

[www.avira.com](http://www.avira.com)



## User Manual

# **Avira** AntiVir Server

UNIX Server



---

# Contents

<b>Chapter 1. About this Manual .....</b>	<b>3</b>
1.1 Introduction .....	3
1.2 The Structure of the Manual .....	4
1.3 Signs and Symbols.....	5
1.4 Abbreviations .....	6
<b>Chapter 2. Product Information .....</b>	<b>7</b>
2.1 Features .....	8
2.2 Licensing Concept .....	9
2.3 Modules and Operating Mode of AntiVir UNIX Server .....	10
2.4 System Requirements .....	11
2.5 Technical Information .....	11
<b>Chapter 3. Installation .....</b>	<b>13</b>
3.1 Getting the Installation Files.....	13
3.2 Licensing.....	14
3.3 Installing the Dazuko Kernel Module .....	15
3.4 Integration on Samba .....	17
3.5 Installing AntiVir .....	20
3.6 Reinstalling AntiVir .....	28
3.7 Installing AntiVir UNIX Server Using the Graphical Installation Routine .....	29
3.8 Integrating Third-Party Products.....	36
<b>Chapter 4. Configuration .....</b>	<b>37</b>
4.1 Overview .....	38
4.2 Configuration Files .....	38
4.2.1. Configuration File avguard.conf.....	39
4.2.2. Configuration File antivir.conf.....	43
4.3 Configuration Scripts.....	45
4.4 Configuring AntiVir Notifications .....	47
4.5 Configuring the Resident AntiVir Guard .....	50
4.6 Configuring AntiVir Samba Scanner .....	58
4.7 Configuring Regular Updates .....	61
4.8 Testing AntiVir UNIX Server .....	67
<b>Chapter 5. Operation .....</b>	<b>69</b>
5.1 Overview of AntiVir Command Line Scanner .....	69
5.2 Using AntiVir Command Line Scanner .....	73
5.3 Reaction to Detecting Viruses/ Unwanted Programs .....	76
<b>Chapter 6. Graphical User Interface (GUI) .....</b>	<b>77</b>
6.1 Overview.....	77
6.2 AntiVir Scanner.....	79
6.2.1. Operating AntiVir Scanner Using the GUI.....	79
6.2.2. Configuring AntiVir Scanner Using the GUI .....	84
6.3 AntiVir Guard.....	91
6.3.1. Operating AntiVir Guard Using the GUI.....	91
6.3.2. Configuring AntiVir Guard Using the GUI.....	95
<b>Chapter 7. Service .....</b>	<b>101</b>
7.1 Support .....	101
7.2 Online Shop .....	101
7.3 Contact.....	102

---

**Chapter 8. Appendix ..... 103**

8.1 Glossary ..... 103

8.2 Further Information ..... 104

8.3 Golden Rules for Protection Against Viruses ..... 105

# 1 About this Manual

In this Chapter you can find an overview of the structure and contents of this manual.

After a short introduction, you can read information about the following issues:

- [The Structure of the Manual](#) – Page 4
- [Signs and Symbols](#) – Page 5

## 1.1 Introduction

We have included in this manual all the information you need about AntiVir and it will guide you step by step through installation, configuration and operation of the software.

The appendix contains a Glossary which explains the basic terms.

For further information and assistance, please refer to our website, to the Hotline of our Technical Support and to our regular Newsletter (see [Service](#) – Page 101).

Your Avira Team







### 1.2 The Structure of the Manual

The manual of your AntiVir software consists of a number of Chapters, providing you with the following information:

<b>Chapter</b>	<b>Contents</b>
<a href="#">1 About this Manual</a>	The structure of the manual, signs and symbols
<a href="#">2 Product Information</a>	General information about AntiVir software, its modules, features, system requirements and licensing
<a href="#">3 Installation</a>	Instructions to install AntiVir UNIX Server on your system – using both the installation script and the graphical installation routine.
<a href="#">4 Configuration</a>	Directions for optimum settings of AntiVir on your system.
<a href="#">5 Operation</a>	Working with AntiVir, after installation; targeted scanning for viruses and unwanted programs; reactions when viruses and unwanted programs are detected
<a href="#">6 Graphical User Interface (GUI)</a>	General information on GUI; operating and configuring AntiVir UNIX Server using the GUI.
<a href="#">7 Service</a>	Avira GmbH Support and Service.
<a href="#">8 Appendix</a>	Glossary of technical terms and abbreviations, Golden Rules for Protection against Viruses.

## 1.3 Signs and Symbols

The manual uses the following signs and symbols:

Symbol	Meaning
	... shown before a condition that must be met prior to performing an action
	... shown before a step you have to perform
	... shown before the result that directly follows the preceding action
	... shown before a warning if there is a danger of critical data loss or hardware damage
	... shown before a note containing particularly important information, e.g. on the steps to be followed
	... shown before a tip that makes it easier to understand and use AntiVir UNIX Server

For improved legibility and clear marking, the following types of emphasis are also used in the text:

Emphasis in text	Explanation
<b>Ctrl+Alt</b>	Key or key combination
/usr/lib/AntiVir/antivir	Path and filename
ls usr/lib/AntiVir	User entries
<b>Choose component</b> <b>Select all</b>	Elements of the software interface such as menu items, window titles and buttons in dialog windows
<a href="http://www.avira.com">http://www.avira.com</a>	URLs
<a href="#">Signs and Symbols – Page 4</a>	Cross-reference within the document

### 1.4 Abbreviations

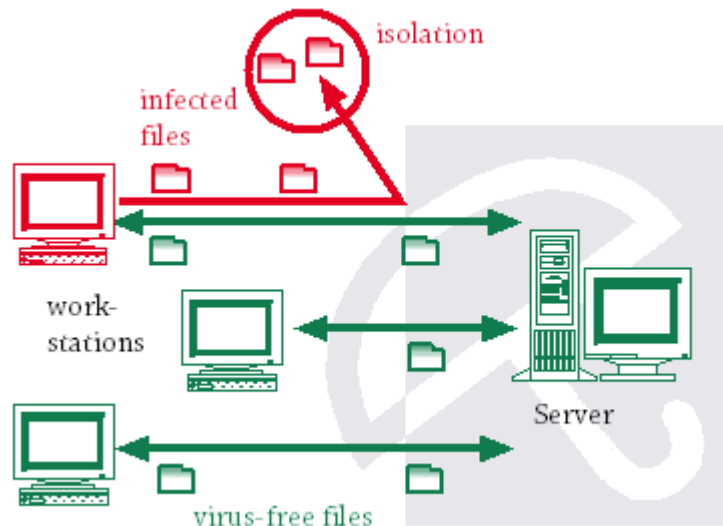
The manual uses the following abbreviations:

<b>Abbreviation</b>	<b>Meaning</b>
FAQ	Frequently Asked Question
FQDN	Fully Qualified Domain Name
GPL	General Public License
GUI	Graphical User Interface
MIME	Multipurpose Internet Mail Extensions
MTA	Mail Transport Agent
PMS	Possible Malicious Software
RFC	Request For Comment
SMTP	Simple Mail Transfer Protocol
VDF	Virus Definition File

## 2 Product Information

You are responsible for numerous workstations and servers in your network but you are only human.

The servers are the heart of the network. So if viruses can freely penetrate and spread on your servers, your network is only a step away from breakdown. This is where AntiVir products for servers come in.



UNIX computers are more often used as file servers or email gateway servers. Thus they transfer and store files that have no connection to UNIX, e.g. Office documents and email attachments. So, viruses can access a server through a Windows Client and freely cause damage.

AntiVir UNIX Server is a comprehensive and flexible tool for confronting viruses and unwanted programs on your server and for reliable protection of your system.

Right from the beginning, two really important hints:



*Losing valuable files usually has dramatic consequences. Not even the best antivirus software can fully protect you against data loss.*

- Ensure that you make regular backups of your files.



*An antivirus program can be reliable and effective only if kept up-to-date.*

- Ensure that you keep your AntiVir programs up-to-date using automatic updates as described in this user guide.

### 2.1 Features

AntiVir UNIX Server offers you extensive configuration possibilities to keep control of your network.

The current features of AntiVir UNIX Server are:

- Easy installation, using the installation script or the graphical installer.
- Simple configuration: support for configuration using the configuration scripts, with help text.
- Command line scanner (On-Demand):  
Configurable search for all known malware types (viruses, Trojans, backdoor programs, hoaxes, worms etc.)
- Resident guard (On-Access):  
Configurable reactions when detecting viruses or unwanted programs: repair, move, block, rename programs or files; automatically remove viruses or unwanted programs.
- Heuristic detection of macroviruses.
- Detection of all common archive types with certain recursion level in the case of nested archives.
- Simple integration with automatic jobs, such as scanning at a set time.
- Automatic updates of AntiVir software via the Internet.
- Comprehensive functions for logging, warnings and messages for the administrator; sending email warnings (SMTP).
- Self-Integrity Program Check, which ensures the antivirus system is operating correctly at all times.
- Optional user-friendly graphical user interface (GUI) for operating and configuring AntiVir UNIX Server.

## 2.2 Licensing Concept

You must have a license to use AntiVir UNIX Server and accept the license terms (see [http://www.avira.com/documents/general/pdf/en/avira\\_eula\\_en.pdf](http://www.avira.com/documents/general/pdf/en/avira_eula_en.pdf)).

There are different license types for using the various functions of AntiVir UNIX Server:

- Demo version
- Full version
- Convenience Package

The license depends upon the number of users in the network who are to be protected by AntiVir.

The license is given in a license file named hbedv.key . You will receive it by email from Avira GmbH. It contains certain data, such as the programs you will use and the period of your license. The same license file may refer to more AntiVir products.

**Demo Version** Without a license file, AntiVir UNIX Server runs as a demo version. You cannot perform automatic updates, so you always have to download the current virus definition files and the new versions of AntiVir scan engine manually from our website.

It is not possible to block access to infected files, to repair or to move them with AntiVir.

**Evaluation Version** Details of the evaluation version can be found on our website: <http://www.avira.com>.

**Full Version** The range of full version features includes:

- Provision of AntiVir versions by Internet download
- License file by email, for converting the demo version to a full version
- Complete installation instructions (digital)
- PDF manuals available for Internet download
- Four weeks installation support, starting from acquisition date
- Newsletter service (by email)
- Internet update service for program files and VDF

- Convenience Package
- In addition to the full version license, the Convenience Package includes:
- Every three months: free delivery of a boot-CD-ROM with the AntiVir Rescue System and all updated AntiVir products
  - Complete installation manual (printed) on first delivery
  - License file on a floppy disk with the first delivery
  - Newsletter service (printed, regular mail delivery)

## 2.3 Modules and Operating Mode of AntiVir UNIX Server

The AntiVir UNIX Server security software consists of the following program components:

- AntiVir Command line scanner
- AntiVir Guard
- AntiVir Samba Scanner
- Internet Updater

### AntiVir Command line scanner

... can always be launched from the command prompt (**on-demand**). Infected files and suspicious macros can be isolated, cleaned or deleted using a number of options. It can be integrated and used within scripts.

### AntiVir Guard

... runs as a daemon process. It permanently monitors all user access in the network (**on access**) and it protects the files against viruses and unwanted programs. It immediately blocks access to infected files which can be automatically renamed, repaired or moved.

### AntiVir Samba Scanner

... runs as a daemon process. It constantly monitors the file traffic through Samba Service (dedicated file and print server for Windows and UNIX workstations). It immediately blocks access to infected files which can be automatically renamed, repaired or moved. Apart from the administration log entries, it issues notifications for the remote users of the files.

### Internet Updater

... ensures that AntiVir is always kept up to date using your Internet connection. It checks if there are any new files to download and automatically updates your software if necessary.

### 2.4 System Requirements

AntiVir UNIX Server asks for the following minimum system requirements on your server:

- Computer i386
- 8 MB free hard disk space for product installation
- 10 MB temporary disk space
- 32 MB free memory space (64 MB recommended)
- Linux with GLIBC or LIBC5; FreeBSD; OpenBSD or Sun Sparc Solaris
- for Samba Scanner: Samba Version with support for VFS Mechanism (Version 2.2.0 or higher)

If you want to use the GUI:

- Java 1.4.0 or higher

### 2.5 Technical Information

AntiVir Guard is based on **Dazuko** (<http://www.dazuko.org>), an open source software project. Dazuko is a kernel module which allows the AntiVir Guard daemon to access the files.

AntiVir Samba Scanner is based on samba-vscan (<http://www.openantivirus.org/projects.php>), an open source software project. **samba-vscan** is a VFS plug-in for Samba and it has a so-called AntiVir Backend, which allows the AntiVir Samba Scanner to access the files.

Please observe the license information in the installation directory /legal.



## 3 Installation

You can find the current version of AntiVir UNIX Server on the Internet. If you have a Convenience Package AntiVir CD-ROM, you may also install the product from it.

AntiVir is supplied as a packed archive. It contains AntiVir Guard, AntiVir Command line scanner and the Internet Updater.

You will be guided step by step throughout the installation procedure. This Chapter is divided into the following sections:

- [Getting the Installation Files](#) – Page 13
- [Licensing](#) – Page 14
- [Installing the Dazuko Kernel Module](#) – Page 15
- [Integration on Samba](#) – Page 17
- [Installing AntiVir](#) – Page 20
- [Reinstalling AntiVir](#) – Page 28
- [Installing AntiVir UNIX Server Using the Graphical Installation Routine](#) – Page 29
- [Integrating Third-Party Products](#) – Page 36

### 3.1 Getting the Installation Files

#### Downloading the Installation Files from the Internet

- ▶ Download the current version file from our website <http://www.avira.com> to your local computer. The file name is antivir-server-prof-<version>.tar.gz (without graphical installer) or antivir-server-linux-gui\_installer.tar.gz (with graphical installation routine).
- ▶ Save the file in a */tmp* folder on the computer on which you want to run AntiVir UNIX Server.

#### Getting the Installation Files from CD-ROM

- ▶ On the AntiVir CD-ROM open */EN/PRODUCTS/UNIX/SERVER* or */EN/PRODUCTS/UNIX/GUI\_INSTALLERS/*.
- ▶ Copy the file *antivir-server-prof-<version>.tar.gz* or *antivir-server-linux-gui\_installer.tar.gz* in a directory, for example in */tmp*.

### Unpacking Program Files

We will now describe the unpacking of the product kit without graphical installation routine:

- ▶ Go to the temporary directory:

```
cd /tmp
```

- ▶ Unpack the archive containing the AntiVir kit:

```
tar xzvf antivir-server-prof-<version>.tar.gz
```

↳ in the temporary directory will then appear antivir-server-prof-<version> .

- ▶ Change to the following directory:

```
cd /tmp/antivir-server-prof-<version>/src
```

- ▶ Unpack the archive containing the dazuko kernel module:

```
tar xzvf dazuko-<version>.tar.gz
```

↳ The dazuko-<version> directory is created.

## 3.2 Licensing

You must have an AntiVir license in order to use the full product (see [Licensing Concept](#) – Page 9). The license comes in a file named hbedv.key.

This license file contains information regarding the scope and period of the license. Without the license file, AntiVir UNIX Server runs only as a demo version with restricted features.

### Purchasing the License

- ▶ You may contact us by telephone or by email ([info@avira.com](mailto:info@avira.com)) to acquire a license file for AntiVir UNIX Server.

↳ You will receive the license file by email.

- ▶ You can easily acquire AntiVir UNIX Server using our Online Shop (for details, visit <http://www.avira.com>).

### Copying the License File

- ▶ Copy the license file hbedv.key to the installation directory on your system  
/tmp/antivir-server-prof-<version>.



*You can also perform the installation without having a license key from the beginning. AntiVir UNIX Server will then run as demo version.*

*You can copy the license file at any time to the AntiVir program directory  
/usr/lib/AntiVir .*

### 3.3 Installing the Dazuko Kernel Module



*Dazuko kernel module is required by all platforms to allow AntiVir Guard functionality.*

Dazuko is necessary for installing the AntiVir Guard resident scanner.



*AntiVir can be installed even without dazuko, but in this case it will run without AntiVir Guard. See more details in [Installing AntiVir without AntiVir Guard](#) – Page 21.*

You must compile the module yourself because your UNIX kernel and Dazuko must be based on the same source files. This is the only way you can ensure that Dazuko will have access to the same system functions as your UNIX kernel.



If your distribution supplier offers an exact matching module to your kernel:

- ▶ skip the following step.
- ▶ Check the name of the module on the system (you might use this information for further installation of AntiVir Guard). Use the following command:

```
find /lib/modules/`uname -r` -name 'dazuko*'
```

The procedure is described, so that you do not need expert knowledge to perform it. Nevertheless, knowledge of UNIX kernel compilation is needed, especially when errors are encountered. Further information on this can be found at:

<http://www.tldp.org/HOWTO/Kernel-HOWTO.html>

### Compiling Dazuko

- ✓ Make sure that the source code for UNIX kernel is in `/usr/src/linux`. If not, install it there. Information on this subject can be found in your UNIX provider documentation.
- ✓ Check if you have on your computer the kernel compiling programs (for example `gcc`). This also applies to UNIX standard installations. If not, install the required packages. Information on this subject can be found in your UNIX provider documentation.
- ✓ Your UNIX kernel must be based on the source code from `/usr/src/linux`, as in most cases, especially in a UNIX reinstallation. You can only be absolutely certain by recompiling the installed kernel using exactly these sources.



*If you are not certain about your UNIX kernel status, you should reinstall it. In the worst case, Dazuko will not be integrated into your UNIX kernel. However, the AntiVir installation checks this and will notify you of this.*

- ▶ Go to the temporary directory where you unpacked Dazuko, for example:  

```
cd /tmp/antivir-server-prof-<version>/src/dazuko-<version>
```
- ▶ Check the configuration of your computer with the configure script. Based on this information, it will provide appropriate guidance for further installation of the software:  

```
./configure
```
- ▶ Compile Dazuko:  

```
make
```
- ▶ Optionally: verify if the newly installed module works with the computer's running kernel:  

```
make test
```

You must keep the `dazuko.o` file in the temporary directory `/tmp/antivir-server-prof-<version>/src/dazuko-<version>`.  
AntiVir installation script will need this file later.



*Further information on Dazuko can be found on the website:*  
<http://www.dazuko.org>.

### 3.4 Integration on Samba



*You need AntiVir Backend for samba-vscan on all platforms in order to use the full features of AntiVir Samba Scanner.*

You need AntiVir Backend for samba-vscan if you want transparent monitoring of the file access via Samba Service.



*You can initially install AntiVir without samba-vscan. In this case, AntiVir runs without the Samba Scanner. You may still ensure appropriate protection of the file release using AntiVir Guard. The notifications to the remote users of the files are then implemented with the option ExternalProgram in AntiVir Guard and with own logic (for example, using UNIX scripts).*

You have to create the AntiVir Backend for samba-vscan yourself (obtained through a VFS Plug-in for Samba) because your Samba Service and the Backend must be based on the same sources. Only this will ensure correct functionality of the VFS Plug-in and the stability of your file server.



*If your distributor has included a suited AntiVir Backend for your Samba Server:*

- ▶ Skip the next step.
- ▶ Check the name of the Backend and of the corresponding configuration file on the system. Use the following command:  

```
find /usr -name 'vscan-antivir.so'
```

```
find /usr -name 'vscan-antivir.conf*'
```

To proceed with this step, you will need knowledge of Samba compiling and samba-vscan. Detailed information is found in the source pack documentation and on the websites of these projects.

## Preparing Samba

- ✓ Check that your system contains the programs needed for compiling sources (gcc, make etc.). This might be the case for standard UNIX installations. If necessary, install the program packs. You can find more information in the documentation of your UNIX distribution.
- ✓ Make sure that you have the source text for samba-vscan in version 0.3.5 or newer on your system. There is a patch for version 0.3.5 which implements AntiVir Backend. Samba-vscan includes AntiVir Backend from version 0.3.6.
- ✓ Make sure you have the exact version of Samba sources that you use for the file server. You do not have to translate and install the entire Samba sources, only samba-vscan pack. The installation of the translated Samba is of course the best way to ensure that the Service and VFS plugin match one another.
- ▶ Change to the temporary directory where you have unpacked Samba. For example:

```
cd /tmp
gunzip < samba-<version>tar.gz | tar xf -
cd samba-<version>/source
```
- ▶ Check the configuration of your system with the configure script and based on the details it finds create the corresponding information regarding further translation of the software:

```
./configure
```
- ▶ Create the additional information needed by samba-vscan:

```
make proto
```
- ▶ Go to the temporary directory where you unpacked samba-vscan. For example:

```
cd /tmp
bunzip2 < samba-vscan-0.3.5.tar.bz2 | tar xf -
cd samba-vscan-0.3.5
```

- Unpack the archive with AntiVir Backend for samba-vscan. This contains AntiVir sources as a patch which applies to samba-vscan 0.3.5 and integrates AntiVir Backend. Apply the patch (from samba-vscan version 0.3.6, this step is no longer needed because AntiVir Backend is already included).

```
gunzip < /tmp/samba-vscan-antivir-0.3.5.tar.gz |  
tar xf -  
  
patch -p0 < patch-sambavscan-hookup.diff
```

- Configure and translate samba-vscan. For this, you have to indicate the Samba-sources:

```
./configure --with-samba-source=/tmp/samba-<version>/  
source  
  
make  
  
make install
```

- You can use a configuration example for AntiVir samba-vscan Backend, which is provided for some settings:

```
cp antivir/vscan-antivir.conf /usr/local/samba/lib
```

To integrate AntiVir Samba Scanner in smb.conf for monitoring of the released files, you must activate the vscan-antivir.so plug-in (see [Configuring AntiVir Samba Scanner](#) – Page 58). There is no need to start additional services apart from Samba, as the plug-in vscan-antivir.so handles this aspect by itself.

### 3.5 Installing AntiVir

AntiVir is automatically installed using a script. This script performs the following tasks:

- Checks integrity of the installation files.
- Checks for the required authorizations for the installation.
- Checks for an existing version of AntiVir on the computer.
- Copies the program files. Overwrites existing obsolete files.
- Copies AntiVir configuration files. Existing AntiVir configuration files are inherited.
- Optionally it creates a link in /usr/bin, so that AntiVir can be called from any folder without needing a given path.
- Optionally it installs AntiVir Updater and the resident scanner AntiVir Guard.
- Optionally it configures an automatic start for AntiVir Updater and AntiVir Guard on system start-up.

The following steps must be taken for the initial installation:

- [Preparing Installation](#) – Page 20
- If Dazuko has not been compiled: [Installing AntiVir without AntiVir Guard](#) – Page 21
- If Dazuko has been compiled: [Installing AntiVir with AntiVir Guard](#) – Page 24

#### Preparing Installation

- ▶ Login as **root**. Otherwise you do not have the required authorization for installation and the script returns an error message.
- ▶ Go to the directory in which you unpacked AntiVir:  
`cd /tmp/antivir-server-prof-<version>`

## Installing AntiVir without AntiVir Guard

If you have not compiled the Dazuko kernel module, you can only install AntiVir without AntiVir Guard. AntiVir Guard can be easily installed later.

► Type the command:

```
./install
```

↳ The installation script starts. It will copy the program files:

```
1) installing command line scanner
creating install directory /usr/lib/AntiVir ... done
checking for existing /etc/antivir.conf ... not found
copying bin/antivir to /usr/lib/AntiVir ... done
copying vdf/antivir.vdf to /usr/lib/AntiVir ... done
copying conf/antivir.conf to /etc ... done
copying sh/configantivir to /usr/lib/AntiVir ... done
linking /usr/bin/antivir to /usr/lib/AntiVir/antivir ... done
installation of command line scanner complete
```

↳ Then you are asked if you want to install the Internet Updater:

```
2) installing automatic internet updater
...
Would you like to install the automatic internet updater? [n]
```



*You do not necessarily need Internet Updater to keep AntiVir up to date. You can perform this operation manually via the Internet. See [Updating AntiVir Manually](#) – Page 74. However, for the initial installation, it is recommended to install the Updater. You can deactivate it in the configuration settings.*

Installation  
with Updater

If you choose to install the Internet Updater (recommended):

► Type **Y** and confirm with **Enter**.

↳ Then, you are asked if Updater should start automatically:

```
copying sh/avupdater to /usr/lib/AntiVir ... done

Would you like the automatic updater to start
automatically? [y]
```

► Press **Enter**. You can make this setting manually later.

↳ The automatic system start is configured:

```
linking /etc/rc.d/rc(LEVEL).d/(S/K)20avupdater to /usr/lib/AntiVir/avup-
dater ...
runlevel 0 ... done
runlevel 1 ... done
runlevel 2 ... done
runlevel 3 ... done
runlevel 4 ... done
runlevel 5 ... done
runlevel 6 ... done
installation of automatic internet updater complete
```

Installation  
without  
Updater

If you choose not to install the Internet Updater, or to do this later, manually:

► Type **N** or press **Enter**.

► Confirm with **Enter**.

Skipping  
AntiVir Guard

You are asked if you want to install AntiVir Guard:

```
3) installing AvGuard
Version 2.1.3 of AntiVir for UNIX is capable of on-access, real-time scanning of
files.
...
There are several ways in which you can install AvGuard.

module - Dazuko will be loaded by the avguard script
kernel - Dazuko is always loaded (an should not be
        loaded by the avguard script)
no install - do not install AvGuard at this time
...
available options: m k n
How should AvGuard be installed? [n]
```

► Type **N** and confirm with **Enter**.

GUI  
installation

The next step is for the installation of the optional user interface (GUI):

```
4) installing GUI
...
Would you like to install the GUI? [n]
```



*AntiVir UNIX Server is provided with a GUI, which enables monitoring of realtime activity, the display of log entries and configuration of the product. However, AntiVir is fully functional even without the GUI.*

If you want to install the GUI:

✓ Java 1.4.0 or higher must be installed on your system

► Answer **Y** when asked about GUI installation.

↳ The GUI program files are copied:

### Starting Configuration

Finally, you can configure AntiVir:

```
5) configuring AntiVir
Would you like to configure AntiVir now? [y]
```



*If you answer **Y**, AntiVir configuration script starts. You can carry out configuration at any time later. We recommend that you first learn about the configuration options and then carry out configuration.*

► End this procedure by answering **N**.

↳ You will see a report that indicates the completion of the installation:

```
Installation of the following features complete:
AntiVir command line scanner
AntiVir Automatic Internet Updater
```

### Installing AntiVir with AntiVir Guard

- ✓ Make sure that the Dazuko kernel module has been compiled (see [Installing the Dazuko Kernel Module](#) – Page 15).

- Type the command:

```
./install
```

- ↳ The installation script starts. It will copy the program files:

```
1) installing command line scanner
creating install directory /usr/lib/AntiVir ... done
checking for existing /etc/antivir.conf ... not found
copying bin/antivir to /usr/lib/AntiVir ... done
copying vdf/antivir.vdf to /usr/lib/AntiVir ... done
copying conf/antivir.conf to /etc ... done
copying sh/configantivir to /usr/lib/AntiVir ... done
linking /usr/bin/antivir to /usr/lib/AntiVir/antivir ... done
installation of command line scanner complete
```

- ↳ Then you are asked if you want to install the Internet Updater:

```
2) installing automatic internet updater
...
Would you like to install the automatic internet updater? [n]
```



*You do not necessarily need Internet Updater to keep AntiVir up to date. You can perform this operation manually via the Internet. See [Updating AntiVir Manually](#) – Page 74. However, for the initial installation, it is recommended to install the Updater. You can later deactivate it in the configuration settings.*

Installation  
with Updater

If you choose to install the Internet Updater (recommended):

- Type **Y** and confirm with **Enter**.

- ↳ The Internet Updater is installed. Then, you are asked if Updater should start automatically:

```
copying sh/avupdater to /usr/lib/AntiVir ... done

Would you like the automatic updater to start automatically? [y]
```

- Press **Y** or **Enter**. You can make this setting manually later.

↳ The automatic system start is configured:

```
linking /etc/rc.d/rc(LEVEL).d/(S/K)20avupdater to /usr/lib/AntiVir/avup-
dater ...
runlevel 0 ... done
runlevel 1 ... done
runlevel 2 ... done
runlevel 3 ... done
runlevel 4 ... done
runlevel 5 ... done
runlevel 6 ... done
installation of automatic internet updater complete
```

Installation  
without  
Updater

If you choose not to install the Updater, or to do this later, manually:

► Type **N** or press **Enter**.

Installing  
AntiVir Guard

You are asked if you want to install AVIRA Guard:

```
3) installing AvGuard
Version 2.0.7 of AntiVir for UNIX is capable of on-access, real-time scanning of
files.
...
There are several ways in which you can install AvGuard.

module - Dazuko will be loaded by the avguard script
kernel - Dazuko is always loaded (and should not be
        loaded by avguard script)
no install - do not install AvGuard at this time
...
available options: m k n
How should AvGuard be installed? [n]
```

► Type **M** and confirm with **Enter**.

↳ You will be asked to enter the path to the compiled Dazuko module file  
dazuko.o :

Enter the full path to dazuko.o:

► Enter the full path to dazuko.o .

For example: If dazuko.o is in /tmp/antivir-server-prof-<version>/src/dazuko-  
<version>/ , you should type:

```
/tmp/antivir-server-prof-<version>/src/dazuko-<versi-
on>/dazuko.o
```

- ↳ The installation script checks whether `dazuko.o` was correctly compiled and then copies the file for AntiVir Guard.

```
testing /tmp/antivir-<version>-server/src/dazuko-<version>/dazuko.o ... ok
detecting kernel version ... linux-2.4.18-4GB
copying /tmp/dazuko.o to /usr/lib/AntiVir/linux-2.4.18-4GB ... done
copying sh/avguard to /usr/lib/AntiVir ... done
linking configavguard to configantivir ... done
```



*If the installation script reports any errors on Dazuko, you should probably recompile your UNIX kernel. For more information, see <http://www.dazuko.org>*

Then you are asked if the AntiVir Guard should be automatically run when the system starts:

```
Would you like AvGuard to start automatically? [y]
```

- Confirm with **Enter**.

- ↳ Finally, the AntiVir Guard is linked to the startup script and the installation is completed.:

```
identifying startup script location ... found (etc/rc.d/)
linking /etc/rc.d/rc(LEVEL).d/(S/K)20avguard to /usr/lib/AntiVir/avguard ...
runlevel 0 ... done
runlevel 1 ... done
runlevel 2 ... done
runlevel 3 ... done
runlevel 4 ... done
runlevel 5 ... done
runlevel 6 ... done
installation of AvGuard complete
```

GUI  
installation

The next step is for the installation of the optional user interface (GUI):

```
4) installing GUI
...
Would you like to install the GUI? [n]
```



*AntiVir UNIX Server is provided with a GUI, which enables monitoring of realtime activity, the display of log entries and configuration of the product. However, AntiVir is fully functional even without the GUI.*

If you want to install the GUI:

- ✓ Java 1.4.0 or higher must be installed on your system
- Answer **Y** when asked about GUI installation.
  - ↳ The GUI program files are copied.

Starting  
Configuration

Finally, you can configure AntiVir:

5) configuring AntiVir  
Would you like to configure AntiVir now? [y]



*If you answer **Y**, AntiVir configuration script starts. You can carry out the configuration at any time later. We recommend that you first learn about the configuration options and then carry out configuration.*

► End this procedure by answering **N**.

↳ You will see a report that indicates the completion of the installation

Installation of the following features complete:  
AntiVir command line scanner  
AntiVir Automatic Internet Updater  
AntiVir Guard

### 3.6 Reinstalling AntiVir

You can launch the installation script at any time. There are several possible situations:

- Installing a new version (upgrade). The installation script checks the prior version and installs the necessary new components. The configuration file settings already made are not overwritten (see [Configuration](#) – Page 37) but are inherited.
- Later installation of some components, e.g. AntiVir Guard or Internet Updater.
- Activating or deactivating the automatic start of Internet Updater or AntiVir Guard.

#### Reinstalling AntiVir

The procedure applies to all these cases:

- ✓ First of all, you have to make sure that AntiVir Guard is stopped:

```
/usr/lib/AntiVir/avguard stop
```

- ▶ Open the temporary directory where you unpacked AntiVir:

```
cd /tmp/antivir-server-prof-<version>
```

- ▶ Type:

```
./install
```

↳ The installation script performs as described in [Installing AntiVir](#) – Page 20).

- ▶ Make the changes you need during installation procedure.

AntiVir is installed with the required features.

### 3.7 Installing AntiVir UNIX Server Using the Graphical Installation Routine

You can also install AntiVir using a simple graphical installation routine. All you need to do is download the corresponding file as described in [Getting the Installation Files](#) – Page 13.



*The graphical installation routine serves for installation only. It is in no way related to the GUI for operating and configuring AntiVir UNIX Server.*



*AntiVir UNIX Server with graphical installation only applies to Linux. It needs Java 1.4.0 or higher.*

- ✓ Unpack the program into the following directory:  
/tmp/antivir-server-linux-gui\_installer.

► Type:

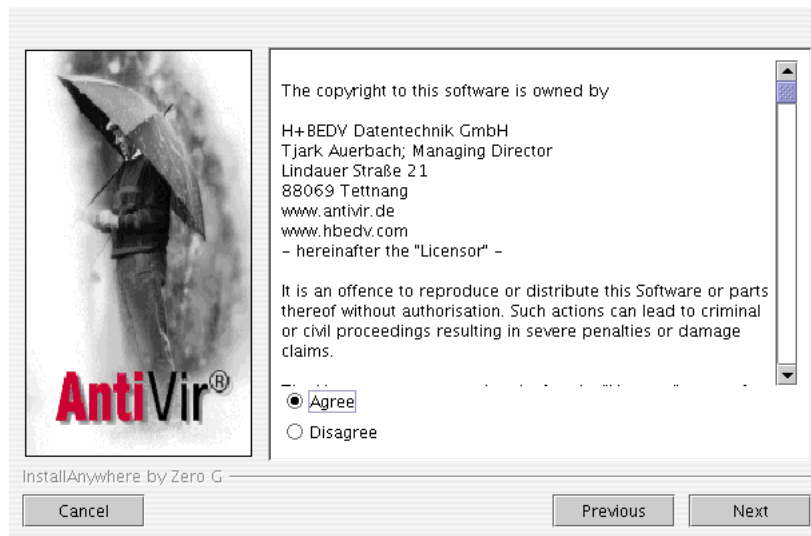
`./install`

↳ The welcome page appears with a program description:



- Click **Next**.

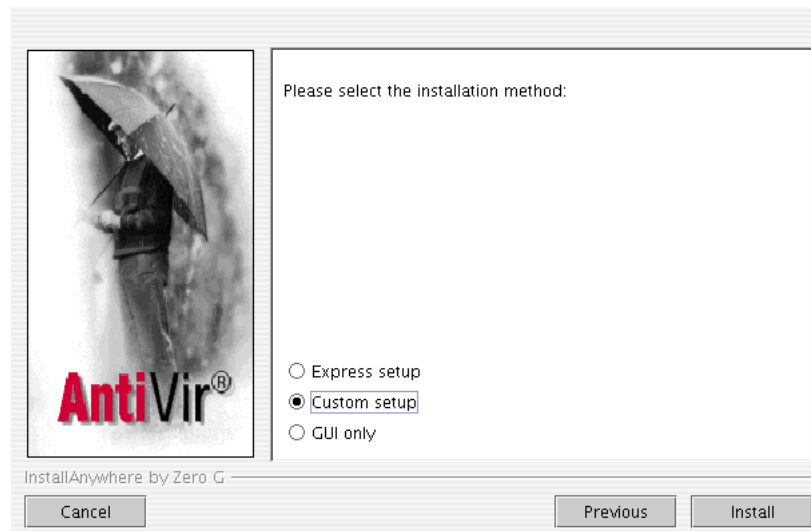
↳ The License Agreement window is displayed:



*You must agree with these conditions in order to continue with the installation. If **Disagree** is active, you cannot proceed.*

► **Select Agree and click Next.**

↳ You will see the following window:



There are three possibilities for installing AntiVir UNIX Server:

- **Express setup:** The program is installed with basic settings.
- **Custom setup:** The program is installed according to the user's options.
- **GUI only:** Only the GUI is installed in `usr/lib/AntiVir`.

## Express setup

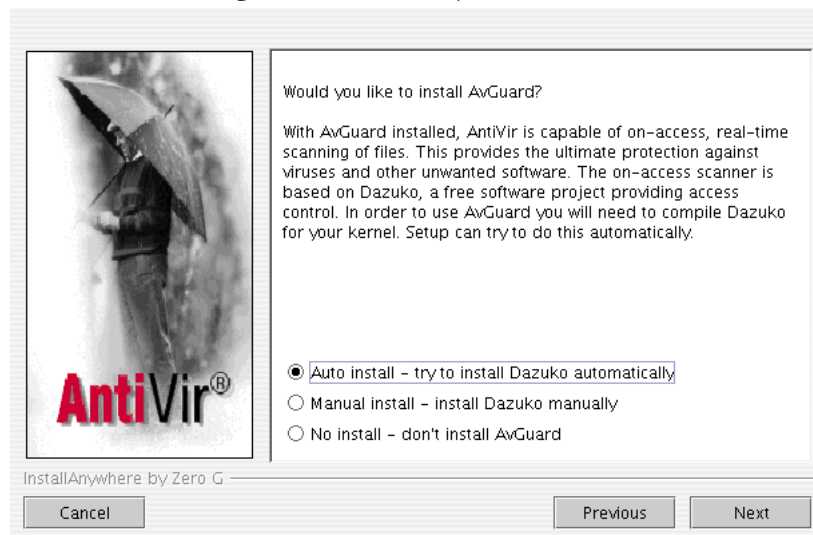
The program is installed with the following basic settings:

- AntiVir UNIX Server is installed in the directory:  
`/usr/lib/AntiVir`
  - AntiVir Guard (on-access scanner) is installed.
  - The automatic Internet Updater is not installed.
  - GUI support is activated.
  - AntiVir Guard will start automatically when booting.
  - The license file is not copied, meaning that AntiVir runs as a demo version.
- Select **Express setup** and click **Next**.  
 ↳ All settings and further instructions appear in a window.
- Click **Install**.  
 ↳ The program is installed.

## Custom setup

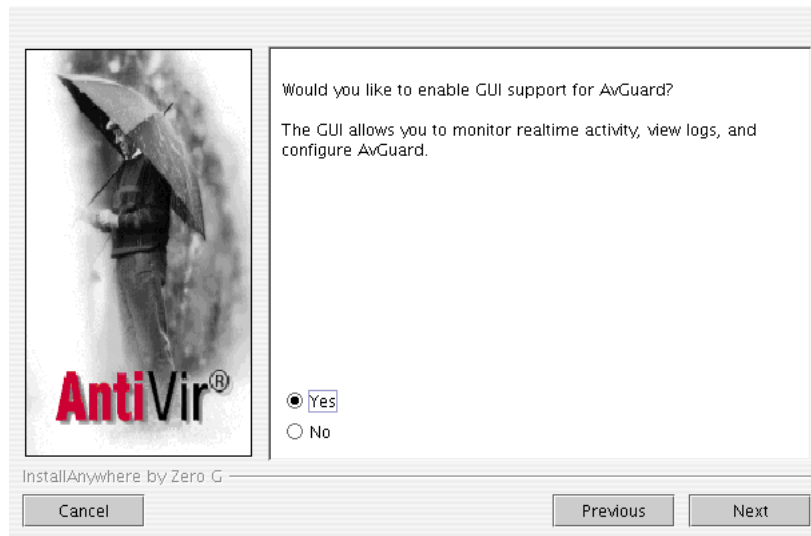
You can install the program with user-defined settings.

- Select **Custom setup** and click **Next**.  
 ↳ The following window asks if you want to install AntiVir Guard.

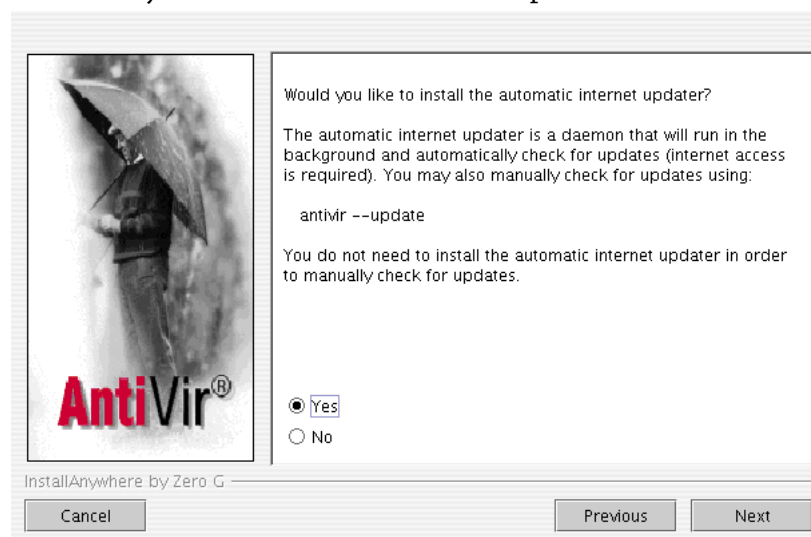


You can handle AntiVir Guard in one of the following ways:

- **Auto install:** Dazuko sources are compiled and the kernel module is integrated.
  - **Manual install:** Dazuko kernel module is created manually (see [Installing the Dazuko Kernel Module](#) – Page 15)
  - **No Install:** AntiVir Guard is not installed.
- Select **Auto install** in order to install Dazuko automatically and click **Next**.  
↳ Then you are asked if you want to activate GUI support (entry in the file `avguard.conf`):



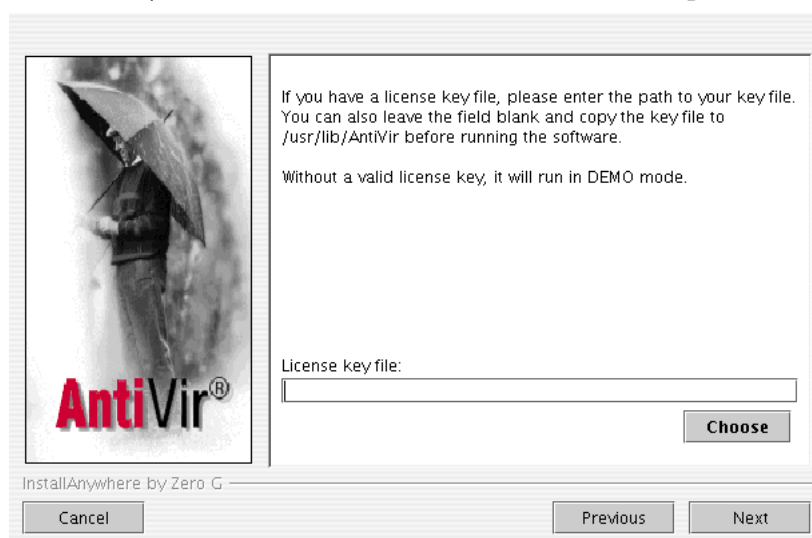
- Select **Yes** or **No** and click **Next**.  
↳ Then you can install the Internet Updater:



If you want to install the Internet Updater:

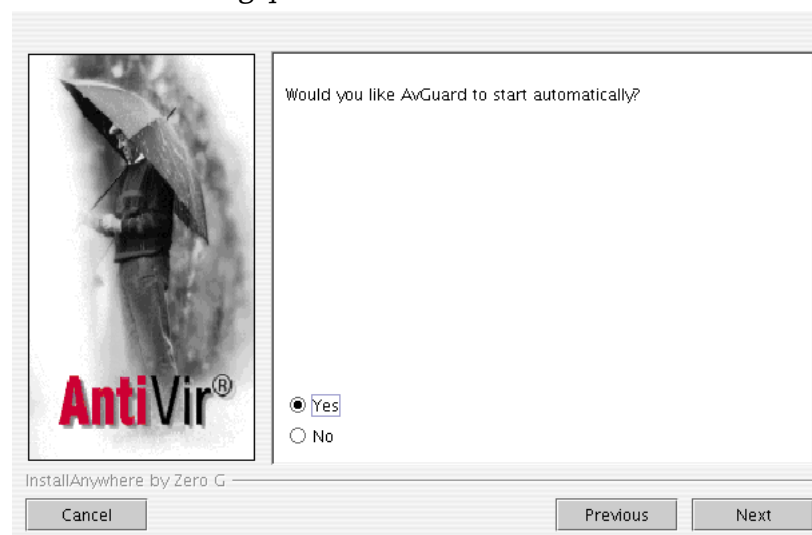
- Select **Yes** and click **Next** (in this case, an additional question appears regarding the automatic start of the Updater).

↳ Then you are asked if a license file should be copied:



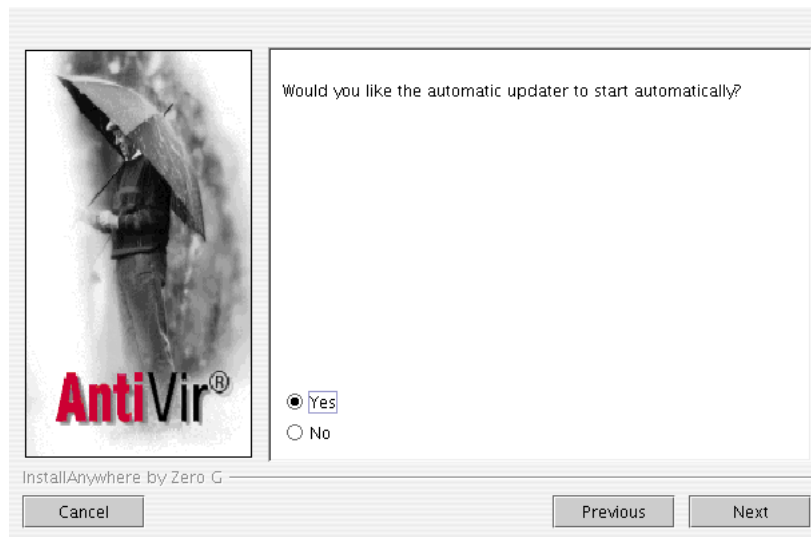
► Follow the instructions and click **Next**.

↳ The following question refers to the automatic start of AntiVir Guard:



► Select **Yes** or **No** and click **Next**.

- ↳ An optional question follows regarding the automatic start of the Internet Updater:



- ▶ Select **Yes** or **No** and click **Next**.

- ↳ Finally, a window with the summary of your settings and further information is displayed:



- ▶ Click **Install**.

- ↳ The program is installed.

### GUI only

Choose this option if you wish to install only the GUI.

- ▶ Select **GUI only** and click **Next**.

- ↳ The GUI is installed in the following directory: `/usr/lib/AntiVir`

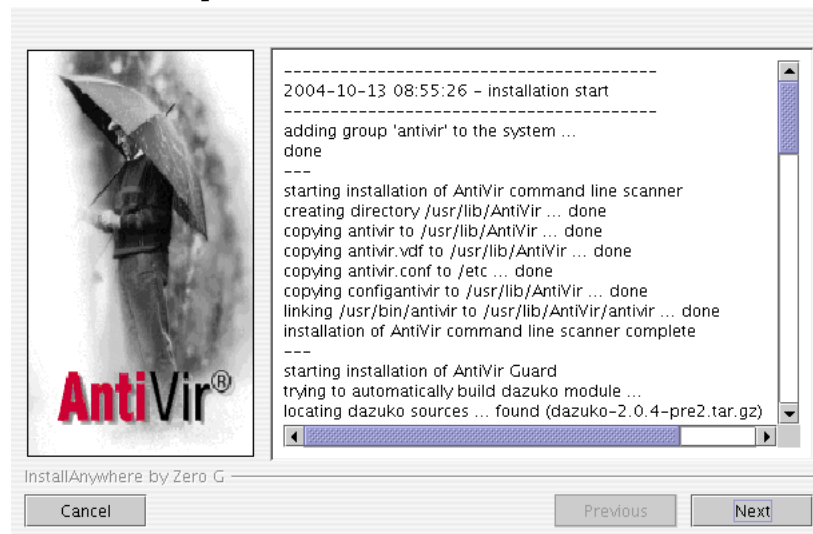
- ↳ All settings and further instructions appear in a window.

- ▶ Click **Install**.

- ↳ GUI is installed.

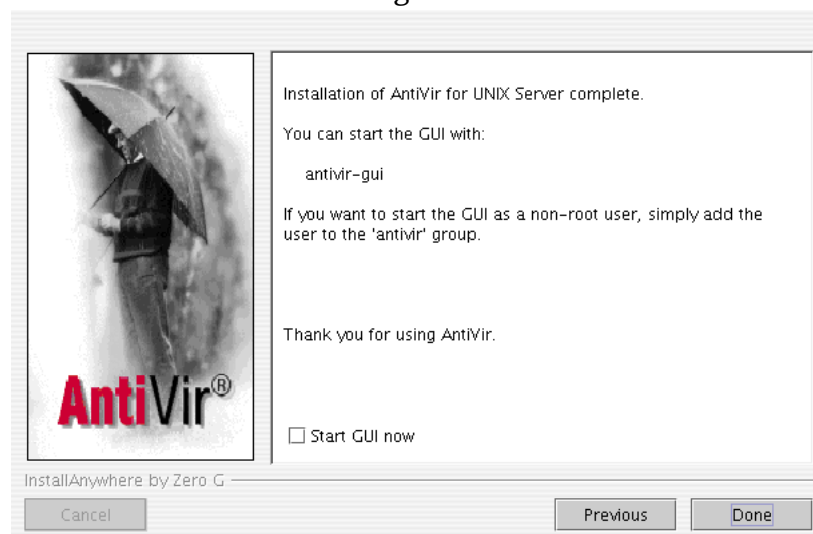
## Completing the Installation

According to the installation type you selected, a window will list the performed installation steps:



► Click **Next**.

↳ You will see the following window:



If you want to start the GUI directly:

► Activate the option **Start GUI now** and click **Done**.

The installation is completed.

### 3.8 Integrating Third-Party Products

#### Integration in AMaViS

"A Mail Virus Scanner (AMaViS)" project (<http://www.amavis.org/>) is already prepared for integration with the AntiVir Scanner. You can either install AMaViS after installing AntiVir, for automatic detection, or explicitly activate AntiVir support during AMaViS installation using the option `--enable-all` or `--enable-hbedv` for the command `./configure`.



*Please note that AMaViS uses the Command line scanner and runs it as a separate process for every message. Unfortunately, this method is not as efficient as a dedicated email scanner. For an environment with higher throughput requirements, you should consider integrating AntiVir MailGate or SAVAPI-based products.*



*You need a license to integrate the Command line scanner with AMaViS. This allows you to generate antivirus scan services for other computers.*

## 4 Configuration

You can adjust AntiVir UNIX Server for optimum performance. You can make the main adjustments immediately after installation. The most common settings are suggested.

You can modify these settings anytime, to adjust the product to your requirements.

After a short overview, you will be guided step by step through the configuration process:

- An overview of the [Configuration Files](#) – Page 38.
- The procedure for using the [Configuration Scripts](#) – Page 45
- Specific configurations for AntiVir:
  - [Configuring AntiVir Notifications](#) – Page 47
  - [Configuring the Resident AntiVir Guard](#) – Page 50
  - [Configuring AntiVir Samba Scanner](#) – Page 58
  - [Configuring Regular Updates](#) – Page 61
- Finally [Testing AntiVir UNIX Server](#) – Page 67, after completing the configuration.

## 4.1 Overview

- Configuration Files    The configuration is defined in three files:
- `antivir.conf` defines basic settings for automatic updates and logfiles when detecting viruses and unwanted programs.
  - `avguard.conf` defines the behavior of the resident AntiVir Guard.
  - `vscan-antivir.conf` defines the behavior of AntiVir Samba Scanner; this file is described in detail in [4.6 Configuring AntiVir Samba Scanner](#).



*The settings can be made directly in the configuration files. This is not very difficult. A more convenient way is to use the script settings included in the program. These intercept the eventual errors and restart the necessary processes.*

- Configuration Scripts    You can use the configuration scripts in `/usr/lib/AntiVir`:
- `configantivir` to edit the settings in `antivir.conf` (Updater settings).
  - `configavguard` to edit the settings in `avguard.conf` and `antivir.conf` (Guard settings).

## 4.2 Configuration Files

This part describes the structure of AntiVir UNIX Server configuration files. AntiVir reads these files on program start-up. It ignores empty lines and commented lines beginning with `#`

The program is provided with default values, which are important for many procedures. Some options can be deactivated with a `#` at the beginning of the line (commented) or can be set with default values. These can be activated by removing the `#` character or by changing the values.



*You must restart the Internet Updater and the AntiVir Guard if you modify any values manually in the configuration files. The changes only take effect after a restart.*

► Type:

```
/usr/lib/AntiVir/avupdater restart
/usr/lib/AntiVir/avguard restart
```

## 4.2.1 Configuration File avguard.conf

This section provides a short description of the entries in avguard.conf . The settings affect only the behavior of AntiVir UNIX Server and no other AntiVir programs. You can also learn how to make these settings using a graphical user interface in [Configuring AntiVir Guard Using the GUI](#) – Page 95.

**Num Daemons** **Number of daemons:**  
The number of simultaneous AntiVir Guard daemons can be set between 0 and 20. The default is 3 and it is appropriate for smaller standard computers. For servers with high traffic, a larger number would be necessary:

```
NumDaemons          3
```

If the value is 0, AntiVir Guard is deactivated.

**AccessMask** **Access mask:**  
This option sets the access type of AntiVir Guard, when scanning files for viruses or unwanted programs:

- 1: Scanning a file when opened
- 2: Scanning a file when closed
- 4: Scanning a file when executed

For setting more access types at the same time, you have to add the above values. For example, to scan files when opened and when closed, the value has to be 3. This is the default value.

```
AccessMask          3
```

**Repair Concerning Files** **Repairing files:**  
AntiVir Guard is able to repair files immediately after access. If this fails, access is blocked. The following option must be active:

```
RepairConcerningFiles true
```

It is deactivated by default.

**LogOnly, Rename... Move...** **Action when detecting viruses or unwanted programs:**  
If RepairConcerningFiles is not set or repair is not possible, access to the file is blocked and the action is logged. The following three options define further actions of AntiVir Guard:

- LogOnly: no further action
- RenameConcerningFiles: renaming the file by adding the .XXX extension.
- MoveConcerningFilesTo: moving the file to another folder. This folder will be automatically created if it does not already exist. For example:

```
MoveConcerningFilesTo /home/unwanted
```

You can select only one of these options. If more than one is activated, AntiVir applies the last one selected in the configuration file.

**IncludePath Scanned directories:**

AntiVir Guard scans the files in the specified folders, including their sub-folders. Usually, the data for the different users is in /home. The default setting is:

```
IncludePath /home
```

You can specify only one folder in a command line. You can enter more folders by typing the command for each one. Example:

```
IncludePath /home
```

```
IncludePath /var
```



*If no folder is specified, AntiVir Guard will not scan any files!*

**ExcludePath Excluded directories:**

AntiVir Guard can exclude certain folders when scanning. For example, a folder containing temporary files of AntiVir components (see [Setting excluded directories](#) – Page 51). There is no default setting.

You can specify only one folder in a command line. You can enter more folders by typing the command for each one. Example:

```
ExcludePath /home/log
```

```
ExcludePath /home/tmp
```



*If you have activated MoveConcerningFilesTo, that folder is automatically excluded.*

**ArchiveScan Scanned archives:**

AntiVir Guard scans archives when opened, depending on the setting for ArchiveMaxSize, ArchiveMaxRecursion and ArchiveMaxRatio. To do this, you must activate the following option:

```
ArchiveScan
```

This is deactivated by default in order to maintain the highest possible performance of AntiVir.

**ArchiveMax Size Maximum archive size:**

This option limits the scanning process to the files with unpacked size smaller than ArchiveMaxSize (in bytes). The zero value means no limit. The default setting is 1 Gigabyte (1073741824 bytes):

```
ArchiveMaxSize 1073741824
```

**ArchiveMax Recursion Maximum recursion level:**

When scanning recursive archives, the level of recursion can be limited. The zero value means all archives are completely unpacked, regardless of their recursion level. Default:

```
ArchiveMaxRecursion 5
```

Archive  
MaxRatio

## Maximum compression rate for archives:

This option limits the scanning to files which do not exceed a certain compression level. It ensures protection against so-called "mail bombs", which occupy an unexpectedly large amount of memory when decompressed. The zero value means all archives are completely decompressed, regardless of their compression rate.

Default:

ArchiveMaxRatio 150



*In order to use the following program function, you need Dazuko 2.0.0 or higher on your system.*

External  
Program

## Starting External Programs When Suspicious Files Are Found:

AntiVir Guard can start an external program when a virus or an unwanted program is found. This can send a notification or perform an action using AntiVir Guard options.

It is possible to send an SMS, to call the appointed responsible person, to show a dialog window on the local screen or on another computer, to save the data in another format or another file.

You can use macros (preceded by %) to pass the results as arguments to the external program. Thus the data can be treated differently and adjusted to the local conditions.

The following table shows the supported macros and their significance:

Option	Function
%h	Path to file (may contain special characters)
%f	Filename only (may contain special characters)
%p	Full path and filename (such as %h/%f), may contain special characters
%U	UID of file (owner identifier)
%G	GID of file (UNIX group identifier)
%S	File size
%m	File access mode
%De	Event type
%DF	File system or partition (device) on which the file is located
%Dp	PID of the process
%Du	UID of the process
%Df	Flag of file operation
%Dm	Access mode of file operation

Option	Function
%Sn	Name of the detected virus / unwanted program
%Sa	Extra information (if available)



*Some of these parameters are not checked by AntiVir but are taken from the file properties and forwarded to the running process, so they must be checked before further processing.*

```
ExternalProgram    /usr/bin/logger -- blocking  
                  access to %p (%Sn)
```

GUISupport

### **Support via graphical user interface (GUI):**

This option must be activated in order for AntiVir to communicate with GUI. You must enter the following parameters:

```
GuiSupport        yes  
GuiCAFile         /usr/lib/AntiVir/gui/cert/cacert.pem  
GuiCertFile       /usr/lib/AntiVir/gui/cert/server.pem  
GuiCertPass       antivir_default
```

In the case of missing or invalid parameters, the GUI is not available.

The log file records possible errors.

## 4.2.2 Configuration File antivir.conf

This section provides a short description of the settings in antivir.conf. These settings affect all AntiVir products you have installed on the computer. For this reason we refer to "AntiVir" in general, instead of just "AntiVir UNIX Server".

You can learn how to edit this file easily in [Configuration Scripts](#) – Page 45.



*You must restart the Internet Updater if you modify any values regarding the Internet Updater manually in antivir.conf, instead of using the configuration script. The changes only take effect after a restart.*

► Type:

```
/usr/lib/AntiVir/avupdater restart
```

EmailTo **Email messages:**

AntiVir can send emails after performing updates. There is no default setting. You must specify a recipient in order to send emails:

```
EmailTo root@localhost
```

LogTo **Logfile:**

AntiVir logs all important operations via the syslog daemon. It can also create an additional logfile. There is no default setting. You must enter the full path to the logfile in order to use this option:

```
LogTo /var/log/antivir.log
```

AutoUpdate... **Update scheduler:**

The security software can check regularly for updates online using the Internet Updater and, if necessary, it performs the update. By default, the possible options are deactivated for security reasons; so the program does **not** start any automatic updates.

For updates every 2 hours, you must activate the following option:

```
AutoUpdateEvery2Hours
```

For daily updates, activate the option below:

```
AutoUpdateDaily
```

In the case of daily updates, you may also set the time for this action, in HH:MM format:

```
AutoUpdateTime 04:23
```

HTTPProxy... **Proxy server:**

If your computer is connected to the Internet via an HTTP proxy server, you must specify this so that the automatic Internet Updater functions properly. By default, the settings are deactivated; a direct connection to the Internet is needed. You must specify:

- HTTP proxy server
- Port

- Username and password for the HTTP proxy server if necessary.

Example:

```
HTTPProxyServer    proxy.domain.com
HTTPProxyPort      8080
HTTPProxyUsername  username
HTTPProxyPassword  password
```

**Updater Keeps Backups** The Internet Updater replaces installed files with newer versions when updates are available. Even if the program is testing the new files, you might want to keep backups of earlier versions.

When activating this option, your existing files will be moved to the newly created sub-directories of  
`/usr/lib/AntiVir, named`  
`updater-backup-YYYYmmdd-HHMMSS`.



*If you activate the backup function of the Internet Updater, you should check this directory regularly and manually delete old versions as the size increases.*

`UpdaterKeepsBackups`

**Syslog...** **Syslog settings:**  
AntiVir sends messages for all important operations to the syslog daemon. You may specify the facility and priority for these messages. Default is:

```
SyslogFacility    user
SyslogPriority     notice
```

These values apply even if the option is not active.

**GnuPG...** **GnuPG settings:**  
The Updater can check the updates for authenticity using GnuPG. For more information, see [Verifying Updates Authenticity with GnuPG](#) – Page 65. If you use GnuPG, you have to enter the path to GnuPG executable, for example:

```
GnuPGBinary       /usr/local/bin/gpg
```

You can also add other options using `GnuPGOptions`, depending on the specific GnuPG installation. This is usually not necessary. For security reasons, both settings are deactivated by default.

**Detect...** **Detection of other types of unwanted programs:**  
Besides viruses, there are other types of harmful or unwanted software. You can activate their detection using the following options:

```
DetectDialer
DetectJoke
DetectGame
DetectPMS
```

Heuristics Macro	<p><b>Macrovirus Heuristics:</b></p> <p>Activates the heuristics for macroviruses in documents. This option is activated by default:</p> <pre>HeuristicsMacro</pre>
Heuristics Level	<p><b>Win32-Heuristics:</b></p> <p>Sets the detection level of Win32-Heuristics. Available values are 0 (off), 1 (low), 2 (medium) and 3 (high). Default:</p> <pre>HeuristicsLevel    0</pre>

## 4.3 Configuration Scripts

You can conveniently set up AntiVir using the configuration scripts, which are able to intercept possible invalid entries and restart the necessary processes.

The script for configuring AntiVir are:

- `configantivir` - to edit the settings in `antivir.conf`
- `configavguard` - to edit the settings in `avguard.conf` and some in `antivir.conf`, applying to AntiVir Guard.

The procedure for using the script is very easy.

If you want a general configuration of AntiVir:

► Type:

```
/usr/lib/AntiVir/configantivir
```

If you want to configure AntiVir Guard:

► Type:

```
/usr/lib/AntiVir/configavguard
```

The scripts read the current settings in `antivir.conf` or in `avguard.conf` and systematically ask if you want to enter new values. They display the possible parameters, while the current ones are shown as default.

If you want to keep one of the current settings:

► Press **Enter**.

If you want to change a setting:

► Type the new value and confirm with **Enter**.

Finally, a summary of the configuration settings is displayed. The following output appears after running `configantivir` (example):

```
Here are the configuration settings you have specified. Look them over to
make sure they are correct.
number of daemons:      3
scan on:                open/close
repair concerning files: yes
handling of concerning files: move to /tmp/unwanted
include paths:          /usr/lib:/usr/bin:/home
exclude paths:          /home/myhome
scan archives:          yes
max archive size:       1073741824 bytes
max archive recursion:  5 levels
max archive ratio       150:1
email notification:     root@localhost
specific logfile:       /var/log/antivir.log
update frequency:       daily (if avupdater is
                        running)
update time:            random (if avupdater is
                        running)
http proxy server:      proxy.domain.com:8080
syslog output:          user.notice
available options:      y n
Save configuration settings? [y]
```

If you do not agree with all displayed options:

- Type **N** to restart the configuration script and correct the values.

If all settings correspond to the configuration you require:

- Confirm with **Y** or **Enter** to save the configuration file with the new values.
  - ↳ The script reports saving of the configuration file. It displays information on handling AntiVir Guard and asks if you want to start AntiVir Guard:

```
saving configuration to /etc/avguard.conf ... done
saving configuration to /etc/antivir.conf ... done

Running AvGuard
...
(Information about AntiVir Guard)
...
Would you like to start AvGuard using the new configuration? [y]
```

- Confirm with **Y** or **Enter** to start AntiVir Guard.

- ↳ AntiVir Guard starts. When running, it will automatically restart in order to apply the new settings. Then the configuration is complete

```
Starting AntiVir: avguard-server.
```

- ↳ The script also provides information on the Internet Updater and asks if you want to start the Updater:

```
Running Automatic Internet Updater
...
(Information about Internet Updater)
...
Would you like to start the updater using the new configuration? [y]
```

- Confirm with **Y** or **Enter** to start the Internet Updater.

- ↳ The Updater starts. When running, it will automatically restart in order to apply the new settings. Then the configuration is complete

```
Starting AntiVir: avupdater
Configuration Complete.
```

- ↳ The configuration overview is then displayed.

## 4.4 Configuring AntiVir Notifications

### Setting the email notifications in the case of viruses and unwanted programs

AntiVir can send an email when it detects a virus or unwanted program.

- Run configantivir:

```
/usr/lib/AntiVir/configantivir
```

- Confirm all settings with **Enter** until you reach the option for email notifications:

```
You may set AntiVir to send out an email message every time a concerning file
is accessed. The message will also list the action that was taken to handle the
file.
```

```
available options: y n
Would you like email notification of alerts? [n]
```

- Type **Y**.

- ↳ Then it asks for the email address:

```
What email address will receive notifications? []
```

- Type the email address:

```
root@localhost
```

- Confirm all remaining settings with **Enter**. The email notifications are configured.



*The email address you set will additionally receive messages about AntiVir Updates.*

### Setting syslog messages

AntiVir reports all important operations in the syslog. You can also specify the facility and priority for these messages.



*You should not change the default values if you have no experience of the syslog daemon. For more details, please refer to your UNIX documentation.*

- ▶ Run configantivir:

```
/usr/lib/AntiVir/configantivir
```

- ▶ Confirm all settings with **Enter** until you reach the option about syslog Facility:

Regardless of the other configuration options, AntiVir will always log important information using syslog. Syslog uses two values to classify the information to log: facility and priority. Facility specifies the type of program making the log entry. Priority specifies the importance of the log entry.

If you are unfamiliar with syslog then you may simply accept the default values. However, it is encouraged that you learn about syslog since it is used by many services to log important events.

available FACILITIES: authpriv cron daemon kern lpr mail news syslog user uucp  
local0 local1 local2 local3 local4 local5 local6 local7

Which syslog FACILITY should AntiVir use? [user]

- ▶ Type the facility.

↳ Then you are asked about the priority:

available PRIORITIES: emerg alert crit err warning notice info debug

Which syslog PRIORITY should AntiVir use? [notice]

- ▶ Type the priority.
- ▶ Confirm all remaining settings with **Enter**.

Syslog is configured.

### Setting AntiVir logfile

Apart from syslog, all messages may be saved in a distinct logfile.

- ▶ Run configantivir:

```
/usr/lib/AntiVir/configantivir
```

- Confirm all settings with **Enter** until you reach the option about logfile:

In addition to logging concerning activity through syslog, you may also specify your own log file. This can make it simpler to review past concerning activity without having to sift through syslog files.

available options: y n

Would you like AntiVir to log to a custom file? [y]

- Type **Y**.

↳ Then you are asked for the path to the logfile:

What will be the log file name with absolute path (it must begin with '/')  
? [/var/log/avupdater.log]

- Type the full path to the logfile (example):

/var/log/antivir.log

- Confirm all remaining settings with **Enter**.

Logfile is configured.

### 4.5 Configuring the Resident AntiVir Guard

#### Setting included directories

AntiVir Guard can permanently monitor certain directories. By default, it scans /home.



*The /home directory and its subdirectories are usually accessed by users, so these can be a frequent source of infection.*

*Usually only administrators can access system directories. Monitoring these directories would only use up unnecessary resources.*

AntiVir Guard scans specified directories and their sub-directories.

- Run configavguard:

```
/usr/lib/AntiVir/configavguard
```

- Confirm all settings with **Enter** until you reach the option for included directories:

AvGuard gives you the option of specifying the paths from which files will be scanned. All sub-directories of specified paths will also be scanned as files are accessed.

Current include paths = /home

available options: y n

Would you like to specify new include paths? [n]

- Type **Y**.

↳ Then you are asked which are the directories you wish to include:

Type in the paths one at time, pressing ENTER after each path. All paths must be absolute (beginning with '/'). When you are finished, simply enter a blank line.

[IncludePath 1]

- Type the path to the required directories. Confirm with **Enter**. After the last directory, press **Enter** twice.



*The existing list will not be extended but deleted. You must enter the entire list with all the paths you wish to include every time.*

- Confirm all remaining settings with **Enter**.

IncludePath is configured.

## Setting excluded directories

AntiVir Guard can exclude certain folders when scanning, for example a folder containing temporary files of AntiVir components.



*If you also use AntiVir MailGate, then AntiVir Guard should exclude the spool and the temporary directory from scanning. Otherwise AntiVir Guard blocks MailGate access to email attachments containing viruses or unwanted programs.*

*If these directories are specified in the included paths (see [Setting included directories](#) – Page 50), you have to exclude them from the list.*

AntiVir Guard will not scan specified directories and all their sub-directories.

- Run configavguard:

```
/usr/lib/AntiVir/configavguard
```

- Confirm all settings with **Enter** until you reach the option for excluded directories:

Unless under the specified included paths, files will not be scanned. You may also want that particular sub-directories within the included paths are also not scanned.

For example, perhaps you want the entire /home directory scanned except for /home/bill. AvGuard allows you to specify sub-directories of the included paths that will not be scanned. These sub-directories are called exclude paths. In this example /home/bill would be an exclude path.  
Current exclude paths = NONE

available options: y n

Would you like to specify new exclude paths? [n]

- Type **Y**.

↳ Then you are asked which are the directories you wish to exclude:

Type in the paths one at time, pressing ENTER after each path. All paths must be absolute (beginning with '/'). When you are finished, simply enter a blank line.

[ExcludePath 1]

- Type the path to the required directories. Confirm with **Enter**. After the last directory, press **Enter** twice.



*The existing list will not be extended but deleted. You must enter the entire list with all the paths you wish to exclude every time.*

- Confirm all remaining settings with **Enter**.



*If you activate the `MoveConcerningFilesTo` option, this directory is automatically added to the `ExcludePath` list.*

`ExcludePath` is now configured.

### Setting the capacity of AntiVir Guard

If more parallel processes are accessing files on your system, AntiVir Guard monitors the access using more daemons. This enhances performance.

The number of simultaneous AntiVir Guard daemons can be set between 0 and 20.



*The default is 3 and it is appropriate for smaller standard computers. For servers with high traffic, a larger number would be necessary.*

*However, only the necessary number of daemons should be running, for saving working space.*

► Run `configavguard`:

```
/usr/lib/AntiVir/configavguard
```

↳ The first option concerns the number of daemons:

Files that are accessed by multiple processes at the same time can be scanned by AvGuard in parallel. This is accomplished by running multiple scanning daemons, which allows your machine to run AvGuard with the least amount of performance reduction.

A typical workstation only requires 3 daemons for optimal performance. If you are running additional servers (such as file, http, ftp, etc) then it is recommended that more daemons are used. You can disable AvGuard by setting a value of 0 here.

available options: 0-20

How many daemons would you like to run? [3]

► Type the desired number of daemons.

► Confirm all remaining settings with **Enter**.

The AntiVir Guard capacity is now configured.

### Setting the scanning method of AntiVir Guard

AntiVir Guard can scan files when opened, when closed and/or when executed:

- If you choose to scan files when opened, you avoid opening, reading and copying infected files.
- If you choose to scan files when closed, you avoid writing, saving, copying or downloading infected files from the Internet. If they contain malware code, AntiVir performs the configured actions (repair, rename, move).
- If you choose to scan files when executed, you avoid spreading malware.

Setting AntiVir to scan files when opened **and** closed provides good protection. This is the default configuration.



*If you choose to scan files when closed, the following may happen: between writing and closing the file, there is a short time when access to reading the file is possible and the configured action is not yet applied. Therefore we strongly recommend that you also choose to scan the files when opened.*

*Please note that in the case of integrating Linux kernels 2.6 with the LSM subsystem, "close" events are not generated, only "open" events. Therefore, you must scan files when opened.*

- ▶ Run configavguard:

```
/usr/lib/AntiVir/configavguard
```

- ▶ Confirm all settings with with **Enter** until you are asked if files should be scanned when opened:

Files may be scanned as they are opened. This is useful for preventing users from accessing concerning files. This includes opening, reading and copying concerning files.

available options: y n

Would you like to scan files as they are opened? [n]

- ▶ Choose **Y** or **N**, according to the configuration you require.

↳ Then you are asked if files should be scanned when closed:

Files may be scanned as they are closed. This is useful for preventing users from creating concerning files. This includes saving, downloading and copying concerning files.

available options: y n

Would you like to scan files as they are closed? [n]

- ▶ Choose **Y** or **N**, according to the configuration you require.

↳ Then you are asked if files should be scanned when executed:

Files may be scanned as they are executed. This is useful for preventing users from running concerning programs

available options: y n

Would you like to scan files as they are executed? [n]

- ▶ Choose **Y** or **N**, according to the configuration you require.



*If you answer N to all three options, AntiVir Guard is deactivated.*

- Confirm all remaining settings with **Enter**.

The AntiVir Guard scanning method is now configured.

### Repairing files when accessed

Normally, AntiVir Guard blocks access to files containing viruses or unwanted programs.

AntiVir Guard is also able to repair files when accessed. If repair is possible, the user can access the repaired file without risk. If the file cannot be repaired, access remains blocked.

The action is reported every time in the logfile.

- Run configavguard:

```
/usr/lib/AntiVir/configavguard
```

- Confirm all settings with **Enter** until you are asked if concerning files should be repaired:

If an concerning file is found, AvGuard can try to remove the problem. If the problem cannot be removed, access to the file will still be blocked. However, if the problem can be removed, the user will be allowed normal access.

available options: y n

Would you like to try to repair concerning files? [y]

- Answer **Y** to activate the repair function.
- Confirm all remaining settings with **Enter**.

Now AntiVir Guard repairs concerning files when accessed.

## Renaming or moving concerning files automatically

If an concerning file cannot be repaired or if this option is not activated, AntiVir Guard can automatically rename or move the file.

Access to the concerning file is safely blocked. The action is reported in the logfile.

- Run configavguard:

```
/usr/lib/AntiVir/configavguard
```

- Confirm all settings with **Enter** until you are asked how AntiVir Guard should react to concerning files:

When an alert is found and cannot be removed, there are several ways in which AvGuard can respond.

log only - the name of the concerning file will only  
be logged using syslog

rename - the concerning file will be renamed to  
have a .XXX extension

move - the concerning file will be moved to a  
directory of your choice

Regardless of which option you choose, the event involving the concerning file will be logged using syslog and access to the file will be blocked.

available options: l r m

How should concerning files be handled? [l]

Renaming  
concerning files

If you want to rename the concerning files:

- Answer **R**.

- Confirm all remaining settings with **Enter**.

All concerning files will receive the extension .XXX .

Moving  
concerning files

If you want to move the concerning files:

- Answer **M**.

↳ Then you are asked to specify the directory for the moved files:

Which directory should they be moved to? []

- Type the full path to the desired directory. Example:

```
/home/quarantine
```

- Confirm all remaining settings with **Enter**.

All concerning files will be moved to the specified directory.



*This directory should be used exclusively for storing concerning files (Quarantine directory).*



*If you have activated the `MoveConcerningFilesTo` option, this directory is automatically interpreted as an excluded path (`ExcludePath`) .*

No action If you do not want to rename or move the concerning files:

- ▶ Type **L**.
- ▶ Confirm all remaining settings with **Enter**.

The concerning files will have the name unchanged and they will remain in their directory. Access is still blocked and the action is reported in the logfile.

### Configuring packed archive scanning

AntiVir Guard can scan compressed archives (e. g. `.zip`, `.gz`, `.tar`) for viruses and unwanted programs. The files are unpacked and scanned.

You may set the following options:

- Maximum size of archived files. AntiVir Guard scans only the files with unpacked size smaller than the given value. There are compressed files with insignificant content, but they are specially made to have a large size and to slow down the computer. This option avoids unpacking such archives.
  - Default value: 1 Gigabyte (1073721824 byte)
- Maximum recursion level. There are packed files which contain other packed files and so on. AntiVir Guard scans only files with a smaller recursion level than the given value. It thus saves processing time.
  - Default value: 5

- ▶ Run `configavguard`:

```
/usr/lib/AntiVir/configavguard
```

- ▶ Confirm all settings with **Enter** until you are asked if compressed files should be scanned:

There may be alerts hiding within compressed files (`.zip`, `.gz`, `.tar`, etc). You may configure AvGuard so that these compressed files are decompressed and searched for concerning files. This will help to ensure that your server is free from unwanted files.

```
available options: y n  
Would you like to scan compressed files? [n]
```

- ▶ Type **Y** to scan compressed files.

- ↳ Then you are asked to specify the maximum unpacked size of compressed files:

In order to scan the contents of compressed files, the files must be decompressed. For very large compressed files it could take a long time to decompress everything. For this reason, you may wish you put a size limit for compressed files that will be scanned. The size limit is given in bytes. For example, 1 gigabyte = 1073741824 bytes. You may set this value to 0 to have no limit on the size of scanned compressed files.

available options: 0-??

What is the maximum size compressed file (in bytes)  
to be scanned? [1073741824]

- Type the maximum value you want in bytes. If you wish to scan all packed files, whatever their size, type 0.

- ↳ Then you are asked to specify the maximum recursion level of the packed files:

It is possible that a compressed file has many compressed files as contents. For example, inside of filename.zip there may be a file1.zip file. Each compressed file within a compressed file is referred to as a recursion level. If AvGuard should decompress apple.zip it must scan recursion level 1. If it is supposed to also decompress seed.zip, it must scan recursion level 2.

Since decompressing takes extra time, you may wish to set a limit on the recursion level that will be scanned. A value of 0 means that there will be no limit.

available options: 0-??

What is the maximum recursion level in compressed files to be scanned? [5]

- Type the maximum level. If you wish to scan all files, whatever their nested level, type 0.
- Confirm all remaining settings with **Enter**.

The archive scanning is configured.

### 4.6 Configuring AntiVir Samba Scanner

AntiVir Samba Scanner consists of a VFS plug-in for Samba and a Scan Service. To use AntiVir Samba Scanners, you must install the VFS plug-in (an AntiVir specific plug-in for samba-vscan software) as described in [Integration on Samba](#) – Page 17.

You have to activate AntiVir VFS Plug-in for the monitored shares in the Samba Service configuration file `smb.conf`. The specification of a configuration file is optional. The new entries to be made are, for example:

```
[myshare]
...
vfs object = vscan-antivir
vscan-antivir: config-file =
/usr/local/samba/lib/vscan-antivir.conf
```

Your distributor may have already carried out this step or you could use a configuration interface to do this.

You can activate the scanner for single shares or for the entire server by making the specific entries in the `[global]` section of the `smb.conf` file.

You may operate single shares using separate configuration files or you can use the same configuration file for all scanners at once. If no configuration file is specified for the scanner, it will be used in the default configuration.

#### Configuration file `vscan-antivir.conf`

The entries in `vscan-antivir.conf` are described in more detail in the order of their appearance. They can be roughly divided into two categories:

- samba-vscan options, which can be similarly supported by all Backends;
- AntiVir-specific options, which operate specific functions of this Backend.

max file size

##### **Maximum file size:**

samba-vscan can skip files when scanning if they exceed a certain size. If the option is set to 0 (default), all files are scanned.

```
max file size = 0
```

verbose file  
logging

##### **Logging file access:**

samba-vscan can report every file access in a log (if this option is set to `yes`) or it can report only the access to files in which it detects a virus or unwanted program (`no`). The default is `no`.


```
verbose file logging = no
```

scan on open/  
scan on close

##### **Scanning files when opened and/or closed:**

samba-vscan scans files for various events when opened and/or closed (Default: both cases).

```
scan on open = yes
scan on close = yes
```

deny access on error/ deny access on minor error	<p><b>Denying access to files:</b></p> <p>samba-vscan can deny access not only when it finds a virus or unwanted program in a file, but also when an error occurs during file processing. This option can be set for different error levels:</p> <p>If the Scanner itself is not available, this is considered an error.</p> <p>If the Scanner, although available, cannot scan files, this is considered a minor error.</p> <p>As this situation allows malware to infiltrate the system, access is blocked by default for this case.</p> <pre>deny access on error = yes deny access on minor error = yes</pre>
send warning message	<p><b>Notifying file access denial:</b></p> <p>samba-vscan can notify remote users of a fileserver every time access is blocked, using pop-ups (Default: yes).</p> <pre>send warning message = yes</pre>
concerning file action (infected file action)	<p><b>File actions:</b></p> <p>Apart from blocking the access to concerning files, samba-vscan is also able to perform further actions:</p> <ul style="list-style-type: none"> <li>• Delete the file</li> <li>• Move the file to a quarantine directory</li> </ul> <p>The values for this option are nothing (default), delete and quarantine.</p>
	<p><i>Please note that the term "infected" is incorrect when used for other unwanted software detected as viruses. Not all findings are infected with a virus, but they may have a different cause. Therefore, for compatibility reasons, the option infected file action has been replaced in the newer versions with concerning file action. You should also use this term in the notification texts for affected users.</i></p> <pre>concerning file action = quarantine</pre>
quarantine directory, quarantine prefix	<p><b>Quarantine directory and prefix:</b></p> <p>If you activate the option to move concerning files to quarantine, when a virus or unwanted program is detected, you can now specify the directory for the quarantine and the prefix to apply to file names. You have to adapt the settings to your system requirements. If the moving reaction fails, the concerning files are deleted by the bulk memory.</p> <pre>quarantine directory = /tmp quarantine prefix = vir-</pre>
max lru files entries, lru file entry lifetime	<p><b>Recently scanned files:</b></p> <p>samba-vscan creates a list with the recently scanned files to ensure a fast reaction to successive file access and to save scan resources. With these settings you can configure the memory for the last recently used (LRU) files. Default: 100 entries,</p>

for up to 5 seconds.

```
max lru files entries = 100
lru file entry lifetime = 5
```

exclude file  
types

### **Excluding files from scanning:**

samba-vscan can exclude certain file types from scanning, classifying the files by the MIME type. You should use this option with great care!

By default the list is empty, so there are no excluded file types.

```
exclude file types =
```

antivir program  
name

### **Path for AntiVir program:**

The VFS Plug-in serves as an interface between Samba and the Scan Service. The "antivir" program has been integrated for the AntiVir Scanner. This option tells the plug-in where to find the "antivir" program. Default:

```
antivir program name = /usr/lib/AntiVir/antivir
```

options for  
archives

### **Checking archives:**

AntiVir Samba Scanner is also able to scan within archives if the option `antivir scan in archive` is set to `yes`. However, there are limits and archives are skipped when they exceed these parameters (maximum compression ratio, maximum contents size, maximum recursion level). If one of these values is 0, the limit does not apply, so it is "infinite".

```
antivir scan in archive = no
antivir max ratio in archive = 150
antivir max archived file size = 1073741824
antivir max recursion level = 5
```

antivir detect ...

### **Detecting unwanted software:**

AntiVir Samba Scanner always scans for viruses in assigned files. It can also detect other types of unwanted software if you activate the appropriate option (set it to `yes`).



*Please note that even if the access to a file is blocked by the option concerning file action, it is not necessarily infected by a virus. By default, the Scanner searches only for viruses.*

```
antivir detect dialer = no
antivir detect game = no
antivir detect joke = no
antivir detect pms = no
antivir detect spy = no
```

It is also possible to activate all detection types with a single option:

`antivir detect alltypes`. If set to `yes`, all the above detect options are considered activated.

## 4.7 Configuring Regular Updates

The performance and effectiveness of antivirus software depend on updating. This is why AntiVir offers the possibility to download current updates via HTTP from the AntiVir web servers and even to schedule them automatically at regular intervals.

These updates ensure that AntiVir components, which provide security against viruses and unwanted programs, are always kept up to date.

All update processes use AntiVir Command line scanner. The command

```
antivir --update
```

enables the update of AntiVir software at any time (see [Updating AntiVir Manually](#) – Page 74).

There are two methods to configure AntiVir updates:

1. You can use the Internet Updater provided with AntiVir, which is easy to configure. This is recommended if you have little UNIX knowledge and if you only want to make small adjustments.
2. You may use AntiVir with cron daemon. This is recommended if you have extensive UNIX knowledge. You have to carry out configuration yourself, but it gives you more flexibility.

### Configuring Internet Connection for Updates

- ✓ Check that your Internet connection is functioning correctly. In most cases, the connection is already configured. If not, refer to your UNIX documentation for the information you need.

**Proxyserver** If your AntiVir UNIX Server computer is connected to the Internet via HTTP proxy server, you must make the necessary settings for AntiVir:

- Run configantivir:

```
/usr/lib/AntiVir/configantivir
```

- Confirm all settings with **Enter** until you reach the proxy server option:

If this machine is sitting behind an HTTP proxy server, you will need to configure AntiVir with the appropriate proxy settings. Internet access is required in order to make updates.

available options: y n

Does this machine use an HTTP proxy server? [n]

- Type **Y**.

↳ You are then asked for the name of the proxy server:

What is the HTTP proxy server name? []

## Configuration

---

- ▶ Type its name (example):

proxy.domain.com

- ↳ Then you are asked for the proxy server port:

Which port number does the HTTP proxy server use? []

- ▶ Type the port:

8080

- ↳ You are asked if you need a username and password for the proxy server:

Proxy servers may be configured to require a username and password. If the HTTP proxy server for this machine requires a username and password AntiVir needs to be appropriately configured.

available options: y n

Does the HTTP proxy server require a username/password? [n]

If this is the case:

- ▶ Type **Y**.

- ↳ Then you are asked for the username and password.

- ▶ Enter the username and password.

- ▶ Confirm all remaining settings with **Enter**.

The Internet update connection is now configured.

## Configuring Automatic Updates through Internet Updater

The Internet Updater is a very simple daemon which performs the following commands at fixed intervals:

```
antivir --update
```



*To enable the following settings, you must first install the Internet Updater i.e. if you have installed AntiVir UNIX Server with Updater as described in [Installing AntiVir](#) – Page 20. Otherwise you have to run the installation script again, see [Reinstalling AntiVir](#) – Page 28.*

You can define the following settings:

- Update intervals. It is possible to:
  - update every two hours
  - update daily
- Time settings for updates (for daily updates). You can:
  - set the time yourself;
  - choose a random time set. In this case, the script will chose a time, which will remain set for every day. It is therefore important for the computer to be permanently online.

► Run configantivir:

```
/usr/lib/AntiVir/configantivir
```

↳ First you are asked how often you need AntiVir to check for updates:

AntiVir is equipped with an Automatic Internet Updater. At specified intervals, AntiVir will connect to an updater server to check for newer versions of the AntiVir engine or the virus data file. If a newer version is available, AntiVir will automatically download and install the updates without requiring any special attention. This allows AntiVir to be kept current against virus attacks. AntiVir can be configured to check for updates every 2 hours (2) or once a day (d). You can also choose to have the Automatic Internet Updater never check (n).

available options: 2 d n

How often should AntiVir check for updates? [n]

► Type:

- **n** if you do not want automatic updates
- **2** for updates every two hours
- **d** for daily updates

↳ If you decide on daily updates, you must then set the time:

The Automatic Internet Updater can be set to always check for updates at a particular time of day. This is specified in a HH:MM format (where HH is the hour and MM is the minutes). If you do not have a permanent connection, you may set it to a time when you are usually online. You may also let AntiVir choose a random time (r).

If you have a permanent connection then a random time may be preferred because it will help to disperse the times when other users are getting updates.

available options: HH:MM r  
What time should updates be done? [16:00]

► Type the time in HH:MM format.

– OR –

Type **r** for random time.

► Confirm all remaining settings with **Enter**.

The automatic updates are now configured. The Internet Updater will start automatically (if not yet performed) or is restarted (if already active).

### Starting and Stopping Internet Updater Manually

If you want to start Internet Updater manually:

► Type:

```
/usr/lib/AntiVir/avupdater start
```

If you want to stop Internet Updater manually:

► Type:

```
/usr/lib/AntiVir/avupdater stop
```

If you want to check the current status of the Internet Updater:

► Type:

```
/usr/lib/AntiVir/avupdater status
```

## Performing Cron Updates



*Performing updates with cron is recommended!*

If you are an experienced UNIX user, you can use cron daemon to perform automatic AntiVir updates.

Cron daemon is used to run regular system processes. For more details, refer to your UNIX documentation.

Using cron for updates, you have more configuration possibilities than with the Internet Updater.

Example: ► Enter the following cron job in `/etc/crontab`:

```
45 */2 * * * root /usr/lib/AntiVir/antivir --update -q
```

↳ This command activates updates every 2 hours, but performs them 15 minutes ahead of the set time: 0:45, 2:45, 4:45 and so on. The `-q` parameter states that no report will be given, see [Options](#) – Page 69

## Starting Internet Updater Automatically

It is important that the Internet Updater starts automatically with every system start-up. If you have performed the installation as described in [Installing AntiVir](#) – Page 20, your system is correctly set.

If Internet Updater has not yet been automatically activated on system start-up:

► Reinstall AntiVir with the necessary settings (see [Reinstalling AntiVir](#) – Page 28).

## Verifying Updates Authenticity with GnuPG

GnuPG is a free alternative to the encryption program PGP (Pretty Good Privacy). Using GnuPG you can verify the authenticity of the AntiVir Updates.



*It is highly recommended to use GnuPG.*

*However, this procedure requires intensive knowledge of UNIX and GnuPG. In the event of configuration errors, there is a danger of deactivating AntiVir updates.*

*These steps must be performed by a user who runs updates on the computer. Usually it is the user with administrator rights.*

You can find more information on GnuPG at <http://www.gnupg.org>

The following steps guide you to activate GnuPG support.

► Download GnuPG from the website <http://www.gnupg.org>. Here you can also find the manual with further information on GnuPG and its features.

► Generate your own PGP key pair, as described in the documentation.

► Import the AntiVir public PGP key to your key-ring:

```
gpg --import antivir.gpg
```

– OR –

Import the AntiVir public key directly from the key server:

```
gpg --keyserver=wwwkeys.pgp.net --recv-keys 0F821C2E
```

- Display the fingerprint of the key to check that it really is the AntiVir PGP key:

```
gpg --fingerprint support@antivir.de
```

↳ The 40-character fingerprint is displayed.

- Check whether the fingerprint corresponds with the one on the AntiVir website

(<http://www.avira.com>).

- Sign the AntiVir public key in order to certify its validity:

```
gpg --sign-key support@antivir.de
```

- Change to /bin subdirectory of the AntiVir installation directory (example):

```
cd /tmp/antivir-server-prof-<version>/bin
```

↳ Here you can find the files antivir and antivir.asc.

- Check the signature with

```
gpg --verify antivir.asc antivir
```

↳ If you do not get any error message, you can use GnuPG for AntiVir updates.

- Activate GnuPG for AntiVir. In /etc/antivir.conf enter the path to GnuPG binaries, using the option GnuPGBinary:

```
GnuPGBinary          /usr/local/bin/gpg
```



*You can only edit this option in antivir.conf manually. Setting in the configuration script is not possible, in order to avoid the danger of configuration errors.*

- Restart Internet Updater to activate the new settings in antivir.conf:

```
/usr/lib/AntiVir/avupdater restart
```

From now on, GnuPG authenticates the updates.

## 4.8 Testing AntiVir UNIX Server

After completing the installation and configuration, you can test the functionality of AntiVir UNIX Server using a test virus. This will not cause any damage, but it will force the security program to react when the computer is scanned.

### Testing AntiVir with a Test-Virus

- ▶ Type the following URL in your Web browser <http://www.eicar.org>.
- ▶ Read the information about the test virus [eicar.com](http://www.eicar.com).
- ▶ Download the test virus to your computer.
  - ↳ According to the AntiVir configuration and eicar version, AntiVir Guard will immediately block the download and it will issue an alert message.
- ▶ Try to access the file, for example by copying:

```
cp eicar.com eicar.com.txt
```

  - ↳ According to the AntiVir configuration and eicar version, AntiVir Guard will immediately block access and take any necessary action, such as rename or move the file.

### Scanning for Possible Errors

If you notice that AntiVir Guard does not display the expected messages or does not take the relevant action, you have to check the configuration.

- ▶ Check whether AntiVir Guard is running. Type:

```
/usr/lib/AntiVir/avguard status
```
- ▶ Start AntiVir Guard if necessary.
- ▶ Check whether the directory in which you are currently working is included in the monitored list, in `/etc/avguard.conf` (see [Configuration File avguard.conf](#) – Page 39)
- ▶ Check the value of `AccessMask` in `/etc/avguard.conf`. If the value is 0, then AntiVir Guard is deactivated.
- ▶ Check the messages in the logfile of AntiVir Guard or in syslog in order to isolate errors.



## 5 Operation

After concluding installation and configuration, AntiVir guarantees continuous scanning on your system. During operating, there will possibly be occasional changes in [Configuration](#) – Page 37.

Nevertheless, a manual scan for viruses or unwanted programs might be needed. This is where you can use AntiVir Command line scanner. This program enables scanning for many specific targets.

AntiVir Command line scanner can be integrated into scripts and also regularly activated by cron jobs. Users familiar with UNIX have various possibilities available to set optimum monitoring of their systems.

This Chapter has the following structure:

- [Overview of AntiVir Command Line Scanner](#) – Page 69 summarizes all options for the Command line scanner.
- [Using AntiVir Command Line Scanner](#) – Page 73 describes some examples of working with the Command line scanner.
- [Reaction to Detecting Viruses/ Unwanted Programs](#) – Page 76 gives you some hints on how to react when AntiVir has done its work.

### 5.1 Overview of AntiVir Command Line Scanner

#### Start

AntiVir Command line scanner starts with

```
/usr/lib/AntiVir/antivir [-option] [directory [...]]
```

If you have created a link in /usr/bin during installation, the following is sufficient:

```
antivir [-option] [directory [...]]
```

If you have not specified any directory, it scans only the current directory.

If you want to scan certain files in a directory, the syntax is:

```
antivir [-option] [directory][filename]
```

#### Options

You can use the following options for the command line scanner, in various combinations:

Option	Function
--allfiles	Scans all files, not only program files.
--alltypes	Searches for viruses and unwanted programs. This option is a contraction for all possible --with-<type> options. See below.

Option	Function
--archive-max-size=N	Excludes archived files, if their unpacked size exceeds the given value.
--archive-max-ratio=N	Excludes archived files, if their compression ratio exceeds the given value.
--archive-max-recursion=N	Excludes archived files, if their recursion level exceeds the given value.
-C <filename>	Name of the configuration file to be used. Default: /etc/antivir.conf
--check	Used with --update: AntiVir checks for available updates. In case of available updates, it issues a message, but it does not perform the update.
-cf<filename>	Activates CRC check and indicates the database <filename>. See <a href="#">Using CRC Database</a> – Page 75
-cn	Used only with -cf. It inserts new files to database. See <a href="#">Using CRC Database</a> – Page 75
-cu	Used only with -cf. It updates CRCs for files in database. See <a href="#">Using CRC Database</a> – Page 75
-cv	Used only with -cf. It calculates CRC over the whole file length instead of the default 16K. See <a href="#">Using CRC Database</a> – Page 75
-del	When virus/unwanted program detected, infected files are deleted.
-dmdas	Deletes all macros in a document, if one is suspicious.
-dmddel	Deletes documents with suspicious macros.
-dmse	Sets the exit code to 101, when a macro is found.
-e -del	Infected files are repaired if possible. If not, they are deleted.
-e -ren	Infected files are repaired, if possible. If not, they are renamed.
--exclude=<dir>	Does not scan inside the specified directory.
--help	Shows all possible options.
--heur-macro	Activates Heuristics for macroviruses in documents.
--heur-nomacro	Deactivates Heuristics for macroviruses in documents.
--heur-level=N	Sets the detection level for Win32 files. Level 0: off Level 1: low Level 2: medium Level 3: high
--home-dir=<dir>	AVIRA searches in <dir> for its own files (for example avira.vdf) .
--info	AntiVir shows the list of all known viruses, Malware and unwanted programs.
-kf<filename>	AntiVir uses the license key from this specified <filename> .
-lang:DE	AntiVir generates German messages.
-lang:EN	AntiVir generates English messages.
--log-email=<addr>	Sends a scan report to the specified email address (in addition to results displayed on the screen).

Option	Function
-noboot	The boot sector test is deactivated. This saves time in targeted scan operations, but otherwise it is not recommended.
-nobreak	Deactivates <b>Ctrl+C</b> and <b>Ctrl+Break</b> . This avoids interruption from a user.
-nolnk	Ignores symbolic links.
-nombr	Master boot sector test is deactivated. This saves time in targeted scan operations, but it is not otherwise recommended.
-once	AntiVir scans once a day only: this option checks if AntiVir already ran on that day. If it has been executed, the scanning is aborted and a message is issued.
-onefs	Ignores links to other file systems. This excludes folders (for example NFS folders) from scanning.
-q	"Quiet": AntiVir suppresses all messages.
-r1	Only viruses, unwanted programs and warnings are logged.
-r2	In addition to -r1, all scanned paths are logged.
-r3	All scanned files are logged.
-r4	Detailed messages are logged.
-ra	The log messages are appended to an existing log file.
-ren	Infected files are renamed when a virus/unwanted program is detected.
-rf<filename>	Creating the logfile with given <filename>. In <filename> you can use the following macros: <ul style="list-style-type: none"> <li>- %d: day</li> <li>- %m: month</li> <li>- %y: year</li> </ul>
-ro	Overwrites logfile.
-rs	Messages about viruses or unwanted programs are output individually.
-s	Scans all subdirectories.
--scan-in-archive	Also scans within packed archives.
--scan-in-mbox	Also scans the email file.
--temp=<dir>	AntiVir Keeps its temporary files in <dir>.
--update	AntiVir performs an update, to keep the virus definition file (VDF) and programs up-to-date.
-v	Performs an intensive scanning on all files and even issues error messages. This option should be used in exceptional cases only, as for example after a virus detection/removal.
--version	Shows AntiVir Version.
--warnings-as-alerts	Treats non-fatal situations as serious errors. Terminates the program when getting warnings, with the same exit code as the one issued for virus detection.
--with-<type>	Activates detection of unwanted programs, which are not viruses. <type> can be dialer, game, joke or pms. You can use this option more than once. (see also --alltypes)

Option	Function
-z @<rspfile>	Corresponds to --scan-in-archive AntiVir reads parameters from "response file" <rspfile>. In <rspfile> every option must be on a separate line. This enables saving of a combination of parameters as a file for later use.

### Exit Codes

AntiVir command line scanner issues exit codes after operation. UNIX users can include them in scripts.

Exit Code	Meaning
0	Normal program termination: no virus/unwanted program, no error.
1	Virus/ unwanted program detected in file or boot sector.
2	Virus/ unwanted program detected in memory.
3	Virus/unwanted program detected in file or boot sector, using heuristics.
100	AntiVir displays only the help text.
101	Macro detected in a file (when -dmse option is used).
102	AntiVir doesn't start, because the parameter -once was used and the program has already run that day.
200	Program aborted; not enough memory.
201	The specified response file was not found.
202	The specified response file contains another @<rsp> directive.
203	Invalid parameter.
204	Invalid directory.
205	The specified log file could not be created.
210	AntiVir could not find a required library.
211	Program stopped, because self check failed.
212	Could not read avira.vdf file.
213	Initialization error.
214	License key not found.

AntiVir command line scanner has other exit codes when used with --update:

Exit Code	Meaning
0	No update available.
1	AntiVir was successfully updated (when - -check is activated, it only reports that an update is available).
>=2	Update failure.

## 5.2 Using AntiVir Command Line Scanner

This paragraph shows examples of using the command line scanner.



*When AntiVir Guard is active, using AntiVir Command line scanner causes double file scanning:*

1. With AntiVir Guard, if the file is opened with AntiVir Command line scanner.
2. With AntiVir Command line scanner itself.

*In order to avoid disturbance, you should first deactivate AntiVir Guard:*

```
/usr/lib/AntiVir/avguard stop
```

*In addition, remember to restart it after scanning:*

```
/usr/lib/AntiVir/avguard start
```

### Performing Complete Scan

After installation, it is important to perform a complete scan of the system.

The following parameters should be used:

<code>--allfiles</code>	Scans all files.
<code>--alltypes</code>	Detects all sorts of suspicious and unwanted files
<code>-s</code>	Scans all subfolders.
<code>-z</code>	Scans packed files, too.

► The command is:

```
antivir --allfiles -s -z --alltypes /
```

### Performing Partial Scan

Usually, scanning the directories that contain incoming and outgoing data (mailbox, Internet, text folders) may be sufficient. These files are usually in `/var`.

If you have any DOS partitions on your UNIX system, you also have to scan them.

You can use the following parameters:

<code>--allfiles</code>	Scans all files.
<code>-s</code>	Scans all subfolders.
<code>-z</code>	Scans packed files, too.

If your DOS partitions are in `/mnt` and the incoming and outgoing files are in `/var`:

► Use the command:

```
antivir --allfiles -s -z /var /mnt
```

### Deleting Infected Files

AntiVir can delete files which contain viruses or unwanted programs. Optionally, AntiVir can first try to repair these files.

The program will first overwrite the files and then delete them; i.e. repairing tools

will not recover them.

You can use the following options:

<code>--allfiles</code>	Scans all files.
<code>-del</code>	Deletes infected files.
<code>-e -del</code>	Tries to repair the infected files and deletes the ones it could not repair.



*In the following examples, files are transformed or deleted. Therefore important data may be lost!*

Examples If you want to delete all infected files from `/home/myhome`:

► Type the command:

```
antivir --allfiles -del /home/myhome
```

If you want to repair infected files from `/home/myhome` and to delete the files that could not be repaired:

► Type the command:

```
antivir --allfiles -e -del /home/myhome
```

### Running AntiVir When Installed in Directory Other Than `/usr/lib/AntiVir`

AntiVir requires information on its installation directory for the self-test if not installed in `/usr/lib/AntiVir`.

If AntiVir is installed, for example in `/usr/local/AntiVir`:

► Type:

```
antivir --home-dir=/usr/local/AntiVir
```

### Updating AntiVir Manually

You can update AntiVir manually at any time.

It is recommended to run AntiVir as **root** during updates.

Advantage: any running processes of AntiVir daemons (such as AntiVir Guard, SAVAPI, MailGate) will be automatically updated with the new security files without interrupting the scanning process. Thus it ensures that all files are scanned.

If AntiVir is not started as **root** during updating, it will not have the necessary authorizations for restarting AntiVir daemons. Consequently, you need to restart manually as **root**.

If you want to update AntiVir:

► Type:

```
/usr/lib/AntiVir/antivir --update
```

If you only want to check for a new AntiVir update without performing it:

► Type:

```
/usr/lib/AntiVir/antivir --update --check
```

## Updating AntiVir Using a Script

Advanced UNIX users can integrate the AntiVir Command line scanner in a script and use the [Exit Codes](#) – Page 72.

Example ► Write a script as below to suppress AntiVir messages and to replace them with your own:

```
----- BEGIN SCRIPT -----
#!/bin/sh

/usr/lib/AntiVir/antivir --update -q
case $? in
  0)
    echo "AntiVir is up-to-date"
    ;;
  1)
    echo "AntiVir has been updated"
    ;;
  *)
    echo "An error occurred during update"
    ;;
esac
----- END SCRIPT -----
```

## Using CRC Database

AntiVir offers the possibility of creating a database with the CRC values of the scanned files and of comparing these values during future scanning processes. It uses by default the first 16 bytes of every file.

Therefore, AntiVir uses these values in the CRC database to compare them with the current CRC values of the files to be scanned. The files are only scanned if they differ. In this way, AntiVir only has to scan the modified or new files.

You can use the following options with AntiVir:

- cf<filename> -cn Adds new CRC values of the scanned files to the database <filename>. This option is used to initialize the database.
- cf<filename> Indicates the database <filename>. If no other CRC options are given, AntiVir compares the CRC values of files scanned with those from the database and scans the files only if the values are different.
- cf<filename> -cu Updates CRC values of the files in the database.

`-cv` Used only with `-cf` option. Generates the entire CRC values of the file instead of the first 16 bytes. It is safer but slower.

Example If you want to create a new CRC database for all files (antivir.db):

► Type the command:

```
antivir -cf/var/tmp/antivir.db -cn --allfiles -s /
```

If you want to scan all files again using CRC database:

► Type the command:

```
antivir -cf/var/tmp/antivir.db --allfiles -s /
```

### 5.3 Reaction to Detecting Viruses/ Unwanted Programs

If correctly configured, AntiVir is set to deal automatically with all the tasks on your computer:

- The infected file is repaired or at least deleted.
- If it could not be repaired, access to the file is blocked and, according to the configuration, the file is renamed or moved. This eliminates all virus actions.

You should do the following:

- Try to detect the way the virus / unwanted program infiltrated your system.
- Perform targeted scanning on the data storage supports you used.
- Inform your team, superiors or partners.
- Inform your system administrator and security provider.

#### Submit Infected Files to Avira GmbH

- Please send us the viruses, unwanted programs and suspicious files that our product does not yet recognize or detect and also any suspicious files. Send us the virus or unwanted program packed in a password-protected archive (PGP, gzip, WinZIP, PKZip, Arj) attached to an email message to [virus@antivir.com](mailto:virus@antivir.com).



*When packing, use the password virus. This way the file will not be deleted by virus scanners on the email gateway.*

## 6 Graphical User Interface (GUI)

### 6.1 Overview

The graphical user interface (GUI or the **AntiVir for UNIX Framework**) assists you in operating and configuring AntiVir UNIX Server and it graphically displays the monitoring process. AntiVir UNIX Server is fully functional and configurable even without GUI. The interface is an independent application which can start and stop without influencing the AntiVir UNIX Server.

You need Java 1.4.0 or higher to use the GUI.

**Permissions** You do not need **root** authorizations to use the program with GUI as a normal user.

However, you must belong to the "antivir" group, created during the installation.

► Type (as root):

```
/usr/sbin/usermod -G group1,group2,group3,antivir user-  
name
```

group1 - group3 are the groups to which the user belongs,  
username is the name of the user.

To set the groups for a user:

► Type:

```
/usr/bin/groups
```

**Starting** ► Start the GUI:

```
antivir-gui
```

If this command does not detect the Java installation:

► Create a soft link in /usr/bin (as root):

```
ln -s /PATH/TO/JAVA/INSTALLATION/bin/java /usr/bin
```

**Communi-  
cation** GUI communicates with AntiVir UNIX Server via SSL over the loopback network interface. You must specify the following parameters in the configuration file avguard.conf:

```
GuiSupport      yes  
GuiCAFile       /usr/lib/AntiVir/gui/cert/cacert.pem  
GuiCertFile     /usr/lib/AntiVir/gui/cert/server.pem  
GuiCertPass     antivir_default
```

If these parameters are missing or invalid, the GUI is not available.

Any errors are recorded in the logfile.

## Graphical User Interface (GUI)

---

**More products** If more AntiVir products are installed on the computer, GUI displays them in separate tabs. Thus you can easily monitor and configure every product. Depending on the tab you click, the GUI displays its own menus and options.

**Problems** Check the following requirements for use of the GUI:

- AntiVir UNIX Server must be installed in `/usr/lib/AntiVir`.
- You must have a COMMERCIAL license for the AntiVir UNIX Server (`antivir --version`).
- The parameter `GuiSupport` must be set in `antivir.conf`.
- The user must belong to the "antivir" group.

If these requirements are not met, an error message appears:

**AntiVir UNIX Server is not available on the computer.**

## 6.2 AntiVir Scanner

### 6.2.1 Operating AntiVir Scanner Using the GUI

You can conveniently configure and perform scanning processes using the AntiVir for UNIX Framework.

#### Starting Scanner GUI

- Start the GUI:

```
/usr/lib/AntiVir/antivir-gui
```

↳ The GUI appears, displaying the **Folders view**.



#### Buttons



Click to start the **Scanning** process, with graphical display.



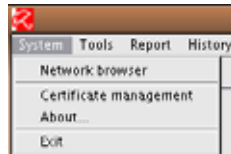
Click to open the **Configuration** window.



Click to view the **Logfile** of the scanning process.

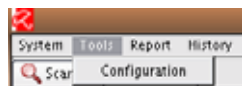
## Menus

### System



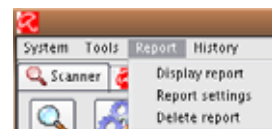
- **Network browser:** to select another computer in the network on which AntiVir GUI runs.
- **Certificate management:** to manage integrated certificates of the other computers in the network.
- **About...:** displays **Product information** and **Support information**
- **Exit:** closes GUI. AntiVir UNIX Server is not stopped.

### Tools



- **Configuration:** to open the configuration window.

### Report



- **Display report:** to display the report file in a window (avscanner.log).
- **Report settings:** to open the configuration window for the report settings.
- **Delete report:** to delete the report file (given in the Report settings configuration window).


### History



- **Display history:** to open the history window, with AntiVir actions reports.
- **History options:** to open the configuration window for the history settings.
- **Delete history:** to delete the Scanner actions reported in history.

### Starting the Scan Process



- ▶ Select the required computers, directories and files to be scanned from the **Folders** view by clicking the corresponding check-box.
- ▶ Click the magnifying glass icon .
  - ↳ AntiVir starts scanning, displaying the scan process window. The Scanner searches through the selected directories using the current configuration.



*All computers must have the executable antivir in the directory specified in the configuration.*



Last detection    The name of the last detected malware.

Number of files    The number of files that have been scanned during the current process.

## Graphical User Interface (GUI)

---

Time	The time taken by the current scanning process.
Warnings	Number of current warnings.
Detections	Number of detections during the current scanning process.
Folder	The number of directories that have been scanned during the current process.
File	Currently scanned file.
Status	The Scanner status.

### Stopping the Scan Process



You can stop the scanning process by pressing the **Stop** button. This button is deactivated if the option "**Allow interruptions**" in **Scanner Configuration/ Search** is not active.

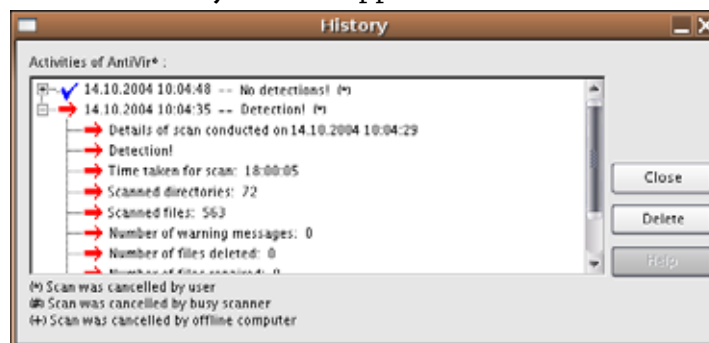
- ▶ Press the **Stop** button.
  - ↳ The scanning process ends.
  - ↳ The **Status** window displays an overview of the process.

### Displaying Scanner History

- ▶ Select the menu option **History / Display history**.
  - OR –

if the **Status** window is open, at the end of a scanning process:

- ▶ Press the **History** button.
  - ↳ The **History** window appears:



There is a History entry for every scanning process. Every node mentions the date and time and it has a blue check-mark (no detections) or a red arrow (malware detected).

The node ends with one of the following symbols:

*	Scan was cancelled by user
#	Scan was cancelled by busy scanner
+	Scan was cancelled by offline computer

When you expand the node (click the plus sign), the following data is listed:

- Details of scan conducted on <Date> <Time>
- Note in the case of cancelled scanning
- Time taken for scan
- Number of scanned directories
- Number of scanned files
- Number of warning messages
- Number of detections
- Name of last detection (e. g. Eicar-Test-Signature virus)

If you want to close the **History** window:

- Press **Close**.
  - ↳ The window closes.

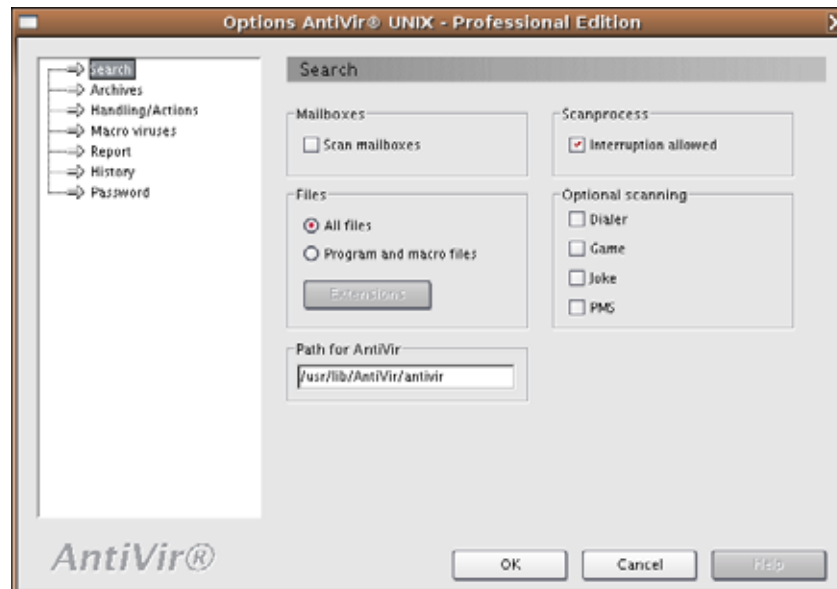
If you want to delete the history:

- Press **Delete**.
  - ↳ All history entries are deleted.

### 6.2.2 Configuring AntiVir Scanner Using the GUI



- Click the Configuration button in the Scanner main window
  - OR –
  - select the menu option **Tools/Configuration**.
- ↳ The **Configuration** window appears:



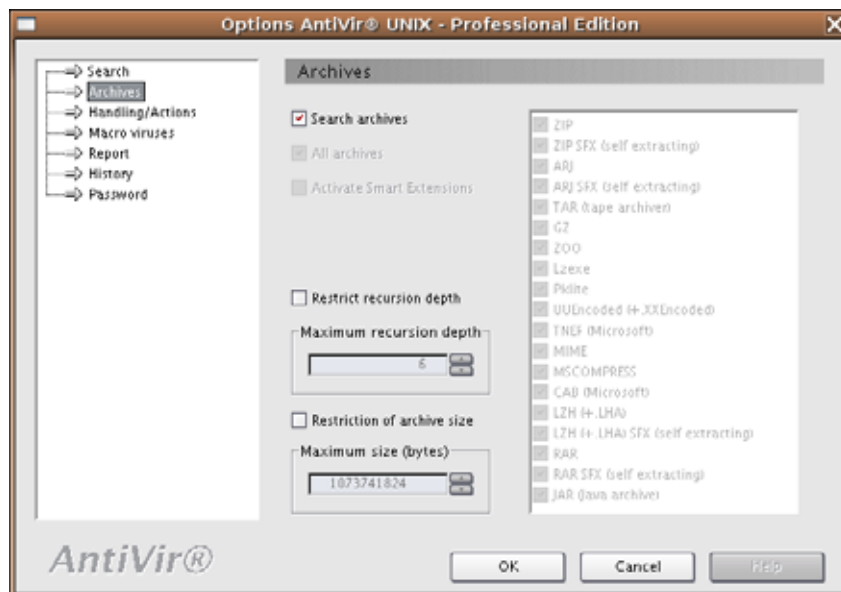
- Click the desired tag in the left panel (Search, Archives, Report... ).
  - ↳ The configuration options are displayed in the right panel.

#### Scanner Search Settings

These are the basic options for the scanning process.

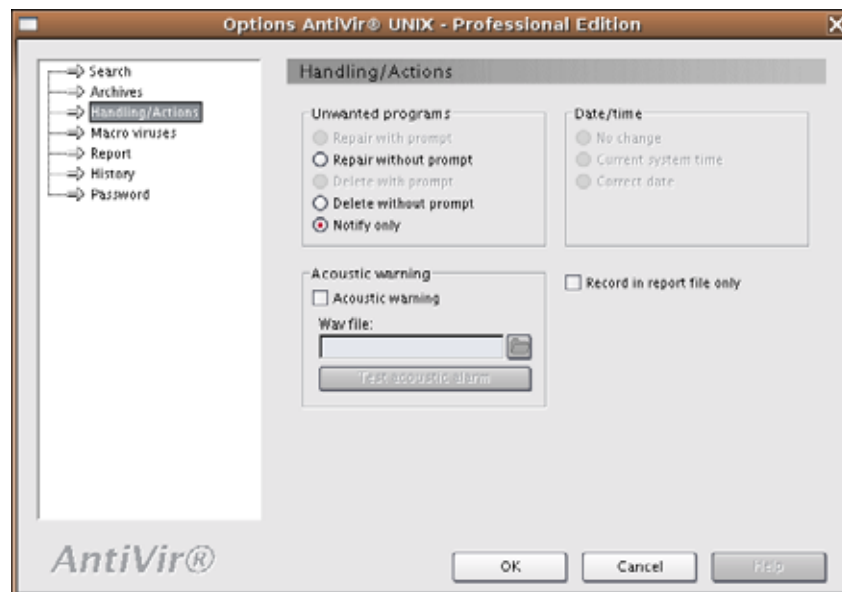
- |                   |  |
|-------------------|--|
| Mailboxes         | If you want to scan the contents of your mailbox: <ul style="list-style-type: none"><li>► Activate <b>Scan mailboxes</b>.</li></ul>  |
| Files             | According to the type of files you want to be scanned ( <b>All files</b> , or only <b>Program and Macro files</b> ): <ul style="list-style-type: none"><li>► Activate the required option.</li></ul> |
| Path for AntiVir  | This field contains the path to the AntiVir program. Usually the file is installed in:<br><code>/usr/lib/AntiVir/antivir</code>  |
| Scan process      | If you want to allow termination of the scan process: <ul style="list-style-type: none"><li>► Activate the check-box <b>Interruptions allowed</b>.</li></ul>   |
| Optional Scanning | If you want the program to scan for dialers, games, jokes or PMS (see <a href="#">8.1 Glossary</a> ): <ul style="list-style-type: none"><li>► Activate the desired options.</li></ul>                |

### Scanner Archive Settings



- Search archives If you want the AntiVir Scanner to search within archives:
- Activate the **Search archives** option.
- Recursion depth If you have activated the archive scanning but you want to scan only those nested archives which do not exceed a certain recursion depth:
- Activate the **Restrict recursion depth** option and type the desired number of levels (**Maximum recursion depth**).
- Archive size If you have activated the archive scanning but you want to scan only those archives which do not exceed a certain size:
- Activate the **Restriction of archive size** option and type the desired size in bytes (**Maximum size**).

### Scanner Settings for Action by Malware



Unwanted  
programs

You may select one of the following actions:

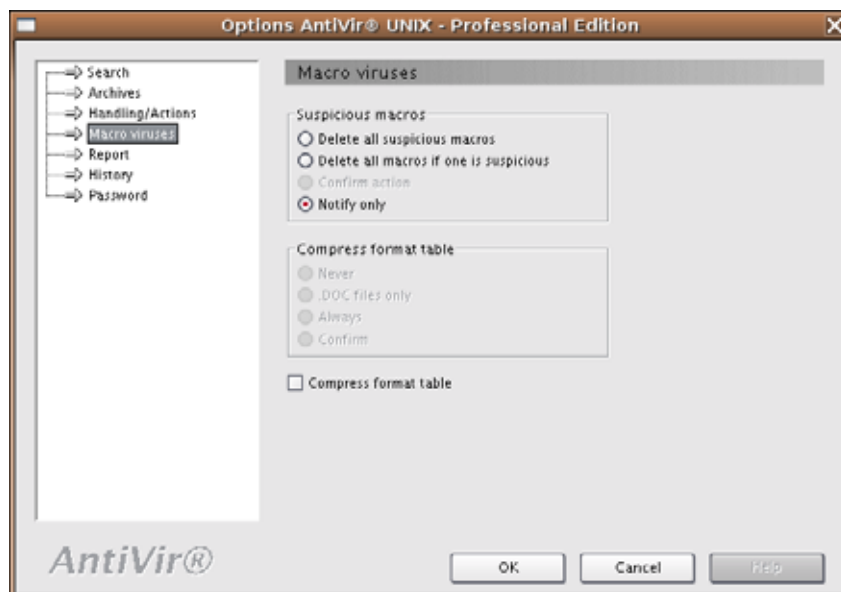
- Repair without prompt
- Delete without prompt
- Notify only

► Activate the desired option.

Acoustic  
warning

► Activate the **Acoustic warning** check-box, browse for the desired **Wave file** and **Test** the sound.

### Macro Viruses Settings



Suspicious  
macros

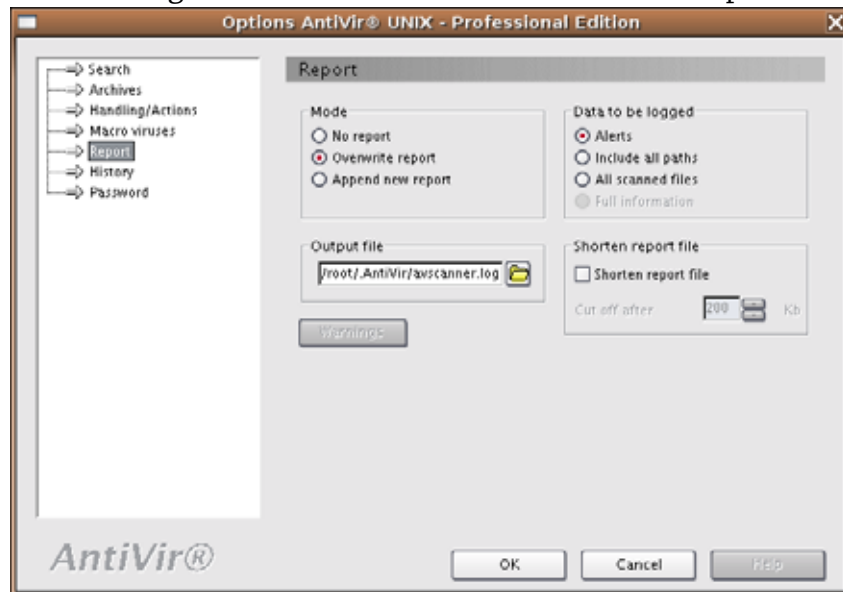
You may select one of the following actions:

- Delete all suspicious macros
- Delete all macros if one is suspicious
- Notify only

► Activate the desired option.

### Scanner Report Configuration

These settings influence the contents of the Scanner report file:



**Mode** The report file records the messages issued by the Command Line Scanner. You have the following options:

- No report
- Overwrite report
- Append new report

**Data to be logged** You can also choose the information type logged by the Scanner:

- Alerts
- Include all paths
- All scanned files

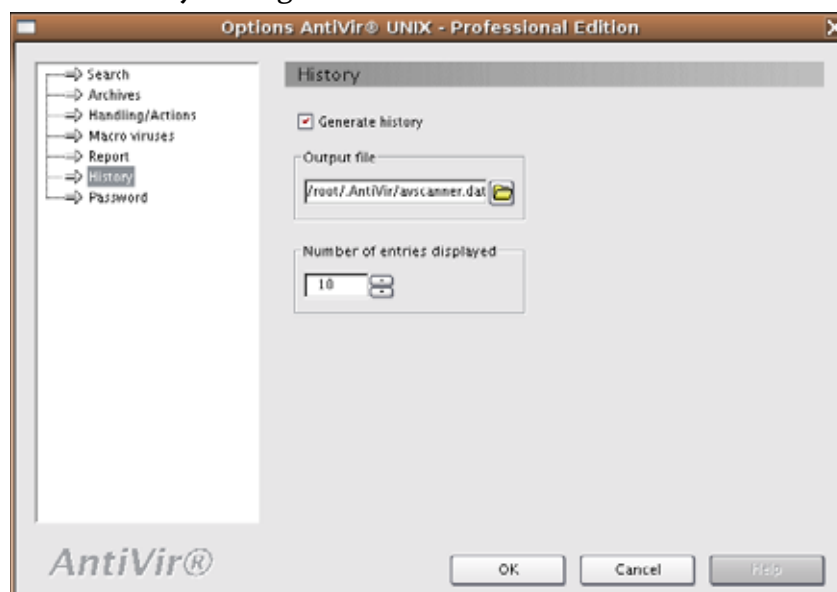
**Output file** ► Type the path to the report file. This is usually:

`/home/username/.AntiVir/avscanner.log`

**Shorten report** If you activate this option, you can select the maximum number of lines saved in the report file (**Cut off after...**).

### Scanner History Settings

AntiVir Scanner offers a useful history of scanning results. You may adjust this list in the **History** settings:



Generate  
history

If you want the Scanner to create short reports in **History**:

- Activate the option **Generate history**.
- Type the path to the **Output file**.

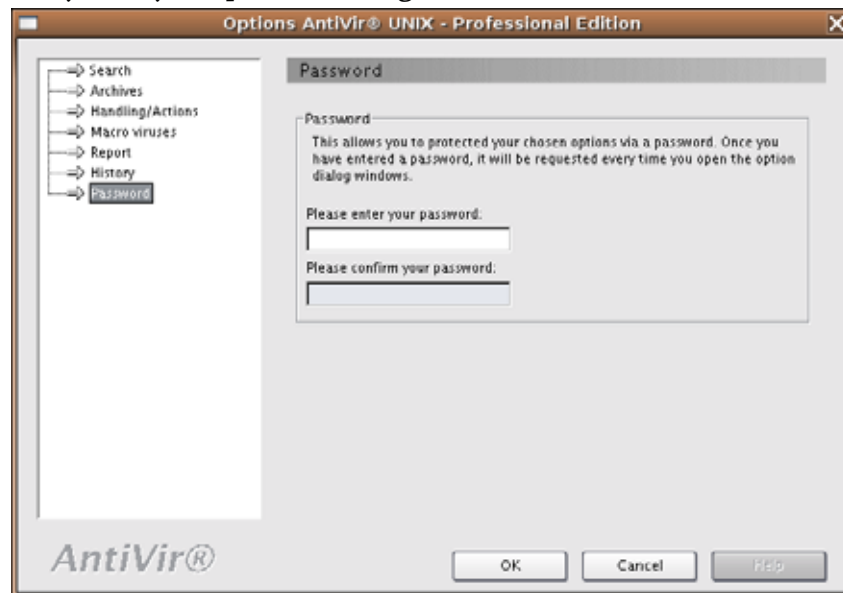
Number of  
entries  
displayed

You can also set the number of short reports displayed in the history list.

- Set the number of entries.

### Scanner Password Settings

You can set a password to protect the GUI options. The password will be required every time you open the configuration window:



- Type a password and confirm it.

## 6.3 AntiVir Guard

### 6.3.1 Operating AntiVir Guard Using the GUI

The AntiVir for UNIX Framework supports the resident guard and you can easily monitor your server using this feature.

#### Starting GUI

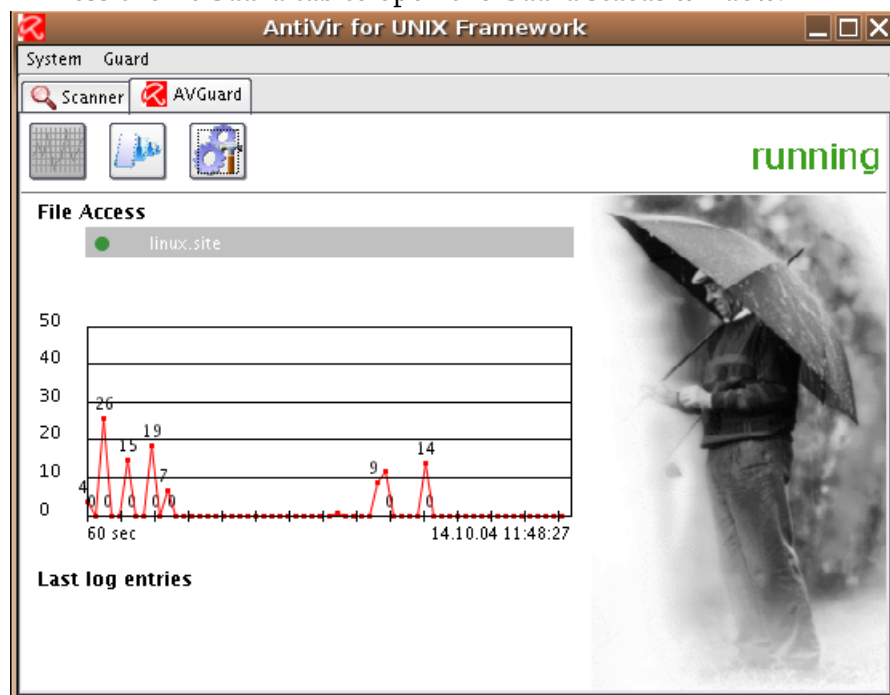
- ✓ The entry `GuiSupport` must be activated in `avguard.conf` in order for AntiVir UNIX Server to communicate with the GUI.

- ▶ Start the GUI:

```
/usr/lib/AntiVir/antivir-gui
```

↳ The GUI appears, displaying the **Folders** view.

- ▶ Press the **AVGuard** tab to open the **Guard status** window.



#### Buttons



Click to display the real-time **Guard status**.



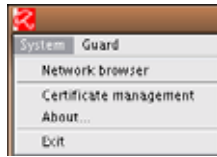
Click to view the **Guard Logfile**.



Click to open the **Configuration** window.

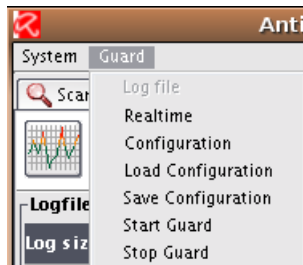
## Menus

System



- **Network browser:** to select another computer in the network on which AntiVir GUI runs.
- **Certificate management:** to manage integrated certificates of the other computers in the network.
- **About...:** displays **Product information** and **Support information**
- **Exit:** closes GUI. AntiVir UNIX Server is not stopped.

Guard



- **Log file:** to view the logfile window.
- **Realtime:** to display the realtime Guard status.
- **Configuration:** to open the configuration window.
- **Load Configuration:** to load a preset configuration.
- **Save Configuration:** to save the current configuration.
- **Start Guard:** to start AntiVir Guard.
- **Stop Guard:** to stop AntiVir Guard

## Realtime Guard Status

See the figure in [Starting GUI](#) – Page 91

The **Guard Status** window contains the following information:

Status    AntiVir Guard's current status: **running** or **stopped**.

## Guard Logfile Window

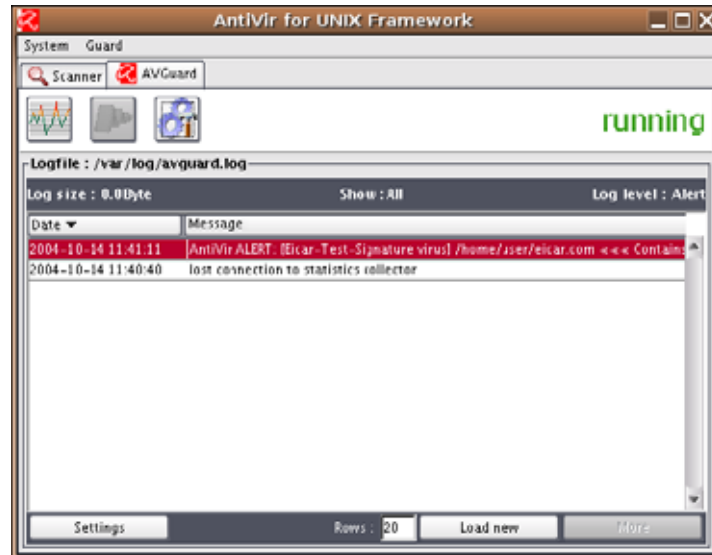


► Click on the **Logfile** button.

– OR –

Select the menu option **Guard/Logfile**.

↳ The **Logfile** window appears:

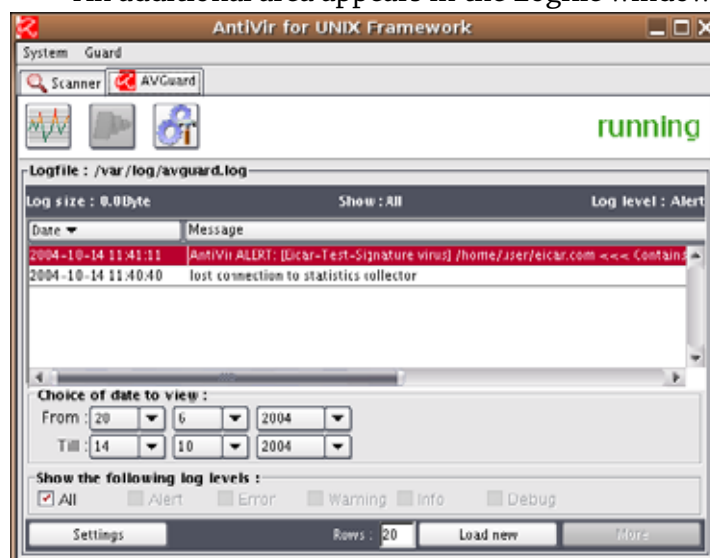


**Logfile** Displays the complete logfile, with full paths, the current size of the logfile in KB, the displayed log levels and the log level used by AntiVir Guard.

Four buttons appear at the bottom of the window: **Settings**, **Rows**, **Load new** and **More**.

**Settings** ► Press **Settings**.

↳ An additional area appears in the Logfile window:



- **Choice of date to view:** selecting the time interval for the logfile entries to be displayed;  
Default: complete logfile.

- **Show the following log levels:** selecting the log levels to be displayed;  
Default: **All**.

Rows    Number of displayed log lines.

Load new    Reloading the logfile.

More    The loaded logfile view is extended with the number of **Lines** given.

### Configuration Window

see [Configuring AntiVir Guard Using the GUI](#) – Page 95

### Starting and Stopping AntiVir Guard

Start    ► Select the menu option **Guard/Start Guard**.

Stop    ► Select the menu option **Guard/Stop Guard**.

### Closing GUI

► Select **System/Exit**.

↳ The GUI is closed.



*When you close GUI, it retains the current status of AntiVir Guard.*

### 6.3.2 Configuring AntiVir Guard Using the GUI

You can use the GUI to set the configuration parameters in `avguard.conf`.

For better understanding, we shall also mention the entry in `avguard.conf` for every parameter. These parameters are fully described in [Configuration Files](#) – Page 38.

#### Opening the Configuration Window

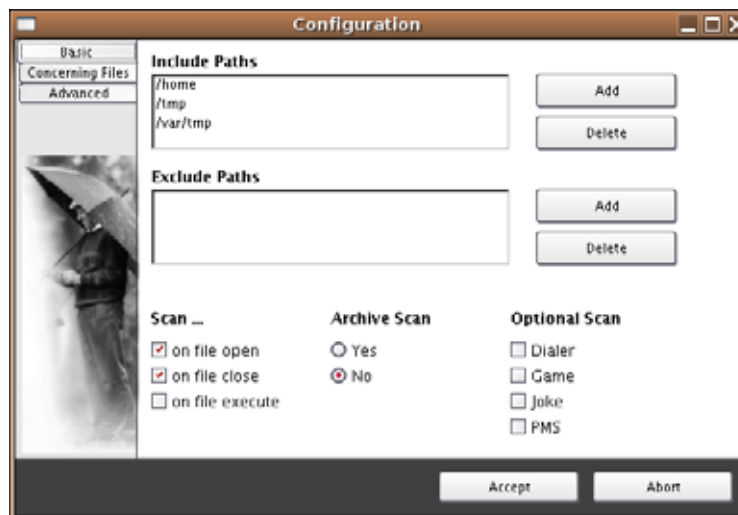


► Press the configuration button.

– OR –

Select the menu option **Guard/Configuration**.

↳ The **Configuration** window appears, with the basic AntiVir Guard **Search** settings:



#### Guard Basic Settings

**Include Paths** AntiVir Guard scans the files in the specified folders, including their sub-folders. Usually the data for the different users is in `/home`.

You can specify only one folder in a command line. You can enter more folders by typing the command for each one. Example: `/home` and `/media`.



*If no folder is specified, AntiVir Guard will not scan any files!*

This option sets the `IncludePath` parameter in `avguard.conf`.

► Click **Add**.

↳ The **New path** window appears.

► Enter the path to the required directory, click **Add** and confirm with **OK**.

If you want to remove a directory from the list:

► Select the desired directory and click **Delete**.

**Exclude Paths** AntiVir Guard can exclude certain folders when scanning. For example, a folder containing temporary files of AntiVir components (see [Setting excluded directories](#)). There is no default setting.

You can specify only one folder in a command line. You can enter more folders by typing the command for every one. Example: /home/log and /home/tmp



*If you activated **Move to directory** in the Actions setting, that quarantine folder is automatically excluded.*

This option sets the `ExcludePath` parameter in `avguard.conf`.

► Click **Add**.

↳ The New **path** window appears.

► Enter the path to the desired directory, click **Add** and confirm with **OK**.

If you want to remove a directory from the list:

► Select the required directory and click **Delete**.

**Scan...** This option sets the access type of AntiVir Guard, when scanning files for viruses or unwanted programs:

- Scanning a file when opened
- Scanning a file when closed
- Scanning a file when executed

This option sets the `AccessMask` parameter in `avguard.conf`.

► Activate the required check-box(es).

**Archive Scan** AntiVir Guard also scans compressed archives on access, according to the settings you made in **Advanced** tab. This option is deactivated by default in order to maintain fast performance.

This option sets the `ArchiveScan` parameter in `avguard.conf`.

If you want the Guard to scan archives:

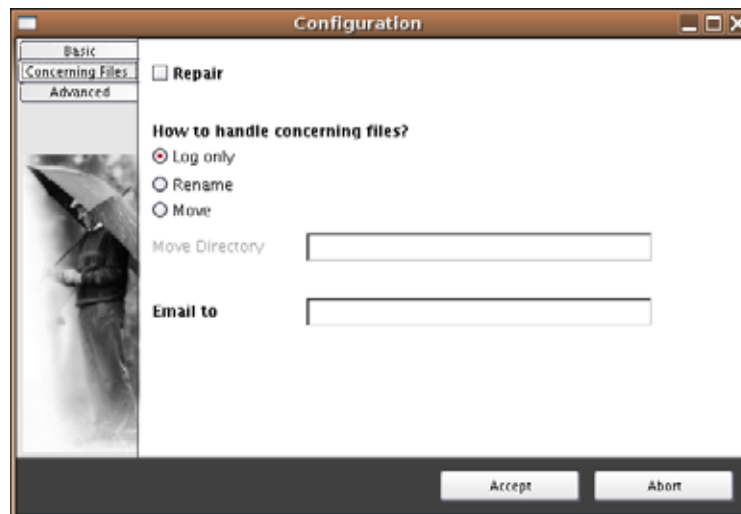
► Select **Yes**.

**Optional Scan** If you want the Guard to scan for dialers, games, jokes or PMS:

► Activate the desired options.

## Concerning Files Settings

AntiVir Guard is able to take specific actions when viruses or unwanted programs are detected:



**Repair** AntiVir Guard is able to repair files immediately after access. If this fails, access is blocked. This option is deactivated by default.

It corresponds to `RepairConcerningFiles` in `avguard.conf`.

► Activate the **Repair** check-box.

**How to handle concerning files?** If **Repair** is not activated or if repair is not possible, access to the files is blocked and the action is logged. The following three options define further actions of AntiVir Guard:

- **Log only:** no further action
- **Rename:** rename the file by adding the `.XXX` extension.
- **Move:** move the file to another folder. This folder will be automatically created if it does not already exist. For example, `/home/unwanted`

These options correspond to `LogOnly`, `RenameConcerningFiles` and `MoveConcerningFilesTo` in `avguard.conf`.

► Select the desired option.

If you activate **Move**:

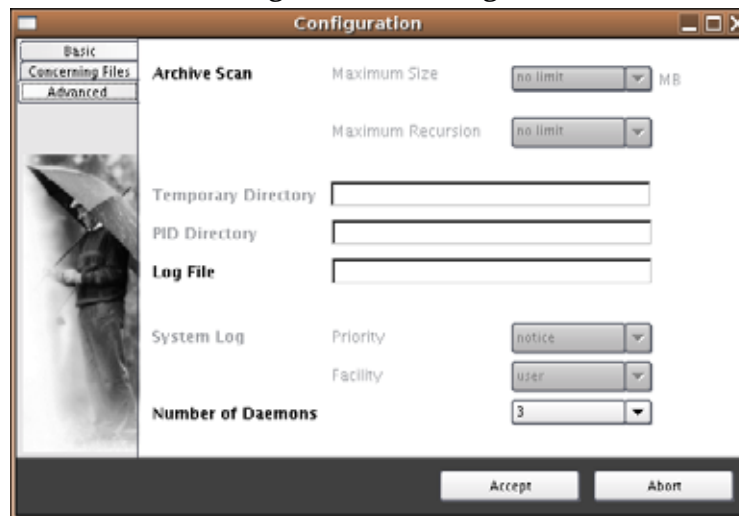
► You have to type in the path to the directory where concerning files will be stored.

**Email** If AntiVir Guard should send emails when a virus or unwanted program is detected:

► Write the email address.

### Guard Advanced Settings

The advanced settings refer to the logfile, daemons and to archive scanning:



**Archive Scan** These settings correspond to `ArchiveMaxRecursion` and `ArchiveMaxSize` in `avguard.conf`

✓ The option **Search archives** has to be activated in the **Basic** settings.

**Maximum Size** This option limits the scanning process to the files with unpacked size smaller than a given value.

If you want to limit the maximum size of unpacked archived files (in MB):

► Select the desired value (in MB)

– OR –

if you do not want to limit their size:

► Select **no limit**.

**Maximum Recursion** This option limits the scanning process to the nested archives with the level of recursion smaller than a given value.

If you want to limit the recursion level of scanned archives:

► Select the desired value

– OR –

if you do not want to limit the recursion level:

► Select **no limit**.

**Log File** Full path and file name for the logfile of AntiVir Guard. For example:  
`/var/log/avguard.log`.

All important AntiVir operations are logged via a syslog daemon.

► Type the full path and file name.

**Number of Daemons** The number of simultaneous AntiVir Guard daemons can be set between 0 and 20. The default is 3 and it is appropriate for smaller standard computers. For servers with a high level of traffic, a larger number would be necessary.

Here you may also **deactivate** AntiVir Guard.

These options correspond to NumDaemons in avguard.conf.

- ▶ Select the required number of daemons.



## 7 Service

### 7.1 Support

Support Service Our website <http://www.avira.com> contains all the necessary information on our extensive support service.

The expertise and experience of our developers is available to you. The experts of Avira answer your questions and help you with difficult technical problems.

During the first 30 days after you have purchased a license, you can use our **AntiVir Installation Support** by phone, email or by online form.

In addition, we recommend that you also purchase our **AntiVir Classic Support**, with which you can contact and obtain advice from our experts during business hours when technical problems are encountered. The annual fee for this service, which includes eliminating viruses and hoax support, is 20 % of the list price of your purchased AntiVir program.

Another optional service is the **AntiVir Premium Support** which offers you, in addition to the scope of the AntiVir Classic Support, the possibility of contacting expert partners at any time - even after business hours in the event of an emergency. When virus alerts occur, you will receive an SMS on your cellphone.

Forum Before you contact our Hotline, we recommend that you visit our user forum at <http://forum.antivir.de>.  
Your questions may already have been answered for another user and posted on the forum.

Email Support Support via email can be obtained at <http://www.avira.com>.

### 7.2 Online Shop

Would you like to buy our products with a mouse-click?

You can visit Avira Online Shop at <http://www.avira.com> and buy, upgrade or extend AntiVir licenses quickly and safely. The Online Shop guides you step by step through the order menu. A **multi-lingual Customer Care Center** explains the order process, payment transactions and delivery. Resellers can order by invoice and use a reseller panel.

### 7.3 Contact

Address    Avira GmbH  
              Lindauer Strasse 21  
              D-88069 Tettnang  
              Germany

Internet    You can find further information on us and our products by visiting  
              <http://www.avira.com>.

## 8 Appendix

### 8.1 Glossary

Item	Meaning
Backdoor (BDC)	<p>A backdoor is a program infiltrated in order to steal data from the computer without the user's knowledge. This program is manipulated by third parties using remote backdoor control software via the Internet or network.</p> <p>AntiVir detects backdoor control programs.</p>
cron (daemon)	<p>A daemon which starts other programs at specified times.</p>
Daemon	<p>A background process for administration on UNIX systems. On average, there are about a dozen daemons running on a computer. These processes usually start up and shut down with the computer.</p>
Demo version	<p>Without a license file, AntiVir UNIX Server runs as a demo version and it only reports the test virus EICAR. It will not block access to infected files. The update function is not available.</p>
Dialer	<p>Paid dialing program. When installed on your computer, this program sets up a premium rate number Internet connection, charging you at high rates. This can lead to huge phone bills.</p> <p>AntiVir detects Dialers.</p>
Engine	<p>The scanning module of AntiVir software.</p>
Heuristic	<p>The systematic process of solving a problem using general and specific rules drawn from previous experience. However, solution is not guaranteed.</p> <p>AntiVir uses a heuristic process to detect unknown macro viruses. When typical virus-like functions are found, the respective macro is classified as "suspicious".</p>
Kernel	<p>The basic component of a UNIX operating system which performs elementary functions (e.g. memory and process administration)</p>
Logfile	<p>also: Report file. A file containing reports generated by the program during run-time when a certain event occurs.</p>
Malware	<p>Generic term for "foreign bodies" of any type. These can be interferences such as viruses or other software which the user generally considers as unwanted (see also Unwanted Programs).</p>
PMS (Possible Malicious Software)	<p>Software that does not usually harm the computer. It is programmed to harm other users.</p> <p>For example, mail bombs: with such a program, the victim can be attacked by thousands of emails.</p> <p>AntiVir detects PMS.</p>

Item	Meaning
Quarantine directory	The directory where infected files are stored to block the user's access to them.
root	The user with unlimited access rights (such as system administrator on Windows)
Signature	A byte combination used to recognize a virus or unwanted program.
Script	A text file containing commands to be executed by the system (similar to batch files in DOS)
SMP (Symmetric Multi Processing)	UNIX SMP: UNIX version for computers with parallel processors.
SMTP	Simple Mail Transfer Protocol: protocol for email transmission on the Internet.
syslog daemon	A daemon used by programs for logging various information. These reports are written in different logfiles. The syslog daemon configuration is in <code>/etc/syslog.conf</code> .
Unwanted programs	The name for programs that do not directly harm the computer but are not wanted by the user or administrator. These can be backdoors, dialers, jokes and games. AntiVir detects various types of unwanted programs.
VDF (Virus Definition File)	A file with known signatures for viruses and unwanted programs. In many cases it is enough for an update to load the most recent version of this file.
VFS	Virtual File System

## 8.2 Further Information

You can find further information on viruses, worms, macro viruses and other unwanted programs at <http://www.avira.com>.

## 8.3 Golden Rules for Protection Against Viruses

- ▶ Always keep boot floppy-disks for your network server and for your workstations.
- ▶ Always remove floppy disks from the drive after finishing the work. Even if they have no executable programs, disks can contain program code in the boot sector and these can serve to carry boot sector viruses.
- ▶ Regularly back up your files.
- ▶ Limit program exchange: particularly with other networks, mailboxes, Internet and acquaintances.
- ▶ Scan new programs before installation and the disk after this. If the program is archived, you can detect a virus only after unpacking and during installation.

If there are other users connected to your computer, you should set the following rules for protection against viruses:

- ▶ Use a test computer for controlling downloads of new software, demo versions or virus suspicious media (floppies, CD-R, CD-RW, removable drives).
- ▶ Disconnect the test computer from the network!
- ▶ Appoint a person responsible for virus infection operations and define all steps for virus elimination.
- ▶ Organize an emergency plan as a precaution for avoiding damage due to destruction, theft, failure or loss/change due to incompatibility. You can replace programs and storage devices but not your vital business data.
- ▶ Set up a plan for data protection and recovery.
- ▶ Your network must be correctly configured and the access rights must be wisely assigned. This is good protection against viruses.

[www.avira.com](http://www.avira.com)



#### **Avira GmbH**

Lindauer Str. 21  
D-88069 Tettnang  
Telephone: +49 (0) 7542-500 0  
Fax: +49 (0) 7542-525 10  
Email: [info@avira.com](mailto:info@avira.com)  
Internet: <http://www.avira.com>

All rights reserved. Subject to change.  
© Avira GmbH

MORE THAN SECURITY

