GeCAD srl

The Software Company

User's Guide

RAV AntiVirus CommuniGate Pro (Windows)

Release date: September 19, 2002
Product Version: 8.1.0
User's Guide revision: 1.1

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

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 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, Viruscan, 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 **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 don't accept the terms of this agreement, you don't 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

Part I: Introduction

Congratulations! You have just acquired a **RAV AntiVirus** product. **RAV AntiVirus** is one of the best antivirus programs, ranked among the first ten in the world.

RAV AntiVirus products and the documentation associated to these products are the exclusive property of GeCAD Software. The products are licensed to the users under the terms of the License Agreement accompanying each product, so please carefully this License Agreement.

We suggest to take a moment to fill the *Registration Form* attached to the *License Certificate* or register to the manufacturer's site. The personal data you fill in this form is strictly confidential and will only be recorded in our database of registered customers to keep you informed on new developments and updates and to activate your technical support account. Any suggestion you make will be taken into consideration for future versions.

Note:	Because of the attention we pay to delivering highly efficient antivirus software, the rapid evolution of viruses and implementation of features requested by our customers, the present documentation may not be up to date. The best source of information on **RAV AntiVirus** products is our website, which you can find at http://www.ravantivirus.com.

Structure of this document

This document is structured in four major components and two appendixes.

The first part, *Introduction*, includes information on the *Scope* of this document, its *Intended audience* and the *Related documentation*. You are also briefed on **RAV AntiVirus**' manufacturer, GeCAD Software, and informed about modalities you can use to obtain the *Technical support* you might need for the product you have acquired.

The second part, *RAV AntiVirus Product Family*, is an overview of the products included in **RAV AntiVirus** product family (**RAV AntiVirus Desktop**, **RAV AntiVirus for Mail Servers**, **RAV AntiVirus MailFilter** and **RAV AntiVirus for File Servers**). All these products are based on *RAV Engine*, a revolutionary antivirus engine. The cutting-edge technologies included in RAV Engine and the most important updates included in RAV Engine version 8.7 are also included in this *RAV AntiVirus Product Family* part.

The third part of the document, *RAV AntiVirus for CommuniGate Pro on Windows*, includes some sections (*Short description, What can it do, How does it work, Who should use it*) briefly presenting **RAV AntiVirus for**

CommuniGate Pro on Windows, its functionality and the potential users. Sections describing the *Currently supported operating systems and MTAs* and the *Hardware and software requirements* are also included, as well as a section presenting in more detail the *features* of **RAV AntiVirus for CommuniGate Pro on Windows**. An *Awards* section containing international acknowledgements gained by this product and a *Registration procedure* section, explaining the main principles fundamental for the license policy of our company, including a detailed description of the main differences between the three different phases in which you can use a **RAV AntiVirus** product (evaluation, registration and activation), are also included in this part of the document.

The fourth part of the document, *Configuration files and man pages*, includes the configuration file for **ravcgate**, as well as the **man** pages for **ravav** and **ravcgate**.

Two appendixes (*Bug Report Form* and *Index*) are included at the end of the document.

Scope

This document describes the features and functionality of **RAV AntiVirus for CommuniGate Pro on Windows**. Additional valuable documentation is also separately available, as specified in the *Related documentation* section below.

To make sure you will be efficiently using **RAV AntiVirus for CommuniGate Pro on Windows** from the very beginning, we strongly recommend you to read carefully this *User's Guide*, even if you have been using a previous version of RAV the product.

Intended audience

This User's Guide is intended for administrators responsible with the installation of **RAV AntiVirus for CommuniGate Pro on Windows**. These persons should have a strong and comprehensive knowledge and an extensive working experience in the operating systems the product is designed for.

Related documentation

Here is a list of documents that should be used in connection with this *User's Guide for RAV AntiVirus for CommuniGate Pro on Windows*:

- **RAV AntiVirus for Mail Servers** – *Product Sheet*;
- **RAV AntiVirus for Mail Servers (Unices)** – *User's Guide*.

These documents and other up-to-date documentation concerning GeCAD

Software's products, as well as white papers on security policies and latest info about viruses are available on our web site (http://www.ravantivirus.com/).

About GeCAD Software

GeCAD Software is a leading technology company specialized in providing top anti-virus solutions for all categories of users. After releasing its first antivirus program, back in 1994, GeCAD Software has grown ever since to be represented, by Distributors, Resellers and OEM Partners, on all the continents around the world. Our strong commitment towards quality has secured us a privileged position in a fast-evolving market, the key advantage being a state of art product based on cutting edge technologies.

Founded in 1992, GeCAD Software is headquartered in Bucharest, Romania. Our activity is focused on the following major activity axes:

- Producing, developing and internationally distributing high-quality anti-virus products; and
- Providing reliable services in fields like software distribution, consultancy and Technical Support.

Technical support

For any details regarding the installation and the functionality of this product, please contact the local dealer you have bought the product from. If he does not offer you the adequate technical support, please contact us.

For any suggestions or problems regarding the copyright, the guarantee and other aspects related to **RAV AntiVirus** products or data recovery from a destructive viral attack, please contact us at the following addresses:

GeCAD Software S.R.L.

Address:	223, Mihai Bravu Blvd, 3rd district, Bucharest, ROMANIA
Phone/Fax:	+40-21-321 78 03
Hotline:	+40-21-321 78 59
E-mail:	
Sales:	mailto:international.sales@ravantivirus.com
Technical support:	mailto:support@ravantivirus.com
Website:	http://www.ravantivirus.com

To keep in contact with other users of **RAV AntiVirus** products, join the *discussion lists* available for our products or subscribe to the free weekly *newsletter* edited by GeCAD Software.

RAV Discussion Lists

Interesting ideas and insights, installation and configuration scenarios, troubleshooting solutions and other information are also available *via* specialized *discussion lists* for **RAV Antivirus** products:

- *rav-cgate* – **RAV AntiVirus for Mail Servers** for CommuniGatePro;
- *rav-courier* – **RAV AntiVirus for Mail Servers** for Courier;
- *rav-desktop-unices* – **RAV AntiVirus Desktop** for Unices;
- *rav-desktop-windows* – **RAV AntiVirus Desktop** for Windows;
- *rav-dmail* – **RAV AntiVirus for Mail Servers** for DMail;
- *rav-enterprise* – **RAV AntiVirus Enterprise**;
- *rav-exchange* – **RAV AntiVirus for MS Exchange Server**;
- *rav-exim* – **RAV AntiVirus for Mail Servers** for Exim;
- *rav-mailfilter* – **RAV AntiVirus MailFilter** for POP3, IMAP, SMTP;
- *rav-nms* – **RAV AntiVirus for Netscape Messaging Server**;
- *rav-novell* – **RAV AntiVirus for Novell Networks**;
- *rav-postfix* – **RAV AntiVirus for Mail Servers** for Postfix;
- *rav-qmail* – **RAV AntiVirus for Mail Servers** for Qmail;
- *rav-sendmail* – **RAV AntiVirus for Mail Servers** for Sendmail.

You can subscribe to these discussion lists by visiting our website http://www.ravantivirus.com/ (*RAV Discussion Lists* section) or by sending an empty e-mail message to: listname-subscribe@lists.ravantivirus.com (replacing "`listname`" with the adequate discussion list you want to subscribe to).

RAV Newsletter

A free weekly *newsletter*, containing virus alerts, advisories and other useful advices for avoiding virus disasters, as well as information regarding updates, tips and tricks and insights on **RAV AntiVirus** products, is also available from GeCAD Software. You can subscribe to this newsletter from our website http://www.ravantivirus.com/ (*RAV Newsletter* section).

Knowledge Base

The **Knowledge Base** is a new service offered to you by the producer of **RAV AntiVirus**. You can access it at the following address: http://www.ravantivirus.com/kb. Here you can find technical information regarding the configuration and usage of all the products included in **RAV AntiVirus** family (**RAV AntiVirus Desktop**, **RAV AntiVirus for Mail Servers**, **RAV AntiVirus for File Servers** and **RAV AntiVirus MailFilter**).

Part II: RAV AntiVirus Product Family

The products

RAV AntiVirus product family is currently having the following members:

- **RAV AntiVirus Desktop** (for Windows and Unices);
- **RAV AntiVirus for Mail Servers**;
- **RAV AntiVirus MailFilter**;
- **RAV AntiVirus for File Servers**.

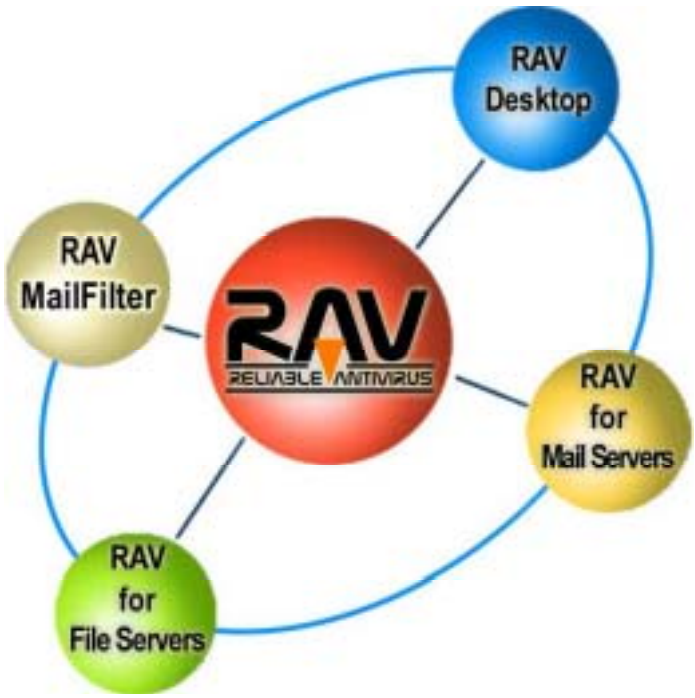

Figure 1: **RAV AntiVirus** - The product family.

RAV AntiVirus for CommuniGate Pro on Windows and all the other products included in **RAV AntiVirus** family are based on *RAV Engine*, now at version 8.9.

The Engine

RAV Engine combines the operational strength, the extensibility, the scalability, the scanning speed and the robustness needed in the fight against viruses and other malicious software (Trojans, worms, hoaxes, etc.).

At this writing, RAV Engine accurately detects over 70,000 viruses and RAV Antivirus Research Team daily adds new signatures in RAV Engine's

database. RAV Engine includes modules for scanning **inside archives** that detect infected files in most common types of archives and can scan archives inside archives no matter how deep they go. RAV Engine also scans inside **packed executables** (`lzexe`, `pklite`, `cryptcom`, `wwpack`, `aspack`, `pepack`, `vgcrypt`, `upx`). Working with Virtual File Systems, RAV Engine can scan the processes in memory and IFS chains, thus detecting and cleaning resident viruses like CIH.

Cutting-edge technologies included in RAV Engine

RAV Engine, now at version 8.9, has some unique features, ranking it among the best antivirus engines in the world. Here is a short description of the cutting-edge technologies included in the latest version of RAV Engine.

The TPI (Total Platform Independent) technology

The same engine is used for detecting and cleaning malwares for each operating system and platform **RAV AntiVirus** is installed on. Thus, the intelligibility, the unity and the easy update of our programs are logically ensured for all the products from **RAV AntiVirus** family (**RAV AntiVirus Desktop**, **RAV AntiVirus for Mail Servers**, **RAV AntiVirus for File Servers** and **RAV AntiVirus MailFilter**).

The IC (Integrity Checker) technology

When the files are scanned for the first time, the detection engine creates a database with all the information it has gathered during the scanning process. When doing a second scan, only the new or changed files are scanned, therefore increasing the detection speed with over 50%.

The MLES (Multi Layer Embedded Scanning) technology

RAV engine is promptly responding to any threat, scanning embedded objects on multiple layers, without affecting the detection speed or slowing down the machine it is installed on.

The HMETH (heuristic method) technology

Using this technology for all electronic threats, RAV Engine can study the behavior of eventual malwares (malicious software, like worms, Trojans and hoaxes) and propose different methods for handling it. Therefore, a virus can be detected and cleaned even if its signature does not exist in the database.

The CF (Content filtering) technology

RAV Engine scans mail messages on three different levels: **Subject**,

Attachments names and **Body**, looking for regular expressions or user-defined strings. RAV Engine can execute the actions you specify for mail messages matching these criteria.

The CUP (Cumulative Update Plug-ins) technology

The cumulative update is another advantage of RAV Engine, being used to add to the main signatures database only the latest available signatures. This procedure results in extremely small files used for the update (10-15Kb), very little download time (5-10 seconds for a 28,8Kbs connection speed) and better management of the virus signatures.

RAV Engine 8.9 vs. 8.7

RAV Engine version 8.9 was released on August 28th, 2002. In comparison with the precedent version of RAV Engine (8.7), the current version is enjoying the following improvements:

1. RAR3 archives are now supported.
2. Improved scanning inside CHM/HXS embedded files.
3. Improved scanning inside SFX archives. Support for these files was significantly improved, and the number of supported types has increased.
4. Improved heuristics/generic detection for Visual Basic-compiled programs.
5. Improved heuristics/generic detection for .NET compiled programs.
6. Added heuristics/generic detection for Visual C compiled programs.
7. Added detection for several heavy-polymorphic Win32 viruses.
8. Added support for `a.out` executable files, and improved the support for damaged ELF files.
9. Improved the LE/LX executable parser to handle damaged/handcrafted files.
10. Scanning inside files packed by several installers was included.
11. Scanning of OMF object files is now supported.
12. Damaged (without headers) MIME files are now supported.
13. PEPatch, PaquetBuilder, PrivateEXE v2.2, EPPE, PeBundle, Shrinker, SPEC AcidCrypt support was included/improved.
14. Improved the loading time and the scanning speed under Win95/Win98 VxD platform.
15. Improved the process scanner under Windows 9x and Windows NT.

Part III: RAV AntiVirus for CommuniGate Pro on Windows

Short description

RAV AntiVirus for CommuniGate Pro on Windows is a highly customizable award-winning antivirus program for mail servers using different operating systems on different platforms.

What can it do

RAV AntiVirus for CommuniGate Pro on Windows scans and cleans mail messages and all types of attachments including archives, exe files, embedded files, etc. It helps you avoid Internet malwares (viruses, worms, Trojans, hoaxes, etc.), bulk mail and information leaks. **RAV AntiVirus for CommuniGate Pro on Windows** is scanning, detecting and removing any electronic threats from the messages flowing to/from your mail server, therefore protecting important data for your company and preventing your computers from being infected by viruses, worms, Trojans and other malwares.

At this writing, **RAV AntiVirus for CommuniGate Pro on Windows** is protecting its users of about 70,000 malwares.

How does it work

The product contains a daemon based on *RAV Engine* (**ravcgate**) and a filter module that interfaces the daemon with your mail server. When a mail message is reaching a mail server protected by **ravcgate**, it is intercepted by the filter and sent to the daemon for scanning (the scan process is executed using RAV Engine). If the message is clean, it is sent back to the filter, which will decode and redirect it to the mail server, to be sent - scanned and cleaned – to the initial destination. If the message is not clean, customizable actions are taken, according to the options set by the user.

Who should use it

RAV AntiVirus for CommuniGate Pro on Windows is targeting three categories of users:

- **large companies**, with heavy traffic on their mail servers and demanding security policies;

- **Internet Solution Providers** (ISPs – over 60% of them are using Linux-based mail servers). **RAV AntiVirus for CommuniGate Pro on Windows** is the perfect solution for ISPs are dealing with heavy traffic and large amount of clients. **RAV AntiVirus for CommuniGate Pro on Windows** can improve the services ISPs are providing to their customers by scanning the mail flow and adding protection against viruses for the hosted domains; and
- **small companies** willing to protect their internet traffic at low cost.

No matter if you're a big or small company or an ISP, the protection offered by **RAV AntiVirus for CommuniGate Pro on Windows** is always working on multiple levels:

- You are protected of viruses and other malwares that might try to infect your machines coming from the Internet, as mail attachments or mail messages.
- The outgoing flow is scanned for viruses and other malwares.

You can also customize the outgoing mail flow for not allowing sensible information to leave your company.

Awards

Starting with March 1st, 2002, **RAV AntiVirus for Mail Servers** (Linux) is awarded the West Coast Labs'[1] Checkmark Certificate *Level 1* and *Level 2*, the two standards to be achieved by antivirus products. **RAV AntiVirus for Mail Servers** is the first (and so far the only) anti-virus software winning both certificates for Linux-based mail servers.

The Checkmark Certificate system establishes standards for computer security products, giving end users a clear idea on reliable anti-virus products. For a product to be certified to Anti-Virus Checkmark, *Level One*, the product must be able to detect all "in the wild" viruses. According to Checkmark, "In the Wild" viruses are currently defined as those appearing on The Wildlist Organization's "In the Wild" list and reported as such by more than one person.

For a product to be certified to Anti-Virus Checkmark, *Level Two*, the product must be able to comply with Checkmark Level One and, in addition, disinfect all "in the wild" viruses capable of being disinfected. The product must also detect all viruses on the wild list more than one month old.

[1] West Coast Labs is an independent organization testing information security products. It is owned by West Coast Publishing Limited which also owns *SC Magazine*, the largest circulation information security magazine in the world.

Currently supported OS-s, platforms and MTAs

RAV AntiVirus for CommuniGate Pro on Windows is a member of **RAV AntiVirus for Mail Servers** family, currently available for the following platforms/operating systems:

- Windows NT and Windows 2000 on i386 platforms;
- Linux (Slackware, Mandrake, SuSe, RedHat, e-Smith, Debian, etc.) on i386 platforms;
- Linux (SuSe, RedHat and Mandrake) on s390 platforms;
- Linux (Yellow Dog) on ppc platforms;
- Linux (Suse) on Sparc platforms;
- FreeBSD on i386 platforms;
- Open BSD (2.8, 2.9 and 3.0) on i386 platforms;
- Solaris on i386 platforms;
- Solaris on Sparc platforms;
- Unixware on i386 platforms;
- Mac OS X on ppc.

RAV AntiVirus for Mail Servers is currently supporting the following MTAs:

- CommuniGate Pro
- Courrier
- DMail
- Exim
- MS Exchange (5.5 and 2000)
- Postfix
- Qmail
- Sendmail
- Sendmail-Milter.

Below you can find a table detailing currently supported MTAs, operating systems and platforms.

Table 1: Currently supported MTAs, operating systems and platforms.

Mail Server / OS/platform	Free BSD	Linux on i386	Linux on ppc	Linux on Sparc	Linux on s390	MacOS X	NetBSD	Open BSD (2.8, 2.9, 3.0)	Solaris I386	Solaris SPARC	Unixware 7.1.1	Win 32
CommuniGate Pro	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓
Courier		✓	✓	✓		✓				✓		
Dmail	✓	✓	✓	✓		✓			✓	✓		✓
Exim	✓	✓	✓	✓	✓		✓	✓	✓	✓		
MS Exchange 5.5												✓
MS Exchange 2000												✓
Postfix	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		
Qmail	✓	✓	✓	✓	✓		✓	✓	✓	✓		
Sendmail	✓	✓	✓	✓	✓		✓	✓	✓	✓		
Sendmail Milter	✓	✓	✓	✓	✓			✓	✓	✓		

Further developments

GeCAD Software is currently working on developing antivirus solutions for different operating systems and platforms. For details on the developing process and other info about the characteristics of our products, please visit our website: http://www.ravantivirus.com.

Features of RAV AntiVirus for CommuniGate Pro on Windows

Some of the distinctive features of **RAV AntiVirus for CommuniGate Pro on Windows** are presented below:

- *Simple installation process*: The installation process is very simple and straightforward;
- *Easy to configure and use:* **RAV AntiVirus for CommuniGate Pro on Windows** is extremely easy to configure: options are available to order the actions to be taken by **RAV AntiVirus** when dealing with an infected file (**Clean, Move/Copy to Quarantine, Delete, Rename, Ignore, Reject**) or with a file containing suspicious code (**Move/Copy to Quarantine, Delete, Rename, Ignore, Reject**).
- *Multi platform virus removal*: RAV Engine detects and removes all known Windows, Linux, Unix and DOS viruses, regardless of the operating system they're stored on or designed for. More than that, **RAV AntiVirus for CommuniGate Pro on Windows** is using heuristic methods, to extend the protection it is offering to its users and act against new viruses and new versions of existing viruses.
- *Integration:* **RAV AntiVirus for CommuniGate Pro on Windows** is an **integrated** suite, containing all the necessary components in one single installation.
- *Enhanced virus scanning:* Mail attachments with multiple recipients are scanned only once, and not for all the recipients, therefore enhancing the scanning speed. Different technologies are also applied, in order to improve the speed and accuracy of the scanning process.
- *Content filtering:* All incoming/outgoing mail messages are scanned by **Subject, Attachment** and **Body**. This way, you can deny incoming mail messages containing suspicious objects and outgoing mail messages containing confidential information, reducing all types of threats to the very minimum. The available options for mail files matching the content filter are: **Move/Copy to Quarantine, Delete, Ignore, Reject**. For more details, please refer to the Advanced Content Filtering feature section.
- *Group configuration:* The system's administrator can define different groups of users and specify different settings for these groups. **RAV AntiVirus for CommuniGate Pro on Windows** will scan these differently configured groups according to their specified scanning settings.
- *Preventing information leaks:* **RAV AntiVirus for CommuniGate Pro on Windows** restricts the mail flow according to defined parameters/patterns. You can configure specific groups (for example one group named Accounting, including all the computers from your company's accounting department) and set **RAV AntiVirus for CommuniGate Pro on Windows** to deny all outgoing mail messages containing confidential informantion, according to the patterns set by your mail server's administrator.

- *Warning mails:* You can configure **RAV AntiVirus for CommuniGate Pro on Windows** to send instantly warning mails when a virus allert occurs to the sender of the message, to the receiver and/or to a third party (i.e. RAV Research Team or the server's administrator).
- *Intelligent Update:* The update process can be performed on demand or on a scheduled basis, according to the administrator's settings. The latest versions of **RAV AntiVirus for CommuniGate Pro on Windows** (including engine updates and documentation) can be found on the following mirror sites:

  ftp://ftp.ravantivirus.com/pub/rav/ (site located in Romania);
  ftp://download.ravantivirus.com/pub/rav/ (site located in USA).

  New mirror sites are expected to be available for update. Please check regularly our website to find out the addresses for these new mirror sites.

Other features of RAV AntiVirus for CommuniGate Pro on Windows

- Modular structure, allowing easy customization for every work environment;
- Extended protection (for new mail boxes);
- Scanning archives inside archives;
- Scanning for packed executables;
- Multiple MIME-type encodings;
- Technical support available by mail and phone for registered users.

Hardware and software requirements

Software requirements:

RAV AntiVirus for CommuniGate Pro on Windows requires:

- Windows 2000 with Service Pack 2 and/or Windows NT 4 with Service Pack 4.
- CommuniGate Pro version 3.4b1 or later.

Hardware requirements:

RAV AntiVirus for CommuniGate Pro on Windows will work on a computer meeting the minimal requirements for the installed Mail Server program:

Processor: Compatible Intel CPU, 150 Mhz or better

Memory: 32 MB of RAM or more.

Note:	In order to send warning messages, according to the settings made in the scanning configuration, you must have your CommuniGate Pro running on the local machine and listening on port 25.

Registration procedure

Due to an extremely flexible licensing system, you can acquire different packages, depending on your needs of protection. **RAV AntiVirus for CommuniGate Pro on Windows** is licensed *per domain*. The more domains you support, the less you pay per domain.

All the products included in **RAV AntiVirus** family are available under a license scheme with three different stages: *evaluation*, *registration* and *activation*. Each different stage has its own characteristics, described below.

Evaluation

The products included in **RAV AntiVirus** family are fully functional and their users benefit of complete update services and technical support for an *evaluation period* of 30 days. During this evaluation period, our potential customers should be able to evaluate all the functionalities and services provided by our products, in order to make a knowingly decision. For details regarding your rights and obligations pertaining to the usage of GeCAD Software's products during the evaluation phase, please read the *Evaluation license* section from the License Agreement.

During the evaluation period, each mail message scanned with a **RAV AntiVirus** product contains info about the number of days remaining for evaluation. After this evaluation period, the product expires. If you do not introduce a valid *Registration Code* during the Evaluation period, you will not be able to use the product anymore. Introducing (anytime) a valid *Registration Code* extends *ad infinitum* the lifetime of the product.

Evaluation for RAV AntiVirus for CommuniGate Pro on Windows

RAV AntiVirus for CommuniGate Pro on Windows can be used *free of charge* for *two domains* for an **evaluation period** of 30 days. During this evaluation period the product is fully functional and you can update free of charge the signatures database. If you do not register your product within 30 days, you will no longer be able to use it for scanning your mail traffic.

Registration

In order to license your **RAV AntiVirus for CommuniGate Pro on Windows**, you have to purchase it from an authorized RAV reseller/distributor. When you purchase **RAV AntiVirus for CommuniGate Pro on Windows** from an authorized RAV reseller/distributor, you receive a *Registration Code*. If the purchasing involves physical delivery, the *License Certificate* will also be available.

After registering your product, you have 30 days to *activate* it by installing an

Activation key (please refer to the next section to see how you can do it). Activating your registered product is very important, because it offers you *free* updates, as well as technical support for *one year*.

Activation

The product's activation is done free of charge, *upon request*, by sending your End User information to GeCAD Software (https://register.ravantivirus.com; alternatively, you can fax this info to the number specified on the License Certificate). Subsequently, you will receive by mail an *Activation Key* and instructions for its installation. Installing this Activation Key enables you to use **RAV AntiVirus for CommuniGate Pro on Windows** for the number of domains you have purchased it for and offers you the following integrated services:

- Free engine extensions for one year;
- Free daily updates for one year;
- Full technical support for one year;
- Virus alerts and security advisories.

You can extend the rights resulted from activating your product by purchasing annual update extensions available at special discounts.

Updates

Given the present rate of appearance of new viruses, an antivirus program becomes obsolete in a few weeks (sometimes even days). To insure an efficient protection, any antivirus product (**RAV AntiVirus for CommuniGate Pro on Windows** included) must be periodically updated.

The latest versions of **RAV AntiVirus** products (including engine updates and documentation) can be found on the following mirror sites:

ftp://ftp.ravantivirus.com/pub/rav/ (site located in Romania);
ftp://download.ravantivirus.com/pub/rav/ (site located in USA).

New mirror sites are expected to be available for update. Please check regularly our website to find out the addresses for these new mirror sites.

Part IV: Configuration files and man pages

In the following section you will find:

- The configuration file for **RAV AntiVirus for CommuniGate Pro on Windows** (`ravcgate.conf`);
- The **man** page for **RAV AntiVirus** command line version (**ravav**);
- The **man** page for **ravcgate** – RAV external filter for CommuniGate Pro.

RAVCGATE.CONF

NAME

`ravcgate.conf` - the configuration file for **RAV AntiVirus for CommuniGate Pro running on Windows**.

SYNOPSIS

This is the configuration file for **ravcgate**, and it contains info on the run-time configuration for RAV AntiVirus mail-scanning daemon. After installation, `ravcgate.conf` resides in your `C:\Program Files\GeCAD\RAV8 CGatePro\etc` directory (assuming you installed **RAV AntiVirus for CommuniGate Pro running on Windows** in the default folder).

This document is part of the *User's Guide for RAV AntiVirus for CommuniGate Pro running on Windows* and should be used only in connection with this User's Guide.

Other documents containing valuable information are also available:

- The *ReadMe, License* and *ravav.pdf* files included in your `C:\Program Files\GeCAD\RAV8 CGatePro\doc` folder (assuming you installed **RAV AntiVirus for CommuniGate Pro running on Windows** in the default folder).
- The *User's Guide for Unices Mail Servers* - you can download it from the following location:

  http://www.ravantivirus.com/rav/mailservers/documentation/pdf/ravmailservers-usersguide.pdf

Structure

This configuration file consists of:

- Description of three declaration sections (the *Regular Expression Declaration* section, the *Action Definitions* section and the *Warning Mails Message Declarations* section),
- Group declarations, and

- Explanation of possible parameters.

The info included in this part of the documentation is for reference purposes. Other valuable sources of information are also available. Information pertaining to the installing process, for instance, is included in the *Install.log* file found in your `C:\Program Files\GeCAD\RAV8 CgatePro` folder. Additional information about **RAV AntiVirus for CommuniGate Pro on Windows** (hardware and software requirements, list of installed files, instructions for configuration and updating) is provided in the *ReadMe* file found in your `C:\Program Files\GeCAD\RAV8 CGatePro\doc` folder.

Definitions

Some concepts frequently used in the programming world might have different understandings for the purpose of this manual. Here you can find these terms and the meanings they are given in this document:

- A **variable** is a place where we can store data;
- A **string** is a sequence of characters ending with a new line or delimited by quotes;
- A **boolean** is one of the keywords: **yes/no**;
- An **enumeration** is a sequence of words separated by commas;
- A **regexp** is a POSIX regular expression.
- A **group** is a category of users (senders or receivers) that have different mail addresses and/or domains, but share the same action parameters for **ravcgate**.
- A **macro** is a stored template of instructions to be replaced with actual values by **ravcgate**;
- A **commented** line is a line beginning with a hash (#) character. All commented lines are ignored. All the lines containing only white spaces are also ignored;
- A **default** is a predefined value for one parameter. If that **parameter** is missing from `ravcgate.conf` then it is considered to have that **default** value.

The values following the '=' sign in *parameters* may be: a **string**, a **boolean**, a **regexp** or an **enumeration**.

Note: The section and parameter names are **not** case sensitive.

SECTION DESCRIPTIONS

Three different sections are included in `ravcgate.conf`: the *Regular Expression Declarations* section, the *Action Definitions* section and the *Warning Mails Message Declarations* section. These sections are presented below in the following format:

- Short description;
- Keyword representing the beginning of the section;
- Syntax;
- Example.

Some *Frequently Asked Questions* (FAQs) are also provided in connection with some relevant aspects of these sections. The *Frequently Asked Questions* are meant to help you with the practical aspects of using **RAV AntiVirus for CommuniGate Pro on Windows**.

The *Frequently Asked Questions* were selected from the questions asked by users of **RAV AntiVirus for CommuniGate Pro on Windows** on the mailing lists available for our products.

For more information, you can subscribe to these discussion lists by visiting our website http://www.ravantivirus.com/ (*RAV Discussion Lists* section) or by sending an empty mail message to: listname-subscribe@lists.ravantivirus.com. For more *Frequently Asked Questions*, please visit our website at http://www.ravantivirus.com/ or consult our *Knowledge Base* available at the following address: http://www.ravantivirus.com/kb.

Regular Expression Declaration section

In the *Regular Expression Declaration* section you can define all the regular expressions you will use for the content filtering feature. This section can appear anywhere in the configuration file, as long as it is placed before the group definitions.

This section begins with the keyword:

```
_define_regular_expressions
```

Syntax

variable = string

or

variable = regexp

Example 1:

```
for_subject_filter = I love you
```

This regular expression defines a filter for all the mails including the string "I love you" in the **Subject**.

Example 2:

```
file_regexp = .*\.exe
```

This regular expression defines a filter for all mail messages having **.exe** attachments.

Action Definitions section

In the *Action Definitions* section you can define the actions you want to be used by **ravcgate**. The *Action Definitions* section can appear anywhere in the configuration file as long as it is placed before group definitions.

This section starts with the keyword: `_define_actions.`

Syntax

variable = enumeration

Depending on the scanning status of the mail message (infected, suspicious, subject/attachment/content filter match), the variable will be associated with some different actions (*clean, move, copy, delete, rename, ignore, reject*). The enumeration contains one or multiple actions separated by a comma. The actions from this enumeration are executed by **ravcgate** in the order you specify.

Depending on the scanning status, the following valid actions are supported:

- for infected files: **clean**, **move**, **copy**, **delete**, **rename**, **ignore**, **reject**.
- *for suspicious files*: **move**, **copy**, **delete**, **rename**, **ignore**, **reject**.
- *for mails matching the subject filter*: **copy**, **ignore**, **reject**.
- *for files matching the attachment filter*: **move**, **copy**, **delete**, **rename**, **ignore**, **reject**.
- *for mails matching the content filter*: **move**, **copy**, **delete**, **ignore**, **reject**.

Note 1:	If the last action you define for infected mails is not one of the following: **Reject** or **Ignore**, the **Reject** action is automatically applied.

The following table includes a description of all the actions available in **ravcgate** (first column), a description of these actions (second column) and a listing of circumstances when each specific action is available (third column), depending on the scanning status:

Action	Description	Scanning status
Clean	Asks RAV AntiVirus to clean the infected file.	Infect
Move	Asks RAV AntiVirus to move the file to quarantine (equivalent to `Copy` + `Delete` actions).	Infect, suspicious, attach match, content match
Copy	RAV AntiVirus is copying the file to quarantine.	Infect, suspicious, subject match, attach match, content match
Delete	RAV AntiVirus is deleting the file and replacing it with a new file automatically generated. The file's name is `warn.txt` and it contains the following text: "*RAV AntiVirus has deleted this file because it contained dangerous code.*" This text is customisable (please see FAQ no 1 for details). Note that **ravcgate** doesn't change the mail file size because of some protocols (like IMAP) may request the mail size first and then the mail body. So, the `warn.txt` file will be filled with spaces to fit the original file length.	Infect, suspicious, attach match, content match
Rename	The file will be renamed using the `rename_ext` extension specified in the configuration file.	Infect, suspicious, attach match
Ignore	The file is ignored, no action is taken and the mail is delivered.	Infect, suspicious, subject match, attach match, content match
Reject	The mail is rejected; it will not be delivered to any of its recipients, but will be bounced back to the sender.	Infect, suspicious, subject filter, attach match, content match

Table 2: ***Actions available in*** *ravcgate.*

The following *Frequently Asked Questions* will eventually help you better understand the characteristics of the actions available in **ravcgate**.

FAQ 1: Scanning existing mails

Question: I just installed **RAV AntiVirus for CommuniGate Pro running on Windows**. How can I scan mail messages existing prior to this installation?

Answer: If you wish to scan mail messages existing prior to the installation of **ravcgate**, do the following:

```
C:\Program Files\GeCAD\RAV8 CGatePro\bin\ravav -AM --smart --
   report= C:\Program Files\GeCAD\RAV8 CGatePro\tmp\ravreport.txt
   [path to mail accounts]
```

This setting results in scanning a mailbox (with **Ignore** as default action) and delivering a report (`ravreport.txt`) in the `tmp` directory.

FAQ 2: Separate domain file

Question: Is it possible to put all scannable domains in a separate hash or normal file?

Answer: Create a `domains.list` file in your `C:\Program Files\GeCAD\RAV8 CGatePro\etc` folder and/or operate the following changes:

In `ravcgate.conf`, replace the "domains to scan (separate them with ',')" section with:

```
domain1.com, domain2.com, domain3.net, domain4.com,
domain5.org
```

Then use:

```
domain = C:\Program Files\GeCAD\RAV8 CGatePro\etc\domains.list
```

Warning Mails Message Declarations section

In the *Warning Mails Message Declarations* section you can define the subjects and the messages for the warning mails that will be sent to those interested. The *Warning Mails Message Declarations* section can be declared anywhere in the configuration file as long as it is placed before the group definitions.

This section starts with the keyword:

```
_define_warning_mail
```

Syntax

variable = string

The string defining one warning mail should give the user some basic information such as: what file has caused the warning, who sent that file and whom was it intended for, what is the warning about, what action was taken by **ravcgate** and so on. One example of good warning message would be the following:

> "*That* file coming from *that* sender and addressed to *this* user is infected with *this* virus. The action taken by **ravcgate** was *this*."

Of course, not all the warning mails are about virus-infected files. There are some other situations when you might want to be alerted by **ravcgate**. For instance, you might want **ravcgate** to alert you when a mail containing one specific type of attachment has arrived on your mail server or when one of your users is trying to transmit a confidential document. Of course, in these cases the warning mail should change accordingly to that specific situation. However, in all the cases some information is *always* included (the name of the file causing the alert, the sender, the action, etc.).

This information always included in a warning mail is based on *macros*. One macro is (for the purpose of this document) a stored template of instructions containing one piece on info from the string representing the warning mail. `FILE_NAME`, for instance, is an example of macro containing the name of the file causing the alert you're receiving. **ravcgate** will replace this macro with the actual name of the trouble-making file.

The string that the warning message will be created from can contain the following macros:

`FILE_NAME`	The full path to the scanned file and its name.
`ATTACH_NAME`	The name of the scanned attachment.
`VIRUS_NAME`	The name of the virus discovered by **ravcgate**.

FROM_USER	The mail address of the sender.
TO_USER(S)	The mail addresses of the receivers.
SUBJECT	The mail's subject.
QUARANTINE_NAME	The name of the file saved to RAV Quarantine using the *Move* or *Copy* action.

These macros are combined in one warning string that might look like this:

```
"The file ATTACH_NAME attached to mail (with subject:SUBJECT)
sent by FROM_USER to TO_USER(S)is infected with virus:
VIRUS_NAME".
```

Note: The macros **FROM_USER** and **VIRUS_NAME** can be used in the warning mail's subject too.

In this case, one attachment file is virus-infected. Info is provided about the attachment's name, the subject of the mail containing the infected attachment (this is an optional info), the sender's name, the addressees' names and the virus name.

The following *Frequently Asked Questions* will hopefully help you better understanding this very interesting feature of **ravcgate**.

FAQ 3: Warning messages not sent

Question: Why don't I get warning messages when viruses are found?

Answer: You probably did not configure correctly **ravms** mail account. Here are the excerpts from the documentation that should help you:

"Default values:

```
ravms_name = ravms

on_host = the official name returned by the gethostbyname()
function

smtp_server = same as host (IP address)

smtp_port = 25
```

Default values are provided and they will probably work. Define these fields only if warning mails are sent when a virus is found or if you want to use a different account instead of **ravms**. Specify **smtp_server** IP address only if that machine is behind a firewall and **ravcgate** can't get its host name".

FAQ 4: Omitting the SUBJECT from warning mail

Question: Is it possible to define that `SUBJECT` should be omitted from the warning for specific viruses? Some of the viruses disclose potentially sensitive information from the victim's hard drive, and puts it in the subject of the email.

Answer: In `ravcgate.conf`, edit the line:

```
infected_m = "The file ATTACH_NAME attached to mail (with
subject:SUBJECT) sent by FROM_USER to TO_USER(S)is infected
with virus: VIRUS_NAME."
```

and remove `"with subject: SUBJECT"`.

The subject will not be displayed anymore in your warning mails. Please note that this solution will be applied to all mails, not just for specific viruses.

FAQ 5: Changing the warning mail message

Question: When a mail with `.exe`, `.com` or other attachments of this type is sent, a warning message is also sent, which is OK, but it says the file is infected with the virus: `UNAUTHORIZED_MAIL_ATTACHMENT`, which seems to scare the average user. Can the message be modified?

Answer: Yes, the message can be modified:

- `In ravcgate.conf` define a variable, for example:

  ```
  infected_attach = "The file ATTACH_NAME attached to mail
  (with subject:SUBJECT) sent by FROM_USER to TO_USER(S) has
  an unauthorized file extension"
  ```

- Then use (in the `_attachment_filter_warning_messages` section):

  ```
  infected_msg = infected_attach
  ```

  instead of

  ```
  infected_msg = infected_m
  ```

- Restart **ravcgate** and you're done.

Group Declarations

What is a group

A group is a category of users (senders or receivers) that have different mail addresses and/or domains, but share the same action parameters for **ravcgate**. Using the group feature of **ravcgate**, you can use the same characteristics (for the scanning engine or the update process, for instance) and the same actions (filters, warning mails and so on) for users having different mail addresses and mail domains. This group structure is very useful in case you use **ravcgate** in a network with hundreds of mailboxes.

In **ravcgate** you have one default group, called [global], containing at the beginning all the users and mail domains protected by ravcgate. When you define a new group, its members are taken away from the [global] group and included in the new group, for which you have to define new group-specific options.

The [global] group

This is the default group, which contains all the users and mail domains that are not defined in the other groups. The [global] group MUST NOT contain any member declaration.

Defining other groups

A new group definition begins with the group name written between "[]". The group definition must be followed by the member declarations (it is mandatory that the members are declared before any other parameters) and the group options.

How do I configure groups

The configuration file must include the [global] group, containing the default options for all mail scanning processes. Besides the [global] group, you can customize **ravcgate** by creating additional groups, with different configurations.

If no value is specified for one parameter in the configuration file for one group, **ravcgate** will use the *default value* for that paramater. If no *default value* is defined, **ravcgate** will use the value specified in the [global] group for that parameter, with the following exceptions: filter_subject, filter_attachment, filter_content, warn_sender, warn_receivers, warn_admin, do_not_warn, do_not_show, admin_addr, do_not_scan.

The following *Frequently Asked Questions* are providing the answers for some of the confusions of the existing users of **RAV AntiVirus for CommuniGate Pro on Windows** in aspects pertaining to group configuration.

FAQ 6: Creating different rules for a domain

Question: How do I create different rules for a domain?

Answer: You can define different rules for a domain by creating a group in which you specify `from_host` and/or `to_host`. Then specify the actions that **ravcgate** can perform for the newly created domain. Here are the steps you should follow for creating different rules for a domain:

- In `ravcgate.conf`, in the section `_define_actions` use:

```
act_for_my_group = clean, delete, ..
```

- At the end of `ravcgate.conf` define the group:

```
[my_domain]
_#from_host=a.com
to_host=a.com
infected_actions=act_for_my_group
```

FAQ 7: Example on how to set the domains and the IP addresses

Question: I need an example on how to set the domains and the IP addresses.

Answer: In `ravcgate.conf`, in the [`global`] section use:

```
domain = localhost, your.host.com
```

In order to receive the warning mails, use:

```
ravms_name = ravms

on_host = your.host.com

smtp_server = ip.address.of.host
```

FAQ 8: Global group configuration

Question: How is the [`global`] group configured?

Answer: Please define in `ravcgate.conf` the following options:

```
ravms_name=ravms

on_host=your.host.com
```

```
smtp_server=127.0.0.1
```
(IP address)

```
smtp_port=25
```

Then start **ravcgate**.

FAQ 9: Excluding one particular account

Question: I need to exclude one account in particular as I receive a daily email of over 60 MB in size and I don't want RAV to try to process that file. What do I get it done?

Answer: You can create a group with that sender and choose not to scan that mail. Please make the following changes:

In `ravcgate.conf`, add at the end of the file define:

```
[group1]

sender=sender@host.com

do_not_scan=yes
```

Then restart **ravcgate**.

Advanced Content Filtering feature

What is this

The **Advanced Content Filtering** is a very powerful feature of **ravcgate** that can help you configure the product to answer your specific needs. Using this feature, you can define filters on different levels (subject, body, attachment contents or attachment file name). You can afterwards define specific actions for the mail messages matching the rules you specify. For instance, you can instruct **ravcgate** to deny incoming mail messages containing one specific string in the **Subject** field (i.e. "I love you"), deny outgoing mail messages containg user-specified strings (i.e. "confidential", "balance sheet") and deny incoming/outgoing mail containing attachment with user-specified file types/names.

How does it work

The *Content Filtering* module of **ravcgate** is using **POSIX regular expressions** for searches executed on the *Subject*, *Attachment file names* and *Body* levels.

The rules you define are processed in the following order:

- Subject,
- Attachment file names,
- Body.

If you define more rules for one single component, the rules will be processed in the order you are defining them.

Here are some *Frequently Asked Questions* users of **RAV AntiVirus for CommuniGate Pro on Windows** have asked about the *Advanced Content Filtering* feature of **ravcgate**. You can even find an example of configuring a content filter for mail messages containing one specific string.

FAQ 10: Rejecting double extension files

Question: Has anyone setup the configuration file to reject any attachment with a double extension?

Answer: Please use in `ravcgate.conf`:

```
var_regexp = .*\..*\..*

var_action = reject
```

In [`global`]:

```
filter_attachment var_regexp var_action
```

Please note that this restrictive action will also filter the `tar.gz` files, for instance.

FAQ 11: Denying certain types of attachments

Question: How can I deny certain types of attachments?

Answer: The content filtering feature of **RAV Antivirus for CommuniGate Pro on Windows** can help you if you want to deny a certain type of attachment from entering your company via email. The content filtering module of RAV AntiVirus uses POSIX regular expressions to find a pattern in *subject* and *attached file names* and user-defined strings to find a pattern in *message body* (and attachment contents). The rules are processed in the following order: **subject, attachments, body**. If you define more rules for the same component, they will be processed in the same order they are specified.

Here is an example for how to deny **.exe** attachment files:

In the `define_regular_expressions` section from `ravcgate.conf`:

```
define file_regexp = .*\.exe
```

In the `_define_actions` paragraph from `ravcgate.conf` define:

```
file_action = delete, reject
```

In the [`global`] section of `ravcgate.conf` define:

```
filter_attachment file_regexp file_action
```

To add other types of attachments separate them with a | symbol on the `regexp` definition.

Example:

```
file_regexp  =  .*\.((vbs)|(vbe)|(js)|(exe)|(com)|(pif)
|(lnk)|(scr)|(bat)|(shs)|(sh))
```

As is the case for each change in the configuration files, you must restart **ravcgate**.

FAQ 12: Example of content filtering for mail subject

Question: Can I have an example of content filtering for mail messages containing one defined expression in the **Subject** field?

Answer: Yes, you can. Here you can find how to create a content filtering rule for mail messages containing the expression "xxx" in the **Subject** field.

The following options are available for the mail messages matching the content filter: **move, copy, delete, ignore, reject**.

For this scenario, the mail will be allowed to pass **RAV AntiVirus for CommuniGate Pro on Windows**. The sender and the receiver will not receive warnings, but a warning will be sent to the administrator.

- In the `_define_regular_expressions` section from `ravcgate.conf`, define the expression `xxx`:

```
subjxxx_regexp = xxx
```

- Define the action for `xxx` in the `_define_actions` section from `ravcgate.conf`:

```
define xxxsubj_action = ignore
```

  This will allow the `xxx` mail to pass the content filtering module of **ravcgate**.

- To add other words, separate them with a | symbol on the `regexp` definition.

  Example:

```
subjxxx_regexp = (word1)|(word2)|(word3)
```

- In the [`global`] section of `ravcgate.conf` specify the administrator's mail address for alerting him that a mail matching an expression from content filter has been entering in the company:

```
admin_addr=administrator@ravantivirus.com
```

- Activate the content filtering by adding the following line:

```
filter_subject subjxxx_regexp xxxsubj_act
```

- As is the case for each change in the configuration files, you must restart **ravcgate**.

Explaining the parameters

The parameters included in this configuration file for **ravcgate** (`ravcgate.conf`) have different functions. Some are used for specifying the domain parameters, other for specifying the group members, the actions for the scanning engine, the warning messages and the sender of warning messages and so one. All the parameters have been grouped below depending on their function.

Some of these parameters are group-specific, meaning that they are different for each defined group. Other parameters are common for different groups and/or are inherited from the [`global`] group. This classification is also important for understanding the way **ravcgate** is working.

Domain parameters

domain = enumeration

Description: This parameter specifies the domains scanned by RAV AntiVirus.

Note:	During the evaluation period of 30 days you can set only two domains. Mails to/from other domains are delivered normally, without being scanned.

This parameter is a global one. It is sufficient to define it in the [`global`] group.

Important:	You **must** specify at least one domain name, or else **ravcgate** will not start.

Example:

```
domain = mail.domain.com, domain.com

domain = second.domain.net
```

Important:	In the acception of **ravcgate** and according to the **License Agreement**, a 'domain' is defined as "*the string which follows the '@' symbol in a mail address*".

Group members

sender = enumeration

Description: Parameter used for specifying the mail addresses of the senders who will be members in the actual group.

Example:

```
sender = user1@domain1.com, user2@domain1.net
```

```
sender = user3@domain2.org
```

receiver = enumeration

Description: Parameter used for specifying the mail addresses of the receivers who will be members in the actual group.

Example:

```
receiver = user4@domain4.com, user5@domain4.org

receiver = user5@domain2.org
```

from_host = enumeration

Description: Parameter used for specifying the hosts that are members in the actual group.

Example:

```
from_host = mail.domain1.com, domain1.net

from_host = domain2.org
```

to_host = enumeration

Description: Parameter used for specifying the receiving host names members in the actual group.

Example:

```
to_host = domain3.com, domain3.net

to_host = domain3.com
```

Engine actions

The following parameters are used to define the actions for the scanning engine: **infected_actions, suspicious_actions.** The `infected_actions` parameter helps you define the actions to be performed when an infected object is found, and the `suspicious_actions` parameter - the actions to be performed when a suspicious object is found.

infected_actions = variable

Description: Parameter used for specifying a variable name defined in the `define_actions` section, which contains the actions to be performed when an infected object is found. If this parameter is not defined then the *reject* action is used for the infected mails.

Example:

```
infected_actions = act_for_infected_files
```

Where:

```
act_for_infected_files = clean, move, delete, reject
```

In this example, when an infected file is detected, **ravcgate** tries first to *clean* that file. If the cleaning action is completed successfully, **ravcgate** moves to the next file. If the cleaning action fails, **ravcgate** tries to *move* (*copy* to quarantine and *delete* that file from mail) the file. If the moving action is completed successfully, **ravcgate** moves to the next file. If the moving action fails, **ravcgate** tries to *delete* the file, and so on. The *ignore* and *reject* actions **always** return success.

Note: RAV AntiVirus appends a *reject* action to the actions enumeration by default.

suspicious_actions = variable

Description: Parameter used for specifying a variable name defined in the `_define_actions` section, which contains the actions to be performed when a suspicious object is found. If this parameter is not defined then the *reject* action is used for the suspicious mails.

Example:

```
suspicious_actions = act_for_suspicious_files
```

Where:

```
act_for_suspicious_files = move, rename, delete, ignore
```

As in the previous example, when **ravcgate** detects a suspicious file, it tries successively to *move*, *rename* and *delete* that file. If the move action fails, **ravcgate** tries to rename the file (see bellow the description for ***rename_ext***). If the *rename* action fails, **ravcgate** tries to *delete* the file. If one of the previous actions is successfully completed, **ravcgate** moves to the next file. Eventually, if all of the actions (*move, rename, delete*) fail, **ravcgate** will ignore that file.

Engine parameters

use_heuristics = boolean

Description: This parameter is used to control the heuristic methods for detecting new viruses.

Default value: **Yes**.

Example:

```
use_heuristics = no
```

scan_packed_executables = boolean

Description: This parameter is used to control the scanning process for packed executables (i.e. `vvpack`, `ucexe`, `pepack`, etc.)

Default value: **Yes**.

Example:

```
scan_packed_executables = no
```

scan_archives = boolean

Description: This parameter is used to control scanning in archive files, like **ZIP**, **ARJ**, **RAR**, **LHA**, **LHZ**, **ACE**, **CAB**, etc. If the boolean value is set to **Yes**, **ravcgate** will scan inside archives. If the boolean value is set to **No**, **ravcgate** will not scan inside archives.

Default value: **Yes**.

Example:

```
scan_archives = yes
```

rename_ext = string

Description: Parameter used for specifying the *extension* used to *rename* the infected/suspicious files. This function is necessary for preventing inexperienced users from accessing by accident infected/suspicious files moved to Quarantine.

Default extension is: **_??**

Example:

```
rename_ext = _??
```

smart_scan = boolean

Description: Parameter used for specifying the scanning modes for **ravcgate**. The available options are:

- scan all files,
- let RAV decide what files to scan.

Note:	If **smart_scan** *is not defined* then **ravcgate** will scan all files. By default, the smart scanning is enabled.

Example:

```
smart_scan = yes
```

Warning messages

The following parameters help you define the messages used to create warning mails in different circumstances (virus found, subject filter match, attachment filter match, content filter match).

If some warning messages are not specified for the [`global`] group, then **ravcgate** uses a default string (`<<not defined>>`). For all the other groups, the warning messages are inherited from the [`global`] group.

_virus_warning_messages

Description: Parameter used for specifying the contents of the warning mail sent by **ravcgate** when a virus is found in one mail message.

_subject_filter_warning_messages

Description: Parameter used for specifying the contents of the warning mail sent by **ravcgate** when the content filtering is enabled and the search in the mail's **Subject** field has yielded a match with one of the user-defined rules.

_attachment_filter_warning_messages

Description: Parameter used for specifying the contents of the warning mail sent by **ravcgate** when the content filtering is enabled and the search in the mail's **Attachment's name** field has yielded a match with one of the user-defined rules.

_content_filter_warning_messages

Description: Parameter used for specifying the *content* of the warning mail sent by **ravcgate** when the content filtering is enabled and the search in the mail's **Body** or **Attachment** has yielded a match with one of the user-defined rules.

warning_mail_subj = variable

Description: Parameter used for specifying the *subject* of the warning mails.

Example:

```
warning_mail_subj = wm_sbj
```

Note:	In the **Warning Mails Message Declarations** section you must specify: `wm_sbj = "RAV AntiVirus scan results."`

infected_msg = variable

Description: Parameter used for specifying the *body* of the warning mail sent by **ravcgate** when an *infected* file is detected.

Example:

```
infected_msg = wm_inf_msg
```

Where:

```
wm_inf_msg = "The file ATTACH_NAME attached to mail
(with subject:SUBJECT) sent by FROM_USER to TO_USER(S)
is infected with virus: VIRUS_NAME."
```

suspicious_msg = variable

Description: Parameter used for specifying the *body* of the warning mail sent by **ravcgate** when a *suspicious* file is detected.

Example:

```
suspicious_msg = wm_sus_msg
```

Where:

```
wm_sus_msg = "The file ATTACH_NAME attached to mail
(with subject:SUBJECT) sent by FROM_USER to TO_USER(S)
contains suspicious code."
```

ignored_msg = variable

Description: Parameter used for specifying the *body* of the warning mail sent by **ravcgate** when an *infected/suspicious* mail file is ignored.

Example:

```
ignored_msg = wm_ign_msg
```

Where:

```
wm_ign_msg = "All defined actions have failed. Do not
use this file."
```

rejected_msg = variable

Description: Parameter used for specifying the *body* of the warning mail sent by **ravcgate** when an *infected/suspicious* mail file is rejected.

Example:

```
rejected_msg = wm_rej_msg
```

Where:

```
wm_rej_msg = "The mail was rejected because it contains
dangerous code."
```

cleaned_msg = variable

Description: Parameter used for specifying the *body* of the info mail sent by **ravcgate** when a file is *cleaned*.

Example:

```
cleaned_msg = clean_ok
```

Where:

```
clean_ok = "The file was successfully cleaned by RAV
AntiVirus."
```

moved_msg = variable

Description: Parameter used for specifying the *body* of the info mail sent by **ravcgate** when a file is *moved*.

Example:

```
moved_msg = move_ok
```

Where:

```
move_ok = "The file was successfully moved to
quarantine with name: QUARANTINE_NAME."
```

copied_msg = variable

Description: Parameter used for specifying the *body* of the info mail sent by **ravcgate** when a file is *copied*.

Example:

```
copied_msg = copy_ok
```

Where:

```
copy_ok = "The file was successfully copied to
quarantine with name: QUARANTINE_NAME."
```

deleted_msg = variable

Description: Parameter used for specifying the *body* of the info mail sent by **ravcgate** when a file is *deleted*.

Example:

```
deleted_msg = delete_ok
```

Where:

```
delete_ok = "The file was successfully deleted by RAV
AntiVirus."
```

renamed_msg = variable

Description: Parameter used for specifying the *body* of the info mail sent by **ravcgate** when a file is *renamed*.

Example:

```
renamed_msg = rename_ok
```

Where:

```
rename_ok = "The file was successfully renamed by RAV
AntiVirus."
```

cannot_clean_msg = variable

Description: Parameter used for specifying the *body* of the warning mail sent by **ravcgate** when a file *cannot be cleaned*.

Example:

```
cannot_clean_msg = not_cleaned
```

Where:

```
not_cleaned = "Cannot clean this file."
```

cannot_move_msg = variable

Description: Parameter used for specifying the *body* of the warning mail sent by **ravcgate** when a file *cannot be moved*.

Example:

```
cannot_move_msg = not_moved
```

Where:

```
not_moved = "Cannot move this file."
```

cannot_copy_msg = variable

Description: Parameter used for specifying the *body* of the warning mail sent by **ravcgate** when a file *cannot be copied*.

Example:

```
cannot_copy_msg = not_copied
```

Where:

```
not_copied = "Cannot copy this file."
```

cannot_delete_msg = variable

Description: Parameter used for specifying the *body* of the warning mail sent by **ravcgate** when a file *cannot be deleted*.

Example:

```
cannot_delete_msg = not_deleted
```

Where:

```
not_deleted = "Cannot delete this file."
```

cannot_rename_msg = variable

Description: Parameter used for specifying the *body* of the warning mail sent by **ravcgate** when a file *cannot be renamed*.

Example:

```
cannot_rename_msg = not_renamed
```

Where:

```
not_renamed = "Cannot rename this file."
```

Specifying the sender of the warning mails

ravms_name = string

on_host = string

smtp_server = string

smtp_port = number

Description: Using these parameters you can define the mail address for the sender of the warning mails. *Default values* are provided and they will probably work. Define these fields only if warning mails are sent when a virus is found or if you want to use a different account instead of **ravms**. Specify the **smtp_server** IP address only if that machine is behind a firewall and **ravcgate** can't get its host name. If you are using Postfix as MTA then you can set **ravcgate** to use a specified port when sending warning mails. Setting **smtp_port** on 10026 (in our configuration example) will make Postfix to send those mails without being

scanned.

Default values:

ravms_name = ravms

on_host = official host name

smtp_server = official host IP address

smtp_port = 25

Example:

```
ravms_name = ravms

on host = ravantivirus.com

smtp_server = 127.0.0.1

smtp_port = 25
```

The mail address displayed in the warning mail will be: "RAV Antivirus Scanner" <ravms@ravantivirus.com>.

no_subject = string

Description: Parameter used for specifying the string replacing the `SUBJECT` macro in the warning mail if **ravcgate** does not find a valid subject in the infected email.

Default value: **--no subject found--.**

Example:

```
no_subject = "original mail didn't contain any subject
field"
```

mailer_daemon = string

Description: Parameter used for specifying the name that will replace the `FROM_USER` macro when the mail sender is **<>**.

Default value: **--unknown--**.

Example:

```
mailer_daemon= "MAILER-DAEMON"
```

Miscellaneous parameters

These parameters are inherited by additional groups from the [global] group.

custom_msg = number

The warning mails are created using the strings defined by the user in the _define_strings section and RAV-related information (always added during the evaluation period). A warning mail looks like this:

RAV AntiVirus for OSTYPE version: x.x.x (snapshot-yyyymmdd)
Copyright (c) 1996-2001 GeCAD The Software Company. All rights reserved.
X more days to evaluate. (or: Registered version for N domain(s).)
Running on host: HOSTNAME

The file ATTACHED_NAME attached to mail (with subject:SUBJECT) sent by FROM_USER to TO_USER(S) is infected with virus: VIRUS_NAME. The file was successfully deleted by RAV AntiVirus.

Scan engine 8.7 () for i386.
Last update: Thu, 27 Jun 2002 15:44:53 +0300
Scanning for 68249 malwares (viruses, trojans and worms).

To get a free 30-days evaluation version of RAV AntiVirus v8 (yet fully functional) please visit:
http://www.ravantivirus.com

The macros are replaced with their corresponding values. In the registered version of **RAV AntiVirus for CommuniGate Pro on Windows**, all RAV-related information can be omitted, except for the first header line.

In the registered version the warning mails can be customized.

Default value: **127** (use all RAV-related information).

Accepted values:

= 0 – No information.

+ 1 – Add "Registered version ..."

+ 2 – Add "Running on host ..."

+ 4 – Add "Scan engine ..."

+ 8 – Add "Last update ..."

+16 – Add "Scanning for ..."

+32 – Add "To get a free 30-days ..."

+64 – Add "Copyright ..."

Example:

custom_msg = 60

```
RAV AntiVirus for OSTYPE version: x.x.x (snapshot-
yyyymmdd)

The file ATTACHED_NAME attached to mail (with subject:
SUBJECT) sent by FROM_USER to TO_USER(S) is infected
with virus: VIRUS_NAME.

The file was successfully deleted by RAV AntiVirus.

Last update: Thu, 27 Jun 2002 15:44:53 +0300
```

timeout_per_file = number

timeout_per_mega = number

Description: These parameters are used to specify the maximum time in seconds that a scanning process can spend on a file. The total timeout is computed using the following formula:

*timeout_per_file + timeout_per_mega * filesize/1Mb*

Accepted values: **10**-**600** (for **timeout_per_file**), respectively **5**-**600** (for **timeout_per_mega**).

Default values: **60** for `timeout_per_file` **30** for `timeout_per_mega`.

Example:

```
timeout_per_file = 120

timeout_per_mega = 25
```

save_infected = boolean

save_suspicious = boolean

Description: Parameter used for specifying if infected/suspicious mail files are saved to the local disk before executing any action. You can set these options to **Yes** or **No**.

Default value: **Yes**.

Note:	The infected/suspicious messages will be placed in the quarantine regardless of the defined `infected_actions` and `suspicious_actions`.

Example:

```
save_infected = no

save_suspicious = yes
```

quarantine = string

Description: String used to specify the directory where the infected/suspicious mails are saved.

Default value: **c:\.**

Example:

```
quarantine = C:\Program Files\GeCAD\RAV8 CGatePro\tmp
```

RAV logging system

When **ravcgate** is launched, a log file containing user-specified parameters is created in: `C:\Program Files\GeCAD\RAV8 CGatePro\log`.

It is possible to use a different log file for every group, with different options for it. For this you have to declare one of the log options in that group. If a group doesn't contain any log options then the log data for the [`global`] group will be used.

Here are the parameters used for RAV logging system:

log_level = number

Description: Number controlling the logging level used by **ravcgate**.

Default value: **4** (use all RAV information).

Accepted values:

0	log only errors (i.e. can't fork, can't read from socket, etc.)
1	level 0 + scanned file name and result of scanning process
2	level 1 + intermediate actions + log rules matched
3	level 2 + log LICENSE LIMIT warnings
4	level 3 + mail sender and receiver names
5	level 4 + the matched group name

log_file_size = number

Description: Number specifying the maximum length of log file in kilobytes. The value must be in the [1000-MAX_INT] interval.

Default value: 200000.

Example:

```
log_file_size = 150000
```

Group-specific parameters

The following parameters must have **different** values for every defined group. If these parameters are not defined for each group, their values are **NOT** copied from the [`global`] group. The *default values* are specified for each of these parameters in the following section.

filter_subject variable_1 variable_2

Description: This parameter is used to filter the mail subject.

variable_1 is a regular expression defined in the Regular Expression Declaration section.

variable_2 is a variable defined in the Action Definitions section. If this parameter is not defined then the content filtering for subject is disabled.

Example:

```
filter_subject subj_regexp subj_actions
```

Where:

```
subj_regexp = I love you
```

```
subj_actions = reject
```

Using this rule, mails having the "I love you" string in the subject field will be rejected. You can use here a regular expression, not just a simple string.

filter_attachment variable_1 variable_2

Description: This parameter is used to filter the names of the mail attachments.

variable_1 is a regular expression defined in the Regular Expression Declaration section.

variable_2 is a variable defined in the Action Definitions section. If this parameter is not defined then the filter for attachment names is disabled.

Example:

```
filter_attachment file_regexp file_actions
```

Where:

```
file_regexp = .*.((vbs)|(exe)|(com))

file_actions = delete, reject
```

This filtering rule deletes all the attached files with extension ".vbs", ".exe" or ".com" from any mail.

If a file cannot be deleted then the whole mail is rejected.

filter_content variable_1 variable_2

Description: This parameter is used to filter the mail body and the contents of the attachments.

variable_1 is a regular expression defined in the Regular Expression Declaration section.

variable_2 is a variable defined in the Action Definitions section. If this parameter is not defined then the content filtering for mail body and the contents of the attachment is disabled.

Example:

```
filter_content body_regexp_1 body_actions_1
filter_content body_regexp_2 body_actions_2
```

Where:

```
body_regexp_1 = confidential.*document
body_regexp_2 = .*salaries.*
body_actions_1 = delete, reject
body_actions_2 = copy, ignore
```

In this case the filter has to search for both the regular expressions specified. Every rule has a priority associated. The rule with the highest priority is the first specified and it has priority 1. The next rules receive a lower priority (2...n). In our example, **ravcgate** will start searching for both regular expressions at the same time. If the first matched is found with the expression of higher priority (`body_regexp_1`) the search stops and actions from `body_actions_1` are executed. If the first match is found with the expression of lower priority (`body_regexp_2`) the search will continue for the rest of the e-mail in order to verify matchings with the expressions of higher priority. If the rest of the e-mail contains a match with `body_regexp_1` **ravcgate** executes `body_actions_1` and ignores the first match. If no match with `body_regexp_1` is found, then **ravcgate** executes `body_actions_2`.

warn_sender = enumeration

Description: Use this parameter to specify when to send warnings to the mail sender. The valid keywords are explained in the table below.

warn_receiver = enumeration

Description: Use this parameter to specify when to send warnings to the mail receivers. The valid keywords are explained in the table below.

warn_admin = enumeration

Description: Use this parameter to specify when to send warnings to the mail receivers. The valid keywords are explained in the table below.

You have to specify *who* is warned by **RAV AntiVirus for CommuniGate Pro on Windows** and *when*. If one of these parameters is not defined then the respective user category will **not** receive warnings. The valid keywords are:

Keyword	Meaning
`found_virus`	Send alert to the defined recipients when a virus is found.
`found_subject`	Send alert to the defined recipients when the subject matches a content filtering rule.
`found_attach`	Send alert to the defined recipients when an attached file name matches a content filtering rule.
`found_content`	Send alert to the defined recipients when the mail body contains a string matched by a content filtering rule.
`always`	Send alert to the defined recipients in all the above-mentioned situations.

Table 3: **Valid keywords for warning mails.**

Please note that these values are not inherited from the [`global`] group. This way you can specify different warning policies for different groups.

Example 1:

```
warn_sender = found_virus, found_subject, found_attach,
found_content

warn_receivers = found_virus

warn_admin = always
```

In this example, the sender is warned whenever a virus is found *or* the subject matches a content filtering rule *or* an attached file name matches a content filtering rule *or* the mail body contains a string matched by a content filtering rule. The receivers are warned whenever a virus is found. The

administrator is always warned.

Example 2:

```
warn_sender = found_virus, found_subject
```

In this example, the sender is warned whenever a virus is found *AND* the subject matches a content filtering rule.

Example 3:

```
warn_receivers = found_virus, found_subject,
found_content
```

In this example, the receivers are warned whenever a virus is found *AND* the subject matches a content filtering rule *AND* the mail body contains a string matched by a content filtering rule.

do_not_scan = boolean

Description: Parameter used for specifying if the mail files for the current group are scanned or not. This way it is possible to exclude some mail addresses and/or domains from the scanning process.

Default value: **No**.

Example:

```
do_not_scan = yes
```

do_not_warn = enumeration

Description: Parameter used for specifying the mail address that will not be notified.

do_not_show = enumeration

Description: Parameter used for specifying the mail address that will be hidden in all warning mails.

Note: Why is this parameter required? There may be cases when one user should not be notified or his mail address should not be displayed in the warning mails. If this is the case, these options will help you solve

the problem. Note that only the receiver's mail address is compared against the specified address.

These parameters have no *default values* (no comparisons will be made).

Example:

```
do_not_warn = user3@domain2.org

do_not_show = user1@domain1.com, user2@domain1.com
```

admin_addr = enumeration

Description: Parameter used for specifying the mail addresses of the administrators that will be notified when an infected or suspicious file has been detected. This warning mail contains messages created using the strings specified for each situation. This parameter has no *default value*.

Example:

```
admin_addr = postmaster@domain1.com,
postmaster@domain2.net, user1@domain1.com

admin_addr = ravmails@stats.ravantivirus.com
```

Note: Forwarding warning mails to ravmails@stats.ravantivirus.com in case of virus infections is highly recommended. This will help RAV Research Team to determine the level of spreading for new viruses or pinpoint potential detection problems. The Technical Support team at GeCAD Software may also diagnose potential problems for the user, such as old updates of the virus signatures database. In any case, the user will be informed about the best solution for solving his problem. GeCAD Software treats each mail in strict confidence.

BUGS

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

RAVAV configuration file

NAME

ravav - RAV AntiVirus command line version for Windows OS-s.

SYNOPSIS

```
ravav [OPTION ...] TARGET [TARGET ...]
```

DESCRIPTION

ravav is a command line antivirus. It is able to detect and remove known and unknown computer viruses, trojans and worms. It uses the same engine as all other RAV products, with daily updates available on our web site: http://www.ravantivirus.com/**.**

OPTIONS

The following parameters are currently recognized by **ravav**:

-h, --help

Print the help screen to the console.

-v, --version

Display **ravav** version.

-V, --virlist

Print viruses list.

--license=AuthorizationCode

Licenses **ravav** using the Authorization Code provided by your supplier, as a string.

-u, --update=engine|full

Start RAV AntiVirus updating process. If the parameter is set to `engine`, only RAV Engine is updated. Is the parameter is set to `full`, all the files pertaining to the product are updates.

--host=host_name

Download files from host_name. Current **ftp** sites are:

ftp://ftp.ravantivirus.com/ (site located in Romania);

ftp://download.ravantivirus.com/ (site located in USA).

--ravpath=ravbasedir

Full path to the installation directory for RAV AntiVirus. Default value for **engine_dir** is `C:\Program Files\GeCAD\RAV8 CgatePro.`

--hostpath=dirname

RAV path on **ftp** host. Default value for **dirname** is `/pub/rav`.

--ftpuser=username

The user name used on the ftp connection. Default value for **ftpuser** is "ftp"

--ftppass=password

The password used on the ftp connection. Default value for **ftppass** is "rave@".

--all

Scan all files (default).

--smart

Use smart scan mode.

--ask

Ask the user what settings to be used for scanning.

--clean

Clean viruses from infected objects.

--delete

Delete infected and suspicious files

--copy

Copy infected/suspicious objects to quarantine.

--move

Move infected/suspicious objects to quarantine.

--rename

Rename infected/suspicious using the extension defined with: **-R** option.

-A, --archive

Scan inside archives.

-M, --mail

Scan mail files.

-H, --heuristics=on|off

Control the heuristic scanning.

-I, --integrity_check=on|off

Enable/disable integrity checker.

-Q, --quarantine=dir_name

Specify the path to the Quarantine folder. Default value for **dir_name** is `c:\.`

-R, --rename_ext=extension

Specify the extension used for rename action. Default extension is "_??".

-l, --listall

List all scanned files.

--report=filename

Report names of viruses found in the **filename** file.

--rptall

Include all scanned files in the **filename** file.

--append

append information to the filename file.

EXIT STATUS

ravav returns the status of the last executed action:

1 The file is clean.

2 Infected file.

3 Suspicious file.

4 The file was cleaned.

5 Clean failed.

6 The file was deleted.

7 Delete failed.

8 The file was successfully copied to quarantine.

9 Copy failed.

10 The file was successfully moved to quarantine.

11 Move failed.

12	The file was renamed.
13	Rename failed.
20	No TARGET is defined.
30	Engine error.
31	Syntax error.
32	Help message.
33	Viruses list.
34	The updating process was successfully completed.
35	The updating process failed.
36	Already updated.
37	The licensing process was successfully completed.
38	The licensing process failed.

BUGS

Please mail bug reports and suggestions to:

mailto:ravteam@ravantivirus.com

RAVCGATE configuration file

NAME

ravcgate.exe - RAV AntiVirus filter for CommuniGate Pro on Windows OS-s

SYNOPSIS

```
rav8basedir/bin/ravcgate.exe [-cdrhRtv] [--config=config_file] [--dump_conf=config_file] [--reload] [--help] [--rav8path=rav8basedir] [--testconf=config_file] [--version]
```

DESCRIPTION

This is the external filter program executed by CommuniGate Pro server in order to scan all messages for virus protection and/or content filtering. The program runs as a "filter client" for RAV AntiVirus mail scanning daemon (**ravcgate**).

ravcgate is powered by the platform-independent *RAV Engine*, so it can detect and clean all viruses detected by this revolutionary engine (Linux, Windows, DOS, macros, Trojans, hoaxes, etc.).

The program can scan e-mail files in **MIME** format containing attachments encoded with: **base64**, **quoted-printable**, **uuencode**, **7bit**, **8bit**.

ravcgate also supports e-mail content filtering for the e-mail subject, attachment file names and message body.

OPTIONS

The following arguments are mandatory for both long and sort options.

-c, --config=config_file

Use the `config_file` instead of `rav8basedir/etc/ravcgate.conf`

-d, --dumpconf=config_file

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

-r, --reload

Sends to the running filter a reload signal. After every modification in the configuration file or after an engine update it is mandatory to send a reload signal to **ravcgate**.

-h, --help

Display the help screen.

-R, --rav8path=rav8basedir

Full path to the installation folder for RAV AntiVirus.

-t, --testconf=config_file

Test the configuration from `config_file`.

-v, --version

Display **ravcgate** version.

FILES

`rav8basedir/etc/ravmd.key`

This file contains an initialization key for **RAV** engine. **ravcgate** is **fully functional** for an *evaluation period* of 30 (thirty) days. During this evaluation period, **ravcgate** can scan all mails received/sent by **two** domains. For registered users, this file contains a unique RAV key string.

`rav8basedir/etc/ravcgate.conf`

File used for managing **ravcgate**'s behaviour. See `ravcgate.conf.pdf` for more information.

USAGE

- Set your domain names as values for the domain field in `ravcgate.conf` (you can find it in `C:\Program Files\GeCAD\RAV8 CGatePro\etc`).
- Open your web browser and connect to the CommuniGate Pro's web administration interface. If you installed CommuniGate Pro using the default values, type http://127.0.0.1:8010 in the address bar.
- Open **Settings->General->Helpers**.

- Check **Content filtering** and add the following path in **Program Path**:
  `C:\Program Files\GeCAD\RAV8 CGatePro\bin\ravcgate.exe`
- Click on the **Update** button.
- Go to **Settings->Rules** and create a new rule (i.e. **rav**) and choose **Action** as **External Filter**.
- Create **ravms** account (this account will be used for sending warning mails via the SMTP local port opened by CommuniGate Pro):

  Go to Accounts->Create Account ravms

Important:	For more details on how to make a rule for an External Filter, visit http://www.stalker.com/CommuniGatePro/VirusScan.html#Scanning.
Note:	RAV AntiVirus can scan multiple files in parallel. To activate this facility you must select more processors in **SETTINGS->Queue->Message Enqueuer**.

BUGS

Please mail bug reports and suggestions to:

mailto:ravteam@ravantivirus.com

Appendix A: Bug Report Form

Although we have extensively tested **RAV AntiVirus for CommuniGate Pro on Windows**, some bugs may get by us, or you may have incompatible hardware or software that we did not test.

If you experience any problems with **RAV AntiVirus for CommuniGate Pro on Windows**, please print out this form and mail it to:

GeCAD Software S.R.L.
223, Mihai Bravu Blvd, 3rd district
Bucharest, ROMANIA,

or fax it at +40-21-3217803.

Alternatively, copy the **Bug Report Form** to your word processor, fill in the blanks and email the text file to support@ravantivirus.com or to betatest@ravantivirus.com (when the product you are reporting the bugs for has been beta released)**.**

Thank you!

Today's Date: ___/___/___ (MM/DD/YY)
Title: [ ] Mrs. [ ] Miss [ ] Ms [ ] Mr. [ ] Other:_____
Name:
Company (if applicable):
E-mail:
Address:
City:
State/Province:
ZIP/Postal Code:
Country:
Telephone (with Area & Country Codes):
Fax (with Area & Country Codes):

Program Name: RAV AntiVirus for CommuniGate Pro on Windows version: __ Registration Code:_____

Bugs, suggestions & comments:

(Please be as specific as possible about bugs. If we cannot duplicate your problem, we cannot help get it fixed. Please read the program's documentation carefully first.)

SYSTEM CONFIGURATION

Type of CPU:

CPU frequency:

OS version:

Memory:

Hard disk:

Other: