from the first char of the names (Alt+E)

Here you can enter the initial letter and subsequent characters via the keyboard. The cursor then scrolls through the name list in alphabetical order (e.g.: 'Ra' will find 'Rabbit').

Search:

Enter the name of a virus or unwanted program or a consecutive string of characters from a virus or unwanted program name. If this name or string exists, the cursor will jump to the corresponding place in the list.

You can use the buttons 'Search Forwards' (Alt+F), 'Search Backwards' (Alt+B) and 'First Match' (Alt+M) to navigate your way through the list of virus and unwanted program names. To remove an entry from the 'Search:' text box, use the button 'Clear Input' (Alt+I).

Names:

Under this heading you will find a list of virus and unwanted program names identifiable by AntiVir. Most of the viruses and unwanted programs in this list can also be removed with AntiVir. The viruses and unwanted programs are arranged in alphabetical order (with special characters and numbers at the top, followed by letters). To move up and down the list, use the scroll bar.

This dialog window contains the following buttons:

{button Search forward,}

Initiates a forward search in alphabetical order.

{button Search backward,}

Initiates a backward search in alphabetical order.

{button First match,}

Jumps back to the first entry found in the list.

{button Clear input,}

Removes the entry from the 'Search:' text box.

{button Close,}

Closes the dialog window.

{button Help,}

Displays this help text.

Options/Repair

{button ,AL('rtoOptions',0,'')} Related topics

This index card allows you to specify what action you want AntiVir to take following the detection of a virus or unwanted program. The possibilities range from simply recording the events to repairing the concerning files.

Most settings in this dialog window can only be selected and are only effective if you have **not** activated the option 'Record in Report File Only'!

Found items

Repair with prompt (Alt+F)

If this setting is selected, whenever AntiVir finds a reparable file it will ask you first whether or not you want to repair the file.

Repair without prompt (Alt+W)

In this case, reported reparable files are repaired immediately without prompting.

Delete with prompt (Alt+D)

In this case, reported files are deleted when you confirm the prompt. If you want to make sure that the file cannot be restored (e.g. with `UNERASE`), you should also highlight the item 'Overwrite Deleted Files' in the Options/Miscellaneous window.

If 'Overwrite Deleted Files' is activated, AntiVir will also delete reported files which are possibly capable of repair.

Delete without prompt (Alt+E)

In this case, reported files are deleted without prompting. If you want to make sure that the file in question cannot be restored (e.g. with `UNERASE`), you should also highlight the item 'Overwrite Deleted Files' in the Options/Miscellaneous window.

If 'Overwrite Deleted Files' is activated, AntiVir will also delete reported files which are possibly capable of repair.

Not repairable items

The settings in this group are only active if you have chosen to repair reported files under 'Found items'.

Delete with prompt (Alt+L)

If an reported file was unable to be repaired, e.g. because it was destroyed by a virus, the file will be deleted after prompting when this setting is active. If you want to make sure that the file in question cannot be restored (e.g. with `UNERASE`), you should also highlight the item 'Overwrite Deleted Files' in the Options/Miscellaneous window.

Delete without prompt (Alt+T)

Once again, this setting is only effective when AntiVir encounters an reported, irreparable file. If you have activated this option, the relevant file will be deleted without prompting. If you want to make sure that the file in question cannot be restored (e.g. with `UNERASE`), you should also highlight the item 'Overwrite Deleted Files' in the Options/Miscellaneous window.

Ignore (Alt+I)

If this option is selected, irreparable files will be neither deleted nor repaired.

Warning: If such a file remains on your system, you should proceed with caution, as although this defective file is probably no longer executable, it still contains virulent code which may cause damage.

Acoustic Warning

Acoustic warning (Alt+O)

If this checkbox is activated, AntiVir emits a short series of warning tones in case of a detection.

Wave file (Alt+V)

In the input box 'Wave File', you can enter the path and name of a wave file of your choice. If this box is empty, the default alarm signal will be used. The button 'Test Acoustic Alarm' can be used to test the selected wave file.

Date/Time

When AntiVir repairs a file, it has to write-access the file in question in order to remove the code. During this process, the date and time of this file is normally set to the current system date. The settings in this group are only active if you have specified under 'Found items' that you want to repair reported files.

No change (Alt+C)

If this setting is activated, the original date and time will be retained.

Current system time (Alt+U)

In this case, the date and time of a repaired file are set to the current system values.

Correct date (Alt+A)

Some viruses manipulate the date or time of a file in order to find out whether or not they have already infected it. An example of this is the Vienna virus, which sets the seconds display of the infected file to 62.

If you select 'Correct Date', AntiVir will reset the file to a valid time and date after repairing it.

Caution: If you have installed any Sierra games on your computer, you should not select this setting, as Sierra adds 100 to the year figure (we are not absolutely sure why), an action also performed by Tremor viruses in order to find out whether the file is already infected. When AntiVir comes to correct the year figure, it cannot be expected to tell whether it is dealing with your favourite game or a virus.

Record in report file only (Alt+N)

If this setting is activated, AntiVir will neither carry out repairs nor delete reported files.

Attention: Detected viruses and unwanted programs are only recorded in the report file!

Concerning files will remain on your computer!

In case of a virus warning or the detection of an unwanted program, it is now up to you to decide what to do with the files.

To make sure a report file is generated in every case, you should not deactivate the report file under Options/Report.

This dialog window contains the following buttons:

{button Text acoustic alarm,}

This button in the group box 'Acoustic Alarm' is for testing the selected wave file.

{button OK,}

Transfers the data from the 'Repair' window and then closes it.

{button Cancel,}

Closes the dialog window without transferring the new settings.

{button Help,}

Displays this help text.

Options/Report

{button ,AL('rtoOptions',0,'')} Related topics

This index card is for selecting the settings for the AntiVir report file.

A report file should be generated in all cases in order to see what action AntiVir has taken following the detection of a virus or unwanted program.

Before a report can be generated, you must enter a valid name for the output file. The report file is always stored in the AntiVir directory.

The report file contains boxes for entering your name in case you ever have to send this report file in to us. To avoid having to fill in all the details by hand in this case, you can create a file named AVWIN.ADR in the AntiVir directory in which to enter all the necessary information. AntiVir will then transfer these data to each report file.

Structure of address file:

[Address]

Institution=H+BEDV Datentechnik GmbH

Department=Development

Name=Mr. X

Street=Lindauer Straße 21

Town=88069 Tettnang

Tel./Fax=07111/111111 07111/11112

EEmail=mr@x.de

The following settings can be changed in order to generate a report file:

Mode

No report (Alt+E)

In this case, AntiVir will not generate a report file. This setting should really only be used for test purposes, when the report file can become relatively large. You should make sure a report file is always generated during normal operation.

Overwrite report (Alt+V)

In this case, AntiVir will overwrite an existing report file after each new scan. This setting should be sufficient as a rule, and has the advantage of restricting the size of the report file.

Append new report (Alt+N)

In this case, AntiVir appends the new report file to an existing report file. Please note, however, that if you use AntiVir regularly and keep adding to an existing file, this file will get larger and larger, and the space on your hard disk will diminish accordingly. You should therefore delete your report file again from time to time.

Data To Be Logged

Reported files (Alt+F)

Only the names of the reported files plus the path are included in the report file.

Include all paths (Alt+D)

All scanned paths are included in the report file in addition to the names of the reported files.

All scanned files (Alt+L)

All scanned filenames and paths are included in the report file.

Full information (Alt+M)

The same data is recorded as for 'All Scanned Files', but additional information is also included, i.e. the files `AUTOEXEC.BAT`, `CONFIG.SYS`, `WIN.INI` and `SYSTEM.INI`. Should you ever have to send us a report file (for debugging), please generate it in this mode.

Please note with regard to all the above settings: if the report is deactivated, nothing will be written in the report file!

Output File (Alt+O)

Use the box in this group box to enter the name of the file under which the report is to be saved. This name can be changed for each scan unless you want to delete the report file immediately.

Shorten Report File (Alt+R)

This group box is used to define the maximum size of the report file. Activate this option and then enter (Alt+A) the desired size in the box 'Cut Off After ... KB'. The advantage of this setting is that it prevents the report file from getting too big. Imagine you are working in the 'Append' mode and choose to write all information to the report file after every scan: if you use AntiVir regularly, the space on your hard disk will steadily decline.

This dialog window contains the following buttons:

{button Warnings,JI('`,`OPTIONS_REPORT_WARNINGS')}

This button is used to open the 'Warnings' window, where you can choose which warnings you want to include in the report file. These settings only relate to warnings, and not to detected viruses, detected unwanted programs or CRC modifications, for example. For more information, please refer to Options/Report/Warnings.

{button OK,}

Transfers the data from the 'Report' window and then closes it.

{button Cancel,}

Closes the dialog window without transferring the new settings.

{button Help,}

Displays this help text.

Report (Contents)

{button ,AL('rtoReport',0,'')} Related topics

Here you will find all the functions relevant to the report file and summary report:

Display

Opens the main window of AntiVir Report containing the last report file created.

Settings...

Opens the options window in which to select the settings for the report file.

Delete

Deletes the report file.

Print...

Prints the report file.

Display Summary Report...

Displays the summary report.

Summary Report Options...

Opens the Options window in which to select the settings for the summary report.

Delete Summary Report

Deletes the summary report.

Report/Delete

{button ,AL('rtoReport',0,'')} Related topics

This function can be used to delete an existing report file.

If there is no report file available, the 'Report' button and all options relating to AntiVir Report except Report/Settings are deactivated.

Report/Display

{button ,AL(`rtoReport',0,`,`')} Related topics

If you select this menu, the program AntiVir Report will be called. This tool is a file viewer which is normally used to load and display the AntiVir report file.

You can also use AntiVir Report to view .TXT or .LOG files.
These file types can also be opened with the drag&drop feature.

Further information can be found in the help file of AntiVir Report.

Report/Print

{button ,AL(`rtoReport',0,`,`')} Related topics

By selecting the menu option 'Print', you can print out the currently displayed file, which is normally the AntiVir report file.

If you have any problems with the printing procedure, you may need to set the printer using the 'Set Up Printer' function. The settings selected here only apply to AntiVir Report: they are not changed universally.

Information on how to install the printer can be found in your Windows documentation.

Options/Report/Summary Report

{button ,AL('rtoOptions',0,'')} Related topics

This index card allows you to select the settings for the summary report. This report is used to record key data for each scan performed by AntiVir, so that you can follow the activities of AntiVir over an extended period. In this way, you can keep track of recent events in your system on the virus and unwanted programs front - provided you have activated 'Generate Summary Report'.

Create summary report (Alt+C)

If this box is checked, the summary report will be written automatically.

Output file (Alt+O)

Here you can enter the filename under which the summary report data are be saved. AntiVir suggests the name 'AVWIN.ACT' by default.

Maximum number of entries (Alt+M)

This function allows you to influence the size of the output file. AntiVir only stores as many entries in the output file as are set here, the maximum number being 999. You can either enter the number of entries directly or change it using the arrows to the right of the input field. Clicking on one of these arrows causes the current value to be incremented by 1, or by 10 if you press the Ctrl button simultaneously.

This dialog window contains the following buttons:

{button OK.}

Transfers the data from the 'Summary report' window and then closes it.

{button Cancel.}

Closes the dialog window without transferring the new settings.

{button Help.}

Displays this help text.

Options/Report/Warnings

{button ,AL('Options',0,'')} Related topics

In this dialog window, you can select which warnings you want to include in the report file. These settings only relate to warnings, and not to detected viruses, detected unwanted programs or CRC modifications, for example. Each of the entries highlighted here will be included in the report file whenever the event in question occurs.

Access denied (Alt+D)

This means that the file cannot be accessed, and was therefore unable to be scanned for viruses or unwanted programs. This message occurs in the case of Windows swap files, for example. Because the swap file remains open throughout the Windows session, it cannot be scanned.

Wrong file size in directory (Alt+W)

The size stored in the directory does not coincide with the actual size of the file.

Wrong creation time in directory (ALT+T)

The file contains an incorrect date or time entry. For example, the Vienna virus enters the value 62 in the seconds display when it infects a file, while a Tremor virus characteristically adds 100 to the year figure. These changes to the time or date are not necessarily always caused by a virus, however: the games manufacturer Sierra, for instance, also adds 100 to the year figure.

COM File is too large (Alt+F)

A COM file must not exceed 65536 bytes. The above warning is issued if a larger COM file is found.

Invalid start address (Alt+I)

In the case of EXE files, the start address of the program is stored in CS:IP in the EXE header. The above warning is issued if an incorrect address is found here.

Invalid EXE header (Alt+E)

The length of a file is stored in the EXE header. If the length indicated here differs from the actual length, the above warning is issued.

Possibly damaged (Alt+P)

This file may have been damaged e.g. by viruses. If you have any problems with it, replace it with the original file.

OLE file is damaged or protected (Alt+L)

A file, which contains information to the Object Linking and Embedding, cannot be examined.

This dialog window contains the following buttons:

{button OK.}

Transfers the data from the 'Warning messages in the report' window and then closes it.

{button Cancel.}

Closes the dialog window without transferring the new settings.

`{button Help.}`

Displays this help text.

Options/Save Settings

{button ,AL(`rtoOptions',0,'')} Related topics

If you select this menu option, all current settings of AntiVir are saved manually at once in the AVWIN.INI file.

Options/Save Settings on Exit

{button ,AL(`rtoOptions',0,'')} Related topics

If this option is selected (identified by a check mark in front of the text), all AntiVir settings will be saved automatically when you exit the program.

If you make any changes when this function is not active, you will be asked whether you want to save these changes before exiting AntiVir.

Tools/Save System Files

(AntiVir Professional only)

{button ,AL('toTools',0,'')} Related topics

This dialog box enables you to save the system files, the boot record of drive C: and the CMOS. These data are saved in the directory 'SYSSAVE' under the AntiVir installation directory.

Boot record of drive C: (Alt+B)

Select this entry if you want to write the boot record of drive C: to the directory 'SYSSAVE' under the installation directory of AntiVir. The record is saved in the file 'BootRecC.DAT'.

System files (Alt+Y)

If this option is selected, all system files from the root directory of drive C: will be written to the directory 'SYSSAVE' under the installation directory. The system files include all files with the system flag (except for swap files!). The following files are always copied, even if they do not have the system flag:

```
COMMAND.COM  
IO.SYS  
MSDOS.SYS  
AUTOEXEC.BAT  
CONFIG.SYS
```

CMOS (Alt+C)

The contents of the CMOS are saved in the directory 'SYSSAVE' under the installation directory of AntiVir.

This dialog window contains the following buttons:

{button Save.}

Transfers the data from the 'Backup system files' window and then closes it.

{button Cancel.}

Closes the dialog window without transferring the new settings.

{button Help.}

Displays this help text.

Scan (Contents)

{button ,AL(`rtScan',0,`,`')} Related topics

In this menu, you can start the scan in the highlighted drives, select which items you want to scan and exit AntiVir.

Start scan (F2)

Scans all drives highlighted in the main window.

Boot Records...

Opens a dialog window in which to highlight the drives whose boot records you wish to scan.

Update Drive List (F5)

Updates the drive list displayed in the Folders tab.

Exit AntiVir (Alt+F4)

Closes AntiVir for Windows.

Tools/Scheduler

{button ,AL(`rtoTools',0,`,`')} Related topics

By selecting this menu option or clicking the corresponding button, you can load the AntiVir Scheduler, an autonomous program which allows you to start AntiVir at fixed times.

This way, you don't have to sit at your computer in order to scan huge hard disks - just tell the Scheduler to start AntiVir every Friday evening at 10 p.m., for example (provided your computer system is running and the Scheduler is activated at that time, of course).

You can also use the Scheduler to call messages at certain times or define the start time of other programs and utilities. This makes it an easy-to-operate tool for controlling regularly recurring routines.

For further information, please consult the AntiVir Scheduler help file.

Options/Search

{button ,AL('rtoOptions',0,'')} Related topics

This index card allows you to specify which files you want AntiVir to scan, where these files are located and which type of scan you want to use.

Boot Records

Boot record of selected drives (Alt+T)

If this function is activated, the boot record of all selected drives are checked at the start of the scan. This option is only active and can only be changed when 'All Boot Records' is deactivated.

All boot records (Alt+L)

(AntiVir Professional only)

On this setting, all preselected boot records are checked, including those of drives not subject to a full scan. When this setting is selected, the setting 'Boot Record of Selected Drives' is deactivated and the 'Boot Records' button is activated:

{button Boot records,JI('','OPTIONS_BOOTSECTOR')}

When 'All boot records' is activated, this button can be used to open a window in which to select the drive types whose boot records you want to check at the beginning of each scan. The drive types are 'Floppy disks', 'Harddisks' and 'RAM disks'.

Files

All files (Alt+A)

If you have selected this menu option, all files on the relevant drives will be scanned, including non-executable files.

This setting should only be activated following the detection of a virus/unwanted program in order to carry out a thorough check on all your files, as it takes much longer. The 'Extensions' button cannot be selected when 'All Files' is activated.

Program and macro files (Alt+P)

If you have selected this function, only files with a specified extension will be scanned (e.g. *.BIN, *.COM, *.EXE, etc.). Default extensions are already given, and can be changed using the 'Extensions' button.

If this option is active and you have deleted all the entries from the file extension list, you will see the words 'NO EXTENSIONS' below the Extensions button.

{button Extensions,JI('','OPTIONS_SCANNER_EXTENSIONS')}

This command opens a dialog window containing all the file extensions to be checked during a scan in the 'Program and macro files' mode. The most common program file extensions are set by default.

Memory

Begin scan with memory (Alt+M)

If this checkbox is highlighted, the main memory of your computer will be examined for viruses and unwanted programs at the beginning of each scan.

Important: This function should be active at all times in order to ensure maximum protection against viruses/unwanted programs. If a virus/unwanted program is active in the memory, you will run the risk of infecting all scanned files. In this case, reboot your system from a virus-free, write-protected system disk.

Priority (Alt+R)

high

In this case, AntiVir appropriates almost all the system resources for the scan, making it virtually impossible to use any other programs in the meantime.

medium

AntiVir is given medium priority (default setting): this means you can still use other programs during the scanning routine.

low

AntiVir is only assigned a small proportion of the system resources, so that it is easily possible to continue using other programs during the scan.

If you wish to continue working with another program while AntiVir is searching for viruses/unwanted programs, we recommend that you select the low priority setting. This will release the processor much more frequently for the other application. If you want to conduct a scan without activating any other programs, choose the high priority setting for the sake of speed.

Additionally this dialog window contains the following buttons:

{button OK.}

Transfers the data from the 'Search' window and then closes it.

{button Cancel.}

Closes the dialog window without transferring the new settings.

{button Help.}

Displays this help text.

Options/Search/Archives

{button ,AL('toOptions',0,'')} Related topics

AntiVir uses internal unpacking routines for the selection of available archives. The corresponding DOS unpackers are not required.

Archives list

In this window you can choose, which kind of archies AntiVir is to scan. Simply mark the appropriate entries.

Search archives (Alt+S)

If this option is highlighted, archives with the internal unpacking routines will be scanned.

All archives (Alt+A)

If this option is highlighted, all listed archive types supported by AntiVir will be selected and scanned.

Activate smart extensions (Alt+M)

(AntiVir Professional only)

If this option is highlighted, the program will also scan archives with different archive type designations. For example, if a ZIP archive has the file ending 'XYZ', the internal routines will unpack this archive too. If the 'smart extensions' are not activated, they will ignore the 'XYZ' archive.

Restrict recursion depth

(AntiVir Professional only)

The recursion depth for searching archives can be chosen freely. It is possible to restrict the search level for files that have been packed multiple times. This helps to save time and system resources, although the archive will not be completely scanned.

Note: In order to detect a virus or unwanted program within an archive, the scanner must scan to the recursion level where the virus/unwanted program is.

Maximum recursion depth

(AntiVir Professional only)

Activate this option and then enter the desired recursion depth.

You can either enter the maximum recursion depth directly or change it using the arrows to the right of the input field.

This dialog window contains the following buttons:

{button OK.}

Transfers the data from the 'Archives' window and then closes it.

{button Cancel.}

Closes the dialog window without transferring the new settings.

{button Help.}

Displays this help text.

Options/Search/Boot Records

(AntiVir Professional only)

{button ,AL('rtoOptions',0,'')} Related topics

This button opens a dialog box in which to specify which boot records you want to scan (provided you have activated the setting 'All Boot Records' in the Scan Options window). All drive types are activated by default.

Highlight the drive types you want to scan (floppy disk drives, hard disks, RAM disks) in this dialog window.

This setting can be used to avoid scanning floppy disk drives, for example: often there is no disk inserted in the drive, yet AntiVir still has to access this slow medium in order to check whether or not a disk is present. This check is carried out with every scan and takes up unnecessary time.

This dialog window contains the following buttons:

{button OK.}

Transfers the data from the 'Boot records' window and then closes it.

{button Cancel.}

Closes the dialog window without transferring the new settings.

{button Help.}

Displays this help text.

Options/Search/Omit Files

{button ,AL('rtoOptions',0,'')} Related topics

Here you can enter the files and paths you want to exclude from the scan for viruses and unwanted programs.

Warning: These files will not be scanned!

Please enter as few files as possible here and only those which - for whatever reason - you don't want to include in a normal scan. We recommend that you check these files in all cases before adding them to this list!

N.B.: The files included in this list are entered in the report file. Please check the report file from time to time for these unscanned files in case your reason for excluding one of them no longer applies and you can remove it from the 'Omitted Files' window again.

To add a file to this list, click on the {button Insert,} button or select a file using the browser, which is activated via the {button Browse,} button. If you enter a filename here together with its full path, this file and only this file will be omitted from the scan for viruses/unwanted programs. If you enter a filename without a path, any file with this name (regardless of path or drive) will be omitted.

To delete an entry, highlight it first and then click on the {button Delete,} button.

Additionally this dialog window contains the following buttons:

{button OK,}

Transfers the data from the 'Omit files' window and then closes it.

{button Cancel,}

Closes the dialog window without transferring the new settings.

{button Help,}

Displays this help text.

Scan/Start scan

{button ,AL(`rtoScan',0,'')} Related topics

Start scan

These are performed by searching for a specific signature, which is like the 'fingerprint' of a virus or unwanted program.

By using a database of virus and unwanted program codes (comparable to a criminal file), AntiVir is able to identify this signature. Suspicious files can be reported and repaired if possible .

You can scan in various ways:

- ▶ by clicking on the 'Scan' button
- ▶ via the menu bar 'Scan/Start Scan'
- ▶ via the key combination (Alt+S / S)
- ▶ via the function key (F2)
- ▶ via the drag & drop function
- ▶ via the shell extension (right mouse key)

The scanning screen of AntiVir, Luke Filewalker, is then displayed and checks the files in the selected areas.

This screen tells you the names of the last viruses/unwanted programs to have been detected, the number of files scanned so far, the time taken, the number of viruses/unwanted programs detected and the number of files repaired and deleted. The name and path of the file currently being scanned are also displayed, together with the current status (e.g. testing memory, testing boot record, scanning, unpacking, repairing).

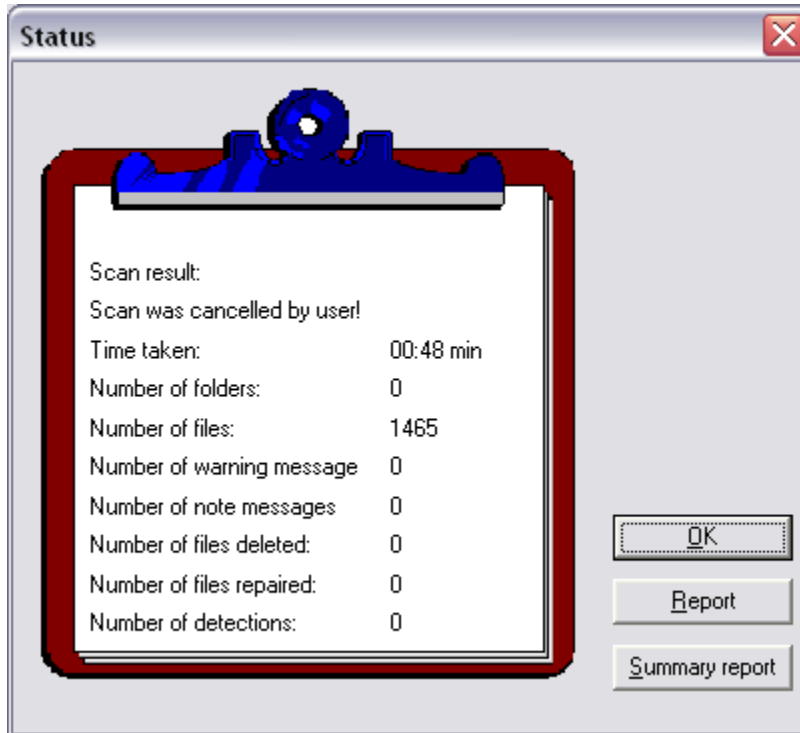
If the box 'Interruption allowed' is checked in the menu Options/Miscellaneous, you can interrupt the scan via the 'Stop' button.

Status

After completing each scan, AntiVir opens the 'Status' window, which contains a summary of the actions performed by AntiVir.

An **exclamation mark** on the right of the notepad indicates that a virus or unwanted program has been detected.

Below the line 'Scan result', you are notified whether AntiVir terminated its scan normally or whether it was aborted by the user.



This is followed by a list containing the following entries:

Time taken

Scanning time in mm:ss.

Number of folders

Total number of scanned folders.

Number of files

Total number of scanned files.

Number of warning messages

Number of warnings issued.

Number of note messages

Number of notes issued.

Number of files deleted

Total number of deleted files.

Number of repaired files

Number of repaired files.

Number of detections

Number of viruses/unwanted programs found.

This dialog window contains the following buttons:

{button OK.}

Closes the dialog window and transfers the current settings.

{button Report.}

Displays a detailed report on the scan.

More Information about Report

{button Summary Report.}

Displays a brief summary of the events of all scans performed so far (or since the last deletion of the summary report).

More Information about Summary Report

Tools (Contents)

{button ,AL('rtoTools',0,'')} [Related topics](#)

AntiVir offers the following tools in this menu:

Save system files...

(AntiVir Professional only)

This menu option opens a dialog window in which you can choose whether to save the boot record of drive C:, the system files from the root directory of drive C: and the contents of the CMOS in the directory 'SYSSAVE' under the installation directory of AVWin.

Scheduler...

Starts the AntiVir Scheduler.

Recognition List...

Displays the names of all viruses and unwanted programs known to AntiVir.

Virus Information...

Calls a Windows help file containing information on viruses.

Start Intranet Update...

(AntiVir Professional only)

If you select this option, the Intranet Update Wizard will search the specified source directory immediately for more recent program files.

You find assistance for configuration under: [Options/Intranet Update](#).

Start Internet Updater

This option starts the Internet Updater. With the Internet Updater you can load new updates from the Internet.

You find assistance for configuration under: [Options/Internet Updater](#).

Load License File...

(AntiVir Professional only)

Reads the license file in order to turn a demo version into a fully registered version.

Read VDF File...

(AntiVir Professional only)

Opens the standard file selection file, in this case in the installation folder of AVWin.

Unwanted Programs

Dialers

Games

Jokes

Possible malicious software (PMS)

Backdoor control programs (BDC)

Dialers

Certain services available in the internet have to be paid for. They are invoiced in Germany via dialers with 0190/0900 numbers (or via 09x0 numbers in Austria and Switzerland; in Germany, the number is set to change to 09x0 in the medium term). Once installed on the computer, these programs guarantee a connection via a suitable premium rate number whose scale of charges can vary widely.

The marketing of online content via your telephone bill is legal and can be of advantage to the user. Genuine dialers leave no room for doubt that they are used deliberately and intentionally by the user. They are only installed on the user's computer subject to the user's consent, which must be given via a completely unambiguous and clearly visible labeling or request. The dial-up process of genuine dialers is clearly displayed. Moreover, genuine dialers tell you the incurred costs exactly and unmistakably.

Unfortunately there are also dialers which install themselves on computers unnoticed, by dubious means or even with deceptive intent. For example they replace the internet user's default data communication link to the ISP (Internet Service Provider) and dial a cost-incurring and often horrendously expensive 0190/0900 number every time a connection is made. The affected user will probably not notice until his next phone bill that an unwanted 0190/0900 dialer program on his computer has dialed a premium rate number with every connection, resulting in dramatically increased costs.

To protect yourself generally from unwanted 0190/0900 dialers, we recommend that you ask your telephone provider directly to deny access to these numbers.

AntiVir recognizes the cost generating dial-up programs (dialer) known to him by default. If you have activated the option "Dialers" under Unwanted programs in the configuration menu of AntiVir, you will receive a warning whenever AntiVir finds something. You now have the option of simply deleting the unwanted 0190/0900 dialers. But if this is a desired dial-up program, you can declare it as an exception file and this file will consequently not be analyzed any longer in future.

Games

There is a place for computer games - but it is not necessarily at work (except perhaps in the lunch hour). Nevertheless, with the wealth of games downloadable from the internet, a fair bit of mine sweeping and Patience playing goes on among company employees and civil servants. Email games are also becoming increasingly widespread, with numerous variants in circulation from simple chess games to "Fleet Manoeuvres" (including torpedo battles). The relevant moves are sent via mail programs to partners who then answer them in turn.

Studies have shown that the number of working hours devoted to computer games has long reached economically significant proportions. It is therefore not surprising that more and more companies are considering ways of banning computer games from workplace computers.

Through its extended scanning and identification routines, AntiVir is capable of detecting games and

eliminating them as unwanted programs. If you have activated the option "Games" under Unwanted programs in the configuration menu, you will receive an appropriate warning whenever AntiVir reports a find. All you have to do now is press delete - and the game is up in the truest sense of the word!

Jokes

Jokes are merely intended to give someone a fright or provide general amusement without causing harm or reproducing. When a joke program is loaded, the computer will usually start at some point to play a tune or display something unusual on the screen. Examples of jokes are the washing machine in the disk drive (DRAIN.COM) or the screen eater (BUGSRES.COM).

But beware! All symptoms of joke programs may also originate from a virus or Trojan. At the very least the user, will get quite a shock or be thrown into such a panic he may do real damage.

Through its extended scanning and identification routines, AntiVir is capable of detecting jokes and eliminating them as unwanted programs. If you activate the option "Jokes" with a tick under Unwanted programs in the configuration menu, you will be notified accordingly of any findings.

Possible malicious software (PMS)

PMS (possible malicious software) will not normally do any damage to your computer. It is programmed to cause damage to other users. Example: Mail bombers - with this type of program the victim may be attacked with thousands of emails.

AntiVir is able to detect 'possible malicious software'. If you have activated the option "Possible malicious software (PMS)" under Unwanted programs in the configuration menu, you will receive a corresponding warning whenever AntiVir reports a find.

Backdoor control programs (BDC)

In order to steal data or manipulate computers, a backdoor server program is smuggled in unbeknown to the user. This program can be controlled by a third party using backdoor control software (client) via the internet or a network.

AntiVir is able to detect 'Backdoor control programs'. If you have activated the option "Backdoor control programs (BDC)" under Unwanted programs, in the configuration menu, you will receive a corresponding warning whenever AntiVir reports a find.

Options/Unwanted Programs

{button ,AL('rtoOptions',0,'')} Related topics

AntiVir protects you against computer viruses.

In addition, it will also scan selectively for dialers, backdoor control software (BDC), games, jokes and possible malicious software (PMS).



Report Backdoor Client (BDC)



Report Dialers



Report Games



Report Jokes



Report Possible malicious software (PMS)

The selection is activated by clicking on the relevant box.

To activate all types, click on [Activate all](#).

If a type is deactivated, files which are identified as being of that program type will no longer be reported entered in the report file.

This dialog window contains the following buttons:

[{button Default Settings.}](#)

This button re-establishes the default values suggested by AntiVir.

[{button OK.}](#)

Transfers the data from the 'Unwanted programs' window and then closes it.

[{button Cancel.}](#)

Closes the dialog window without transferring the new settings.

[{button Help.}](#)

Displays this help text.

Scan/Update Drive List

{button ,AL(`rtScan',0,`,`')} Related topics

If you select this menu option or press the function key (F5), the drive list in the Folders tab will be updated.

You should activate this function if you connect or disconnect your workstation to/from a network drive while the main window of AntiVir is open. When you restart AntiVir, all accessible drives will be displayed in this list.

Update Wizard

(AntiVir Professional only)

In order to supply workstations in a network with updates, we have developed the Intranet Update Wizard. This function is only available with a multiple AntiVir license (for 3 or more users).

If correctly configured, this tool will ensure that your workstation computer updates itself automatically with the latest versions of AntiVir. The Update Wizard is already entered in the RUN key of the Windows registry during the installation routine and will check a particular directory on a particular server for any new AntiVir programs or new virus signatures whenever it is logged onto the system.

Further information on how to install the Update Wizard can be found on the H+BEDV CD-ROM in the directory

[\\[language\]\products\windows\workstat\setup\disk_1\admin.htm](#)

Verifiably Clean DOS Disk

The 'verifiably clean DOS disk' can be used in an emergency to reconstruct your computer. This disk - you can use to if you need to - should contain all the programs and tools your computer needs to get it going again.

In order to create a 'verifiably clean DOS disk', your computer must be absolutely virus-free. If a virus has found its way onto your system at this stage, an infection will be very hard to detect, as this disk is always assumed to be completely clean.

To begin with, make a bootable operating system disk using the DOS command `FORMAT`. The parameter `/u` (= `UNDELETE`) is only available from DOS 5.0 onwards, in which case the system disk will not contain any information for salvaging the system data:

```
format a: /s /u
```

Once formatted, your disk is already bootable.

Now generate an `AUTOEXEC.BAT` and a `CONFIG.SYS` file on this disk. These files might look like this, for example:

CONFIG.SYS:

```
DEVICE=A:\HIMEM.SYS
FILES=40
BUFFERS=20
STACKS=9,256
SHELL=A:\COMMAND.COM /E:1024 /P
```

AUTOEXEC.BAT:

```
KEYB GR
```

If you need any other drivers in order to boot successfully, copy them to this disk too and modify `CONFIG.SYS` accordingly. Drivers are available for hard disk drives (`SSTOR.SYS`, `HARDDRIVE.SYS`, `DMDRV.BIN`), floppy disk drives (IBM PS/2 - `DASDRVS.SYS`) or networks (please consult the manufacturer's instructions for the relevant call parameters). The keyboard driver may also have a different name. Please do not enter any programs or files in `CONFIG.SYS` which are loaded via a hard disk, i.e. do not use 'C:' etc.!

Be sure to include the drivers for your CD-ROM drive: these usually comprise a `*.SYS` driver supplied by the manufacturer for `CONFIG.SYS` and the `MSCDEX.EXE` of your DOS version for `AUTOEXEC.BAT`.

Then copy a few other important operating system programs to this disk, e.g.:

```
FDISK.*
COMP.*
KEYB.*
FORMAT.*
LABEL.*
HIMEM.*
SYS.*
DISKCOPY.*
DEBUG.*
XCOPY.*
```

Once again, you can add any other programs you want to hang on to.

Then copy the most important utilities to the disk. Essential utilities are your Backup program, its corresponding Restore program and - if available - the Norton Utilities. If you don't have enough space on your disk, you can store these programs on other resource disks which you know to be clean.

To complete your 'verifiably clean DOS disk', slide the write-protect tab to the 'open' position (on a 3½' disk) and keep the disk in a safe place (where you are likely to find it again!).

First Aid: Virus Found

AntiVir has found a virus or other malware.

As a rule, there is no cause for alarm if AntiVir or the AntiVir Guard finds a virus in an everyday situation: such viruses will be removed either with or without prompting depending on the AntiVir configuration (for details of the possible ways of handling concerning files, see the description of the available options).

If AntiVir encounters an **active virus in the memory** during installation or on starting the program, you will be notified by a message which you can't miss.

In this case, you are asked to boot from a write-protected system disk (either your 'verifiably clean DOS disk', a bootable Windows start disk or the bootable AntiVir CD-ROM).

Once you have been notified of a firmly suspected virus: **do not carry out a warm start, e.g. with (Ctrl)+(Alt)+(Del) or a boot program, as some resident viruses can survive this.** Make sure you only start programs from the emergency or system disks, as the programs on the hard disks may already be infected.

1. Make a backup of the relevant data medium - a backup with a virus is better than no backup at all.
2. Start your computer from the verifiably clean DOS disk.
If you don't have a 'verifiably clean DOS disk', you can also use the original DOS installation disk, except that you won't be able to use certain system files and tools which could make life easier for you. Do **not** access the hard disk, as the *.COM, *.EXE and other executable files may already be infected.

The easiest (and usually most successful) way is to remove the virus with the program `AVE32.EXE`:

3. Boot your computer system from a 'verifiably clean DOS disk' or the bootable AntiVir CD-ROM.
4. The drivers for your CD-ROM drive (usually a *.SYS driver supplied by the manufacturer for `CONFIG.SYS` and the `MSCDEX.EXE` of your DOS version for `AUTOEXEC.BAT`) must be available and activated. If not, install these drivers now.
5. Insert the H+BEDV Datentechnik GmbH CD-ROM in the CD-ROM drive and your license disk containing the file `HBEDV.KEY` in the 3 1/2' drive if you have not already done so.
If you received the license file (`HBEDV.KEY`) by email, you should copy the file on a disk.
6. At DOS level, call the program `AVE32` with the parameter `/ALLHARD` on the CD-ROM in the directory `ANTIVIR\`. The command line should look like this:
`X:\...\ANTIVIR\AVE32.EXE /ALLHARD`
The 'x:' stands for the letter of the CD-ROM drive containing the H+BEDV Datentechnik GmbH CD-ROM.
7. Confirm this DOS command line with the 'Return' key.

Without any further inputs, `AVE32` will now test all files in all subdirectories on all accessible drives including all boot records starting with drive A: **Any detected viruses will not be deleted in this mode. Abnormal events such as a corrupt file or a virus are reported in the report window of AVE32.**

8. If infected files are reported, you should carry out a repair routine with `AVE32` using the parameter `/e`. **Please note that any irreparable files will be deleted in the process.** You should therefore make sure you don't need these infected files first.

Once you have successfully completed this procedure, AntiVir can usually be installed or started without difficulty.

9. Start a scan on all accessible drives by clicking the 'Scan' button.
If no more viruses were found in the memory but infected files were reported, we recommend that you check all program files of *all* available drives and data media for viruses. This is because some viruses don't only spread on the current drive, but also infect other data media, especially floppy disks and exchangeable hard disks, as well as network drives.
10. Check the report file to see whether all viruses were repaired or whether some files were irreparable.
11. Once all files have been successfully repaired and the corrupt files deleted, your computer is virus-free. If you have not deleted corrupt files, the virus could be activated when you load the files in question (if they are still executable), and thus start spreading again. You should handle these files with extreme caution: we recommend that you delete them in any case and copy or install the files on the hard disk again from the original disks or a virus-free backup

If AntiVir for Windows still refuses to be installed or loaded, there is a second, more time-consuming way of solving virus problems via a temporary Windows version:

- a) Boot from a non-infected Windows start disk.

If you do not have a 'verifiably clean Windows disk', we recommend that you reinstall Windows in a temporary directory from the write-protected original disks - even if it means a lot of extra work.

Whatever you do, do not start Windows from the hard disk, as some Windows files may already be infected. If you do not have a 'verifiably clean Windows disk', we recommend that you reinstall Windows in a temporary directory from the write-protected original disks - even if it means a lot of extra work.

- b) Create a temporary directory (e.g. TEMPWIN) and copy all the files from the 'verifiably clean Windows disk' to this directory, taking care to maintain the directory structure.
- d) Start Windows from this directory.
- e) Make sure you **only start the programs and tools from this directory**. All other programs on the drive may already be infected.
- f) Reinstall AntiVir from the original disks.
- g) When asked whether you want your hard disk to be scanned for viruses, answer 'Yes'.
- h) Once it has been successfully installed, load AntiVir.
- i) Under the menu item 'Options/Repair', you can choose whether or not to confirm the repair procedure for each infected file.
- k) Start a scan by clicking the 'Scan' button
If no viruses were found in the memory but infected files were reported, we recommend that you check all program files of *all* available drives and data media for viruses. This is because some viruses don't only spread on the current drive, but also infect other data media, especially floppy disks and exchangeable hard disks, as well as network drives.

- l) Check the report file to find out whether all files were repaired or whether some were deemed irreparable.

Once all files have been successfully repaired and the corrupt files deleted, your computer is free of viruses. If you have not deleted corrupt files, the virus could be activated when you load the files in question (if they are still executable), and thus start spreading again. You should handle these files with extreme caution: we recommend that you delete them in any case and copy or install the files on the hard disk again from the original disks or a virus-free backup.

AntiVir distinguishes between the following:

File Virus

Boot Record Virus

Partition Table Discrepancy

Virus Information

The following section provides information on two viruses which have caused recent uproar, namely the ExploreZip virus and the CIH virus.

Detecting the ExploreZip virus with AntiVir

General information:

W32/ExploreZip (listed under Tr.ExploreZip.Worm in our products)

| | |
|------------------|--|
| Alias: | Worm.Explore.Zip Zipped Files Troj.Explore.Zip |
| Characteristics: | Trojan horse, worm |
| Text string: | zipped_files |
| Length: | 210432 bytes |
| Platform: | Windows 9x/Windows NT |

W32/ExploreZip is spread via email on Windows 9x and Windows NT computer systems. Email programs at risk include any email client with MAPI capability, e.g.:

MS Outlook
NetScape Mail
MS Exchange
Outlook Express

In the active state, it spreads via MAPI commands by sending itself as an attachment with the name 'zipped_files.exe'. Unlike Melissa, W32/ExploreZip sends itself automatically to the addresses of unanswered mail in the inbox. Melissa, on the other hand, sent copies of itself to up to 50 recipients from the address book.

This trick makes the email look perfectly harmless to the recipient - a normal reply to a message sent to a known recipient.

An infected email looks like this:

From: *[name of email sender]*
Subject: re:*[subject of unanswered message]*
To: *[name of email recipient]*
Hi *[name of email recipient]* !
I received your email and I shall send you a reply ASAP.
Till then, take a look at the attached zipped docs.
Bye or sincerely
[Name of email sender]
Attachment: zipped_files.exe

By then, however, the virus is already active and 'at work'. It copies itself either under the name 'Explore.exe' or '_setup.exe' to the respective system directory, i.e. %windir%\System (normally c:\windows\system) under Windows 9x or %windir%\System32 (normally c:\winnt\system32) under Windows NT.

It then modifies the WIN.INI file under Windows 9x or the registry under Windows NT. By modifying the INI file or registry, the virus ensures that it will be reloaded every time you boot the system. That way it can answer new incoming mail too.

The damage routine of the virus is multi-threading, i.e. it generates two 'killer threads'. One of these threads is responsible for 'email handling' and the other for 'emptying' files. The first thread monitors new incoming mails via MAPI. This enables it to 'answer' incoming emails immediately with itself. Existing unread messages are also answered immediately.

A second thread 'empties' files with the extensions '.doc', '.c', '.cpp', '.h', '.asm', '.xls' and '.ppt'. 'Emptying' means shortening the files to 0 bytes via the Windows function 'Create File'. This means that files are not deleted, nor can they be restored via the recycling bin. They cannot be restored, however, because their contents have been lost.

Increased hard disk activity is a sign that files are being emptied. However, the virus also empties files which are available via 'mapped' drives up to the drive letter 'Z:' which are used as network drives (WnetEnumResource).

The damage routine of the virus remains active as long as the virus itself remains in the memory. The virus can be removed quite easily, however, by deleting the infected files and modifying WIN.INI or the registry.

Removing the autostart entries under Windows 9x:

These can be removed from WIN.INI (via SysEdit) by deleting the following line:

run=C:\WINDOWS\SYSTEM\Explore.exe

(run=%windir%\SYSTEM\Explore.exe)

or

run=C:\WINDOWS\SYSTEM_setup.exe

(run=%windir%\SYSTEM_setup.exe)

Removing the autostart entries under Windows NT:

Remove a key from the following registry path (via RegEdit):

HKEY_CURRENT_USER\Software\Microsoft\WindowsNT\CurrentVersion\Windows

Delete the following entry under \Run:

run=C:\\WINNT\\SYSTEM32\\Explore.exe

(run=%windir%\SYSTEM32\Explore.exe)

or

run=C:\\WINNT\\SYSTEM32_setup.exe

(run=%windir%\SYSTEM32_setup.exe)

Removing the infected file under Windows 9x:

After a restart or 'zapping' of the virus via the Task Manager, the virus itself should be deleted. The file can be found under the name 'Explore.exe' or '_setup.exe' under:

c:\windows\system\Explore.exe

or

c:\windows\system_setup.exe

Removing the infected file under Windows NT:

The paths for Windows NT are (after restart or 'zapping'):

c:\winnt\system32\Explore.exe

or

c:\winnt\system32_setup.exe

The danger of emails with unknown file attachments cannot be stressed enough, therefore. It is also rather unusual for documents to be sent with self-extracting .EXE files. Users should check all files of their computer system with suitable AntiVir programs once in a while purely as a precautionary measure. That way the temporary files of the various email programs will also be checked and any viruses they may contain detected.

Again, the aggressive destructive part of this virus clearly shows how a systematic assignment of rights within networks can limit the damage inflicted.

General information on the W95/CIH virus:

| | | |
|------------------|-------------------------------------|---------------|
| Name: | W95/CIH | |
| Alias: | PE_CIH, CIH | |
| Characteristics: | Resident, PE infector (Windows-EXE) | |
| Text string: | Version 1.2 | CIH v1.2 TTIT |

| | | |
|-----------|-----------------------|-----------------|
| | Version 1.3 | CIH v1.3 TTIT |
| | Version 1.4 | CIH v1.4 TATUNG |
| Length: | Version 1.2 | 1003 bytes |
| | Version 1.3 | 1010 bytes |
| | Version 1.4 | 1019 bytes |
| Platform: | Windows 95/Windows 98 | |

W95/CIH is a resident virus which attacks Windows programs (PE files). It infects PE files in such a way that the length of infected files remains unchanged. By using its knowledge of unused areas within these PE files, it is able to divide itself into several parts. W95/CIH contains the following destructive damage routines: overwriting of the BIOS in the flash ROM and overwriting all hard disks.

This virus has been an increased incidence of this virus recently in USA. Central Command already provided an effective and powerful detector with version 5.13.1. From version 5.13.2, however, it is also possible to repair this virus. For this purpose, AntiVir does not follow the usual course of simply deactivating the load function of the virus ('butcher's knife method'), but repairs the file using the more subtle 'scalpel method'. Since W95/CIH divides itself into several parts when infecting a file and spreads these over different sections of the file, all the sections modified by the virus have to be treated separately by the repair routine. That way AntiVir does not run the risk of leaving parts of the virus intact.

Many other AntiVir programs simply overwrite the installation routine of the virus or 'repair' it solely by correcting the program entry. This means that other parts of the virus in the (still infected) file remain in executable form. In other words, the damage routines are still present in the file and may still be capable of uncontrolled execution (e.g. due to a program crash, an error in the host program, a double infection, etc.).

Since AntiVir knows the exact structure of both the virus and the PE files, it is able to carry out quality repairs. AntiVir removes the individual parts of the virus in the various sections and restores the internal management information of each section. That way the programs are safe to use again after having been repaired by AntiVir.

The damage routines of the virus vary from one version to the next. Version 1.2 attempts to overwrite the BIOS in the flash ROM on 26 April and version 1.3 on 26 June of a particular year. Version 1.4, which is currently the most widespread, appears to be a refinement of previous versions, and attempts to overwrite the BIOS in the flash ROM on the 26th of every month. Common to all versions is their additional habit of overwriting all hard disks on the relevant trigger date by direct access. This is likely to render most emergency disks worthless unless a full backup is available in addition!

Viruses and other malware

Malware

Malware (malicious software) is the collective term for all kinds of programs with harmful functions. Malware is characterised by concealed functions which can trigger uncontrollable damage within IT systems or in data stocks through deletion, overwriting or manipulation. Malware generates extra work and costs, adversely affects the confidentiality and availability of programs and data and is in some cases able to spread by itself.

The category malware includes viruses (e.g. access viruses, Active-X viruses, AmiPro viruses, batch viruses, boot and master boot record viruses, companion viruses, file viruses, DOC viruses in RTF files, droppers, email viruses, Excel macro viruses, file system viruses, packed viruses, HTML viruses, Java viruses, Linux viruses, Macintosh viruses, multipartite viruses, OS/2 viruses, PDA viruses, polymorphic file viruses, polymorphic macro viruses, PowerPoint macro viruses, script viruses, stealth viruses, TSR viruses, viruses in embedded OLE, viruses in compressed-runtime files, viruses in shell scrap files, Visio viruses, Word macro viruses), Trojans (incl. logic bombs) or worms.

Viruses

A computer virus is a program with the ability to 'attach' itself automatically in some way to other programs when loaded, thus infecting those programs. Viruses are self-reproducing, a feature which distinguishes them from Trojans and bombs. They do not necessarily have to contain destructive program elements, however. A computer virus essentially requires a foreign code (host code), the sequence of which it alters by infecting it. The hosts serve merely as a vehicle, i.e. the sequence of the host code is not changed.

The definitions given here correspond to those in Martin Rösler's German virus FAQs (Frequently Asked Questions).

Worms

The term 'worm' has two meanings. The first definition is: 'Program which duplicates itself within networks and steals processing time'. This occurs on networked mainframes, for example, as a result of process bifurcation.

The second definition is: 'A worm is a program which duplicates itself but does not infect any host codes'. An example would be a program called WURM.COM containing commands telling it to copy itself to all available drives in the active folder. Worms cannot therefore become part of other program sequences and only constitute a hazard if they generate their own task within multitasking systems and are able to trigger themselves as part of this task. Otherwise a worm can only be spread by human intervention when started by the user.

Trojan horses

A Trojan horse or Trojan is a program which purports to have a useful function, but, once loaded, reveals its true self and begins its (usually) destructive work. Trojans differ from viruses and worms in that they cannot duplicate themselves. Most Trojans are programs with either an inconspicuous or an intriguing name (STARTME.EXE or SEX.EXE), which are activated immediately on execution and may format the hard disk or mix up data, for example. There is also a special kind of Trojan called a dropper: this implants viruses and is thus itself a 'victim' which infects the computer when the Trojan is called, thereby causing a snowball effect.

The definitions given here correspond to those in Martin Rösler's German virus FAQs (Frequently Asked Questions).

Logic bombs

Strictly speaking, a logic bomb (or bomb for short) is a special kind of Trojan horse. Bombs are

program sections which are embedded in useful code and which consist of a trigger and a payload. The destructive functions of such bombs lie dormant for a certain period of time. However, when a trigger condition is eventually fulfilled (e.g. after reaching a certain date or loading the program fifty times), the bomb 'explodes' and begins its destructive work.

A special case is the so-called ANSI bomb which redefines the keyboard configuration via the ANSI.SYS driver.

The definitions given here correspond to those in Martin Rösler's German virus FAQs (Frequently Asked Questions).

