



RAVMD file

Release Date: December 17, 2002

Product version: 8.4.1

Document revision: 2.0

Address: 223, Mihai Bravu Blvd, 3rd district, Bucharest, Romania
Phone/Fax: +40-21-321.78.03, Hotline: +40-21-321.78.59

Copyright © since 2001 GeCAD Software® S.R.L.

All rights reserved. This material or parts of it cannot be reproduced, in any way, by any means.

The product and the documentation coming with the product are protected by GeCAD Software's copyright.

GeCAD Software reserves itself the right to revise and modify its products according to its own necessities.

This document describes the product at this writing and may not correctly describe the latest developments. For this reason, we recommend you to periodically check our website, <http://www.ravantivirus.com>, for the latest versions of product documentations.

GeCAD Software cannot be hold responsible for any special, collateral or accidental damages, related in any way to the use of this document.

GeCAD Software's entire liability, depending on the action, cannot go beyond the price paid for the product described in this material.

GeCAD Software does not guarantee either implicitly or explicitly the suitability of this material for your specific needs. This material is provided on an "as-is" basis.

GeCAD Software trademarks: GeCAD, GeCAD Fast Commander, GFC, RAV Reliable AntiVirus, A.V.A.C., RAlert, RAVUtil, RAVeSpy, R.A.C.E., RAX, WisDOM.

The following are registered trademarks of their respective owners: Times New Roman, Courier, Arial, IBM, OS/2, Intel, Microsoft, MS-DOS, Windows, Windows95, Windows98, WindowsNT, QEMM, F-PROT, TBSCAN, VirSCAN, TBAV, DSAV, DrWEB, AVP, MSAV, MS Office, MS Word, MS Access, MS Excel, MS Visual Basic, NetWare.

Terms and conditions of the License Agreement

RAV Reliable AntiVirus is a registered trademark of GeCAD Software S.R.L. (hereafter referred as "GeCAD Software"). All the products from the **RAV AntiVirus** family are offered to our clients under the terms and conditions of the License Agreement accompanying all the products of GeCAD Software.

Before installing or using The Software, please read carefully this License Agreement, because it represents a legal agreement between you and GeCAD Software for the software product you are installing, which includes the software itself and the related documentation. By installing or otherwise using the software, you accept all the terms and conditions of this agreement. If you do not accept the terms of this agreement, you do not have the rights to install or otherwise use The Software.

On the distribution CD-ROM, you may find other programs, in addition to the one you have bought. These programs are offered for evaluation only and are the object of separate terms of license. These terms are included in the **Evaluation license** section of the **License Agreement**.

CONTENTS

RAVMD file	4
<i>NAME</i>	4
<i>SYNOPSIS</i>	4
<i>DESCRIPTION</i>	4
<i>DEFINITIONS</i>	4
<i>OPTIONS</i>	5
<i>EXIT STATUS</i>	7
<i>BUGS</i>	7
<i>SEE ALSO</i>	7

NAME

ravmd - rav mail scanning daemon

SYNOPSIS

```
`${BINDIR}/ravmd [-cdfhtvugsLTBIEDR] [--config=config_file][--dump_conf=config_file]
[--foreground] [--help] [--testconf=config_file] [--version] [--user=user_name][--group=group_name]
[--syslog] [--license] [--temp-path=directory] [--bin-path=directory] [--lib-path=directory]
[--etc-path=directory] [--data-path=directory] [--rave-path=directory]
```

DESCRIPTION

DEFINITIONS

“filter client”

A program that resides in the `\${BINDIR}` directory and whose name depends on your MTA (i.e. **ravexim**, **ravsendmail**, **ravpostfix**, etc.). Its function is to hook the MTA’s e-mail flux and pass every mail to **ravmd** for scanning. Depending on the response the “filter client” is receiving from **ravmd**, it will deliver or discard the respective mail message.

ravmd is powered by the platform independent *RAV Engine*, so it can detect and clean all malwares detected by this (i.e. Linux, Windows, DOS or Unices-based, viruses, macros, Trojans, hoaxes, etc.). The program can scan e-mail files in MIME format containing attachments encoded with: **base64**, **quoted-printable**, **uuencode**, **7bit**, **8bit**.

ravmd also supports:

- e-mail *content filtering* for the e-mail subject, attachment file names and message body; and
- an antispam functionality, based on the new bulk mail module, integrated in **ravmd** starting with its version 8.4.0, and older features like **Real-time Blackhole List** (RBL) or **White-Black List** (WBL), available in **ravmd** since version 8.3.3. For more details, please read the *ravmd configuration file* section in the *User Guide for RAV AntiVirus for Mail Servers*, available [here](#).

When **ravmd** starts, it loads its configuration from `\${ETCDIR}/ravmd.conf. If there are some errors (i.e. missing or bad format of these files), **ravmd** exits with non zero status. In all the other cases, **ravmd** starts in background and binds an UNIX socket `\${DATADIR}/run/_ravmdcom) and listens it for “filter clients” queries. When a “filter client” connects to this socket, **ravmd** forks and the child will process “filter client” commands.

If started with `--syslog`, the daemon uses the system mail info log file for logging. The following command should display that file:

```
cat /etc/syslog.conf |grep -e ^[^\#].*mail\[^\ acdenw] | \  
awk '{print $2}'
```

If you would like to perform periodic updates to the RAV AntiVirus engine and virus signature files, you should use a scheduling daemon (**cron**, **fcron**, **ucron**...) to execute the `ravmdupdate.sh` script located in `${BINDIR}`. Please modify that script file to fit your configuration. We recommend configuring the scheduling process so that the update process is executed once or twice an hour.

*Example for **fcron**:*

```
su  
fcrontab -e
```

Insert the following line to run `ravmdupdate.sh` every 30 minutes:

```
@ 30 ${BINDIR}/ravmdupdate.sh
```

*Example for **cron**:*

```
su  
crontab -e
```

Insert the following line to run `ravmdupdate.sh` every 30 minutes:

```
*/30 * * * * ${BINDIR}/ravmdupdate.sh
```

OPTIONS

Arguments are mandatory for both long and sort options.

-c, --config=config_file

Use the `config_file` instead of `${ETCDIR}/ravmd.conf`.

-d, --dumpconf=config_file

Print the configuration from `config_file` to **stdout**.

-f, --foreground

Run the daemon in foreground instead of background.

-h, --help

Display the help screen.

-t, --testconf=config_file

Test the specified `config_file` configuration file.

-v, --version

Display the version of `ravmd`.

-u, --user=user_name

-g, --group=group_name

Use `user_name` and `group_name` as real user and real group for `ravmd` processes. By default the current user `uid` and `gid` are used.

Important: For security reasons, when `ravmd` is executed as root, it is highly recommended to use these options in order to drop the superuser privileges to an unprivileged user.

-s, --syslog

Use `syslog` daemon instead of RAV logging system.

-L, --license

Display the current license.

-T, --temp-path=directory

The temporary directory used to unpack large mail attachments (i.e. archived files).

-B, --bin-path=directory

The path to RAV binaries. The default value is `${BINDIR}`.

-l, --lib-path=directory

The path to RAV libraries. The default value is `${LIBDIR}`.

-E, --etc-path=directory

The path to RAV configuration files. The default value is `${ETCDIR}`.

-D, --data-path=directory

The path to RAV data files (`rave`, `log`, `run`, `tmp`, `ravmd.key`, etc.). The default value is `${DATADIR}`.

`-R, --rave-path=directory`

The path to RAV Engine directory (**rave**). The default value is `${DATADIR}/rave`.

EXIT STATUS

On error it returns non-zero, else returns zero.

BUGS

Please mail bug reports and suggestions to: ravteam@ravantivirus.com

SEE ALSO

`ravmd.conf(5)`, `ravav(8)`, `syslogd(8)`