



DATENTECHNIK GMBH

AntiVir[®] **for Linux**

A Brief Guide

Copyright © 1999-2000 by
H+BEDV Datentechnik GmbH
Lindauer Strasse 21, D-88069 Tettnang

Tel: (+49) 7542/93040
Fax: (+49) 7542/52510
Internet: <http://www.hbedv.com>
Mailbox (+49) 7542/52110

Please address all feedback and queries concerning
AntiVir[®] for Linux to: linux_support@antivir.de

Queries concerning sales (update service, licence
extensions, other anti-virus software by H+BEDV)
should be addressed to: vertrieb@antivir.de



About AntiVir[®] for Linux

AntiVir[®] for Linux is an efficient anti-virus program based on the tried-and-tested AntiVir[®] software by H+BEDV. This program can be used to scan systematically for viruses and repair infected files using various command line parameters.

To protect your electronic post office under Linux against viruses we offer a further anti virus tool: AntiVir for Linux MailGate. AntiVir MailGate is a store and forward agent which is compatible with numerous common Mail Transport Agents (MTA). It operates at high speed, is easy to configure and checks both incoming and outgoing e-mails.

How to install AntiVir[®] for Linux

Installing the AntiVir CD-ROM

- ➔ Insert the AntiVir CD-ROM in your CD drive and insert your licence disk containing the file 'hbedv.key' in the 3 ½" drive.
- ➔ Copy all files from '[language]\PRODUCTS\LINUX\' in the directory 'GLIBC' or 'LIBC5' from the directory 'SERVER\SETUP' to a temporary directory on your computer.
- ➔ If you have registered your AntiVir for Linux, also copy the file 'hbedv.key' from your licence disk to the temporary directory.
- ➔ Enter the script './install.sh' as the root (or as a user with write-access to /usr/lib and /usr/bin):

```
sh ./install.sh
```

The script will then copy the necessary files to the directory '/usr/lib/AntiVir'.

- ➔ If you enter ☒ in response to the query 'Create symbolic link?', a symbolic link to '/usr/lib/AntiVir/antivir' in the directory '/usr/bin' will be created. This symbolic link allows you to start AntiVir for Linux without entering the entire path.
- ➔ If you have registered your AntiVir for Linux, copy the file 'hbedv.key' to the directory '/usr/lib/AntiVir'.
- ➔ The temporary directory can now be deleted again.

Installing 'avlinux.tgz'

If you obtain AntiVir for Linux via Internet or via a Linux-Distribution, you will usually receive a file named 'avlglibc.tgz' or 'avlibc5'.

- ➔ Copy the file 'avlinux.tgz' to a temporary directory, for 'avlglibc.tgz' e.g.:

```
mkdir /tmp/av.inst
cd /tmp/av.inst
cp /[path]/ avlglibc.tgz
```

- ➔ Unpack the archive using the command

```
tar xzvf avlglibc.tgz
```

- ➔ Complete the installation process with the command

```
./install.sh
```

- ➔ Delete the temporary directory

```
rm -f /tmp/av.inst
```

Starting a scan with AntiVir® for Linux

- ➔ Load AntiVir for Linux from the directory '/usr/lib/AntiVir' using the parameter '-allfiles':

```
/usr/lib/AntiVir/antivir -s -allfiles
```

The path points to the installation directory of AntiVir for Linux. If a symbolic link has been set up, there is no need to enter the path.

AntiVir for Linux will now test all files in the current directory without any further inputs. Detected viruses are not deleted in this mode, but any abnormalities such as a destroyed file or a virus are logged in the report file of AntiVir for Linux.



In our experience, it is not essential to check all the directories of a Linux system, as the amounts of data involved would take up too much time. As a rule, it should be enough, even after installation, to check the directories containing incoming and outgoing data (mailbox, Internet, test directory). If there are mounted DOS partitions on the Linux system, the partitions should be checked too. The command line for a scan would then be as follows, for example:

```
/usr/lib/AntiVir/antivir -s -allfiles /var /m
```

Summary of command line parameters



AntiVir for Linux can be used to scan systematically for viruses and repair infected files using various commands. Do make sure, however, that you select logical combinations of parameters.

-? or **-h** allows a summary of all current command line parameters to be displayed on the screen.



Please decide exactly which parameters you wish to use **before** starting a scan. This is particularly important in the case of all parameters involving the deletion of files or macros, as these data will be lost - unless you have a (non-infected) backup.

-allfiles	Scan all files
-s	Scan all subdirectories in addition
-nolnk	Do not follow symbolic links
-onefs	Do not follow symbolic links to other file systems. This allows you to omit directories mounted by NFS, for example.
-noboot	Deactivate boot record test
-nobreak	Prevent scans from being interrupted with the key combination Ctrl + C or Ctrl + Pause
-nodef	Scan specified file types only (e.g. *.DOC)
-cf<filename>	Activate CRC test. <filename> is the wildcard for the name of the CRC database.
-v	Scan whole files (whereby incorrect detection cannot be ruled out)
-e	Repair infected files. Irreparable files are deleted!
-ren	Rename infected files (e.g. *.COM > *.VOM; *.EXE > *.VXE)
-del	Delete infected files
-dmdel	Delete Word documents containing suspicious macros
-dmds	Delete suspicious macros
-dmda	Delete all macros
-dmdas	Delete all macros if a suspicious one is found
-dmcnv	Convert templates
-dmpack	Pack template data table

- dmtl<value>** Set trigger threshold to token length specified as <value>
- r1** Only write infections and alarms to report file
- r2** Record all scanned paths in addition to /r1
- r3** Record names of all scanned files
- r4** Select detailed report mode
- rs** Display virus messages on one line
- rf<filename>** Create report file with the name <filename>
%d = day, %m = month, %y = year (2 digits each)
- ra** Append new report files
- ro** Overwrite existing report file
- q** Display virus and error messages only
- once** Run AntiVir once a day only
- x<dir>** Make AntiVir search for its own files, e.g. 'antivir.vdf' in <dir>
- if<filename>** Make AntiVir use the specified INI file
- kf<filename>** Make AntiVir use the licence file substituted for the wildcard
<filename>
- /@<rspdatei>** Read parameters from the file <rspdatei>, with each option in
a separate line



Tip: Begin by starting a scan in the directories in which data are moved around ('/var') and in the mounted DOS partitions. If viruses are found, you should then check the report file to see if it includes any destroyed files. Only carry out repairs with the '-e' parameter once you are absolutely sure that you no longer need these destroyed files.

Examples: Check all files in the directory '/var' (these are the kind of directories in which most of the "temporary junk" is stored, e.g. e-mails, temporary files, various items from the Internet, ...):

```
antivir -s /var
```

or check program files and archives in the directory '/usr':

```
antivir /usr -s
```



Note: bash expands command line parameters containing wildcards (* or ?). If you wish to suppress this expansion, you must place such parameters in quotes.

To check all files in the directory /var/spool and below, for example, enter the following:

```
antivir "/var/spool/*" -s
```

It is also possible to quote the character "*" with a "\", for example:

```
antivir /var/spool/\* -s
```

List of return codes:

- 0:** Program terminated normally, no viruses, no errors
- 1:** Virus found in file (or boot record)
- 2:** Virus found in memory (possibly active)
- 100:** AntiVir only displayed help text
- 101:** Macro found in a file
- 102:** AntiVir is unable to start because the parameter '-once' is selected and it has already been run once today
- 200:** Program aborted due to lack of memory
- 201:** Specified response file not found
- 202:** '@<rsp>' specified in a response file
- 203:** Invalid parameter specified
- 204:** Invalid directory specified
- 205:** Unable to create specified report file
- 210:** AntiVir unable to find one of the necessary DLLs
- 211:** Program aborted due to failure of self-check
- 212:** File 'antivir.vdf' not found / read error
- 213:** Initialisation error

If you have specified a different directory for AntiVir (e.g. in order to use AntiVir in a "chroot" environment), please enter '-x<Pathname>' as the parameter. AntiVir will then search for itself (for the self-test) and the virus database (antivir.vdf) in this directory. If the parameter '-x...' is not specified, AntiVir will search for itself using the environment variable 'PATH'.

Please note that AntiVir uses the standard output (console) for ongoing status displays. This means that control characters are displayed which – when re-directed to a file – look rather strange. In order to write AntiVir report displays to a file, please use the parameter "-rf<Filename>". The specified report file will be overwritten by default. In order to attach new report files to an existing file, please use the parameter "-ra".

It is of course possible to send stdout and stderr to /dev/null:

```
antivir -rf/var/log/antivir -ra >/dev/null 2>&1
```



Please address all feedback and queries concerning AntiVir® for Linux to: linux_support@antivir.de

Licence file, Fast Update Service and registration

Your AntiVir for Linux comes with a licence file without which AntiVir for Linux can only be run in a non key mode. Your licence file will release AntiVir according to the purchased AntiVir licence and update service.



Certain parameters can only be released for use once AntiVir for Linux has located the valid licence file in the installation directory.

Keeping up to date is the only way to guard against new viruses. To give you the security of knowing that you are using the latest version of AntiVir for Linux, we have devised the Fast Update Service with different update intervals.

Depending on the required degree of security, you can choose between two-monthly updates (FUSE 6 = **F**ast **U**pdate **S**ervice inclusive **6** updates) and the weekly update service (FUSE 6/wi = **F**ast **U**pdate **S**ervice inclusive **6** updates with further updates via internet) each for a period of one year. The updates via internet are generally issued once a week. All updates can be downloaded from our Internet server or via our mailbox.

You can register with H+BEDV as soon as you receive this program package. As a registered user, you will enjoy two major advantages: unrestricted access to all our support channels and you will receive the two-monthly updates automatically by post.



Please address all queries concerning sales (update service, licence extension, information on other anti-virus software by H+BEDV) to: vertrieb@antivir.de