TECHNICAL NOTE

WebConfig for RAV AntiVirus for Mail Servers

Release date: November 28, 2002
Product version: 2.0
Technical Note revision: 1.1

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

TECHNICAL NOTE

CONTENTS

TECHNICAL NOTE

Scope

This document describes the features and functionality of the **WebConfig for RAV AntiVirus for Mail Servers**. Additional valuable documentation is also separately available - see the Related documentation section below.

To make sure you will be efficiently using **RAV AntiVirus for Mail Servers** from the very beginning, we strongly recommend you to read carefully this *Technical Note*, even if you have been using a previous version of this product.

Intended audience

This *Technical Note* is intended for administrators responsible with the installation of **RAV AntiVirus for Mail Servers**. 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 document:

- **RAV AntiVirus for Mail Servers** – *Release Notes* (available here);
- **RAV AntiVirus for Mail Servers** – *Product Sheet* (available here);
- **RAV AntiVirus for DMail on Windows** - *User Guide* (available here**);**
- **RAV AntiVirus for CommuniGate Pro on Windows -** *User Guide* available here**).**

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 producing, developing and internationally distributing high quality anti-virus products.

TECHNICAL NOTE

Description

The **WebConfig** was created to help the system administrator configure **RAV AntiVirus for Mail Servers** (**ravmd**) using a more logical and comprehensible *web interface*.

While this **WebConfig** was created as a module for Webmin configuration tool, there is absolutely no technical limitation whatsoever for installing the program on any web server (e.g. Apache), provided of course you have the required knowledge about installing CGI programs on your server and that you can secure the server against unwanted intruders.

WebConfig is sitting right between you and your configuration file for **RAV AntiVirus for Mail Servers**, trying to ease-up the configuration process by grouping the parameters in logical categories.

As you are probably aware by now, while there is a plethora of configuration parameters in `ravmd.conf`, at minimum you need to define only 1 (one) parameter before starting the daemon: the domain parameter. It is highly advisable to set the language parameter, used for the warning messages - in fact you can now achieve this using the **WebConfig**.

These two parameters (the domain and the language) are part of a default group called `[global]`. The `[global]` group must be always included in your configuration. So at minimum, **ravmd** will work after defining only one group (the `[global]` one) and two parameters: the domain and the language parameters.

What happens when you choose not to define any other parameter besides the domain and the language parameters? In this case **ravmd** will use the "default" values. According to the definition you can find in the corresponding *User Guide* (see section Related documentation above), a default is a predefined value for one parameter. If that parameter is missing from `ravmd.conf` then it is considered to have that default value.

However, if you want to feel the real power of **RAV AntiVirus for Mail Servers**, you should set the other parameters of **ravmd** according to your needs. These parameters can be divided logically in several Sections:

- **Globals**: This section contains really global parameters defining how the daemon should start, the scanning settings, the domains to be scanned, etc.
- **Warnings**: This section allows you to specify in what conditions **ravmd** should send warning messages, to whom, etc.
- **Logging**: Parameters setting the way **ravmd** treats its log files.
- **Embedding**: Parameters specifying in what conditions should **ravmd** embed a copy of the message in the warning emails.
- **Content Filtering**: Parameters and rules for tuning **ravmd**'s built-in content filtering mechanism.
- **White/Black List (WBL)**: Rules allowing you to specify people or computers from which you want to unconditionally accept/reject messages.
- **Real-time Blackhole List (RBL)**: Parameters and site names for the **ravmd**'s built-in Real-time Blackhole List mechanism.

For more information about these sections and the corresponding parameters, please read the "Configuration file for **ravmd**" (see the section Related documentation above).

If you need more flexibility and complexity, **ravmd** allows you to create additional groups complementing the `[global]` one. You can set the name of these groups whatever you like (using letters and numbers). All what **ravmd** wants is to understand how is the newly created group different from the `[global]` one. Therefore for any newly created group you should define at least one of the following parameters: `from_host` or `to_host` or `sender` or `receiver`.

TECHNICAL NOTE

As in the **[global]** group's case, we advise you (and enforce it with this **WebConfig**) to set the language for the newly created groups.

Each newly created group supports pretty much the same categories as the **[global]** one. The notable differences are the lack of the RBL section (there is only one RBL parameter, in the Globals category: **use_rbl**) and the occurrence of the 4 group-specific parameters described in the previous paragraph.

For most of the regular groups parameters, if you do not define a value, the default one will be inherited from the **[global]** group. For more info, please refer to the "Configuration file for **ravmd**".

If you understand the logical organization of **ravmd** using groups (global and other regular groups) then you understand 90% of the configuration. The rest of the logical categories are only some auxiliary tools that serve the groups. Let's analyse them:

- *Regular expressions*: Allow you to define some variable names, containing a regular expression (regexp). These regular expressions can be afterwards used wherever a group parameter needs one, for identifying some text patterns in different conditions (e.g. filter rules from "Content Filtering" section of any group).
- *Actions*: Allow you to define some variable names, containing an enumeration of action that will be performed. These actions can be afterwards used wherever a group parameter needs one, for deciding what to do if a certain event occurred (e.g. again the filter rules from "Content Filtering" section).
- *Strings*: Messages definitions that are independent of any language (they are only a unique set). Currently, the strings are used further only in "Antispam directives" section.
- *Antispam directives*: Allow you to define groups of directives for 4 levels of antispam detection accuracy. After defining them you can add them to the "Global" section of any group.
- *Languages*: The languages allow you to re-define the set of messages used by any of your groups. You can modify the existent messages for a language, add a new language and delete an old one. Subsequently you should assign a language to each group.

TECHNICAL NOTE

Features

WebConfig is trying to limit your error-prone actions as much as possible. Therefore, each time you should answer a yes/no question you'll have a list with yes/no values to pick, eliminating the possible spelling errors. You will also have the possibility of choosing the correct items from the lists of regular expressions, actions, languages end so on. These will be built dynamically to include your new additions in the correspondent **Auxiliary** section.

The most complex list is the one presented for the **`antispam_configuration`** parameter, under the "Globals" section for each group. This list will allow you to add/remove values from the parameter in a LIFO mechanism by adjusting dynamically the list of directives you are allowed to use. To clarify the reasons for constructing such a push/pop mechanism, just let us remind you that the **`antispam_configuration`** parameter should not contain 2 (or more) antispam directives for the same accuracy level.

Another type of updating is used for adding rules for content filtering or for WBL. I am talking here about lists formed by existing rules (if any) with different types of controls presented on each line.

- To add a new rule you should use the last input line on screen (the one with empty values) and then click the corresponding "Update line #" button.
- To delete a rule you should select an empty value for any of the controls on that line and then click the "Update line …" button.
- To modify a rule, select the elements from the list or re-enter values in the box provided and the click the correspondent "Update line ..." button.

All the parameters in a page are presented in alphabetical order.

All the **Updates** or **Save** buttons in the group parameters have immediate effect. The page will just reload with the new values and if you updated something on the top of the page (without scrolling) there is good chance you will not even notice when the reloading is executed (if you have a good server and a fast connection). Consequently, there is no problem in pressing a **Save/Update** button for several times: this will just re-save the same values.

Some input you provide will be automatically re-arranged for maximum clarity. For example the lists of comma-separated values can be entered or updated in any style inside the text area box, but they will be displayed one-per-line (e.g. the **`from_domain`** parameter in the **`[global]`** group).

TECHNICAL NOTE

Interface

The interface is organised similarly to the Logical View described above. The functionality allowed is as follows:

"Groups" category

- *"Global group"*: Takes you directly to the "Globals" section of your `[global]` group. Here you can access any other section in the `[global]` group or go one level up to the group management page.
- *"Other groups management"*: Allows you to see the existent groups, to add a new one by inheriting (or not) an existent one, to delete a group (**warning:** you are not allowed to delete the `[global]` group), and to access the edit page for each group. In addition you can use the valuable **include/exclude** mechanism allowing you to keep/edit different groups configurations but to tell **ravmd** that only some of them should be included in the main configuration for the moment. This way, there is no need for deleting a group since you can exclude it now and include it later, according to your needs.

"Auxiliary sections" category

- *"Regular expressions"*: Lets you add/modify/delete regular expressions variables.
- *"Actions"*: Lets you add/modify/delete list-of-actions variables.
- *"Strings definitions"*: Lets you add/modify/delete string variables for later use in the "Antispam directives".
- *"Antispam directives"*: Lets you add/modify/delete lists of antispam directives, that can be later used for the `antispam_configuration` parameter in the "Global" section of each group.

"Languages" category

- *"Language Management"*: Displays a page similar to the group management one, offering you the possibility to add a new language inheriting (or not) an existent one, to edit the messages for each defined language and to delete a language. In addition you can use the **include/exclude** mechanism allowing you to tell **ravmd** to disregard a language or to include it in the main configuration file. There is no need to delete a language since you can exclude it and re-consider it later.

"Control" category

- *"Control panel"*: Offers you the possibility of controlling your configuration files and **ravmd** daemon. On this page:

The **Configuration status** line displays the validity of the config as well as if it was loaded into the daemon or not.

The **Restart** button allows you to end-up an editing session and load it in **ravmd** (if it's valid!).

You'll be able to rollback to the last saved configuration or o any saved config in the past (if not deleted) as well as you'll be able to perform some maintenance on you saved configs, by deleting the ones you don't consider necessary anymore.

Finally you have the possibility to display the **ravmd** licensing information on screen.

TECHNICAL NOTE

General operations

The following control buttons are available on screen:

- The **Magnifier** button: Tests your configuration and gives you as much feedback as possible if you have errors.
- The **Go-back-round-arrow** button: Goes to the upper logical section. The button is displayed only when this section exists (for example when you edit a group it'll get you to the "Group management" page.
- The **Home** button: Return to the main page of **WebConfig**.
- The **Power on/off** button: Takes you back to the main page of **Webmin**.

Browser compatibility

As far as the browser compatibility is concerned, please note that the Web interface does not use JavaScript and DHTML, therefore we do foresee a very large compatibility. Nor does **WebConfig** use cookies (but Webmin does).

However, please note that the product has been extensively tested and is working just fine with the following browsers and versions:

- Internet Explorer 5.x, 6.x
- Netscape Navigator 4.x, 6.x, 7.x
- Mozilla 1.x
- Konqueror 3.x
- Opera 5.x/6.x

Software requirements

The **WebConfig** works with **RAV Antivirus for Mail Servers** version 8.4.1 beta or later.

Concurrent access

The **WebConfig** module does NOT have a file-locking mechanism so concurrent accesses are not allowed. Since it is a configuration interface it is not supposed to be run in multiuser mode, so please take all the precautions needed.

TECHNICAL NOTE

The backup/restore mechanism

For the backup/rollback mechanism we have implemented something similar to the SQL transactions.

Let's consider that your configuration is valid and loaded into **ravmd** and at one moment you decide that you should update a certain parameter.

The moment you click the Save/Update button of any parameter or section of parameters (even without changing any value!) **WebConfig** will make a `tar.gz` mirror of your current configuration before updating the values. In addition an update flag is raised and kept that way from now on.

When you consider you are done with all the required changes and you want to reload **ravmd** read again the configuration, use the **"Control Panel"-> "Restart"** button.

That very moment, if the configuration is valid, **ravmd** is restarted and the update flag is lowered. This is similar to a SQL `commit` event and takes you to the starting point. From now on, the first time you update/save anything a new backup will be generated prior to data modification.

In any moment you have the possibility to:

- Rollback to the previous saved configuration; or
- Restore any of the previous saved configurations.

The configurations are saved in an easy-to-follow `yyyy_mm_dd_hh_mm_ss.tar.gz` format and they can be restored back through the same "Control panel".

If you bring one configuration back you should re-load the **ravmd** afterwards as to read it. The "Configuration Status" line in the control panel is very useful in figuring out what's the status of your recent modifications.

The languages mechanism

While before **WebConfig** it was possible to assign your messages to any variable name and further to use that variable in a `.equiv` mapping, this is no longer the case if you use **WebConfig**.

You should now proceed directly with defining your messages for a language and then assigning the language to the group you desire. **WebConfig** will do for you all the mappings between the group parameters and the messages transparently when you indicate the corresponding language in the "Globals" configuration section.

Example:

Let's suppose you have two defined groups and you want German language to be used for both of them, but with (slightly) different messages. If you already have a `german` language, you should create a `german1` language by inheriting (with the appropriate changes) the first one. Then include both languages in the configuration (using the language **include/exclude** mechanism) and go to your groups and assign `german` and `german1` as required.

The disk file structure

While you must not alter by hand the files if you use **WebConfig** since it might render it unusable, we think you should know how your files are distributed.

Starting with the configuration directory, the file structure is:

- `ravmd.conf`: It has a fixed content, **WebConfig** does not write in `ravmd.conf`.
- `Regexp`: The place where all regular expressions are read/written.

TECHNICAL NOTE

- **Actions**: The place where all actions definitions are read/written.
- **Strings**: The place where all the strings definitions are read/written.
- **Langs**: The place where all available languages are displayed.
- **Antispam**: The place where the antispam directive lists are read/written.
- **Grps**: The place featuring the groups included in you configuration file.
- **Updflag**: A flag file for signalling the updating stage (this file can appear and disappear as necessary).
- **./languages**: Directory containing all existing languages, 2 files per language, whether included in your configuration or not.
- **./groups**: Directory containing all existing groups, 1 file per group, whether included in the configuration or not.
- **./backups**: Directory containing all backups, 1 files per backup.
- **Others...**: Even if **WebConfig** does not use any other files it is very possible that your **ravmd** does (e.g. **rup.conf**).

Copyright

Feedback & technical support

GeCAD Software SRL welcomes your comments and/or suggestions. If you have any problems, please contact us at:

GeCAD Software S.R.L.

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

TECHNICAL NOTE

Knowledge Base

The Knowledge Base is a new service offered to you by the producer of RAV AntiVirus. You can access the Knowledge Base 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 the **RAV AntiVirus** family (RAV AntiVirus Desktop, RAV AntiVirus for Mail Servers, RAV AntiVirus for File Servers, RAV AntiVirus MailFilter and RAV AntiVirus for Instant Messengers).

Virus Encyclopaedia

The **Virus Encyclopedia** is a professional knowledge resource, specially designed to allow you to be always up-to-date with the latest virus information and threats. The Virus Encyclopedia includes information on the most important and interesting viruses, including details on the Description, Payload, Likelihood, Technical Description, Removal Instructions and other important info.

The **Virus Encyclopedia** is available at the following address:
http://www.ravantivirus.com/pages/virus.php

RAV Outbreak Security Service

RAV Outbreak Security Service is a free subscription-based service offered by GeCAD Software as a first-hand information putting users *en-garde* in case of virus outbreaks. In order to subscribe to **RAV Outbreak Security Service**, please visit our website at http://www.ravantivirus.com/pages/outbreak.php and just enter your e-mail address in the field below and press on the **Subscribe** button.