AVIRA Desktop for Unix v.1 [Linux]

User Guide

Contents

1. About this User Guide

1.1. Introduction

This manual describes the installation, configuration and operation of AVIRA Desktop for Unix v. 1 software and its components.

The Appendix contains a glossary that explains basic terms, as well as golden rules for protection against viruses.

Additional information and assistance is also provided on our website and by our Technical Support.

AVIRA Team

1.2. User Guide Structure

AVIRA Desktop for Unix User Guide consists in the following sections:

1. About This User Guide	The structure of the guide; signs and symbols.
2. Product Information	General notions about AVIRA software structure, functions, system requirements and licensing.
3. Installation	Instructions for installing AVIRA on your system.
4. Configuration	Instructions for optimum integration of AVIRA in your system.
5. Operating	AVIRA operating after installation; settings for virus/unwanted programs scanning; product's behavior when detecting viruses or unwanted programs.
6. Service	AVIRA Technical Support information.
Appendixes	Glossary for special terms and abbreviations, golden rules for protection against viruses.

1.3. Signs and symbols

The following characters and symbols are used in this manual.

Symbol	Explanation
✓	... shown before a condition that must be met before an action is carried out
▶	... shown before a step you perform
↳	... shown before the result that directly follows the preceding action
	... shown before a warning in case there is a danger of critical data loss or hardware damage
	... shown before a note containing particularly important information, e.g. on the following steps
	... shown before a tip that makes it easier to understand and use AVIRA

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

Emphasis in Text	Explanation
[Ctrl] + [Alt]	Key or key combination
D:\programs\AVIRA	File names and paths
Choose Component **Select All**	Elements of the software interface such as menu items, window titles and buttons in dialog windows
`copy *.* d:\`	User entries
http://www.avira.com	URLs
Characters and symbols	Cross-references within the document

2. Product Information

Unix computers are exposed to danger when exchanging and sharing files with Windows systems. Unix viruses have also made their presence known and every system needs protection. This is where AVIRA Products come in handy.

AVIRA Desktop for Unix is a comprehensive and flexible tool for confronting viruses and unwanted programs on your desktop and for reliable protection of your system.

Right from the beginning, two really important hints:

Loosing valuable files usually has dramatic consequences. Not even the best antivirus software can fully protect you against file loss.

- Ensure regular backups for your files.

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

- Ensure that you maintain your AVIRA up-to-date, using Automatic Updates. You will learn how to do this in this user guide.

2.1 Features

The essential features of AVIRA Desktop for Unix are:

- Simple configuration helped by additional configuration scripts.
- Command line scanner (on-demand): configurable scanning for all known Malware types (viruses, Trojans, backdoors, hoaxes, worms etc.).
- Resident guard (on-access): configurable behavior of the product when finding viruses or unwanted programs: clean, move, block, isolate programs or files; automatic removal of viruses or unwanted programs.
- Heuristic macro virus detection.
- Easy integrating in automatic jobs, as scheduled scanning.
- Automatic Internet update.
- Extensive logging, warning and notification functions for the administrator; sending email warnings (SMTP).
- Protection against modifying program files, by intensive self-testing.
- Optional user-friendly graphical interface, using a free additional module (see **AVIRA with Graphical Interface TKAVIRA**).

2.2 Licensing Concept

You are required to accept the license terms of AVIRA in order to be able to use AVIRA products.

After you acquire the license, you will receive a Registration Code you have to use for Registration at http://register.avira.com, in order to benefit of Standard Technical Support and Content Updates, which include constant virus definitions updates and software upgrades.

The Registration Code will be sent to you by AVIRA as a string in an email or annexed to the purchase document.

Registration has to be done as soon as the Registration Code is received. Based on Registration details, AVIRA delivers the Activation Key that should be used to activate the product for Standard Technical Support and Content Updates.

The Activation Key will be sent to you by AVIRA as an email file attachment called “avira.rck”.

Until activation, the Software can only be used as a limited version, without being possible to use all its functionalities for the entire licensing period.

For registering and activating the product, please follow the indications received in the appropriate email.

Registered Version

The range of features of a license include:

- Provision of the AVIRA version for downloading from the Internet
- Registration Code for enabling Update Service
- Detailed installation instructions (digital)
- Provision of PDF manuals for downloading from the Internet
- Update Service for the program files and the virus definition files via the Internet (for 1 year)
- Free change within a product line and crediting of existing licenses against upgrades/additional licenses
- Standard Technical Support.

You can extend the Update Service beyond the first year usually for twelve months.

Update Extension

Update Extension range of features include:

- Update Service for the program files and the virus definition files via the Internet (for 1 year)
- Standard Technical Support
- Provision of PDF manuals for downloading from the Internet
- Free change within product line and crediting of existing licenses against upgrades/additional licenses

2.3 AVIRA Operating Modes

AVIRA Desktop for Unix security solution consists in the following program components:

- AVIRA Command Line Scanner
- AVIRA Guard
- AVIRA Updater

AVIRA 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.

AVIRA Guard

… runs in the background. It guards the files against viruses and unwanted programs, when accessed by network users (on-access). It immediately blocks the access to infected files. The files can automatically be isolated, recovered or moved.

AVIRA Updater

… ensures that AVIRA is always kept up-to-date. It checks if there are any new files to download and automatically updates your software, if necessary.

2.4 System Requirements

AVIRA Desktop for Unix needs the following minimum requirements to be met on your system:

- Platform: i386
- Operating System: Linux with 2.2 Kernel and GLIBC 2.2 or better
- 8MB free hard disk space for product installation
- 10MB free hard disk space for the working directory
- 32MB free memory space (64 MB recommended)

2.5 Technical Information

AVIRA Guard is based on Dazuko (http://www.dazuko.org), an open-source software project. Dazuko is a kernel module, which allows file access control to AVIRA Guard daemon.
Please, note the license information in the installation subdirectory */legal*.

3. Installation

You can find the current version of AVIRA Desktop for Unix on the Internet or, if you have the AVIRA CD-ROM, you can install the files from it.

AVIRA is supplied as packed archive. This archive contains AVIRA Guard, AVIRA Command Line Scanner and AVIRA Updater.

You will be guided step-by-step throughout the installation in the following topics.

3.1 Getting the Installation Files

Downloading Installation Files from the Internet

- Type the following URL in your web browser:
http://www.avira.com/download/
- Download on your local computer the .tgz file located under AVIRA Desktop for Unix.
- Save the file in */tmp* folder on your computer.

Getting Installation Files from CD-ROM

- On the CD-ROM open
/EN/PRODUCTS/LINUX/DESKTOP
- Copy the .tgz file into a folder, for example in */tmp*.

Unpacking Program Files

- Go to the temporary directory:
cd /tmp
- Unpack AVIRA archive:
tar xzvf ai-lx-desktop-i386.tar.gz
  - ↳ in the temporary directory will then appear *avira-desktop-x.x.x* folder, where *x.x.x* is the current version number of AVIRA Desktop for Unix.
- Then go to the following directory:
cd /tmp/avira-desktop-x.x.x/src
- Unpack the kernel module Dazuko archive:
tar xzvf dazuko-x.x.x.tar.gz
  - ↳ in the temporary directory will then appear *dazuko-x.x.x* folder, where *x.x.x* is the current version of Dazuko.

3.2 Installing Dazuko Kernel Module

Dazuko kernel module is necessary on all platforms for AVIRA Guard's functionality.

Dazuko kernel module is necessary to support the resident scanner of AVIRA Guard.

AVIRA can also be installed without Dazuko kernel module, but in this case, it will run without AVIRA Guard. See **Installing AVIRA without AVIRA Guard**.

You must compile the module yourself, because your Linux 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 Linux kernel.

The further action is described below. Nevertheless, knowledge of Linux kernel compilation is needed, especially when errors are met. Further information about this can be found at: http://www.digitalhermit.com/linux/Kernel-Build-HOWTO.html.

Compiling Dazuko

- Make sure that the source code for Linux kernel is in */usr/src/linux*. If not, install it there. Information on this subject can be found in your Linux provider documentation.
- Check if you have on your computer the kernel compiling programs (for example *gcc*). If not, install the required packages. Information on this subject can be found in your Linux provider documentation.
- Your Linux kernel must be based on the source code from */usr/src/linux,* as in most of cases, especially in a Linux reinstallation. You can gain absolute certainty only by recompiling the installed kernel using exactly these sources.

If you are not certain about your Linux kernel status, you should perform again its installation. In the worst case, Dazuko will not be integrated in your Linux kernel. However, AVIRA checks this and will send you a notice about it.

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

```
cd /tmp/avira-x.x.x-desktop/src/dazuko-x.x.x
```

- Let the *configure* script check the configuration of your computer. Based on this information, it will provide appropriate guidance for further installation of the software:

```
sh configure
```

- Compile Dazuko:

```
make
```

Optionally: verify if the new installed module works with the computer's running kernel:

```
make test
```

You must keep the *dazuko.o* file in the temporary directory `tmp/avira-desktop-x.x.x/src/dazuko-x.x.x.` AVIRA installation script will need this file later.

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

3.3 AVIRA Initial Installation

AVIRA 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 AVIRA on the computer
- Copies the program files. Overwrites existing obsolete files
- Copies AVIRA configuration files. Existing AVIRA configuration files are inherited
- Optionally it creates a link in */usr/bin*, so that AVIRA could be called from any folder without needing a given path.
- Optionally it installs AVIRA Updater and the resident scanner AVIRA Guard.
- Optionally it configures an automatic start for AVIRA Updater and AVIRA Guard by system start.

The following steps must be made for the initial installation:

- Preparing Installation (see below)
- If Dazuko has not been compiled: **Installing AVIRA without AVIRA Guard**
- If Dazuko has been compiled: **Installing AVIRA with AVIRA Guard**

Preparing Installation

- Login as **root**. Otherwise, you don't have the required authorization for installation and the script returns an error message.
- Go to the directory in which you unpacked AVIRA:

```
cd /tmp/avira-desktop-x.x.x
```

Installing AVIRA without AVIRA Guard

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

- Type:

```
./install
```

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

```
1) installing command line scanner
creating install directory /usr/lib/AVIRA ... done
checking for existing /etc/avira.conf ... not found
copying bin/avira to /usr/lib/AVIRA ... done
copying vdf/avira.vdf to /usr/lib/AVIRA ... done
copying vdf/avira.conf to /usr/lib/AVIRA ... done
copying sh/configavira to /usr/lib/AVIRA ... done
```

↳ Then you will be asked if you want to create a link in */usr/bin*:

```
Would you like to create a link in /usr/bin ? [y]
```

- Answer with Y or [Enter]. With this option, you can call AVIRA from any directory, without needing a given path.

↳ Then, you are asked if you want to install AVIRA Updater:

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

You don't necessarily need AVIRA Updater to keep AVIRA up-to-date. You can perform this operation manually over the Internet. See **AVIRA Manual Update**. However, for the initial AVIRA installation, it is recommended to install the Updater. You can deactivate it in the configuration settings.

Installation with Updater:

If you choose to install AVIRA Updater (recommended):

- Type Y.

↳ AVIRA Updater is installed. Then, you are asked if Updater should be automatically run when the system starts:

```
copying sh/aiupdater to /usr/lib/AVIRA ... done

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

- Answer this question with Y or [Enter]. You can later make this setting manually.
  - ↳ The automatic system start is configured:

```
identifying startup script location … found (/etc/)
linking /etc/rc(LEVEL).d/(S/K)20aiupdater to /usr/lib/AVIRA/aiupdater ...
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].
- Confirm with [Enter].

Skipping AVIRA Guard:

- ↳ You are asked if you want to install AVIRA Guard:

```
3) installing AiGuard
Version 1.1.1 of AVIRA for Unix is capable of on-access,
real-time scanning of files.
...
There are several ways in which you can install AiGuard.

        module     - Dazuko will be loaded by the aiguard script

        kernel     - Dazuko is always loaded
                     (and should not be loaded by the aiguard script)

        no install - do not install AiGuard at this time
...
available options: m k n

How should AiGuard be installed? [m]
```

- Type N and confirm by pressing [Enter].

Start Configuration:

At the end, you can configure AVIRA:

```
4) configuring AVIRA
Would you like to configure AVIRA now? [y]
```

If you answer Y, AVIRA configuration script starts. You can make the configuration anytime later. We recommend that you first learn about the configuration options and then perform it.

- End this procedure by answering N.
  - You will see a report that indicates the completion of these features:

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

Installing AVIRA with AVIRA Guard

Make sure that the Dazuko kernel module has been compiled (see **Installing Dazuko Kernel Module**).

- Type:

```
./install
```

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

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

  - Then, if it is the first installation, you will be asked if you want to create a link in */usr/bin*:

```
Would you like to create a link in /usr/bin ? [y]
```

- Answer with Y or [Enter]. With this option, you can call AVIRA from any folder, without needing a given path.

Then, you are asked if you want to install AVIRA Updater:

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

You do not necessarily need AVIRA Updater to keep AVIRA up-to-date. You can perform this operation manually over the Internet. See **AVIRA Manual Update**. However, for the initial AVIRA 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 AVIRA Updater (recommended):

- Type Y.
  - ↳ AVIRA Updater is installed.

Then, you are asked if the Updater should be automatically run when the system starts:

```
copying sh/aiupdater to /usr/lib/AVIRA ... done

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

- Answer this question with Y or [Enter]. You can later make this setting manually.
  - ↳ The automatic system start is configured:

```
identifying startup script location … found (/etc/)
linking /etc/rc(LEVEL).d/(S/K)20aiupdater to /usr/lib/AVIRA/aiupdater
...
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 AVIRA Guard:

You are asked if you want to install AVIRA Guard:

```
3) installing AiGuard
Version 1.1.1 of AVIRA for Unix is capable of on-access,
real-time scanning of files.
...
There are several ways in which you can install AiGuard.

        module     - Dazuko will be loaded by the aiguard script

        kernel     - Dazuko is always loaded
                     (and should not be loaded by the aiguard script)

        no install - do not install AiGuard at this time
...
available options: m k n

How should AiGuard be installed? [m]
```

- 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/avira-desktop-x.x.x/src/dazuko-x.x.x/*, you must type:
`/tmp/avira-desktop-x.x.x/src/dazuko-x.x.x/dazuko.o`

  - ↳ The installation script checks if *dazuko.o* was correctly compiled and then copies the file for AVIRA Guard:

```
testing /tmp/avira-desktop-x.x.x/src/dazuko-x.x.x/dazuko.o ...
ok
detecting kernel version ... linux-2.4.18
copying /tmp/dazuko.o to /usr/lib/AVIRA/linux-2.4.18 ... done
checking for existing /etc/aiguard.conf ... not found
copying conf/aiguard.conf to /etc ... done
copying sh/aiguard to /usr/lib/AVIRA ... done
```

If the installation script reports any error on Dazuko, you probably should recompile your Linux kernel. For more information, see http://www.dazuko.org.

Start Configuration:

At the end, you can configure AVIRA:

```
4) configuring AVIRA
Would you like to configure AVIRA now? [y]
```

If you answer Y, the AVIRA configuration script starts. You can make the configuration anytime later. We recommend that you first learn about the configuration options and then perform it.

- End this procedure by answering N.
  - ↳ You will see a report that indicates the completion of these features:

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

3.4 Reinstalling AVIRA

You can always launch the installation script. There are more 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**), but inherited.
- Later installation of some components, e.g. AVIRA Guard or AVIRA Updater.
- Activating or deactivating the automatic start of AVIRA Updater or AVIRA Guard.

Reinstalling AVIRA

✓ First of all, you have to make sure that AVIRA Guard is stopped:
`/usr/lib/AVIRA/aiguard stop`

Then, you can start the reinstallation:

- open the temporary directory where you unpacked AVIRA:

cd /tmp/avira-desktop-x.x.x

- type:

`./install`

  - ↳ the installation script performs as described in **AVIRA Initial Installation**.

- Make the changes you need during installation procedure.

AVIRA is installed, with the desired features.

4. Configuration

You can tune AVIRA for optimal performance. Right after the installation, you have the possibility to make the most important adjustments.

You can modify these settings anytime, to optimize AVIRA performance.

After a short summary, you will be guided step-by-step in the configuration process:

- You can overview the **Configuration Files**. If you want to use the configuration scripts, you can skip this part.
- Explanations in dealing with **Configuration Scripts**.
- Specific AVIRA configurations are explained in:
  - **AVIRA Reports Configuration**
  - **AVIRA Guard Configuration**
  - **Regular Updates Configuration**
- Details about **Testing AVIRA Desktop for Unix**, to check if you have correctly configured it.

4.1 Overview

Configuration Files:

The configuration is defined in two files:

- *avira.conf* defines the automatic software update and the protocol for virus and unwanted programs detection.
- *aiguard.conf* defines the behavior of AVIRA Guard.


The settings can be made directly in the configuration files. This is not so difficult, but a comfortable way is using the script settings for program configuration. These scripts intercept the eventual errors and restart the necessary processes.

Configuration Scripts:

There are two configuration scripts in */usr/lib/AVIRA*:

- *configavira* edits the settings in *avira.conf*
- *configaiguard* edits the settings in *aiguard.conf* and then in *avira.conf*, in order to make them work with AVIRA Guard.

4.2 Configuration Files

This part describes the configuration files' content. These files are read by AVIRA when it starts. It will ignore empty lines or lines beginning with #.
They are delivered with predetermined values, which are significant for many applications. Some entries are deactivated or commented out, using # and they can be activated by deleting the # sign.


When you enter values manually in the configuration files, without using the configuration scripts, you must first restart the AVIRA Updater and AVIRA Guard, for the changes to take place.

▶ To do this, you have to type:

```
/usr/lib/AVIRA/aiupdater restart
/usr/lib/AVIRA/aiguard restart
```

avira.conf Configuration File

The settings in *avira.conf* are further described, in order of their appearance. These settings affect all AVIRA programs installed on your computer.

It is also possible to use a configuration script to set these parameters. More information you can find below.

If you manually change the updating parameters in a*vira.conf,* you must restart AVIRA Updater manually in order to make them effective:

- Type the command:

```
/usr/lib/AVIRA/aiupdater restart
```

AutoUpdate…

AVIRA software can check automatically for updates and can perform the update if necessary. Note that only the last selected option will be activated. These options are by default deactivated; therefore no automatic update is performed.
For daily updates, you can use:
`AutoUpdateDaily`
For updates at every two hours:
`AutoUpdateEvery2Hours`
For daily updates, additional settings can be made in order to specify the exact time, in HH:MM format:
`AutoUpdateTime  04:23`

EmailTo

Email address to receive notifications.
AVIRA can send emails to report a detected infection or unwanted program. In order to send emails, an address has to be specified (no default is provided).
EmailTo root@localhost

LogTo

Logging into a separate file.
All important AVIRA operations are reported to the syslog. These reports can be also written in a separate log file. For writing in a separate log file too, AVIRA needs the full path to it (no default provided).
LogTo /var/log/AVIRA.log

HTTPProxy…

Proxy server settings.
If a HTTP proxy server is required to reach the Internet, you can use this option for successfully performed updates.

These options must not be confused with those from other product specific config files. The settings made in a*vira.conf* influence only the Internet connection for automatic updates.

No defaults are provided, so you must specify the following:
- a HTTP proxy server (name or address);
- a port number;
- a username and password for HTTP proxy server (optional).

Example:

```
HTTPProxyServer  proxy.mydomain.com
HTTPProxyPort          8080
HTTPProxyUsername      user
HTTPProxyPassword      pass
```

Updater Keeps Backups…

AVIRA Updater normally replaces installed files with newer versions, when updates are available. Even if the new files are tested by AVIRA, you might want to keep backups of the earlier versions, in case something goes wrong. When activating this option, your existent files will be moved in newly created subdirectories of /usr/lib/AVIRA, named as: *updater-backup-YYYYmmdd-HHMMSS*.

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

Syslog…

Syslog settings.
All important messages are logged by AVIRA to the syslog. Two additional syslog options Facility & Priority can be specified through the following parameters:

```
SyslogFacility   user
SyslogPriority   notice
```

If these settings are not specified (or are commented out), the values shown above are defaults.

GnuPG…

GnuPG settings.
AVIRA Updater can check the updates for authenticity using GnuPG. For more information, see **Verify the Updates' Authenticity with GnuPG** section.
There are only 2 parameters you have to specify in avira.conf to use GnuPG:
- the path to GnuPG executable file:

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

- Specific additional options to be passed to GnuPG, normally not required for most installations.

```
GnuPGOptions     ...
```

Both parameters are initially commented-out and have no defaults.

Detect…

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

```
DetectDialer
DetectGame
DetectJoke
DetectPMS
```

Heuristics…

AVIRA is capable of using heuristics to determine if a file is malicious. Thus, new/ unknown malicious code is detected before performing an update. HeuristicsMacro deals with macros in Office documents. HeuristicsLevel deals with all types of files and can be set to a certain level of intensity: from 0 (disabled) to 3 (full intensity).

```
HeuristicsMacro
HeuristicsLevel 0
```

License

It defines the Registration Code and the Activation Key for your product. It may appear more than once in the file, defining several licenses.

- If you have only the Registration Code, than the concerning line will look like this:

```
License DhHTGp7r8GSs94gh58GscOFg
```

- If you have the Registration Code and the Activation Key, than the line will be:

```
License DhHTGp7r8GSs94gh58GscOFg etc/<activation_key>
```

aiguard.conf Configuration File

Here you can find short descriptions of *aiguard.conf* parameters, in the order of their appearance.

NumDaemons

Daemons Number:
The number of simultaneously running AVIRA Guard daemons can be set between 0 and 20. The default is 3 and it is appropriate for smaller standard computers. For computers with high traffic, a larger number would be necessary:
If the value is 0, AVIRA Guard is deactivated.

AccessMask

Access Mask:
Here is established the access type of AVIRA Guard when scanning files for viruses or unwanted programs:
1: scanning a file when opened;
2: scanning a file when closed;
3: scanning a file when executed.
The initial value is: `AccessMask 3`. You can sum the numbers for the events you want to activate.

Repair Concerning Files

Repairing Files:
AVIRA Guard is able to repair files right after access.
You need to activate the following option:
`RepairConcerningFiles`
This option is initially deactivated.

LogOnly, Rename… Move…

Action When Detecting Viruses or Unwanted Programs:
If *RepairConcerningFiles* option is not set or the repair is not possible, access to the file is blocked. The following three options define further action:
- *LogOnly*: no further action (Default value);
- *RenameConcerningFiles:* renaming the file by adding the .xxx extension.
- *MoveConcerningFilesTo*: moving the file in another folder. This folder will be automatically created, if it doesn't exist. For example:
`MoveConcerningFilesTo /home/unwanted`
You can activate only one of these options. If more than one is activated, AVIRA will choose the last one performed in the configuration file.

IncludePath

Scanned Folders:
AVIRA Guard scans the files of specified folders, including their subfolders. Usually, the data for the different users is in `/home` directory. The initial setting is:
`IncludePath /home`
You can specify only one folder in a command line. You can enter more folders, but they must be entered one by every command line. Example:
```
IncludePath /home
IncludePath /var
```

If no folder is specified, AVIRA Guard will not scan any files.

ExcludePath

Excluded Folders:
AVIRA Guard can exclude certain folders when scanning, for example a folder containing temporary files with AVIRA components (see **Defining Excluded Folders**). Any directories that are not specified using IncludePath option are

already excluded from scanning. There is no default setting.
You can specify only one folder in a command line (this includes all subdirectories). You can enter more folders, but they must be entered one by every command line. Example:

ExcludePath `/home/log`
ExcludePath `/home/tmp`

If you have activated *MoveConcerningFilesTo* option, that folder will be automatically excluded.

External Program

Starting External Programs When Finding Suspicious Files:
AVIRA Guard can start an external program when finding a virus or an unwanted program. This can send a notification or perform an action using AVIRA Guard options.
It is possible to send SMS, to call the appointed responsible person, to show a dialog window on the local screen or on other computer, to save the data in another format or another file.
You can use macros (starting with %) to pass as arguments to the external program. The following table shows the supported macros:

Option	Function
%h	Path to file (may contain spaces)
%f	File name only (may contain spaces)
%p	The full file name (%h / %f) (may contain spaces)
%U	The file's UID
%G	The file's GID
%s	File size
%m	File mode
%De	Event type
%DF	File system or partition where the file is (device)
%Dp	PID of the process
%Du	UID of the process
%Df	Operation's flag
%Dm	Operation's mode
%Sn	Virus/unwanted program's name
%Sa	Extra information (if available)

Dazuko 2.0.0 or higher is required in order to use this feature.

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

4.3 Configuration Scripts

You can comfortably setup AVIRA using a configuration script. The script intercepts the possible errors and restarts the necessary processes.

AVIRA has two configuration scripts:
- *configavira* edits the settings in *avira.conf*
- *configaiguard* edits the settings in *aiguard.conf* and then in *avira.conf*, in order to make them work with AVIRA Guard.

Using the script is very easy. If you want to perform AVIRA general configuration:
- you must type:

```
/usr/lib/AVIRA/configavira
```

If you want to perform AVIRA Guard configuration:
- you must type in:

`/usr/lib/AVIRA/configaiguard`

The script reads the current setting values from *avira.conf* or *aiguard.conf* then ask you to enter new values (if desired). Possible values will be shown, while the current values are set as default.

If you want to keep the current value:
- press [Enter].

If you want to change a value:
- enter the new value.

In the end, you can see the summary of the configuration. After using *configaiguard*, the following table appears:

```
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:      no
handling of concerning files: log only
include paths:                /home/testScan
exclude paths:
email notification:           no
specific logfile:             /var/log/server.log
update frequency:             every 2 hours (if aiupdater is
running)
http proxy server:            proxy.yourcompany.com:3128
syslog output:                user.notice

available options: y n

Save configuration settings? [y]
```

If you see a wrong setting:
- type N, to restart the configuration script and to correct the wrong values.

If all settings are correct:
- confirm with Y or [Enter], to save the configuration files with the new values.
  ↳ The script reports the saving of the configuration files. It shows information about AVIRA Guard and asks if you want to start AVIRA Guard:

```
saving configuration to /etc/aiguard.conf ... done
saving configuration to /etc/avira.conf ... done

Running aiguard
...
Would you like to start AiGuard using the new configuration? [y]
```

- Press Y or [Enter], to start AVIRA Guard.

↳ AVIRA Guard will start. If AVIRA Guard is currently running, it will automatically restart, to activate the new settings:

```
Starting AVIRA: aiguard-desktop
```

↳ Then, the script shows information about AVIRA Updater and asks if you want to start AVIRA Updater:

```
Would you like to start the updater using the new configuration?
[y]
```

- Press Y or [Enter], to start AVRA Updater.
  ↳ AVIRA Updater will start. If AVIRA Updater is currently running, it will automatically restart, to apply the new settings. Then the configuration is finished.

In the end, you can see the summary of the configuration.

4.4 AVIRA Reports Configuration

Sending Email Messages When Finding Viruses or Unwanted Programs

AVIRA can send an email when detecting a virus or an unwanted program.

- Run *configavira*:

`/usr/lib/AVIRA/configavira`

Confirm the settings by pressing [Enter], until you meet the option for email reports:

```
You may set AVIRA 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]
```

- Press Y.
  ↳ you will be asked for the email address:

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

- Type the email address. Example:

`root@localhost`

- Confirm all remaining settings with [Enter].

Now the email report is configured.

All reports about AVIRA updates will be sent to the email address you specified.

Setting Syslog Reports

AVIRA reports all important operations through *syslog*. You can specify the facilities and priorities for these reports.

If you have no experience working with syslog daemon, you should not change the default values. You can find further information on syslog daemon in your Linux documentation.

- Run *configavira*:

```
/usr/lib/AVIRA/configavira
```

- Confirm the settings by pressing [Enter], until you meet the option for *syslog facility*:

```
Regardless of the other configuration options, AVIRA 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 AVIRA use? [user]
```

- Type the new facility:
  - ↳ then you are asked for the *priority*:

```
Available PRIORITIES: emerg alert crit err warning notice info
debug
```

- Type the new priority.
- Confirm all remaining settings with [Enter].

Settings for AVIRA File

Apart from *syslog*, all reports can be written in a distinct log file.

- Run c*onfigavira*:

```
/usr/lib/AVIRA/configavira
```

- Confirm the settings by pressing Enter, until you meet the option for log file:

```
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 AVIRA to log to a custom file? [y]
```

- Press Y.
  - ↳ then you are asked for the log file path:

```
What will be the log file name with absolute path (it must begin
with '/')
```

- Enter the full path for the log file. Example:
`/var/log/avira.log`
- Confirm all remaining settings with [Enter].

Now the log file is configured.

4.5 AVIRA Guard Configuration

Defining Scanned Folders

AVIRA Guard can scan the folders you desire. The initial setting is */home*.

Generally, the user has access to */home* folder and its subfolders, so here is the greatest danger of virus or unwanted program occurrence. The system folders are usually accessed by the administrator. A permanent scanning on these folders would possibly cause unnecessary system resources costs.

AVIRA Guard scans the chosen folders and all their subfolders. To define the folders for scanning:

- Run *configaiguard*:
`/usr/lib/AVIRA/configaiguard`
- Confirm the settings by pressing [Enter], until you are asked if you want to reset the scanned folders:

```
AiGuard 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. You must specify at
least one path.

Current include paths = /home

available options: y n

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

- Press Y.
  - ↳ then you are asked for the paths to the desired folders:

```
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]
```

- Enter the paths individually. Confirm every path pressing [Enter]. After the last one, press [Enter] twice.

The prior paths list will not be kept. It will be deleted. So you must enter the entire paths list every time you reset it.

- Confirm all remaining settings with [Enter].

Now the scanned folders are defined.

Defining Excluded Folders

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

If you use AVIRA MailGate, then AVIRA Guard should exclude the spool folder and AVIRA MailGate's temporary folder. If not, AVIRA Guard will block the access of AVIRA MailGate to email attachments containing viruses or unwanted programs.

If there are infected folders among your scanned folders (see **Defining Scanned Folders**), exclude them from scanning.

The scanning will exclude the chosen folders together with their subfolders.

- Run *configaiguard*:

```
/usr/lib/AVIRA/configaiguard
```

- Confirm the settings by pressing [Enter], until you are asked if you want to reset the excluded folders:

```
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. AiGuard 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]
```

- Press Y.
  ↳ then you are asked for the paths to the desired folders:
- Enter the paths individually. Confirm every path by pressing [Enter]. After the last one, press [Enter] twice.

The prior paths list will not be kept. It will be deleted. So you must enter the entire paths list every time you reset it.

- Confirm all remaining settings with [Enter].

If you have activated *MoveConcerningFilesTo* option, that folder will be automatically interpreted as ExcludePath also.

Now the excluded folders are defined.

Setting AVIRA Guard number of daemons

You can set more AVIRA Guard daemons to scan file access simultaneously. This increases performance.

The number of these daemons can be set between 0 and 20.

The initial value is 3 and it is appropriate for standard computers. For computers with high traffic, a larger number would be necessary to scan an increased simultaneous file access. To avoid unnecessary memory usage, you should not use more daemons than required.

- Run c*onfigaiguard*:
`/usr/lib/AVIRA/configaiguard`
  - ↳ the first screen displays the number of daemons.
- Type the desired number of daemons.
- Confirm all remaining settings by pressing [Enter].

The AVIRA Guard number of daemons is now set.

Setting AVIRA Guard Scanning Method

AVIRA Guard can scan files when they are opened, closed and/or executed:
- By scanning files when opened, you can avoid opening, reading or copying infected files.
- By scanning files when closed, you can avoid writing, saving, copying or Internet downloading of infected files.
- By scanning files when executed, you can avoid virus spreading along with it.

By scanning files when opened and closed, you have a good protection. This is the default setting.

- Run *configaiguard*:
`/usr/lib/AVIRA/configaiguard`
- Confirm the settings by pressing [Enter], until you are asked if you want to scan files 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? [y]
```

- Type Y or N, according to your preference.
  - ↳ then you are asked if you want files to 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? [y]
```

- Type Y or N, according to your preference.
  ↳ then you are asked if you want files to 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]
```

- Type Y or N, according to your preference.

 If you answer all these questions with N, AVIRA Guard will be deactivated!

- Confirm all remaining settings by pressing [Enter].

The scanning method is now set.

Repairing Files in Real Time

AVIRA Guard normally blocks the access to an infected file, but it is able to repair infected files in real time (during access). If the file can be repaired, the user can regain access without danger. If the repairing is not possible, the access remains blocked. The process is always logged.

- Run config*aiguard*:
`/usr/lib/AVIRA/configaiguard`
- Confirm the settings by pressing [Enter], until you are asked if you want to repair the infected files:

```
If a concerning file is found, AiGuard 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? [n]
```

- Type Y for enabling file repairing.
- Confirm all remaining settings by pressing [Enter].

From now on, AVIRA Guard will clean the infected files.

Automatically Renaming or Moving Infected Files

If AVIRA Guard can not repair an infected file in real time or if this option is not activated, then it can rename or move that file. All this time, the access to the file is blocked and the process is logged.

- Run config*aiguard*:
`/usr/lib/AVIRA/configaiguard`
- Confirm the settings by pressing [Enter], until you are asked how AVIRA Guard should react to infected files:

```
When an alert is found, there are several ways in which AiGuard 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]
```

- If the infected files should be renamed, type R and confirm all remaining settings by pressing [Enter]. For the future, the infected files will have the *.xxx* extension added.
- If the infected files should be moved, type M.
  - ↳ you will be asked for the folder in which you want these files to be moved:

```
Which directory should they be moved to? []
```

- Enter the full path of this folder. Example: `/home/quarantine`
- Confirm all remaining settings by pressing [Enter]. From now on, all infected files will be moved to the specified folder.

This folder should be used exclusively for infected files (quarantine folder).

If *MoveConcerningFilesTo* option is active, this folder is automatically seen as *ExcludePath*.

- If the infected files should neither be renamed nor moved, type L and confirm all remaining settings by pressing [Enter]. From now on, the infected files will keep their name and location, but the access is still blocked and logged through *syslog*.

4.6 Regular Updates Configuration

The performance and effectiveness of antivirus software depend on updating. This is why AVIRA offers you the possibility to download current updates via HTTP from AVIRA servers and to automatically do this at regular intervals.
These updates ensure that AVIRA components, which provide security against viruses or unwanted programs, are always kept up-to-date.

All update processes use AVIRA command line scanner. The command `avira --update` updates AVIRA software at any time (see **AVIRA Manual Update**).

There are two possible methods to configure AVIRA updates:

1. you can use AVIRA Updater, which was delivered together with your AVIRA product and it is easy to configure. This is recommended, if you have little Linux knowledge and you only need to make a few adjustments.
2. you can use AVIRA and cron daemon. This is recommended if you have intensive Linux knowledge. In this way you must make the configuration yourself, but you can do it more freely.

Configuring Internet Connection for Updates

✓ Check if your Internet connection is functioning correctly. Usually this connection is already configured. If not, refer to your Linux documentation for the information you need.

Proxy server

If you are connected to Internet via HTTP proxy server, you must configure AVIRA accordingly:

- Run config*avira*:

`/usr/lib/AVIRA/configavira`

- Confirm the settings by pressing [Enter], until you meet the proxy server option:

```
If this machine is sitting behind an HTTP proxy server, you will need
to configure AVIRA 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? [y]
```

- Answer Y.
  - ↳ you are asked for the proxy server's name:

```
What is the HTTP proxy server name? []
```

- Type the proxy server's name. Example:
  `proxy.domain.com`
  - ↳ you are asked for the proxy server's port:

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

- Type the port. Example:
  `8080`
  - ↳ you are asked if you need an 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 AVIRA 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.
  ↳ you are asked for the username and password.
- Type the username and password.
- Confirm all remaining settings with [Enter].

The Internet connection is now configured.

Automatic Updates with AVIRA Updater Configuration

AVIRA Updater is a very simple daemon, which performs the following command at fixed intervals: `avira --update`

To enable the following settings, you must first install AVIRA Updater. This is also the case, if you have performed **AVIRA Initial Installation**. If it is not the case, you will have to perform **AVIRA Reinstallation**.

You can define the following options:

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

- Run config*avira*:

`/usr/lib/AVIRA/configavira`

  ↳ first, you are asked how often you need AVIRA to check for updates:

```
AVIRA is equipped with an Automatic Internet Updater. At specified
intervals, AVIRA will connect to an updater server to check for newer
versions of the AVIRA engine or the data files. If a newer
version is available, AVIRA will automatically download and install
the updates without requiring any special attention. This allows AVIRA
to be kept current against attacks and problems.

AVIRA 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 AVIRA check for updates? [n]
```

- Choose:

- N, if you don't want automatic updates
- 2 for updates every 2 hours
- D for daily updates.

  ↳ If you choose daily updates, you are then asked to 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 AVIRA 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? [RANDOM]
```

- Enter the time in HH:MM format

- OR -

type R for random time.

- Confirm all remaining settings by pressing [Enter].

The automatic updates are now configured. AVIRA Updater will automatically start (if it was not yet performed) or restart (if already active).

Manual Operating of AVIRA Updater

If you want to start AVIRA Updater:

- Type:

```
/usr/lib/AVIRA/avupdater start
```

If you want to stop AVIRA Updater:

- Type:

```
/usr/lib/AVIRA/avupdater stop
```

If you want to set AVIRA Updater status:

- Type:

```
/usr/lib/AVIRA/avupdater status
```

Performing Cron Updates

Performing updates with cron is highly recommended!

If you are an experienced Linux user, you can use cron daemon to perform automatic AVIRA Updates. Cron daemon is used to cyclical run system processes. Using cron for updates, you have more configuration possibilities at your disposal, than with AVIRA Updater. You can find further information in your Linux documentation.

Example:

- Enter the following cron job in */etc/crontab*:

```
45 */2 * * * root /usr/lib/AVIRA/avira --update –q
```

↳ this command activates updates every 2 hours, but performs them 15 minutes ahead of the set hours: 0:45, 2:45; 4:45 … The –q parameter states that no report will be given (see **Options**).

Automatic Start of AVIRA Updater

If you do not use cron, you can use AVIRA Updater. If you have performed **AVIRA Initial Installation**, your system is ready.

If AVIRA Updater has not yet been automatically activated by system start:
- You have to perform **Reinstalling AVIRA**, for the necessary settings.

Verify the Updates' Authenticity with GnuPG

GnuPG is a free alternative to PGP (Pretty Good Privacy). With GnuPG the updates authenticity can be verified.

It is highly recommended to use GnuPG, however this requires Linux and GnuPG knowledge. If errors are made during configuration, there is a danger to deactivate AVIRA updates. For further information on GnuPG, please visit: 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 a manual with further information about GnuPG and its features.
- Generate your PGP key pair, as described in the documentation.
- Import AVIRA's public PGP key (this key is included in the product kit, in the /pgp subdirectory):

```
gpg --import avira.gpg
```

- Display the fingerprint of the key:

```
gpg --fingerprint support@avira.com
```

  ↳ the 40-character fingerprint is displayed.
- Check that the fingerprint corresponds with the one on our website (http://www.avira.com), in the Download section. Go on only if it is ok (i.e. the public key is indeed AVIRA's).
- Sign AVIRA's public key:

```
gpg --sign-key support@avira.com
```

- Change directory into /bin subdirectory of your AVIRA installation directory:

```
cd /tmp/AVIRA-.../bin
```

  ↳ (where instead of "…" is AVIRA product name and license). Here you should see the files *avira* and *avira.asc*
- Check the signature with:

```
gpg --verify avira.asc avira
```

  ↳ if you don't get any error messages, GnuPG is ready to use with AVIRA.
- Activate GnuPG for AVIRA. Enter the path to GnuPG executable file in */etc/avira.conf*:

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

This option can only be activated manually. Setting in the configuration script is not possible, for avoiding the danger of configuration errors.

- Restart AVIRA Internet Updater, for activating the changed settings in a*vira.conf*:

```
/usr/lib/AVIRA/aiupdater restart
```

Now, the updates will be verified for authenticity.

4.7 Testing AVIRA Desktop for Unix

After performing installation and configuration, you can test AVIRA functionality using a test virus. This will not cause any damage, but it will force the program to react when a computer scan is performed.

Testing AVIRA 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*
- Download the test virus on your computer.
  - ↳ according to AVIRA configuration and to test virus version, AVIRA Guard will block the saving and will send a message to logs.
- Try to access the test virus, for example by copying:

```
cp eicar.com eicar2.com
```

  - ↳ according to AVIRA configuration, AVIRA Guard will block the access and will eventually perform other actions, as renaming or moving the test virus.

Searching for Errors

If AVIRA Guard didn't perform the expected actions, you must check your configuration.

- Check if AVIRA Guard is running:

```
/usr/lib/AVIRA/aiguard status
```

- Start AVIRA Guard, if needed.
- In */etc/aiguard.conf* check if the folder you work in is one of the scanned folders (see **aiguard.conf Configuration File**).
- In */etc/aiguard.conf* check the *AccessMask* value. If it is set to 0, AVIRA Guard is deactivated.
- Check AVIRA Guard reports on your log file or in *syslog*, for locating the errors.

5. Operating

After concluding installation and configuration, AVIRA guarantees continuous scanning on your system. During operating, there will possibly be occasional changes in **Configuration**.

Nevertheless, there might be needed a manual search for viruses or unwanted programs. This is where you can use AVIRA command line scanner. This program enables searching by many specific targets. AVIRA command line scanner can be integrated in scripts and also regularly activated by cron jobs. An advanced Linux user has unlimited possibilities to coordinate optimum system scanning.

This chapter has the following structure:

- **AVIRA Command Line Scanner Overview** - an overview over the command line scanner's options.
- **Using AVIRA Command Line Scanner** - examples of using the command line scanner.
- **AVIRA with Graphic Interface TKAVIRA** - using AVIRA command line scanner with a graphical front-end.
- **Reaction to Detecting Virus/ Unwanted Programs** - some hints about what you should do when AVIRA has done its work.

5.1 AVIRA Command Line Scanner Overview

Run

You can launch AVIRA command line scanner with the command:
`/usr/lib/AVIRA/avira [-option] [folder […]]`

If you've placed a link in */usr/bin* when installing AVIRA (as recommended), then you can skip the path:
`avira [-option] [folder […]]`

If no directory is specified, AVIRA command line scanner will scan the current directory. If you need to scan a certain file, you have to specify its name:
`avira [-option] [folder] filename.exe`

Wildcards are also allowed when specifying filenames:
`AVIRA "*.exe"`
This will scan every file with.exe extension in the current directory. To prevent certain wildcards to be interpreted by the shell, you should include them in double quotes (").

AVIRA needs information about the installation folder if it is other than */usr/lib/AVIRA*. If, for example, AVIRA was installed in */usr/local/AVIRA*, you should launch the command line scanner using:
`avira --home-dir=/usr/local/AVIRA`

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.

`-C <filename>`	Name of the configuration file to be used. Default: */etc/avira.conf*
`--check`	Used with --update AVIRA just checks for updates and displays a message, but does not perform the update.
`-del`	When virus/unwanted program detected, infected files are deleted.
`-dmcnv`	Document templates are converted to documents.
`-dmda`	Deletes all macros, unconditionally.
`-dmdas`	Deletes all macros in a document, if one is suspicious.
`-dmdel`	Deletes documents with suspicious macros.
`-dmds`	Deletes suspicious macros from documents.
`-dmpack`	Compresses document templates.
`-dmse`	Sets AVIRA 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>`	Do not scan inside the specified directory (even if inside the scanning zone).
`--help`	Shows all possible options.
`--home-dir=<dir>`	AVIRA searches in <dir> for its own files (for example *avira.vdf*).
`--info`	AVIRA shows the list of all known viruses, Malware and unwanted programs.
`-kf<filename>`	AVIRA uses the license key from this specified file.
`-lang:DE`	AVIRA generates German messages.
`-lang:EN`	AVIRA generates English messages.
`--log-email=<addr>`	Sends a scan report to the specified email address (in addition to results displayed on the screen).
`-noboot`	The boot sector test is deactivated. This saves time in targeted scan operations, but otherwise it is not recommended.
`-nobreak`	Deactivates [Ctrl]+C and [Ctrl]+[Break]. 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`	AVIRA scans once a day only: this option checks if AVIRA was already run on that day.
`-onefs`	Ignores links to other file systems. This excludes folders (for example NFS folders) from scanning.
`-q`	“Quiet”: AVIRA 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>	Indicates the log file. In this filename you can use the following macros: -%d: Day -%m: Month -%y: year.
-ro	The log file is overwritten.
-rs	Messages about viruses or unwanted programs are output individually.
-s	Scans all subdirectories.
--temp=<dir>	Keeps its temporary files in <dir>.
--update	Performs an update, to keep the virus definition file (VDF) and programs up-to-date.
-v	An intensive scanning is performed, on all files. This option should be used in exceptional cases only, as for example after a virus detection/removal.
--version	Shows AVIRA version.
--warnings-as-alerts	Handles warnings as errors. Terminates the program when getting warnings, with the same exit codes as those 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).
@<rspfile>	AVIRA reads parameters from <rspfile> “response file”. In <rspfile>, every option must be on a separate line. This enables saving a combination of parameters as a file, for later use.

Exit Codes

AVIRA command line scanner issues exit codes after operation. Linux 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.
100	AVIRA has only displayed the help text.

101	Macro detected in a file (when –dmse option is used).
102	AVIRA doesn't start, because the parameter –once was used and the program was 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	AVIRA 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.

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

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

5.2 Using AVIRA Command Line Scanner

This paragraph shows examples of using the command line scanner.

When AVIRA Guard is active, using AVIRA command line scanner causes double file scanning:

1. With AVIRA Guard, if the file is open with AVIRA command line scanner.
2. With AVIRA command line scanner itself.

In order to avoid disturbance, you should first deactivate AVIRA Guard:
`/usr/lib/AVIRA/aiguard stop`
And remember to restart it after scanning:
`/usr/lib/AVIRA/aiguard start`

Performing Complete Scanning

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

The following parameters should be used:

`--allfiles` Scans all files.
`--alltypes` Detects all sorts of suspicious and unwanted files.
`-s` Scans all subfolders.

- the command is:

```
avira --allfiles -s --alltypes /
```

Performing Partial Scanning

Usually, scanning the folders that contain in- and outgoing data (Mailbox, Internet, Text folders) can be enough. These files are usually in */var*.

If there are any DOS partitions on a Linux system, these must be scanned, also.

You can use the following parameters:

`--allfiles`	Scans all files.
`-s`	Scans all subfolders.

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

- use the command:

```
avira --allfiles -s /var /mnt
```

Deleting Infected Files

AVIRA can delete files which contain viruses or unwanted programs. Optionally, AVIRA can first try to repair these files. The program will first overwrite the files and then it will delete them; this means that repairing tools will not recover them.

You can use the following options:

`--allfiles`	Scans all files.
`-del`	Deletes infected files.
`-e -del`	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 can be lost!

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

- type the command:

```
avira --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:

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

Deleting Suspicious Macros

AVIRA is provided with the so-called “macro viruses heuristic”. Hereby, macros which show typical virus fingerprints can be classified as “suspicious”, without actually detecting a known virus or unwanted program. These suspicious macros are reported.

AVIRA has the following options:

`-dmds`	Suspicious macros are deleted. It is possible that other virus-related macros to remain within the file.
`-dmdas`	All macros in a file are deleted if there is a suspicious one. It is possible that other useful macros to be deleted.
`-dmda`	All macros in all files are unconditionally deleted.

`-dmdel` Documents with suspicious macros are completely deleted. This is “the most drastic” method.

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

If you want to delete all macros in files with suspicious macros from */home/myoffice*:
▸ type the command:
`avira -dmdas /home/myoffice`

Converting Document Templates

AVIRA can:
- Convert document templates into documents after deleting macros.
- Compress document templates, so that macros are deleted together with their names and references. This avoids other anti-virus programs to react to these macro names and report a non-existing virus or unwanted program.

For converting templates into documents, AVIRA has the following options:

`-dmcnv` Document templates are converted to files.
`-dmda` Deletes all macros in all files.
`-dmpack` Compresses templates.
`-dmdas` All macros in a file are deleted, if there is a suspicious one. It is possible that other useful macros to be deleted.

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

If you want to delete all macros from */home/office-XXX* and to convert all templates to files:
▸ type the command:
`avira -dmda -dmcnv /home/office-XXX`

If you want to delete all suspicious macros from */home/office-XXX* and to compress the templates:
▸ type the command:
`avira -dmds -dmpack /home/office-XXX`

AVIRA Manual Update

AVIRA can be manually updated anytime. It is recommended that AVIRA should run as **root** when updating. The advantage is that AVIRA daemon processes (AVIRA Guard, SAVAPI, MailGate…) will be automatically updated, without interrupting running scan processes.

If AVIRA is not run as **root** when updating, it does not have the required rights for restarting AVIRA daemons. In this case, you must restart the daemons manually.

If you want to update AVIRA:
▸ type the command:
`/usr/lib/AVIRA/avira --update`

If you only want to know if a new AVIRA version is available, without performing the update:

- type the command:

```
/usr/lib/AVIRA/avira --update --check
```

Using Scripts for AVIRA Updating

Advanced Linux users can integrate AVIRA command line scanner with scripts, using the Exit Codes.

Example:

- write a script in the following form, for suppressing and replacing some AVIRA messages:

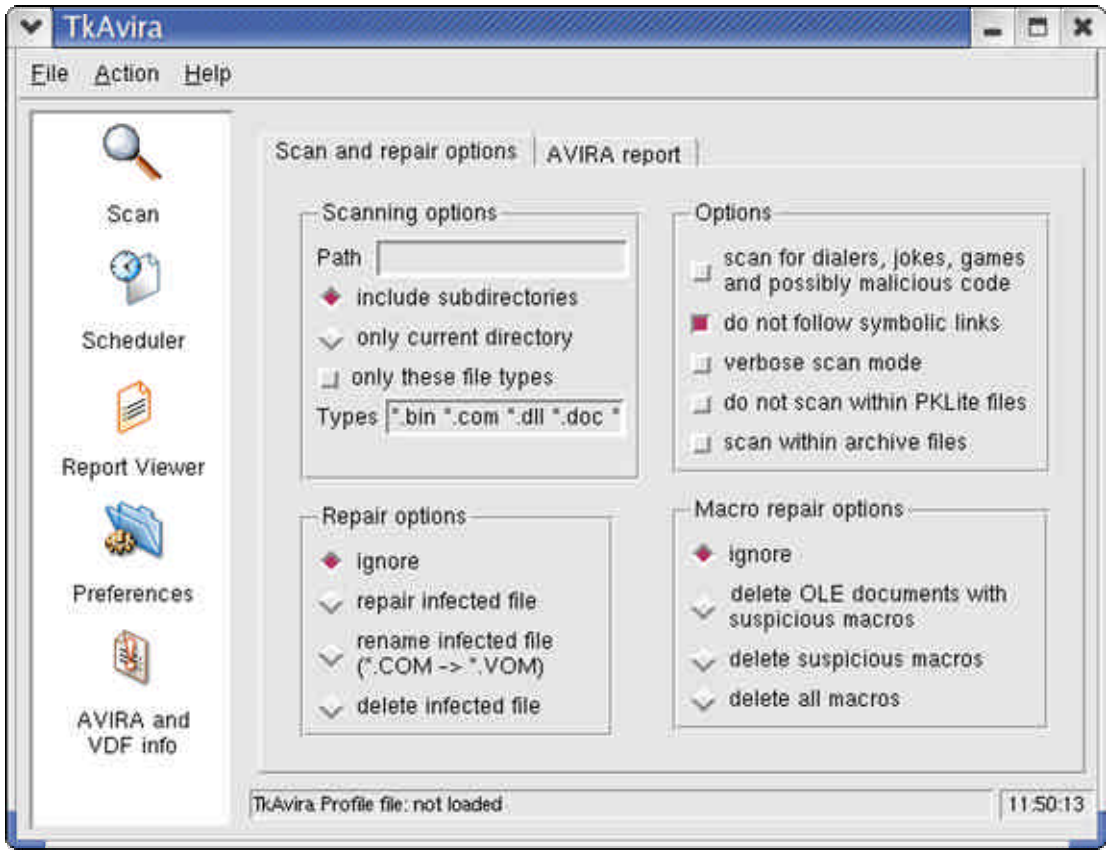
```
------------------ BEGIN SCRIPT ------------------
#!/bin/sh
/usr/lib/AVIRA/avira --update -q
case $? in
0)
echo "AVIRA is up-to-date"
          ;;
1)
echo "AVIRA has been updated"
;;
*)
echo "Update error"
;;
esac
------------------- END SCRIPT --------------------
```

5.3 AVIRA with Graphical Interface TKAVIRA

You can comfortably use the free open-source TKAVIRA front-end to benefit from the features of our antivirus products: AVIRA Desktop and AVIRA for Server. It is an attractive, user-friendly graphic interface, which helps you schedule and run AVIRA programs.

Main features

- You can use the on-demand component of AVIRA Desktop/for Server without learning any command line options.
- The report viewer offers the possibility to view and print virus scan reports.
- TKAVIRA Scheduler makes possible to benefit from the automatic Internet updates at specific times and intervals.



TKAVIRA Main Window

TKAVIRA is not an antivirus program itself. AVIRA GmbH is not liable for any problems arising out of using TKAVIRA and it does not offer any guarantees. For technical problems, please contact TKAVIRA's author. If you want to use AVIRA Desktop, please contact AVIRA GmbH. The use of TKAVIRA with an unregistered AVIRA Desktop is not recommended.

5.4 Reaction to Detecting Viruses/Unwanted Programs

If correctly configured, AVIRA 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, the 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 “sneaked” on your system.
- Perform targeted scanning on the data storage supports used.
- Inform your team, superiors or partners.
- Inform your system administrator and security provider.

Submit Infected Files to AVIRA

Please, send us the viruses, unwanted programs and suspicious files that our product does not yet recognize or detect. 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 email gateway.

6. Service

6.1 Support

You can find information on our complete support service at http://www.avira.com/support. Our competent and experienced experts are at your disposal. They will answer to your questions and will help you with the tricky technical problems.

Email Support

You can get email technical support at support@avira.com.

6.2 Contact

Address: Grabenstrasse 2
D-88069 Tettnang
Germany
Phone: +49 7542 500 400
Fax: +49 7542 500 418
Email: office@avira.com

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

Appendixes

Glossary

Item	Meaning
Cron (Daemon)	A daemon that starts other programs on specified times.
Daemon	A background process for Linux systems. On average, there are about a dozen daemons running on a computer. These processes usually start up and shut down with the computer.
Dialer	Paid dialing program. When installed on your computer, this program builds a Premium Rate Number Internet connection, charging you at higher rates. This can lead to huge phone bills. AVIRA recognizes dialers.
Eicar	European Institute for Computer Antivirus Research, which amongst other activities, offers you the possibility to use a test virus. For more information: http://www.eicar.org.
Engine	The scanning module of AVIRA software.
GPL	General Public License: an alternative to commercial licensing concept. Briefly, the software is distributed for free, but it must be used and kept as such.
Heuristic	The systematic process of solving a problem using common-sense rules drawn from previous experience. AVIRA uses a heuristic process for detecting unknown macro viruses. When typical virus-like functions are found, the respective macro is classified as “suspicious”.
Kernel	The base component of a *nix operating system, which performs elementary functions (e.g. memory-, process administration).
Log File	Also: report file. A file containing reports generated by the program at run-time, when a certain event occurs.
Malware	Malware is usually used for describing any form of malicious software like viruses, trojans, malicious active content, etc. The major categories of malwares are represented by viruses, worms, trojans and hoaxes.
MIME	Multipurpose Internet Mail Extensions is a standard used to integrate files into Internet emails. In addition, MIME supports multipart emails, enabling conveying different file types in a single email.
MTA	Mail Transfer Agent: a program that supports email sending over SMTP, for example sendmail, postfix, exim.
Quarantine directory	The directory where all infected files are moved and the user’s access is blocked.
Root	The user with unlimited access rights for system administration.
(Virus) signature	A combination of strings used to recognize a virus or an unwanted program.
Script	A text file containing commands to be executed by the system.
SMTP	Simple Mail Transfer Protocol: protocol for email transport on Internet.
syslog daemon	A daemon used by programs for logging various information. These reports are written in different log files.

	The *syslog* daemon configuration is in */etc/syslog.conf*.
Unwanted Programs	The name for programs that do not directly harm the computer, but are not desired by the user or administrator. These can be backdoors, dialers, jokes and games. AVIRA detects various types of unwanted programs.
VDF (Virus Definition File)	File with known virus signatures. Maintaining this file updated is most important.

Further Information

You can find further information on viruses, worms, macro viruses and other unwanted programs at http://www.avira.com, following the “About Malware” link.

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 backup 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 with virus infection operations and establish all steps for virus elimination.
- Organize an emergency plan as a precaution for avoiding damage due to destruction, robbery, 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 a good protection against viruses.

AVIRA GmbH
Grabenstrasse 2
D-88069 Tettnang, Germany
Phone: +49 7542 500 400
Fax: +49 7542 500 418
Email: office@avira.com
Internet: http://www.avira.com

Version: September 2004