About AntiVir Guard

The AntiVir Personal Edition with the resident scanner AntiVir Guard has been developed especially for home users. It is completely free of charge for private use and can be obtained from the following Internet URL: http://www.free-av.com.

AntiVir 6 Professional

If you need support of network drives or if you need any more functionality, we recommend the enhanced version of AntiVir: AntiVir 6 Professional.

Currently there are the following AntiVir products available:

DOS, Windows 3.1x, Windows 9x, Windows Me, Windows NT, Windows 2000, Windows XP, OS/2, Linux (i386), FreeBSD (i386), OpenBSD (i386) Novell NetWare, Windows 2000 Server, Exchange Server, Exchange Workstation, Outlook, Eudora Mail Client and MS Mail.

More information about these products is available from one of the address below or from the Internet:

H+BEDV Datentechnik GmbH	Internet:	http://www.hbedv.com
Lindauer Strasse 21	Email:	info@hbedv.com
88069 Tettnang	Phone:	+49 (0) 7542 - 500 0
Germany	Fax:	+49 (0) 7542 - 525 10

About AntiVir Guard

This dialog box displays some information about the AntiVir Guard VxD and the control program.

Hotline

Technical support is available via Internet only.

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.

Additional Product Information

This section contains the information how to contact us if you need information or assistance concerning our AntiVir Professional products.

AntiVir Professional Edition

Besides the AntiVir Personal Edition, H+BEDV Datentechnik GmbH offers the **AntiVir 6 Professional Edition**. This package provides a much enhanced functionality and a flexible and cheap licensing, especially in multi-user environments.

Additional Features:

- ▶ Support of network drives.
- ▶ Support of network messages and warnings.
- ▶ Support of search profiles.
- ▶ Scanning of single and multiple directories.
- ▶ Scanning of user-defined archives.
- ▶ Explicit scanning of boot records.
- ▶ Intranet-Update-Wizard. This is a tool to distribute the software in your network.
- ▶ Start of external programs depending on the search results.
- ▶ Scheduler.
- ▶ Password protection for the configuration.
- ▶ CRC option.
- ▶ Enhances configuration possibilities for the scan- and repair engine.
- ▶ The email scanner for MS Mail, Qualcomm Eudora, MS Outlook and MS Exchange Client are included.

Currently there are the following AntiVir products available:

DOS, Windows 3.1x, Windows 9x, Windows Me, Windows NT, Windows 2000, Windows XP, OS/2, Linux (i386), FreeBSD (i386), OpenBSD (i386) Novell NetWare, Windows 2000 Server, Exchange Server, Exchange Workstation, Outlook, Eudora Mail Client and MS Mail.

Information about these products is available at:

H+BEDV Datentechnik GmbH	Internet:	http://www.hbedv.com
Lindauer Strasse 21	Email:	info@hbedv.com
88069 Tettnang	Phone:	+49 (0) 7542 - 500 0
Germany	Fax:	+49 (0) 7542 - 525 10

Configuration

This menu displays a property sheet to configure the AntiVir Guard.

The button has the same effect.

The property sheet contains the following property tabs:

Scanner   All settings used by the scanner.
Action   Actions to perform if a virus or unwanted program has been found.
Heuristic   Settings for the AntiVir virus heuristic.
Report   Report file settings

Contents

The following pages are available:

Demo Version

Demo-Version

If you don't have a valid license key file, AntiVir Guard Personal Edition will run in the restricted demo mode. This means that it will only scan files on the volume C: of your computer.

Exit and Close

Select this function if you wish to exit the control program of the AntiVir Guard and close it completely. Thereafter, the program can only be started via the corresponding icon in the program folder of AntiVir Guard.

Exit and Minimize

or use the button

Select this entry if you wish to exit the AntiVir Guard control program without closing it completely. In this case, it will be reduced in size (minimized) and you will then see the program icon in the bottom right-hand corner of the taskbar display area.
To enlarge the control program again, simply double-click on the reduced icon. In the minimized state, the program does not take up any CPU cycles. After minimizing the icon, you can call up the Context menu by clicking the right mouse key on the reduced icon.

File Action

In this box, you will see the currently selected action to be performed by AntiVir Guard in case of a detection.

Repair File

AntiVir Guard will try to repair the reported file. If a repair is not possible, the action set with <u>Action if file not repaired</u> will be taken.

Please note that the following actions will only be performed if the concerning file is unable to be repaired.

Delete File

The concerning file will be deleted. It is not possible to restore the file anymore.

Move File

The concerning file will be moved to the quarantine directory set in the filed <u>Quarantine Directory</u>. The files in this directory can be repaired later on or you can send us such files for further investigations if needed.

Rename File

The concerning file will be renamed to *.VIR. Any direct shell shortcut to the file will be disabled. You can re-rename and repaired the file later on.

Deny Access

AntiVir Guard will deny access to an concerning file. If enabled, only an entry will be written to the <u>logfile</u>.

File Extensions

The file extensions used by AntiVir Guard when <u>Use file extension list</u> is enabled are stored in this list.

You can edit the list as follows:

{button OK,}

> This closes and saves the current list

{button Cancel,}

> The changes made are cancelled.

{button Insert,JI(`',`HELP_EDIT_EXTENSION')}

> Opens a window to edit and insert a new file extension.

{button Delete,}

> This deletes the currently marked item in the list.

{button Default,}

> The list in this window shows all file extensions to be included in a scan if the option <u>Use file extension</u> list is activated. By default, the most common program file extensions are selected, along with any documents which might also contain macros.
>
> **N.B.**: Resetting this list to the default setting will cause your own modifications and entries to be lost.

{button Help,}

> Displays this help screen

Main Window

The main window of AntiVir Guard for Windows (Personal Edition) consists of 3 main areas: the menu bar, the tool bar and the display area for statistical data. More detailed statistical data and additional configuration options are available with our professional version, AntiVir 6 Professional.

The menu bar options

File
Options
Help

Display group: AntiVir Guard

VxD-Status	shows the current status of the AntiVir Guard VxD (Active, Not Active, Not Loaded).
Notify User	notify the user when an detection occurs or take the action automatically.
File Action	this field shows the action to be performed when the user warnings are deactivated.
Files To Scan	indicates what is to be scanned: all files or only those with special file endings (program files).
File Count	shows the number of scanned files.
Last Detection	tells you the name of the last detected virus or unwanted program.
Detections	display the number of detected viruses or unwanted programs.

Display group: Last scanned file

This field displays the last file scanned by AntiVir Guard.

New File Extension

You can enter a new file extension in this dialog box. The maximum length of a new extension is 6 characters.

{button OK,}

The current extension will be inserted into the list of file extensions.

{button Cancel,}

The current extension will be thrown away and not inserted into the file extension list.

{button Help,}

Displays this help screen.

Property Tab Action

This sheet configures how AntiVir Guard shall react if a virus or unwanted program has been detected.

Action if file not repaired

When AntiVir Guard discovers a virus or unwanted program, it will display a text mode dialog to let the user selects the action to be taken. If the file could be repaired and the auto-repair mode is enabled, the user can select to repair the file. If this repair fails, the action selected in this group box will be taken. If the user selects another option in the displayed dialog box, the selected action will be taken.

Delete file

The concerning file will be deleted but can be restored using appropriate tools.

Move to quarantine directory

The concerning file is placed in the quarantine directory so that it can no longer be directly accessed.

The files in this directory can be subsequently repaired or - if necessary - sent to us for further analysis.

Please note that only the administrator should have access to this directory.

Rename file to *.VIR

The concerning file is renamed according to the pattern *.v01, *.v02 etc. This means that it can no longer be executed directly by the shell. You can repair these files later on and rename them back again.

Deny access to file

The detection is merely entered in the report file if activated.

Quarantine directory

If a file is to be moved to the Quarantine Directory, AntiVir Guard will move it to the directory specified in this field.

Property Tab Heuristic

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 a 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.

Property Tab Report

AntiVir Guard has a very powerful reporting function included. It is able to give the administrator a complete report of what's going on with your machine.

Report file

Reporting enabled

If selected, AntiVir Guard will activate the reporting feature. A default report file name will be inserted to the edit field for the logfile name.

Name of logfile

This is the name and the path of the report file to write. Each entry will be added to this file.

Property Tab Scanner

These settings are used to configure the scanner of AntiVir Guard.

Files to scan

AntiVir Guard can be configured to use a filter to exclude some files that are normally not hosts for viruses and unwanted programs. This can improve the system performance depending on you environment.

All Files

If this option is selected, all files are automatically scanned for viruses and unwanted programs.

Use file extension list

In this case, only files with a file extension included in the list are scanned for viruses and unwanted programs.

{button File extensions,JI(`',`HELP_FILE_EXTENSIONS')}

The button "File Extensions" opens a window containing a list of all extensions included by AntiVir Guard in a scan. Default extensions are already set, but you can add or remove entries as required. Please note that the default list may vary from one version to another.

Drives

At least with the AntiVir Professional Edition AntiVir Guard may monitor network and local drives differently. The Personal Edition only supports local drives.

Reported files

Repair automatically

This function is used to activate the repair mode of AntiVir Guard. Unless this option is activated, AntiVir Guard cannot repair reported files and does not offer to do so in the dialog box.

In other words, this option **must be activated** in order to be able to select the repair option on receipt of a warning message.

System shutdown

Warn if floppy disk in drive A:

If this option is activated, AntiVir Guard checks before shutting down the system whether there is still a floppy disk in drive A:. If so, you will receive a corresponding warning message. This option is recommended, as many viruses are still spread via the boot records of floppy disks. If you forget to remove an infected floppy disk from drive A: on shutting down the computer and the starting option in the BIOS of the computer is set to A: / C:, you run the risk of infecting it with a boot record virus next time you boot the system. In fact, if you see the message "Non system disk or disk error", a virus or unwanted program may already have infected your system.

The File Menu

This menu contains the following sub menus:

Activate AntiVir Guard

This menu option activates and deactivates AntiVir Guard. After initial installation, AntiVir Guard should always be ready activated. You can use this menu option to activate AntiVir Guard (tick visible) or temporarily deactivate it (tick invisible).

Start AntiVir Main Program

This is a shortcut to start the AntiVir Main Program (on-demand scanner) easily.
This menu option is an easy way of starting the AntiVir main program from AntiVir Guard, e.g. in order to carry out a scan on the entire C:\ drive.

Start Internet Update

The internet updater can now also be started via this menu option. This improves user-friendliness, as you no longer have to load the main program whenever you want to start the updater. This menu option is only selectable provided the internet updater is already installed and activated.

Exit and Minimize or button

Select this entry if you wish to exit the AntiVir Guard control program without closing it completely.

Exit and Close

Select this entry if you wish to exit the control program and close it completely.

The Help Menu

In this menu, you will find information on AntiVir Guard and how to operate it.

<u>**Help (F1)**</u> **or** **button**

   Opens the context-sensitive help system (these pages).

<u>**Using Context Sensitive Help**</u>

   This tells you how to use the context-sensitive help system.

<u>**Help Index**</u>

   Displays a page containing cross-references to all available help pages.

<u>**About AntiVir Guard**</u>

   This menu option opens a window containing further information on AntiVir Guard together with our addresses.

The Options Menu

This menu contains the following entry:

<u>Configuration</u> or button

　　Select this to configure the AntiVir Guard.

Trouble Shooting

If AntiVir Guard Personal Edition does not work properly or if you have any problems with AntiVir Guard or if you have an detection which you are not able to manage yourself, please check the following:

▶   Please check if the VxD is active. The small red umbrella in the system tray must be opened. Please activate the VxD if necessary by clicking the item <u>Activate AntiVir Guard</u> in the "File" menu.
▶   Check the settings of the group <u>Files To Scan</u>. If <u>File extensions</u> is selected, you should have a look into the <u>file extension list</u>. Please set it to default values if needed.
▶   To be able to repair a file, it is important that the option <u>Repair automatically</u> is enabled.
▶   It is strongly recommended that you do not use resident virus guards from other vendors besides AntiVir Guard. Multiple virus guards lead to an instable system in most cases.

More information can be found in the file README.TXT in the program directory of AntiVir or in the internet at <u>www.free-av.com</u>.

AntiVir Support Forum

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

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

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.

To enable us to help you efficiently, please add the following information to your request:

- Version information of virus definition file, serach engine and program.
- The version information of your operating system and the possibly installed service packs.
- Installed software packages, e.g. antivirus applications from other vendors.
- The exact (!) messages displayed by the application or shown in the logfile.

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

Virus Infection

This provides a brief introduction to the steps to take if AntiVir Guard finds a virus, for example. Please note that there are some limits to the functionality of the AntiVir Personal Edition. Should you require antivirus software for other platforms or an extended range of functions, we would recommend the version AntiVir 6 Professional.

If AntiVir Guard detected a virus ...

1. Don't panic and beware calm!

AntiVir Guard has done all the important jobs automatically if it is configured correctly. If you tried to access or to start an infected file, it will be disinfected or moved or the access to this file will be denied. After successful disinfection, you can work with that file as usual. If disinfection is not possible, the file will be normally moved to the quarantine directory and you'll get a warning.

2. Follow the antivirus instructions step by step, don't rush the things!

Now, it is important to check your complete workstation and all possibly infected floppy disks for viruses. It would be a good choice to let AntiVir do this job since it has already been installed on your system. Please try to disinfect all infected files and boot records on your hard disk and all floppy disks. Ask your dealer or call H+BEDV if you need any assistance. Possibly it would be a good idea to activate the automatic repair option inside AntiVir Guard. If AntiVir or AntiVir Guard is not able to disinfect the file, please send us a copy for further analysis. We will provide you with a solution as fast as possible. At least, try to investigate where the virus did come from. Check your anti-virus strategy if needed to beware of further infections.

3. Inform your colleagues, your boss and your business partners!

It is not a very pleasant job, however information is very important in such cases. Especially, if the virus has been imported from outside your site. Please inform your colleagues, your boss or your security manager about the infection!

4. Unknown new viruses and suspicious files

Please send new unknown viruses and suspicious files in an encrypted archive as an email attachment to virus@free-av.com. Please don't forget to mention the password and a short virus/file description.

VxD-Status

This field displays the current service-status of AntiVir Guard VxD.

Active

This means that the scan of the VxD is active and in the process of being carried out according to the settings.

Not Active

The AntiVir Guard VxD scan has been deactivated. In other words, no scan is being carried out and all files can pass through the system unchecked.

Attention: When the Guard is deactivated, you have no automatic protection against viruses and unwanted programs!

Not Loaded

The resident virus guard AntiVir Guard VxD is not loaded. In other words, no scan is being carried out and all files can pass through the system unchecked.

Attention: When the Guard is deactivated, you have no automatic protection against viruses and unwanted programs!