Avira Server Security | Unix

User Manual

AVIRA

User Manual

Avira AntiVir Server (Unix)
Avira AntiVir Professional (Unix)

Avira Operations GmbH & Co. KG
Kaplaneiweg 1
88069 Tettnang
Germany
Telephone: +49 (0) 7542-500 0
Fax: +49 (0) 7542-525 10
Internet: http://www.avira.com

Issued Q1-2013

Contents

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:

1.1 Introduction

We have included in this manual all the information you need about Avira AntiVir Server/ Professional 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 46).

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:

Chapter	Contents
1 About this Manual	The structure of the manual, signs and symbols
2 Product Information	General information about Avira AntiVir Server/ Professional, its modules, features, system requirements and licensing.
3 Installation	Instructions to install AntiVir on your system – using the installation script.
4 Configuration	Directions for optimum settings of AntiVir components on your system.
5 Operation	Working with AntiVir, after installation; targeted scanning for viruses and unwanted programs; reactions when viruses and unwanted programs are detected.
6 Updates	Carrying out automatic or manual Internet updates.
8 The Dazuko Kernel Module	Information about compiling and using dazuko.
7 Service	Support and Service.
9 Appendix	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.

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

Emphasis in text	Explanation
Ctrl+Alt	Key or key combination
/usr/lib/AntiVir/guard/avscan	Path and filename
`ls /usr/lib/AntiVir/guard`	User entries
http://www.avira.com	URLs
Signs and Symbols – Page 4	Cross-reference within the document

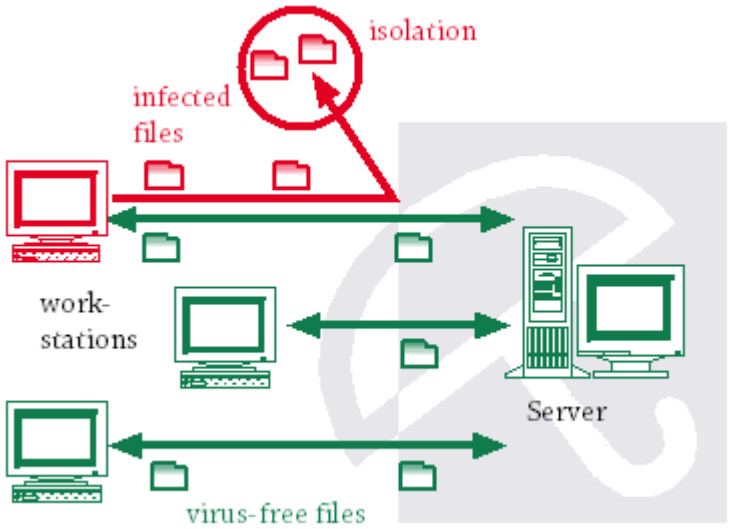
1.4 Abbreviations

The manual uses the following abbreviations:

Abbreviation	Meaning
CLS	Command Line Scanner
FAQ	Frequently Asked Question
GUI	Graphical User Interface
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management 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.



Avira AntiVir Server/ Professional is a comprehensive and flexible tool for confronting viruses and unwanted programs and for reliable protection of your systems.

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 Server/ Professional offers you extensive configuration possibilities to keep control of your network.

The current features of AntiVir Server/ Professional are:

- Easy installation, using the installation script.
- Command Line Scanner (on demand):
  Configurable on-demand 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, 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 Internet Updates for product, scan engine and VDF.
- 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.

2.2 Licensing Concept

You must have a license to use AntiVir Server/ Professional. You have to accept the license terms
(see http://www.avira.com/documents/general/pdf/en/avira_eula_en.pdf).

There are two license modes for using AntiVir Server/ Professional:

- Test version
- Full version

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

The license is given in a license file named *hbedv.key* . You will receive it by email from Avira Operations GmbH & Co. KG. 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.

Test Version

Details about the 30-days Test License can be found on our Website:
http://www.avira.com.

Full Version

The range of full version features includes:

- Download of AntiVir versions from the Internet
- License file by email, for converting the test 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

Self-Integrity Check

Each AntiVir executable binary is signed and performs a self-integrity check during startup.

The self-integrity check cannot protect against forgery (e.g. to check if the complete package is faked) or crafted attacks (e.g. the function call that performs the self-integrity check is bypassed). Such a verification has to be performed from outside the package.

2.3 Modules and Operating Mode

The Avira security software consists of the following program components:

- AntiVir Engine
- AntiVir Guard
- AntiVir Command Line Scanner
- Avira Updater

AntiVir Engine

AntiVir Engine essentially represents the scanning and repairing modules of Avira software. These are also used by the other AntiVir products.

AntiVir Guard

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 Command Line Scanner

AntiVir CLS 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.

Avira Updater

Avira Updater downloads current updates from the AntiVir web servers and installs them at regular intervals, manually or automatically. It can also send update notifications by email. You can update Avira AntiVir entirely or only the scanner.

2.4 System Requirements

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

- i386 (Linux) or Sparc (SunOS) processor;
- 200 MB free hard disk space;
- 2 GB temporary disk space;
- 256 MB (512 MB on SunOS) free memory space;
- Linux with glibc; SunOS.

Officially supported distributions for Avira AntiVir Server:

- Red Hat Enterprise Linux 5 Server
- Red Hat Enterprise Linux 4 Server
- Novell SUSE Linux Enterprise Server 9, 10 - 10.2, 11 (SP2 is not supported)
- Debian GNU/Linux 4 (stable), Debian etch
- Ubuntu Server Edition 8
- Sun Solaris 9 (SPARC)
- Sun Solaris 10 (SPARC)
- Novell Open Enterprise Server

Avira AntiVir Professional asks for the following minimum system requirements on your server:

- i386 (Linux) or Sparc (SunOS) processor;
- 100 MB free hard disk space;
- 20 MB temporary disk space
- 192 MB (512 MB on SunOS) free memory space;
- Linux with glibc; SunOS.

You need sufficient disk space on your hard drive to save the temporary guard files. We therefore recommend that there are at least 4GB available for the temporary directory.

Officially supported distributions for Avira AntiVir Professional:

- Red Hat Enterprise Linux 5 Desktop
- Red Hat Enterprise Linux 4 Desktop
- Novell SUSE Linux Enterprise Desktop 9, 10 - 10.2, 11 (SP2 is not supported)
- Debian GNU/Linux 4 (stable)
- Ubuntu Desktop Edition 8
- Sun Solaris 9 (SPARC)
- Sun Solaris 10 (SPARC)

2.5 Technical Information

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

3 Installation

You can find the current version of Avira AntiVir Server/ Professional on our website www.avira.com.

AntiVir is supplied as a packed archive. It contains AntiVir Engine, Guard, Command Line Scanner and the Avira Updater.

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

3.1 Getting the Installation Files

Downloading the Installation Files from the Internet

▶ Download the current version of Avira AntiVir Server/ Professional from our website http://www.avira.com to your local computer.

Save the file in the temporary folder (*/tmp*) on the computer on which you want to run *Avira AntiVir Server/ Professional*. The file name is
antivir-server-prof.tar.gz
or:
antivir-workstation-prof.tar.gz

Unpacking Program Files

▶ Go to the temporary directory:

```
cd /tmp
```

▶ Unpack the archive containing the AntiVir kit:

```
tar -xzvf antivir-server-prof.tar.gz
```

or:

```
tar -xzvf antivir-workstation-prof.tar.gz
```

↳ In the temporary directory will then appear:
antivir-server-prof-<version> or *antivir-workstation-prof-<version>*

3.2 Licensing

You must have an AntiVir license in order to use the product (see Licensing Concept – Page 6). The license comes in a file named *hbedv.key*.

This license file contains information regarding the scope and period of the license.

Purchasing the License

▶ You may contact us by telephone or by email (sales@avira.com) to acquire a license file for Avira AntiVir Server/ Professional.

↳ You will receive the license file by email.

▶ You can easily acquire Avira AntiVir Server/ Professional 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>
or in *./tmp/antivir-workstation-prof-<version>*.

You can also perform the installation without having a license key from the beginning. You can copy the license file at any time to the AntiVir program directory /usr/lib/AntiVir/guard.

3.3 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 permissions 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.
- Optional: it creates a link in */usr/bin*, so that AntiVir can be called from any folder without needing a given path.
- Optional: it installs the resident scanner AntiVir Guard and the dazuko module.
- Optional: it installs a Gnome plug-in.
- Optional: it installs Avira Updater.
- Optional: it configures an automatic start for Avira Updater and AntiVir Guard on system start-up.
- Optional: it installs the plug-in for Avira Security Management Center.

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>`
or
`cd /tmp/antivir-workstation-prof-<version>`

Installing AntiVir (example for AntiVir Server)

For using Avira AntiVir Server/ Professional v.3 with AntiVir Guard, we recommend and support dazuko3/dazukofs.

The installation script will also install dazuko3, if it detects the needed build components on your system. *If the installation script cannot detect a supported linux kernel version, you can only install Avira AntiVir without AntiVir Guard. AntiVir Guard can be easily installed later. For more details, see* The Dazuko Kernel Module – Page 48.

▶ Type the command:
`./install`

Please note the dot and slash in the command syntax. Typing the command without this path specification, leads to another command, which is not related to AntiVir installation process and this would result in error messages and unwanted actions.
Press ***q*** to close the license text view.

↳ The installation script starts. After you agree with the license terms, it will copy the program files. The Installer can read an existing license key:

```
Do you agree to the license terms? [n] y

creating /usr/lib/AntiVir/guard ... done
copying AV_SRV_PROF to /usr/lib/AntiVir/guard ... done
copying LICENSE to /usr/lib/AntiVir/LICENSE-server ... done

1) installing AntiVir Core Components (Engine, Savapi and Avupdate)
copying uninstall to /usr/lib/AntiVir/guard ... done
copying etc/file_list to /usr/lib/AntiVir/guard ... done
.....

Enter the path to your key file: [HBEDV.KEY]
copying HBEDV.KEY to /usr/lib/AntiVir/guard/avira.key ... done

installation of AntiVir Core Components (Engine, Savapi and Avupdate) complete
```

↳ After you type the path to the key file, the installer continues with updates' configuration:

```
2) Configuring updates
An internet updater is available...
...
Would you like to create a link in /usr/sbin for avupdate-guard? [y]
```

▶ Type ***y*** and confirm with ***Enter***.

↳ Then the script can create a cron task for automatic updates:

```
linking /usr/sbin/avupdate-guard ... done

Would you like to setup Scanner update as cron task ? [y]
```

The update cron job uses the minute when the product was installed. If you want another update time, you can change the entries later, in /etc/cron.d/avira_updater

▶ Press ***Enter***. You can change this setting later.

↳ Then select the update interval (daily - d; every two hours - 2):

```
Please specify the interval to check.
Recommended values are daily or 2 hours.

available options: d [2]
```

▶ Enter ***d*** or ***2***.

↳ If you selected daily updates, you can specify the time of the day when the updates should start:

```
The AntiVir 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.

available option: HH:MM

What time should updates be done [00:15]?
```

▶ Press ***Enter*** or set another time first.

↳ Then the installer asks if you want to check for Product updates every week:

```
Would you like to check for Guard updates once a week ? [n]
```

▶ Press ***y***, if you want to create this task, or just press ***Enter***, if you don't.

↳ The next step of the installation process is installing the main program.
If no dazuko device is detected on your system, the script tries to install dazuko:

```
3) installing main program
copying doc/avserver_en.pdf to /usr/lib/AntiVir/guard ... done
copying bin/linux_glibc22/libdazuko3compat2.so to /usr/lib/AntiVir/guard...
done
...
No Dazuko device found on your system
Would you like to install dazuko now ? [y]
```

▶ Press ***y***, if you want to install dazuko and use AntiVir Guard, then press ***Enter.***

↳ Dazuko3 package is installed.

```
installing dazuko ... Available Dazuko3-Package: '3.0.0-rc4'

checking for needed build components:
    checking for C compiler cc ... found
    checking for C compiler gcc ... found
    checking for kernel sources ... found

detecting kernel version ... 2.6.18
unpacking dazuko-3.0.0-rc4_2.6.18 ... done
installing dazuko-3.0.0-rc4_2.6.18 ...

initiate dazukofs ...
done

linking /usr/lib/AntiVir/guard/libdazuko.so to /usr/lib/AntiVir/guard/
libdazuko3compat2.so...
```

If the attempt to install dazuko fails, you have to compile the module yourself. For more details, see The Dazuko Kernel Module – Page 48.

AntiVir can be installed even without dazuko, but in this case it will run without AntiVir Guard.

↳ The installer then reads */etc/fstab*, to check the directories to be mounted as dazukofs. If no entry is found, it asks you to enter one directory to be scanned by the Guard:

```
Guard will automatically protect all directories
 which are mounted upon dazukofs filesystem.

Please specify at least one directory to be protected
by Guard to add in /etc/fstab: [/home]
```

There are some file systems that should not be overlayed by dazukofs, since no security gain would be achieved, but on the contrary, it could lead to system malfunction. Examples of these file systems are `sysfs (/sys)`, `procfs (/proc)`, `usbfs`. *These file systems do not allow the creation of files anyway, so they do not need to be protected against malware.*

The special directory "/" (`root`*) should not be mounted with dazukofs, because it may also be the root for other file systems, which likewise should not be mounted with dazukofs.*

Mounting "/" could also be dangerous due to the fact that there will very likely be processes already working on files under/ before dazukofs is mounted. This might result in undefined file states, if those files are later accessed through the dazukofs layer.

▶ Type one directory, which you want to be protected on-access (for example, `/home`) and press ***Enter***.
If you want to modify the list of protected directories, you can add or remove entries later, by editing */etc/fstab* file and remounting dazukofs.

↳ Then the installer checks if the default quarantine directory exists:

```
/home/quarantine, the AVIRA Guard default quarantine directory, does not exist.

INFO: You can change the quarantine directory in /etc/avira/avguard.conf.
    and /etc/avira/avscan.conf after the installation.

Would you like to create /home/quarantine ? [y]
```

▶ Type ***Enter***, to create the directory, if necessary. You can change it later in the configuration files.

↳ Then the script can install a GNOME plug-in, which would allow you to add the status icon for AntiVir Guard to the panel (- Guard is active; - Guard is inactive):

```
Would you like to install the AVIRA Guard GNOME plugin? [n]
```

▶ Type ***y*** and press ***Enter***, if you want to install the plug-in,
or just press ***Enter***, if you don't.

↳ Then you are asked if you want to create a link to *avguard* and if the Updater should be automatically activated at system start:

```
Would you like to create a link in /usr/sbin for avguard ?[y]
linking /usr/sbin/avguard to /usr/lib/AntiVir/guard/avguard ... done

Please specify if boot scripts should be set up.
Set up boot scripts [y]:
```

▶ Confirm with ***Enter***.

↳ The automatic system start is configured:

```
setting up boot script ... done
installation of AVIRA Guard complete
```

↳ Then the script can install the optional plug-in for Avira Security Management Center:

```
4) activate SMC support
The AntiVir Security Management Center (SMC) requires this feature.
Would you like to activate the SMC support? [y]
```

▶ If you are using Avira SMC, type ***y*** or confirm with ***Enter***.

↳ The plug-in is installed and the installation process is complete. You can start AntiVir Guard, if dazuko is correctly compiled:

```
Would you like to start AVIRA Guard now? [y]
Starting Avira AntiVir Server...
Starting: avguard.bin
```

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

```
Installation of the following features complete:
    AntiVir Core Components (Engine, Savapi and Avupdate)
    AVIRA Internet Updater
    AVIRA Guard
    AntiVir SMC plugin
```

▶ Finally, you can start AntiVir:

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

Modified binaries will not run.
For example, if binaries are prelinked: Either disable prelinking or add /usr/lib/AntiVir/guard as an excluded prelink path in /etc/prelink.conf

3.4 Reinstalling and Uninstalling AntiVir

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

- Later installation of some components, e.g. AntiVir Guard or Avira Updater.
- Activating or deactivating the automatic start of Avira Updater or AntiVir Guard.

Reinstalling AntiVir

The procedure applies to all above mentioned cases:

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

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

▶ Open the temporary directory where you unpacked AntiVir Server:

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

or, for AntiVir Professional:
`cd /tmp/antivir-workstation-prof-<version>`

- Type:
  `./install`
  ↳ The installation script performs as described in Installing AntiVir – Page 10).
- Make the changes you need during installation procedure.
  ↳ AntiVir is installed with the required features.

Uninstalling AntiVir

You can use the *uninstall* script, located in the temporary AntiVir directory, to remove Avira AntiVir Server/ Professional. The syntax is:

```
uninstall [--product=productname] [--inf=inf-file] [--force]
[--version] [--help]
```

where `productname` is `Guard`.

- Open the AntiVir directory:
  `cd /usr/lib/AntiVir/guard`
- Type:
  `./uninstall --product=Guard`
  ↳ The script starts uninstalling the product, asking you step by step, if you want to keep backups for the license file, for the configuration files and logfiles; it can also remove the cronjobs you made for Guard and Scanner.
- Answer the questions with ***y*** or ***n*** and press ***Enter***.
  ↳ Avira AntiVir Server/ Professional is removed from your system.

3.5 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 Avira 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 Server/ Professional 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:

- Description of the configuration files:
  - Configuration of AntiVir Guard in avguard.conf – Page 17
  - Configuration of the Command Line Scanner in avscan.conf – Page 25
  - Scanner specific configuration in avguard-scanner.conf – Page 30
  - Configuration of Avira Updater in avupdate-guard.conf – Page 31
- Testing AntiVir Server/Professional - Page 33, after completing the configuration.

4.1 Configuration Files

The configuration is defined in four files:

- */etc/avira/avguard.conf* configures the on-access scanner.
- */etc/avira/avscan.conf* configures the on-demand scanner.
- */etc/avira/avguard-scanner.conf* configures Savapi3.
- */etc/avira/avupdate-guard.conf* defines the automatic updates.

The settings can be made directly in the configuration files or as parameters when using the Command Line Scanner.

The parameters given in command lines take precedence of those saved in configuration files.

This part describes the structure of AntiVir Server/ Professional configuration files. AntiVir Server/ Professional 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 AntiVir Guard if you modify any values manually in the configuration files. The changes only take effect after a restart.

▶ Type:

```
/usr/lib/AntiVir/guard/avguard restart
```

4.1.1 Configuration of AntiVir Guard in avguard.conf

This section provides a short description of the entries in *avguard.conf* . The settings affect only the behavior of AntiVir Server/ Professional and no other AntiVir programs.

OnAccess Management

Enable/ Disable on-access protection:
This option allows you to explicitly enable/ disable on-access protection of specified directories provided by Guard using dazukofs/dazuko kernel module.

When set to `auto` Guard will determine if the system has dazuko/dazukofs support at startup and use it to provide on-access protection automatically.

If you set it to `no` or the system has no dazuko/dazukofs support, Guard will not provide any on-access protection. In this case only the on-demand scanner (avscan) can be used..

All on-access options will be inactive if you disable the Guard. For setting on-demand scanner options check the *avscan.conf* file.

```
OnAccessManagement auto
```

Num Daemons

Number of daemons:
The number of simultaneous AntiVir Guard daemons can be set between 3 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.

Repair Concerning Files

Repairing files:
If `RepairConcerningFiles` is set AntiVir Guard will try to remove any alert by repairing the infected file. If the repair has been carried out successfully, access is granted and no further action besides logging is taken.
If the repair fails, access is blocked and the AlertAction, if you have selected one, is carried out. The following option must be active:

```
RepairConcerningFiles
```

It is not activated by default.

AlertAction

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

- `none` or `ignore`: no further action
- `rename` or `ren`: renaming the file by adding the *.XXX* extension.
- `delete` or `del`: delete the concerning file.
- `quarantine`: move the concerning file into quarantine, if you defined one (see below).

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

```
AlertAction none
```

Quarantine Directory

You have to define the quarantine directory, if you want to use the `quarantine` option for `AlertAction` (see above).

Note: If you fail to specify a quarantine directory, the following directory is created by default and the infected files are moved into it:

```
QuarantineDirectory /home/quarantine
```

Alert Conditions

Alert Actions Based on Configurable Conditions:

You can set actions based on the reported alert condition (eg. for encrypted files or archives that are tagged as suspicious).

Specific alert actions are only available for scan result flags that are supported by Savapi.

In case multiple alert flags trigger simultaneously, the action with the highest escalation level takes precedence.

Based on the specific action, the alert is treated as follows:

- `ignore` - the alert is ignored.
- `warn` - the condition is logged as a warning; access is not blocked by the guard.
- `block` - access is blocked.
- `alert` - access is blocked; the alert action is performed (highest priority).

Each of the following conditions can be set to: `ignore`, `warn`, `block` or `alert`.
Default settings:

- `ArchiveMaxSizeAction block`
- `ArchiveMaxRecursionAction block`
- `ArchiveMaxRatioAction block`
- `ArchiveMaxCountAction block`
- `ScanIncompleteAction warn`
- `ArchiveEncryptedAction warn`
- `ArchiveMultiVolumeAction warn`
- `ArchiveUnsupportedAction warn`
- `ArchiveHeaderMalformedAction warn`
- `ArchiveBombAction block`
- `TaggedSuspiciousAction warn`
- `ArchiveProcErrorAction warn`

AccessMask

Access mask (only for dazuko2):

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 (default).

```
AccessMask 3
```

Please note that AntiVir Guard is able to react to these situations and to scan files, only if the kernel module supports these events. Not every operating system supports all events in every kernel version. Moreover, some kernel modules offer the possibility to activate or deactivate certain events. Independent from the use of the other events, we recommend that you always keep the option ***Scanning files when opened*** activated.

IncludePath

Scanned directories (only for dazuko2):

AntiVir Guard scans the files in the specified directories, including their subdirectories. Usually, the most vulnerable file system is */home* since the data of different users is located there:

```
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 /var/tmp
IncludePath /tmp
```

If no folder is specified, AntiVir Guard will not start!

Dazuko3 ignores this option. It it therefore not advisable to use it in conjunction with **Dazuko3.** AntiVir Guard will otherwise fail to start.

ExcludePath

Excluded directories:
If you dont want all subfolders within an `IncludePath` to be protected, AntiVir Guard can exclude certain folders from scanning. For example, a folder containing temporary files of AntiVir components. There is no default setting.

You can specify only one path in a command line (trailing slash necessary). You can enter more, by typing the command for each one. Example:

```
ExcludePath /home/log/
ExcludePath /pub/log/
```

ExcludePattern

Excluded PCRE patterns from on-access scanning:
This option specifies files/directories that should be excluded from on-access scanning. The files/directories are not scanned, if their names match the given PCRE pattern (Perl-compatible regular expression).

```
ExcludePattern [regex]
```

You can also exclude multiple PCRE patterns from the scan. Simply combine all the expressions you want to exclude by specifying one after the other as consecutive configuration file options. Example:

```
ExcludePattern usr/share
ExcludePattern src/kernels
ExcludePattern usr/lib
ExcludePattern(so|h|mo|gz)$
```

Default: `ExcludePattern NONE`.

Although file names often indicate the file type (even under Unix), there is no technical connection between file names and file types under Unix. Therefore it may be a security flaw to exclude certain files from being scanned based on file names.

Please take into account that filenames are normalized before the pattern match is applied. Therefore, parts of the pathname may also trigger an unwanted match if the expression is not written carefully.

When scanning symbolic links, the files they point to are matched.

ExcludeExt

Excluded file extensions:
This option allows you to specify file extensions that should be excluded from on-access scanning.

`ExcludeExt [spec]`

where `[spec]` is a colon-separated list of file extensions, e.g. `exe:bat:com`.

Default: `ExcludeExt NONE`

Temporary Directory

Temporary location of Guard files:
Temporary files of the Guard are written in this directory. Example:

`TemporaryDirectory /tmp`

Note: Please make sure that there is sufficient disk space, i.e. at least 4GB, available at the location of the temporary files directory.

ScanMode

Configuring files to be scanned:
This entry sets the procedure to determine whether a file is to be scanned or not. The available methods are:

- `extlist`: scan only files with certain extensions;
- `smart`: scan files based on both their name and file type;
- `all`: always scan files, of all types and names.

The default is:

`ScanMode all`

ArchiveScan

Scanning archives on-access:
AntiVir Guard scans archives when opened, depending on the setting for `ArchiveMaxSize`, `ArchiveMaxRecursion` and `ArchiveMaxRatio`. This is activated by default in order to maintain the highest security:
`ArchiveScan yes`

MailboxScan

Scanning mailbox containers on-access:
If `ArchiveScan` is set to `yes`, AntiVir Guard scans mailboxes on-access, when the following option is active:
`MailboxScan yes`

This is active by default.

ArchiveMax Size

Maximum archive size:
This option limits the scanning process to the files with unpacked size smaller than the specified value (in bytes, KB, MB, GB). The zero value means no limit. The default setting is approx. 1 Gigabyte:
`ArchiveMaxSize 1GB`

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 20`

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`

Archive MaxCount

Number of files in an archive:
The archive scanning is limited to a given number of files within a recursion level. The zero value means no limit is set. Default:

`ArchiveMaxCount 0`

MaxReports PerFile

Limit the number of scanner alert messages:
The upper limit of messages that are issued per scanned file. Usually this only affects archive scanning. This option can be used to prevent the scanner from Denial Of Service attacks generated by crafted archives that otherwise would provoke millions of alerts. A value of 0 means no limit is set.

`MaxReportsPerFile 100`

SendSNMPTraps

SNMP traps configuration:
SNMP traps can be used as a method to monitor the status of system and network services. Both on-demand and on-access scanners support this protocol, sending SNMP traps (simple text messages) to inform system monitoring tools about scanner's current status, license issues, virus alerts and update status. These messages are logged.

To enable SNMP traps:

`SendSNMPTraps yes`

Default: disabled (`no`).

SNMP VerbosityLevel

To set the verbosity level of SNMP traps:

`SNMPVerbosityLevel [notice|information|warning|error|alert|snmp]`

Defines for which issues traps should be sent when files are scanned. Default: only snmp-specific alerts and important status information are sent (`snmp` level):

`SNMPVerbosityLevel snmp`

Apart from `snmp`, it supports syslog levels. For example:

`SNMPVerbosityLevel information`
The following messages will be sent via snmp: messages with prio "information", "warning", "error", "alert" PLUS the snmp-specific messages.

The `SNMPVerbosityLevel` does not affect the `syslog` verbosity and vice versa.

SNMPRecipient

Specify a hostname or an IP address, to configure the recipient of SNMP traps:

`SNMPRecipient <hostname | IP address>`

Default: `SNMPRecipient localhost`

External Program

Please use this feature with extreme caution! Check your external programs for correctness and keep in mind, that an attacker might use crafted file names (containing spaces, commands, etc.) for injecting arguments into your 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 (octal)
%De	Event type
%DF	File system or partition (device) on which the file is located (hexadecimal)
%Dp	PID of the process
%Du	UID of the process
%Df	Flag of file operation (hexadecimal)
%Dm	Access mode of file operation (hexadecimal)
%Sn	Name of the detected virus / unwanted program
%Sa	Extra information about the alert (if available)
%SU	Alert URL.

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 /bin/sh /usr/lib/AntiVir/guard/popup_message.sh
[%Sn] %p
```

Default: NONE

There are no status reports on the invocation of external programs.

EmailTo **Email messages**:
AntiVir Guard can send emails, when it detects viruses or unwanted programs. There is

no default setting. You must setup your mail daemon and specify a recipient in order to send emails:

```
EmailTo root@localhost
```

Suppress Notification Below

Filtering email notifications as required:
This option can exclude certain messages, when notifications are sent, according to their priority level. The recipients will only receive notifications with the selected priority or higher.

Syntax:

```
SuppressNotificationBelow scanner <level>
```

The possible priority levels (in ascending order) are `notice`, `information`, `warning`, `error` and `alert`.

Example:

```
SuppressNotificationBelow scanner warning
```

LogFile

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:

```
LogFile /var/log/avguard.log
```

Syslog...

Syslog settings:
AntiVir Server/ Professional 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
```

Setting the `SyslogPriority` determines that all those messages which are equal or higher than the priority specified are logged. Consequently you receive with the `Priority Warning` all those messages labelled `Alert`, `Error` or `Warning`. Since `Info` has a lower priority than `Warning` you will not receive any `Info` messages.

These values apply even if the `LogFile` option is not active.

DetectPrefixes

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. The virus detection is not optional and you can not deactivate it. The available categories are:

- `adspy` - software that displays advertising pop-ups or software that very often without the user's consent sends user specific data to third parties and might therefore be unwanted.
- `appl` - an application of dubious origin or which might be hazardous to use.
- `bdc` - the Control software for backdoors. BDCs are generally harmless.
- `dial` - a Dial-Up program for connections that charge a fee. Its use might lead to huge costs for the user.
- `game` - a game, that causes no damage on your computer.
- `hiddenext` - a file with an executable extension, hidden behind a harmless one.
- `joke` - a harmless joke program, present as file.
- `pck`- a file compressed with an unusual runtime compression tool.
- `phish` - faked emails that are supposed to prompt the victim to reveal confidential information such as user accounts, passwords or online-banking data on certain websites.

- `spr` - software that may compromise the security of your system, initiate unwanted program activities, damage your privacy or spy out your user behavior and might therefore be unwanted.
- `alltypes` - option to detect all supported malware types.

Syntax: list of types, separated by whitespace or colon.

```
DetectPrefixes <type>[=<bool>] <type>[=<bool>] ...
```

Example:

```
DetectPrefixes adspy=yes appl=no bdc=yes dial=yes game=no
hiddenext=no joke=no pck=no phish=yes spr=no
```

Heuristics Macro

Macrovirus Heuristics:
Activates the heuristics for macroviruses in office documents.
`HeuristicsMacro yes`

Heuristics Level

Win32-Heuristics:
Sets the level of heuristic detection in all types of files. Available values are `0` (off), `1` (low), `2` (medium) and `3` (high - could result in false alerts!).
`HeuristicsLevel 1`

GUISupport

Support via graphical user interface (GUI):
This option must be activated in order for AntiVir Server/ Professional to communicate with the GUI of Avira SMC. You must enter the following parameters:

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

In the case of missing or invalid parameters, the GUI support is not available. The log file records possible errors.

ActiveLockFile

Guard's shared lockfile:
You must specify the absolute path to the Guard's lockfile, so that other software on the computer can detect Guard's presence. The file is also used for the Gnome plug-in.

```
ActiveLockFile /var/lock/LCK..avguard
```

Default: `ActiveLockFile NONE`

4.1.2 Configuration of the Command Line Scanner in *avscan.conf*

A new configuration file for the on-demand scanner has been introduced, starting with AntiVir Server/ Professional v 3.0.0: *avscan.conf*.

Repair Concerning Files

Repairing files:
The CLS is trying to repair infected files. If this fails, access is blocked. The following option must be active:

```
RepairConcerningFiles yes
```

It is not activated by default.

AlertAction

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 options define the actions of the CLS (check the user permissions!):

- `none` or `ignore`: no further action

- `rename` or `ren`: renaming the file by adding the *.XXX* extension.
- `delete` or `del`: delete the concerning file.
- `quarantine`: move the concerning file into quarantine directory, if you have defined one (see below).

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

```
AlertAction none
```

Quarantine Directory

You have to define the quarantine directory, if you want to use the `quarantine` option for `AlertAction` (see above). Default is:

```
QuarantineDirectory /home/quarantine
```

ExcludePattern

Excluded PCRE patterns from on-demand scanning:
This option specifies files/directories that should be excluded from on-demand scanning. The files/directories are not scanned, if their names match the given PCRE pattern (Perl-compatible regular expression).

```
ExcludePattern [regex]
```

You can also exclude multiple PCRE patterns from the scan. Simply combine all the expressions you want to exclude by specifying one after the other as consecutive configuration file options. Example:

```
ExcludePattern usr/share
ExcludePattern src/kernels
ExcludePattern usr/lib
ExcludePattern(so|h|mo|gz)$
```

Default: `ExcludePattern NONE`..

Although filenames often indicate the file type (even under Unix), there is no technical connection between filenames and file types under Unix. Therefore it may be a security flaw to exclude certain files from being scanned based on filenames.

When scanning symbolic links, the files they point to are matched.

ExcludeExt

Excluded file extensions:
This option allows you to specify file extensions that should be excluded from on-demand scanning.

```
ExcludeExt [spec]
```

where `[spec]` is a colon-separated list of file extensions, e.g. `exe:bat:com`.

Default: `ExcludeExt NONE`

Temporary Directory

Temporary location of CLS files:
Temporary files of the CLS are written in this directory. Example:

```
TemporaryDirectory /tmp
```

FollowSymlink

Setting the on-demand scanner behavior for symlinks:
Symbolic links are followed by default. You can use this option to change the behavior.

```
FollowSymlink yes
```

ScanMode

Configuring files to be scanned:
This entry sets the procedure to determine whether a file is to be scanned or not. The available methods are:

- `extlist`: scan only files with certain extensions;
- `smart`: scan files based on both their name and file type;
- `all`: always scan files, of all types and names.

The default is:

```
ScanMode smart
```

ArchiveScan

Scanning archives on-demand:
The CLS scans archives on-demand, depending on the setting for `ArchiveMaxSize`, `ArchiveMaxRecursion` and `ArchiveMaxRatio`. This is activated by default in order to maintain the highest security:

```
ArchiveScan yes
```

MailboxScan

Scanning mailbox containers on-demand:
If `ArchiveScan` is set to `yes`, the CLS scans mailboxes on-demand, when the following option is active:

```
MailboxScan yes
```

This is active by default.

ArchiveMax Size

Maximum archive size:
This option limits the scanning process to the files with unpacked size smaller than the specified value (in bytes, KB, MG, GB). The zero value means no limit. The default setting is 1 Gigabyte:

```
ArchiveMaxSize 1GB
```

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 20
```

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
```

Archive MaxCount

Number of files in an archive:
The archive scanning is limited to a given number of files within a recursion level. The zero value means no limit is set. Default:

```
ArchiveMaxCount 0
```

SendSNMPTraps

SNMP traps configuration:
SNMP traps can be used as a method to monitor the status of system and network services. Both on-demand and on-access scanners support this protocol, sending SNMP traps (simple text messages) to inform system monitoring tools about scanner's current status, license issues, virus alerts and update status. These messages are then logged.

To enable SNMP traps:

`SendSNMPTraps yes`

Default: disabled (`no`).

SNMP VerbosityLevel

To set the verbosity level of SNMP traps:

`SNMPVerbosityLevel [notice|information|warning|error|alert|snmp]`

Defines for which issues traps should be sent when files are scanned. Default: only snmp-specific alerts and important status information are sent (`snmp` level):

`SNMPVerbosityLevel snmp`

Apart from `snmp`, it supports syslog levels. For example:

`SNMPVerbosityLevel information`

The following messages will be sent via snmp: messages with prio "information", "warning", "error", "alert" PLUS the snmp-specific messages.

The `SNMPVerbosityLevel` does not affect the `syslog` verbosity and vice versa.

SNMPRecipient

Specify a hostname or an IP address, to configure the recipient of SNMP traps:

`SNMPRecipient <hostname | IP address>`

Default: `SNMPRecipient localhost`

External Program

Please use this feature with extreme caution! Check your external programs for correctness and keep in mind, that an attacker might use crafted file names (containing spaces, commands, etc.) for injecting arguments into your external program.

Starting External Programs When Suspicious Files Are Found:

The CLS can start an external program when a virus or an unwanted program is found. This can send a notification or perform an action using certain 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 (octal)

Option	Function
%De	Event type
%DF	File system or partition (device) on which the file is located (hexadecimal)
%Dp	PID of the process
%Du	UID of the process
%Df	Flag of file operation (hexadecimal)
%Dm	Access mode of file operation (hexadecimal)
%Sn	Name of the detected virus / unwanted program
%Sa	Extra information about the alert (if available)
%SU	Alert URL.

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 /bin/sh /usr/lib/AntiVir/guard/popup_message.sh
[%Sn] %p
```

LogFile

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:

```
LogFile /var/log/avscan.log
```

Syslog...

Syslog settings:

AntiVir Server/ Professional 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
```

With the SyslogPriority you specify that all those messages are logged which have an equal or higher priority than the one specified.

These values apply even if the `LogFile` option is not active.

DetectPrefixes

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. The virus detection is not optional and you can not deactivate it. The available categories are:

- `adspy` - Software that displays advertising pop-ups or software that very often without the user's consent sends user specific data to third parties and might therefore be unwanted.
- `appl` - an application of dubious origin or which might be hazardous to use.
- `bdc` - the Control software for backdoors. BDCs are generally harmless.
- `dial` - a Dial-Up program for connections that charge a fee. Its use might lead to huge costs for the user.
- `game` - a game, that causes no damage on your computer.
- `hiddenext` - a file with an executable extension, hidden behind a harmless one.

- `joke` - a harmless joke program, present as file.
- `pck`- a file compressed with an unusual runtime compression tool.
- `phish` - faked emails that are supposed to prompt the victim to reveal confidential information such as user accounts, passwords or online-banking data on certain web-sites.
- `spr` - software that may compromise the security of your system, initiate unwanted program activities, damage your privacy or spy out your user behavior and might therefore be unwanted.
- `alltypes` - option to detect all supported malware types.

Syntax: list of types, separated by whitespace or colon.

```
DetectPrefixes <type>[=<bool>] <type>[=<bool>] ...
```

Example:

```
DetectPrefixes adspy=yes appl=no bdc=yes dial=yes game=no
hiddenext=no joke=no pck=no phish=yes spr=no
```

Heuristics Macro

Macrovirus Heuristics:
Activates the heuristics for macroviruses in office documents.

```
HeuristicsMacro yes
```

Heuristics Level

Win32-Heuristics:
Sets the level of heuristic detection in all types of files. Available values are `0` (off), `1` (low), `2` (medium) and `3` (high - could result in false alerts!).

```
HeuristicsLevel 1
```

GUISupport

Support for Avira Security Management Center:
This option must be activated in order for AntiVir Server/ Professional to communicate with the GUI of Avira SMC. You must enter the following parameters:

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

In the case of missing or invalid parameters, the GUI support is not available. The log file records possible errors.

4.1.3 Scanner specific configuration in *avguard-scanner.conf*

A new configuration file has been introduced, starting with AntiVir Server/ Professional v3.0.0: *avguard-scanner.conf*. It contains configuration options specific to the new scanner backend. Usually, you don't have to change the options in this file, but there might be a few exceptions.

Syslog Facility

Facility used when logging.

```
SyslogFacility user
```

ReportLevel

The scanner can be set to log on different levels:

- 0 - Log errors
- 1 - Log errors and alerts
- 2 - Log errors, alerts and warnings
- 3 - Log errors, alerts, warnings and debug messages

"alerts" means information about potential malicious code.

Default:

```
ReportLevel 0
```

LogFileName Path to the scanner logfile.

```
LogFileName NONE
```

AlertURL You can use this option to retrieve information about virus alerts via Internet.

Currently supported URLs:

English: http://www.avira.com/en/threats?q=%1

German: http://www.avira.com/de/threats?q=%1

```
AlertURL=<URL>
```

4.1.4 Configuration of Avira Updater in *avupdate-guard.conf*

This section provides a short description of the settings in *avupdate-guard.conf*. The settings affect the Avira Updater.

Updates ensure that AntiVir Server/ Professional components (Guard, Scanner, VDF and Engine), which provide security against viruses or unwanted programs, are always kept up to date.

With Avira Updater you can update Avira software on your computers, using Avira update servers.

To configure the update process, use the options in */etc/avira/avupdate-guard.conf* described below. All parameters from *avupdate-guard.conf* can be passed to the Updater via command line. For example:

- parameter in avupdate-guard.conf:

```
temp-dir=/tmp
```

- command line:

```
/usr/lib/AntiVir/guard/avupdate-guard --temp-dir=/tmp
```

internet-srvs The list of Internet update servers.

```
internet-srvs=http://dl1.pro.antivir.de, http://
dl2.pro.antivir.de, http://dl3.pro.antivir.de
```

master-file Specifies the master.idx file.

```
master-file=/idx/master.idx
```

install-dir Specifies the installation directory for updated product files.

```
install-dir=/usr/lib/AntiVir/guard
```

temp-dir Temporary directory for downloading update files.

```
temp-dir=/tmp/avira_update/guard
```

HTTP proxy settings

proxy... If you use an http proxy server for Internet updates, you have to provide the following data:

```
proxy-host=
proxy-port=
proxy-username=
proxy-password=
```

Setting update email reports

All reports on AntiVir updates are sent to the email address given in *avupdate-guard.conf*:

smtp... Authentication for smtp connection. Activate the `auth-method` option and then provide the smtp server, port, user and password.

```
mailer=[smtp | sendmail]

auth-method=password
smtp-user=<your_username>
smtp-password=<your_password>
smtp-server=<servername>
smtp-port=<port>
```

notify-when There are three situations to set for email notifications:

- 0 - no email notifications are sent,
- 1 - email notifications are sent in case of "successful update", "unsuccessful update", or "up to date".
- 2 - email notification only in case of "unsuccessful update".
- 3 - email notification only in case of "successful update".

```
notify-when=3
```

email-to The recipient of notification emails.

```
email-to=root@localhost
```

Logfile settings

log Specify a full path with a filename to which AntiVir Updater will write its log messages.

```
log=/var/log/avupdate.log
```

log-rotate
log-append By default, the logfile is overwritten (`log-rotate`). You can use this option to append the logfile:

```
log-append
```

4.2 Testing AntiVir Server/ ProfessionalTesting

After completing the installation and configuration, you can test the functionality of AntiVir Server/ Professional 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 Guard with a Test-Virus

- ▶ Go to http://www.eicar.org.
- ▶ Read the information about the test virus *eicar.com*.
- ▶ Download the test virus to your computer (for exp, in a directory named /TEST).
- ▶ On dazuko3 systems, mount the directory in which you downloaded *eicar.com*
  `mount -t dazukofs /TEST /TEST`
- ▶ Try to access the file, via the shell command “less”:
  ↳ AntiVir Guard will deny the access.

Testing AntiVir Command Line Scanner with a Test-Virus

- Go to http://www.eicar.org.
- Read the information about the test virus *eicar.com*.
- Download the test virus to your computer (for exp, in a directory named /TEST).
- Execute the command:
  `avscan /TEST`
  ↳ AntiVir will notify you about malware detection and will ask you to select an action.

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/guard/avguard status`
- Start AntiVir Guard if necessary.
- If you use AntiVir Guard in conjunction with dazukofs ensure that the file system location for which you want to enable OnAccess protection, is mounted with dazukofs.
  Use the `mount` command to see a list of all mounted file systems/partitions.
- If you use AntiVir Guard in conjunction with dazuko2 make sure that the file system location you want to protect is specified by means of the `IncludePath` option. Also ensure that the `AccessMask` is set to a value different from 0, since AntiVir Guard will otherwise fail to start.
- 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 Guard guarantees continuous scanning on your system. During operation, there may be the need for occasional changes in Configuration – Page 17.

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:

- Scanning on-access with AntiVir Guard – Page 34 summarizes all options for the resident scanner *avguard*.
- Scanning on-demand with AntiVir Command Line Scanner – Page 37 lists the options for on-demand scanner *avscan* and describes some examples of working with the Command Line Scanner.
- Reaction to Detecting Viruses/ Unwanted Programs – Page 42 gives you some hints on how to react when AntiVir has done its work.

5.1 Scanning on-access with AntiVir Guard

Syntax

To start, stop or restart the AntiVir Guard as root, or to check its status:

```
avguard {start|stop|status|restart}
```

Example:

If the Guard is running, the command

```
avguard status
```

returns the message "*Status: avguard.bin running*".

To scan on-access, using certain parameters:

```
avguard [option]
```

Options

Option	Function
`--alert-action=<spec>`	Sets the action to be taken, when detecting viruses or unwanted programs. See the actions' list at AlertAction – Page 18 `--alert-action=quarantine`
`--archive-max-count=<spec>`	Limits the number of files packed in archive or mailbox. The Guard does not scan beyond the configured limits.

`--archive-max-count-action=`	Alert action for the above condition. It can be set to `ignore`, `warn`, `block` or `alert`. See "Alert Conditions" on page 19
`--archive-max-ratio=<spec>`	Limits the archive or mailbox ratio. The Guard does not scan beyond the configured limits.
`--archive-max-ratio-action=`	Alert action for the above condition. It can be set to `ignore`, `warn`, `block` or `alert`. See "Alert Conditions" on page 19
`--archive-max-recursion=<spec>`	Limits the archive or mailbox recursion. The Guard does not scan beyond the configured limits.
`--archive-max-recursion-action=`	Alert action for the above condition. It can be set to `ignore`, `warn`, `block` or `alert`. See "Alert Conditions" on page 19
`--archive-max-size=<spec>`	Limits the archive or mailbox size. The Guard does not scan beyond the configured limits.
`--archive-max-size-action=`	Alert action for the above condition. It can be set to `ignore`, `warn`, `block` or `alert`. See "Alert Conditions" on page 19
`--archive-encrypted-action=`	Alert action in case of an encrypted archive. It can be set to `ignore`, `warn`, `block` or `alert`. See "Alert Conditions" on page 19.
`--archive-multivolume-action=`	Alert action in case of a multivolume archive. It can be set to `ignore`, `warn`, `block` or `alert`. See "Alert Conditions" on page 19.
`--archive-unsupported-action=`	Alert action in case of an unsupported archive. It can be set to `ignore`, `warn`, `block` or `alert`. See "Alert Conditions" on page 19.
`--archive-header-malformed-action=`	Alert action in case of a malformed archive header. It can be set to `ignore`, `warn`, `block` or `alert`. See "Alert Conditions" on page 19.
`--archive-bomb-action=`	Alert action triggered by a bomb archive. It can be set to `ignore`, `warn`, `block` or `alert`. See "Alert Conditions" on page 19.
`--archive-procerror-action=`	Alert action triggered by an archive processing error. It can be set to `ignore`, `warn`, `block` or `alert`. See "Alert Conditions" on page 19.
`--config`	Prints a sample configuration.

`-C <configuration-file>`	Use a specific configuration file instead of the default one.
`--detect-prefixes=<spec>`	Specifies which kind of malware or unwanted software should get detected. (Virus detection is always active.) Accepts whitespace or colon separated list of "<type>[=<bool>]". `--detect-prefixes='adspy=yes:joke=no:spr:bdc'` To scan for all types of malware: `--detect-prefixes=alltypes` See the list of accepted types at DetectPrefixes – Page 24.
`--exclude-ext=<ext>{:<ext>}`	Specifies that the given extensions are excluded from scanning. Example: `--exclude-ext=exe:com:bat` Note: When scanning symbolic links, the files they point to are scanned.
`--exclude-path=<dir>`	Specifies a directory to be excluded from on-access scanning.
`--exclude-pattern=<spec>`	Specifies what to exclude from scanning. It accepts a comma separated list of Perl-compatible regular expressions (PCRE). Example: `--exclude-pattern="^/tmp/TEST/"` Warning: *Please take into account that filenames are normalized before the pattern match is applied. Therefore, parts of the pathname may also trigger an unwanted match if the expression is not written carefully.* Note: *When scanning symbolic links, the files they point to are matched.*
`--help`	Prints usage information about *avguard.bin*
`--heur-level=<int>`	Specifies the Win32 file heuristics level. Available values are `0` (off), `1` (low), `2` (medium) and `3` (high - could result in false alerts!). Not activated by default.
`--heur-macro[=<bool>]`	Enables or disables macro heuristics.
`--log-email=<addr>`	Specifies to what address(es) the notification messages will be sent. Accepts a whitespace separated list of email addresses.
`--scan-in-archive[=<bool>]`	Enables or disables recursion into archive containers. By default on.

`--scan-in-mbox[=<bool>]`	Enables or disables recursion into archive mailbox. By default on.
`--scan-incomplete-action=`	Alert action in case of incomplete scan. It can be set to `ignore`, `warn`, `block` or `alert`. See "Alert Conditions" on page 19.
`--scan-mode=<spec>`	Instructs the scanner how a sample should be scanned. `ScanMode {all|smart|ext}`
`--send-snmp-traps=yes|no`	Enables or disables SNMP traps. Default: no.
`--snmp-verbosity-level=<level>`	Sets the verbosity level of SNMP traps; apart from `snmp`, it supports syslog levels `notice|information|warning|error|alert`. Default: only snmp-specific alerts and important status information are sent.
`--snmp-recipient=<localhost| ip address>`	The string holds the localhost or IP address, needed to configure the recipient(s) of SNMP traps.
`--temp-dir=<dir>`	Defines the absolute path of the temporary directory
`--version`	Prints version information.

5.2 Scanning on-demand with AntiVir Command Line Scanner

Syntax

To scan on-demand, using certain parameters:

```
avscan [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:

```
avscan [option] [directory][filename]
```

Options

You can use the following options for the Command Line Scanner, in various combinations. All non-option strings are considered files or directories to be scanned (by default, no recursion beyond the first level of the directory structure).

Option	**Function**
`--alert-action=<spec>`	Sets the action to be taken, when detecting viruses or unwanted programs. See the actions' list at AlertAction – Page 18 `--alert-action=quarantine`

`--archive-max-count=<N>`	Limits the number of files packed in archive or mailbox. The CLS does not scan beyond the configured limits.
`--archive-max-ratio=<N>`	Limits the archive or mailbox ratio. The CLS does not scan beyond the configured limits.
`--archive-max-recursion=<N>`	Limits the archive or mailbox recursion. The CLS does not scan beyond the configured limits.
`--archive-max-size=<N>`	Limits the archive or mailbox size. The CLS does not scan beyond the configured limits.
`--batch`	Enables "batch mode": If you enable this option avscan will enter the non-interactive batch mode. In this mode all decisions are carried out based on the given configuration file and command-line settings. The user will not be asked to make or confirm any decisions. Note: If you had set the alert action to `delete` the alert action for files which are only considered suspicious is automatically reset by avscan to `quarantine` when operating in batch mode.
`--config`	Prints a sample configuration.
`-C <configuration-file>`	Use a specific configuration file instead of the default one.
`--detect-prefixes=<spec>`	Specifies which kind of malware or unwanted software should get detected. (Virus detection is always active.) Accepts whitespace or colon separated list of "<type>[=<bool>]". `--detect-prefixes='adspy=yes:joke=no:spr:bdc'` To scan for all types of malware: `--detect-prefixes=alltypes` See the list of accepted types at DetectPrefixes – Page 24.
`-e`	Repair concerning files if possible.
`--exclude-ext=<ext>{:<ext>}`	Specifies that the given extensions are excluded from scanning. Example: `--exclude-ext=exe:com:bat` Note: When scanning symbolic links, the files they point to are scanned.

`--exclude-pattern=<spec>`	Specifies what to exclude from scanning (a comma separated list of PCRE- Perl-compatible regular expressions, using absolute paths). Example: `--exclude-pattern="^/tmp/TEST/"` Warning: *Please take into account that filenames are normalized before the pattern match is applied. Therefore, parts of the pathname may also trigger an unwanted match if the expression is not written carefully.* Note: *When scanning symbolic links, the files they point to are matched.*
`--follow-symlink[=yes|no]`	Follows symbolic links. Default: yes.
`--help`	Prints usage information about *avscan* (abbreviation: `-h` or `-?`)
`--heur-level=<int>`	Specifies the Win32 file heuristics level. Available values are `0` (off), `1` (low), `2` (medium) and `3` (high - could result in false alerts!). Not activated by default.
`--heur-macro[=<yes|no>]`	Enables or disables macro heuristics.
`--log-file=<filename>`	Specifies the file for log messages.
`--max-runtime=<seconds>`	This option can be invoked for normal or scheduled scanning. It defines a soft overall time limit. If the time limit is exceeded, the job will stop after completing the currently pending subtask (scan/ database action).
`--query-results`	In scheduler mode, avscan will query the database instead of scanning files. *Note: Option must not be invoked at the same time as --scan-scheduled-files.*
`--query-alerts`	In scheduler mode, avscan queries the database and shows only files that have triggered an alert. *Note: Option must not be invoked at the same time as --scan-scheduled-files.*
`--query-warnings`	In scheduler mode, avscan queries the database and shows only files that have triggered a warning. *Note: Option must not be invoked at the same time as --scan-scheduled-files.*

`--query-statistics`	In scheduler mode avscan queries the database and shows statistics about the last scheduled scan and overall scheduled scan results. *Note: Option must not be invoked at the same time as --scan-scheduled-files.*
`--quarantine-dir=<dir>`	Specifies the quarantine directory for infected files.
`-s`	This option enables recursive scanning of all subdirectories within a specified path.
`--scan-continue-file=<filename>`	In scheduler mode, avscan resumes an aborted scheduled scanning.
`--scan-in-archive[=<yes|no>]`	Enables or disables recursion into archive containers. By default on.
`--scan-in-mbox[=<yes|no>]`	Enables or disables recursion into archive mailbox. By default on.
`--scan-mode=<spec>`	Instructs the scanner how a sample should be scanned `ScanMode {all|smart|extlist}`
`--schedule-scan=yes|no`	Enables the scanner scheduler, by updating the database, instead of performing a direct scan. Default: `no`.
`--send-snmp-traps=yes|no`	Enables or disables SNMP traps. Default: no.
`--snmp-verbosity-level=<level>`	Sets the verbosity level of SNMP traps; apart from `snmp`, it supports syslog levels `notice|information|warning|error|alert`. Default: only snmp-specific alerts and important status information are sent.
`--snmp-recipient=<localhost| ip address>`	The string holds the localhost or IP address, needed to configure the recipient(s) of SNMP traps.
`--scan-scheduled-files`	Starts the worker process to perform the scheduled scan. Restricted to the root user. *Note: Option must not be invoked at the same time as --query-results, --query-alerts, --query-warnings or --query-statistics.*
`--temp=<dir>`	Defines the absolute path of the directory for temporary files.

`-v` `--verbose`	Set verbose mode on. This option should be used in exceptional cases only, as for example after a virus detection/removal.
`--version`	Prints version information.

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, nothing found, no error.
1	Found concerning file.
3	Suspicious file found.
4	Warnings were issued.
249	Scan process not completed.
250	Cannot initialize scan process.
251	The avguard daemon is not accessible.
252	The avguard daemon is not running.
253	Error while preparing on-demand scan.
254	Configuration error (invalid parameter in command-line or configuration file).
255	Internal error.

Example: Performing Complete Scan

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

The following parameters should be used:

`--scan-mode=all`	Scans all files.
`--detect-prefixes=alltypes`	Scans for all types of malware.
`-s`	Scans all subfolders.
`--scan-in-archive`	Scans packed files, too.

▶ The command is:
`avscan --scan-mode=all --detect-prefixes=alltypes -s --scan-in-archive /`

Example: 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:

`--scan-mode=all`	Scans all files.
`-s`	Scans all subfolders.
`--scan-in-archive`	Scans packed files, too.

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

▶ Use the command:

```
avscan --scan-mode=all -s --scan-in-archive /var /mnt
```

Example: Deleting Infected Files

Avira AntiVir Server/ Professional can delete files which contain viruses or unwanted programs. Optionally, AntiVir can first try to repair these files. Otherwise, the program will delete them completely; i.e. repairing tools will not recover them.

You can use the following options:

`--scan-mode=all`	Scans all files.
`--alert-action=delete`	Deletes infected files.
`-e --alert-action=delete`	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!

If you want to delete all infected files from */home/myhome* (Check user permissions!):

▶ Type the command:

```
avscan --scan-mode=all --alert-action=delete /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:

```
avscan --scan-mode=all -e --alert-action=delete /home/
myhome
```

5.3 Reaction to Detecting Viruses/ Unwanted Programs

If correctly configured, Avira AntiVir Server/ Professional 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@avira.com.

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

6 Updates

With Avira Updater you can update Avira software on your computers, using Avira update servers. The program can be configured either by editing the configuration file (see 4.1.4 Configuration of Avira Updater in avupdate-guard.conf), or by using parameters in the command line.

It is recommended to run the Updater as ***root***. If the Updater does not run as ***root***, it does not have the necessary rights to restart AntiVir daemons, so the restart has to be made manually, as ***root***.

Advantage: any running processes of AntiVir daemons (such as Scanner, AntiVir Guard) are automatically updated with the current antivirus files, without interrupting the running scan processes. It is thus ensured that all files are scanned.

6.1 Internet Updates

Manually

If you want to update Avira AntiVir Server/ Professional or some of its components:

▶ Use the command:

```
/usr/lib/AntiVir/guard/avupdate-guard --product=[product]
```

As `[product]`, you can use:
- `Scanner` - (recommended) to update the scanner, engine and vdf files.
- `Guard` - complete update (Guard, Scanner, engine and vdf files).

If you just want to check for a new AntiVir version without updating AntiVir:

▶ Use the command:

```
/usr/lib/AntiVir/guard/avupdate-guard --check --product=[product]
```

The `[product]` values are the same as above.

Automatic updates with cron daemon

Regular updates are made using cron daemon.

The settings for automatic updates in */etc/cron.d/avira_updater* **have already been made if**, when installing AntiVir Server/ Professional with the *install* script, the answer for installing Avira Updater and starting it automatically was `yes`.

You can find further information on cron daemon in your UNIX documentation.

To make or change the settings for automatic updates in crontab manually:

▶ Add or edit the entry in */etc/crontab*, similar to the example below.

Example: for an hourly update at *:23, enter the following command:

```
23 * * * * root /usr/lib/AntiVir/guard/avupdate-guard --
product=[product]
```

As `[product]`, you can use:
- `Scanner` - (recommended) to update the scanner, engine and vdf files.
- `Guard` - complete update (Guard, Scanner, engine and vdf files).

▶ Start the update process to test the settings:

```
/usr/lib/AntiVir/guard/avupdate-guard --product=[product]
```

where `[product]` takes the same values as above.

↳ If successful, a report will appear in the logfile */var/log/avupdate.log*

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 FAQ

Before you contact our Hotline, we recommend that you visit our user forum at http://forum.antivir.de, as well as the FAQ section on our website.
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 Operations GmbH & Co. KG
Kaplaneiweg 1
D-88069 Tettnang
Germany

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

8 The Dazuko Kernel Module

Dazuko kernel module is required by all platforms, for allowing the on-access scanner AntiVir Guard to run. AntiVir Server/ Professional can be installed even without dazuko, but in this case it will run without AntiVir Guard.

For using AntiVir Server/ Professional (Unix) v.3 with AntiVir Guard, we recommend and support dazuko3/dazukofs.

The installation script will also install dazuko3, if it detects the needed build components on your system:

- C compiler cc,

- C compiler gcc,

- kernel sources (kernel versions 2.6.18, 2.6.20, 2.6.22, 2.6.24, 2.6.26 or 2.6.27).

However, if you want to use dazuko2, this Chapter offers some basic instructions.

If the attempt to install dazuko with the product's install script fails, you have to compile the module yourself.

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

▶ 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 installation pack for SunOS (Sparc and i386) contains a binary module and you do not have to install it on this platform yourself.

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

8.1 Compiling Dazuko on your own

✓ Make sure that the source code for UNIX kernel is in */usr/src/linux*. If not, install or link 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 proceed with the installation. In the worst case, Dazuko will not be integrated into your UNIX kernel and the AntiVir Guard will not start. A message will be displayed and you can solve the situation afterwards.

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

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

- Check the configuration of your computer with the configure script. This information 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
  ```

  ↳ Depending on your operating system, you will receive the file *dazuko.o* or *dazuko.ko* in the temporary directory. AntiVir installation script will ask for the path to this file later.

Further information on Dazuko can be found on the website: http://www.dazuko.org. You may find distribution-specific details already documented in the FAQ section.

8.2 Known Issues with dazukofs

Mounting dazukofs

It is highly recommended to mount dazukofs very early during system startup, via */etc/fstab*, for optimum functionality and protection.

It is not recommended to unmount dazukofs, once loaded.

For more details, please refer to the dazukofs documentation: http://dazuko.dnsalias.org/files/README-dazukofs

Mounting removable media

Removable media such as USB-sticks and CD-ROMs should be automatically mounted. Else:
- If the media is not mounted via dazukofs, it is not protected;
- If it is mounted via dazukofs, you cannot unmount the media without unmounting dazukofs first (which can break some applications).

Scanning on-access: symlinks

Please note how dazukofs handles symlinks: In case a folder is mounted as dazukofs and a file (*file.a*) within that folder is a symbolic link to another file (which is not in a folder mounted as dazukofs, for example *file.b*), access to *file.a* is always granted, while *file.b* is not scanned, since it is not accessed through dazukofs.

9 Appendix

9.1 Glossary

Item	Meaning
Backdoor (BDC)	A backdoor is a program infiltrated in order to steal data or to control the computer, without the user's knowledge. This program is manipulated by third parties using a backdoor client via the Internet or local network.
cron (daemon)	A daemon which starts other programs at specified times.
Daemon	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.
dazuko	See www.dazuko.org: a cross-platform device driver that allows applications to control file access on a system.
Dialer	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. AntiVir detects Dialers.
Engine	The scanning module of AntiVir software.
Heuristic	The systematic process of solving a problem using general and specific rules drawn from previous experience. However, solution is not guaranteed. AntiVir uses a heuristic process to detect unknown macro viruses. When typical virus-like functions are found, the respective macro is classified as "suspicious".
Kernel	The basic component of a UNIX operating system which performs elementary functions (e.g. memory and process administration).
Logfile	also: Report file. A file containing reports generated by the program during run-time when a certain event occurs.
Malware	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).
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)
SAVAPI	Secure AntiVirus Application Programming Interface
Script	A text file containing commands to be executed by the system (similar to batch files in DOS)
Signature	A Byte combination used to recognize a virus or unwanted program.
SMP (Symmetric Multi Processing)	UNIX SMP: UNIX version for computers with parallel processors.

Item	Meaning
SMTP	Simple Mail Transfer Protocol: protocol for email transmission on the Internet.
SNMP	Simple Network Management Protocol: SNMP is used by network management systems to monitor network-attached devices for events that require administrative attention.
syslog daemon	A daemon used by programs for logging various information. These reports are written in different logfiles. The syslog daemon configuration is in */etc/syslog.conf*.
Test version	Without a license file, AntiVir Server/ Professional runs as a test version and it only reports the test virus EICAR. It will not block access to infected files. The update function is not available.
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

9.2 Further Information

You can find further information on viruses, worms, macro viruses and other unwanted programs at http://www.avira.com/en/threats/index.html .

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

9.3 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.

Issued Q1-2013

AVIRA

live *free.*™

Avira Operations GmbH & Co. KG
Kaplaneiweg 1 | 88069 Tettnang
Germany

Telephone: +49 7542-500 0
Facsimile: +49 7542-500 3000
www.avira.com