

# About AntiVir Guard

The AntiVir PersonalEdition Classic 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 ProfessionalEdition

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

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**  
Lindauer Strasse 21  
88069 Tettnang  
Germany

Internet: <http://www.hbedv.com>  
Email: [info@hbedv.com](mailto:info@hbedv.com)  
Phone: +49 (0) 7542 - 500 0  
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 PersonalEdition Classic 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 ProfessionalEdition products.

## 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@free-av.com](mailto:virus@free-av.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.

# AntiVir ProfessionalEdition

Besides the AntiVir PersonalEdition Classic, H+BEDV Datentechnik GmbH offers the **AntiVir ProfessionalEdition**. 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**  
Lindauer Strasse 21  
88069 Tettnang  
Germany

Internet: <http://www.hbedv.com>  
Email: [info@hbedv.com](mailto:info@hbedv.com)  
Phone: +49 (0) 7542 - 500 0  
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:

<b><u>Scanner</u></b>	All settings used by the scanner.
<b><u>Action</u></b>	Actions to perform if a virus or unwanted program has been found.
<b><u>Heuristic</u></b>	Settings for the AntiVir virus heuristic.
<b><u>Report</u></b>	Report file settings.
<b><u>Unwanted Programs</u></b>	AntiVir reports detected viruses or malware as a matter of course. If you wish, you can also set it to report unwanted programs.

# Contents

The following pages are available:

[About AntiVir Guard](#)  
[AntiVir ProfessionalEdition](#)  
[Configuration](#)  
[Demo Version](#)  
[Exit and Close](#)  
[Exit and Minimize](#)  
[File Extensions](#)  
[Main Window](#)  
[New File Extension](#)  
[Property Tab Action](#)  
[Property Tab Heuristic](#)  
[Property Tab Report](#)  
[Property Tab Scanner](#)  
[Property Tab Unwanted Programs](#)  
[The File Menu](#)  
[The Help Menu](#)  
[The Options Menu](#)  
[Trouble Shooting](#)  
[Unwanted Programs](#)  
[Virus Infection](#)  
[VxD-Status](#)

# Demo Version


## Demo-Version

If you don't have a valid license key file, AntiVir Guard PersonalEdition Classic 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 Extensions

The file extensions used by AntiVir Guard when Use file extension list 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 Use file extension 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 (PersonalEdition Classic) 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 ProfessionalEdition](#).

## The menu bar options

File  
Options  
Help

## Display group: AntiVir Guard

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

In this dialog the actions are configured that AntiVir Guard is to perform if a virus or unwanted program is found.

## Action to be taken

If AntiVir Guard detects suspicious code, it issues an alert. Further handling of the file depends on the settings in this group.

### Repair file

The repair mode of AntiVir Guard is enabled. If repair of the file involved is not possible, access to the file is automatically blocked. An alternative option can also be selected in the alert dialog (delete, move, rename).

### Delete file

The relevant file is automatically deleted, but can be restored with a corresponding program.

#### Note:

In the alert dialog displayed, no alternative selection possibility is available.

### Move file

The relevant file is moved to the quarantine directory, so that direct access is no longer possible.

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

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

#### Note:

In the alert dialog displayed, no alternative selection possibility is available.

### Rename file

The relevant file is automatically renamed \*.vir etc. Direct Shell access to these files (e.g. double click) is generally no longer possible. You can repair and rename these files later.

#### Note:

In the alert dialog displayed, no alternative selection possibility is available.

### Deny access to file

If this option is selected, the detection is only entered in the report file if activated. If the option It is possible to select in the alert dialog whether the file should be deleted, moved or renamed. If the file involved can be repaired, this option is also available.

## Quarantine directory

If a file is to be moved, AntiVir Guard will transfer it to the directory indicated in this box.

# Property Tab Heuristic

This property tab contains the settings the heuristic of the AntiVir search engine.

AntiVir contains very powerful heuristics that can also detect unknown (new) viruses, worms or Trojans. This is done by intensive analysis and scanning of the corresponding code for functions that are typical for viruses, worms or Trojans. If the scanned code has these characteristic features, it is reported as suspicious. However, this does not necessarily mean that the code is actually a virus, a worm or a Trojan; false alerts may also occur. The user has to decide what to do with the relevant code, e.g. based on his knowledge of whether the source containing the code is trustworthy.

## Macro virus heuristic

AntiVir contains a very powerful macro virus heuristic. In the event of a possible repair, all macros are deleted, or alternatively suspicious documents are only reported, i.e. you receive an alert.

## Win32 file heuristic

AntiVir contains a very powerful heuristic for Windows file viruses, worms or Trojans that can also detect unknown viruses, worms or Trojans. If it is enabled, you can set how "aggressive" this heuristic should be.

### Detection level low

With this setting AntiVir detects slightly fewer viruses, worms or Trojans, the risk of possible false detections is low.

### Detection level medium

This is the default setting if you have selected to use this heuristic.

### Detection level high

In this setting AntiVir detects very many unknown viruses, worms or Trojans, but you must also expect false reports.

# 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,Jl('`,`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 ProfessionalEdition AntiVir Guard may monitor network and local drives differently. The PersonalEdition Classic only supports local drives.

## 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.

# Property Tab Unwanted Programs

AntiVir protects you against computer viruses.

In addition, it will also scan selectively for dialer, Backdoor Clients, games, jokes, Security Privacy Risk Software, Unusual Runtime Compression Tools, Double Extension Files.

- ▶ Security Privacy Risk (SPR)
- ▶ Jokes (JOKES)
- ▶ Games (GAMES)
- ▶ Dialer (DIALER)
- ▶ Backdoor Client (BDC)
- ▶ Unusual Runtime Compression Tools (PCK)
- ▶ Double Extension Files (HEUR-DBLEXT)

The selection is activated by clicking on the relevant box.

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

The button {button Set to Defaults,} re-establishes the default values suggested by AntiVir.

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.



# 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.

Help (F1) or  button

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

## Using Context Sensitive Help

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

## Help Index


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

## About AntiVir Guard

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:

**Configuration** or button 

Select this menu option to open the window Configuration AntiVir Guard, in which you can edit the settings for AntiVir Guard.

**Show Logfile** or button 

Shows the logfile of the AntiVir Guard.

# Trouble Shooting

If AntiVir Guard 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 Activate AntiVir Guard in the "File" menu.
- ▶ Check the settings of the group Files To Scan. If File extensions is selected, you should have a look into the file extension list. Please set it to default values if needed.
- ▶ 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 [www.free-av.com](http://www.free-av.com).

## 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: <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.

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

- Version information of virus definition file, search 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!**

# Unwanted Programs

Dialer (DIALER)

Games (GAMES)

Jokes (JOKES)

Security Privacy Risk (SPR)

Backdoor Clients (BDC)

Unusual Runtime Compression Tools (PCK)

Double Extension Files (HEUR-DBLEXT)

## Dialer (DIALER)

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 known to him by default. If you have activated the option "Dialer (DIALER)" 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 nevertheless is a desired dial-up program, you can declare it as an exception file in the main program and this file will consequently not be analyzed any longer. In the AntiVir Guard you have the possibility to disable the dialer recognition in the configuration dialogue under Unwanted programs.

## Games (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 Maneuvers" (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 (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 (JOKES)" with a tick under Unwanted programs in the configuration menu, you will be notified accordingly of any findings.

## Security Privacy Risk (SPR)

Software that maybe is able to compromise the security of your system, initiate unwanted program activities, damage your privacy or spy out your user behaviour and might therefore be unwanted.

AntiVir is able to detect "Security Privacy Risk" Software. If you have activated the option "Security Privacy Risk (SPR)" under Unwanted programs in the configuration menu, you will receive a corresponding warning whenever AntiVir reports a find.

## Backdoor Clients (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 Client (BDC)" under Unwanted programs, in the configuration menu, you will receive a corresponding warning whenever AntiVir reports a find.

## Unusual Runtime Compression Tools (PCK)

Files that have been compressed with an unusual runtime compression tool and that can therefore be classified as possibly suspicious.

AntiVir is able to detect "Unusual Runtime Compression Tools". If you have activated the option "Unusual Runtime Compression Tools (PCK)" under Unwanted programs in the configuration menu, you will receive a corresponding warning whenever AntiVir reports a find.

## Double Extension Files (DBLEXT)

Executable files that hide their real file extension behind a false one and that can therefore be classified as possibly suspicious.

AntiVir is able to detect "Double Extension Files" Software. If you have activated the option "Double Extension Files (HEUR-DBLEXT)" under Unwanted programs in the configuration menu, you will

receive a corresponding warning whenever AntiVir reports a find.

# 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 PersonalEdition Classic. Should you require antivirus software for other platforms or an extended range of functions, we would recommend the version [AntiVir ProfessionalEdition](#).

## 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. 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](mailto: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!

