

Doctor Web, Ltd.

Dr.Web[®] antivirus

Integration with CommuniGate Pro for Windows

Administrator Manual

Version 4.33

The material published herein is the property of Doctor Web, Ltd. and may not be reproduced in any form without written permission of Doctor Web, Ltd. and proper attribution.

Dr.Web is a Registered trademark of Doctor Web, Ltd.

Other products mentioned herein are trademarks or registered trademarks of their respective companies.

There might be further improvements and changes in the software not described in this manual. The corrected and supplemented versions of this manual are available at www.drweb.com.

© Doctor Web, Ltd., 2004-2005

Russia, Moscow - Saint Petersburg

<http://www.drweb.com/>

Contents

1.	<i>Introduction</i>	4
1.1.	What is this manual about?	4
1.2.	Terms and abbreviations	5
1.3.	Dr.Web plug-in requirements to OS and Computer	5
2.	<i>Installing and setting up the plug-in</i>	7
2.1.	Installing the plug-in	7
2.2.	Program registration. Key files	9
2.3.	Configuring CommuniGate Pro	10
2.4.	Configuring the Dr.Web plug-in	11
3.	<i>Configurable parameters of the Dr.Web plug-in</i>	13
3.1.	Configuration file parameters	13
3.2.	Blocked masks list	28
3.3.	Notification templates	31
3.4.	Denying sending notifications to specified addresses	34
3.5.	Setting the plug-in reaction restrictions for specified viruses	35
4.	<i>Automatic updating of the virus bases and the plug-in files</i>	37
5.	<i>Contacts</i>	40

1. Introduction

1.1. *What is this manual about?*

The present manual describes a specially designed for antivirus traffic filtering Dr.Web module (plug-in) for CommuniGate Pro for Windows.

The Dr.Web antivirus module (further named as *plug-in*) uses common for all programs of the Dr.Web family engine drweb32.dll and common virus bases.

The documentation describes:

- installation of the plug-in and necessary settings providing for compatibility with CommuniGate Pro
- updating procedures of the virus bases and the plug-in
- configurable plug-in parameters and their impact on the antivirus protection

The documentation does not describe CommuniGate Pro itself. Read the documentation for this mail system, if necessary.



The manual is meant for the employee concerned in the antivirus security (antivirus security administrator), named administrator in this manual.

The Dr.Web antivirus program is in constant development. The additions of the databases of the known viruses are released, as a rule, several times a day. The program itself gets upgraded too. The diagnostics techniques and counteraction to viruses, as well as integration with other applications get constantly improved in the program. And it is not improbable, that some settings and functions of the current version will differ from those described in this manual. To get the present-day information on the program read the electronic documentation included into the delivery package.

1.2. **Terms and abbreviations**

The following terms are used in the manual (table 1).

Table 1. Legend

Legend	Interpretation
 <i>Important</i>	Important remark or instruction
 Attention	Warning on potentially dangerous or erroneous event
<i>Plug-in</i>	A term used as definition or references to a definition
<code>drweb32.dll</code>	Names of files and directories, extracts from configuration files

The following abbreviations are used without further explanation in the Manual:

- OS — operating system.

1.3. **Dr.Web plug-in requirements to OS and Computer**

CommuniGate Pro for Windows is required to install and operate the plug-in.

The Dr.Web plug-in, as well as the mail system itself, run under Windows NT/2000/XP.

The plug-in requirements to the OS and hardware are similar to those of CommuniGate Pro.

Integration of Dr.Web with CommuniGate Pro for Windows



The operation of the updating system of the virus bases and the plug-in files may have certain peculiarities depending on the OS installed (read p. 4).

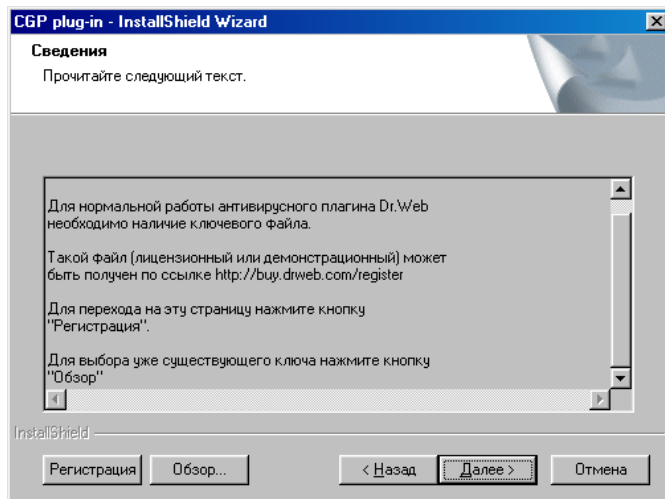
2. Installing and setting up the plug-in

2.1. *Installing the plug-in*

The plug-in distribution is delivered as an executable file. In addition, the distribution kit may contain a license key file (read below for details).

To install the plug-in:

1. Run the executable file of the distribution. You will be invited to select the interface language (Russian or English) of the installation program and to accept or not the terms of the license agreement.
2. Then, you will be asked to install a key file (pic. 1).



Picture 1. Installing a key file

3. To install the key file press the Browse button and choose the necessary file in the standard Windows browser.
To receive a license key file from the web site of the program

Integration of Dr.Web with CommuniGate Pro for Windows

supplier press the `Register` button. A key file request page will open in the web browser's window.

If you are a registered program user and have a serial number, fill in the web form with your personal data stating obligatory the correct e-mail address. The license key file will be sent to the specified address.

You can also receive a demo key file (read below for more details on demo key files). To receive a demo key file select the `Demo key request` item in the `Buy` menu in the left area of the window. A page with the web form will open. You should fill in the form stating as more details as possible. Employees of Doctor Web, Ltd. will decide individually whether or not to send a demo key file (read p. 2.2).

4. Next, you will be invited to select a directory the `drweb` installation directory will be placed to. By default, it is the `BaseDir` directory of CommuniGate Pro.
5. With all the fields filled in, the installation program will ask you either to continue the installation, or to return to previous steps to modify some parameters. To continue installation press the `Install` button.
6. Finally, you will be invited to receive the updates of the virus bases from the Internet and read the electronic documentation file.



Demo key files allow to enjoy full functionality of the program and the virus definitions updates, but have a limited term of use for one month. No users' support is provided.

2.2. **Program registration. Key files**

User's rights to use the antivirus are regulated by the special file called the *key file*.



The electronic signature provides for the write-protected format of the key file. Editing the file makes it invalid. Consequently, it is not recommended to open your key file with a text editor, which may occasionally corrupt it

The location and name of the key file are specified in the program configuration file (read p. 3.1.1).

Users who have purchased Dr.Web from our certified partners obtain a *license key file*. The parameters of the key file are specified according to the license the user has paid for. The license key file contains the name of the user (or a company name), and the name of the selling company.

For evaluation purposes users may also obtain *demo key files*. Demo key files allow to enjoy full functionality of the program and the virus definitions updates, but have a limited term of use and no users' support is provided.

The key file may be supplied with the `key` extension, or as a `zip` archive containing the key file.

The key file may be received in one of the following ways.

- supplied or sent as a zip archive containing a file with the `key` extension (usually after the registration on the web site, explained below).
- included into the distribution package.
- supplied on a media as a file with the `.key` extension.

Integration of Dr.Web with CommuniGate Pro for Windows

The license key file is sent to users via email, as a rule after the registration on the web site (the location of the web site is specified in the registration card accompanying the product). Visit the indicated site, fill in the web form with the customer data and put in the registration serial number (printed in the registration card). The key file will be sent to the specified address.

You should activate the file if, during the installation, there was no key file, or if it was received by you later.

For this:

- Extract the key file from an archive, if it was archived
- Copy it to the directory the `drwebupw.exe` updating plug-in resides (by default, it is `drweb\bin`). Let us agree that the name of this file is `drweb32.key`
- Open the program configuration file (by default, it is `drweb\etc\drweb_cgp.conf`) with a text editor and edit the `Key` parameter of the `[Engine]` section (read p. 3.1.1); the appropriate line should look as follows (in case of default settings)
`Key = drweb\bin\drweb32.key`
- Restart the plug-in

2.3. *Configuring CommuniGate Pro*

To enable CommuniGate Pro (further named as CGP) to check the content of the transferred messages by the antivirus plug-in you should do the following:

- connect CGP through WebAdmin
- go to the `Settings` menu, select the `General` submenu and then `Helpers`

- enable `Content Filtering` and specify the path (absolute or relative to the `BaseDir` directory of the mail system) to the plug-in, and, if necessary, specify the command line parameter for starting the plug-in (read below for details). By default, the plug-in installation program will place the executable file to the relative address `drweb\bin\drweb-cgp.exe`
- specify the `Auto-Restart` parameter value, different from disabled (required for the versions update)
- you may disable the `Timeout` parameter (set the disabled value), or specify the value greater than the `ScanTimeout` parameter value from the `[Scanning]` section of the plug-in configuration file (read p. 3.1.2 for details)
- to enable messages filtering get to `Settings` and select the `Rules` item. To create a new rule specify its name (for example, `drweb-filter`) and press `Create New`. After that select the `External Filter` value for the `Action` parameter, and specify a name of the filter (exactly as you name it in the `Settings -> General -> Helpers`) in the `Parameter` field.

2.4. **Configuring the Dr.Web plug-in**

The main settings of the antivirus plug-in are specified in the program configuration file. By default, this file is named `drweb_cgp.conf` and is located in the program's installation directory. If you wish to use another configuration file specify the appropriate command line of the plug-in startup in `Content Filtering` of the mail system:

```
path_to_plug-in\drweb-cgp.exe --  
                                conf=config_file_name
```

Integration of Dr.Web with CommuniGate Pro for Windows

The name of the configuration file is specified with absolute or relative name.

The format of the configuration file and the values of the settings specified in it are described in p. 3.1.

3. Configurable parameters of the Dr.Web plug-in

3.1. *Configuration file parameters*

Configuration file is a plain text file. The file is divided into sections prepended by the headers in square brackets. Each section contains an arbitrary number of assigned parameter values. The headers of sections and assignments are separated by the line limits. The file generally looks as follows:

```
[Section1]
Parameter1 = value
.....
ParameterN = value
.....
[Section X]
Parameter1 = value
.....
ParameterY = value
```

The parameter values can be of the following types:

- string parameters (STRING), those of paths, names, actions, etc.
- lists of strings parameters (STRING_LIST), the lines separated by commas
- numeric parameters (COUNT), numbers from 0 to $2^{31} - 1$
- octal parameters (OCTAL), numbers in octal representation
- Boolean parameters (BOOL), the values of such variable can be *yes*, *on*, *true* and are used to enable some option (mode), or *no*, *off*, *false* used for disabling (suppose, of any of the given examples, case-insensitive)

Below go the descriptions of the parameters presented as follows: each description begins with the line

```
parameter_name = type_of_value(default_value)
```

or

```
Parameter_name = type_of_value(absent)
```

followed by a detailed description and commentaries on how to apply it.



If setting the relative paths as the parameter values, the `BaseDir` directory of the mail service is considered a current directory.

3.1.1. Antivirus engine parameters

The antivirus engine parameters are specified in the `[Engine]` section.

Key = STRING (absent)

The path (including the name) to the key file.



The parameter is obligatory; if it is absent, or point to incorrect key file, the program will terminate operation.



The current program version requires a key file to be placed to the same directory (`drweb\bin`) where the `drwebupw.exe` automatic updating module resides, otherwise the updating module will fail to operate correctly (read p. 4 for details).

EnginePath = STRING (absent)

The path to the directory with the antivirus engine (`drweb32.dll`).

VirusBases = STRING (absent)

The path to the directory with antivirus bases (vdb files).

TempDir = STRING (absent)

The path to the directory used for the temporary storage of extracted files. If the parameter is not specified, the %TEMP% system directory will be used.



If you have any antivirus resident monitors installed, then include this directory to the excluded paths list.

UpdateTimeout = COUNT (300)

Interval in seconds between the check specifying if the virus bases were updated (drwtoday.vdb was changed).

MaxLoadEngines = COUNT (10)

Maximum number of simultaneously loaded engines.

PreLoadEngines = COUNT (1)

Number of engines loaded at start. If they fail to cope with the loading additional threads will be created, but not exceeding the MaxLoadEngines value.

FreeEngineTimeout = COUNT (120)

Interval (in seconds) for unloading of unused engine.

3.1.2. Setting scan modes

The scan modes parameters reside in the [Scanning] section.

ScanTimeout = COUNT (30)

Timeout (in seconds) for one message scanning.

CheckArchives = BOOL (no)

Enables/disable archives (RAR, ZIP, etc.) scanning.

The following three parameters are used for the protection of the plug-in from the "denial of service" (DoS) attacks (for example, ZIP-death). If a message contains files marching these criteria, it will not be scanned and the action specified in the `ArchiveRestriction` parameter (read p. 3.1.3 below) is applied to it. The value set to 0 for any of these options means it will not be applied.

MaxFileSizeToExtract = COUNT (0)

Maximum size (in kilobytes) of a file to be extracted from an archive. If the file size exceeds this value, the file will neither extracted, and therefore, nor scanned.

MaxCompressionRatio = COUNT (0)

Maximum compression ratio, i.e. the ratio of the unpacked file size to the packed file size (inside an archive). If the ratio exceeds the value the file will neither be extracted, nor checked.

MaxArchiveLevel = COUNT (16)

The maximum archive's nesting level. The files exceeding the specified nesting level will neither be extracted, nor checked.

HeuristicAnalysis = BOOL (on)

Enables/disables the heuristic detection of unknown viruses (may cause false alarms).

IncludeReport = BOOL (yes)

Specifies whether or not the plug-in report should be included into notifications (read p. 3.3, the `$DAEMON_REPORT$` macros).

IncludeStats = BOOL (no)

Specifies whether or not short statistics should be included in notifications (read p. 3.3, the `$SCAN_STAT$` macros).

ReportMaxSize = COUNT (4096)

Daemon's maximum report size (if `IncludeReport = yes`). The value set to 0 means the report size will not be controlled; this may be dangerous, as the reports on "mail bomb" may be of several megabytes.

Below follows a group of the three parameters setting the deny check modes of some messages.

DenyList = STRING (absent)

The parameter sets the path to a file with blocked masks (mail domains and user names); if the parameter is not specified, they are absent (read p. 3.2). The two parameters going below set the mode of integration of the specified masks.

DenyMode = STRING (absent)

The parameter sets the correspondence rule disabling the check for viruses depending on the availability of the sender's and recipient's addresses in the file specified by the `DenyList` parameter.

Disabling of check means a message will be delivered to all the addressees unchecked. The following rules disabling the check are allowable:

- `byAll` — disable, if all the addresses (those of a sender and recipients) are specified as blocked (with correspondent roles) in the blocked masks file
- `byOne` — disable, if at least one address (that of a sender or of recipients) is specified as blocked (with the correspondent role) in the blocked masks file

- `bySender` — disable, if a sender's address is specified as blocked in the blocked masks file
- `bySenderAndOneRecipient` — disable, if a sender's address and of at least recipient are specified as blocked (with correspondent roles) in the blocked masks file
- `byOneRecipient` — disable, if the address of at least one recipient is specified as blocked in the blocked masks file
- `byAllRecipients` — disable, if all the recipients' addresses are specified as blocked in the blocked masks file

DenyByDefault = `BOOL` (`no`)

The parameter instructs to block (with the value set to `yes`) or permit (`no`) the messages check, if not a single address of recipients and senders is not specified in the correspondent blocked masks file.

3.1.3. Setting the plug-in actions

The parameters setting the plug-in actions for different events are located in the `[Actions]` section.



The notifications templates (read p. 3.3) presuppose the default program reaction (particular in cases when, by default, a message is supposed to be moved to the quarantine, the location of the quarantine files is specified in the message). If you modify the default settings you should accordingly edit the notifications templates.

LicenseLimit = `STRING` (`pass`)

Enables the action if a message was not checked due to the license restrictions. The following values are allowable:

- `reject` — deny the receipt of such messages

- `pass` — skip such messages
- `tempfail` — instruct CommuniGate Pro to deliver it later

Infected = STRING (quarantine)

Enables the action if an "infected" object was found in the message body (known virus). Allowable modes are:

- `reject` — deny receipt of such messages
- `quarantine` — move a message to the quarantine and deny delivery
- `redirect` — redirect to the address set by the `RedirectMail` parameter (read below) and deny current delivery of the message
- `discard` — "silently" destroy a message

Suspicious = STRING (reject)

Enables the action if a "suspicious" object is found in the message body, possibly a new virus. Allowable modes are:

- `pass` — skip such messages
- `reject` — deny delivery of such messages
- `quarantine` — move a message to the quarantine and deny delivery
- `redirect` — redirect to the address set by the `RedirectMail` parameter (read below) and deny current delivery of the message
- `discard` — "silently" destroy a message

Adware = STRING (quarantine)

The action taken if a message contains an advertizing software. Allowable modes are:

- `pass` — skip such messages

Integration of Dr.Web with CommuniGate Pro for Windows

- `reject` — deny delivery of such messages
- `quarantine` — move a message to the quarantine and deny delivery
- `redirect` — redirect to the address set by the `RedirectMail` parameter (read below) and deny current delivery of the message
- `discard` — "silently" destroy a message

Dialers = STRING (quarantine)

The action taken if a message contains a dialer program. Allowable modes are:

- `pass` — skip such messages
- `reject` — deny delivery of such messages
- `quarantine` — move a message to the quarantine and deny delivery
- `redirect` — redirect to the address set by the `RedirectMail` parameter (read below) and deny current delivery of the message
- `discard` — "silently" destroy a message

Jokes = STRING (quarantine)

The action taken if a message contains a joke program or hoax. Allowable modes are:

- `pass` — skip such messages
- `reject` — deny delivery of such messages
- `quarantine` — move a message to the quarantine and deny delivery

- `redirect` — redirect to the address set by the `RedirectMail` parameter (read below) and deny current delivery of the message
- `discard` — "silently" destroy a message

Riskware = STRING (quarantine)

The action taken if a message contains a potentially dangerous software. Allowable modes are:

- `pass` — skip such messages
- `reject` — deny delivery of such messages
- `quarantine` — move a message to the quarantine and deny delivery
- `redirect` — redirect to the address set by the `RedirectMail` parameter (read below) and deny current delivery of the message
- `discard` — "silently" destroy a message

Hacktools = STRING (quarantine)

The action taken if a message contains an intrusion tool also known as hacktool. Allowable modes are:

- `pass` — skip such messages
- `reject` — deny delivery of such messages
- `quarantine` — move a message to the quarantine and deny delivery
- `redirect` — redirect to the address set by the `RedirectMail` parameter (read below) and deny current delivery of the message
- `discard` — "silently" destroy a message

Integration of Dr.Web with CommuniGate Pro for Windows

`EmptyFrom = STRING (continue)`

Enables an action if a message has a blank sender's address <>.

Allowable modes are:

- `continue` – continue processing of such messages
- `reject` – deny receipt of such message
- `discard` – "silently" destroy a message



When setting the reaction different from `continue`, your mail system will no longer comply with the requirements of p. 2.6.1 rfc-2505 (The MTA MUST accept messages with <> sender) and can be placed to the www.rfc-ignorant.org blacklist.

`SkipObject = STRING (reject)`

Enables the action if an object, which cannot be checked by the antivirus daemon, is found in a message (for example, a password protected archive). Allowable modes are:

- `pass` – skip such messages
- `reject` – deny receipt of such messages
- `quarantine` – move a message to the quarantine and deny delivery
- `redirect` – redirect to the address set by the `RedirectMail` parameter (read below) and deny current delivery of the message

`ArchiveRestriction = STRING (reject)`

Enables the action if an archive, which cannot be checked by the antivirus plug-in, because its nesting level (or that of a file compressed in it) exceeds the restriction set by the

`MaxCompressionRatio`, `MaxFileSizeToExtract` or `MaxArchiveLevel` parameters, is found in a message. (read p. 3.1.2). Allowable modes are:

- `pass` — skip such messages
- `reject` — deny receipt of such messages
- `quarantine` — move a message to the quarantine and deny delivery
- `redirect` — redirect to the address set by the `RedirectMail` parameter (read below) and deny current delivery of the message

ScanningErrors = STRING (reject)

Enables the action if errors in the daemon occurred during the message processing (for example, insufficient memory or an access for a file was denied).

- `pass` — skip such messages
- `reject` — deny receipt of such messages
- `quarantine` — move a message to the quarantine and deny delivery
- `redirect` — redirect to the address set by the `RedirectMail` parameter (read below) and deny current delivery of the message
- `tempfail` — instruct CommuniGate Pro to deliver it later

ProcessingErrors = STRING (reject)

Enables an action if error in the filter occurred during the message possessing (for example, insufficient memory or connection with the daemon failed). Allowable modes are:

- `pass` — skip such messages

Integration of Dr.Web with CommuniGate Pro for Windows

- `reject` — deny receipt of such messages
- `quarantine` — move a message to the quarantine and deny delivery
- `redirect` — redirect to the address set by the `RedirectMail` parameter (read below) and deny current delivery of the message
- `tempfail` — instruct CommuniGate Pro to deliver it later

AdminMail = STRING (absent)

Specifies the mail address the notifications for an administrator will be sent. The `$POSTMASTER$` macros (read p. 3.3) will be replaced by this address.

FilterMail = STRING (absent)

The address to substitute the notification sender's address. The `$FILTER_MAIL$` macros (read p. 3.3) will be replaced by this address.

RedirectMail = STRING (absent)

The address to which the messages matching the `redirect` action will be directed.

OnUpdateNotify = BOOL (yes)

Specifies whether or not an administrator should be notified on the updates of the virus bases and the search module.

OnStopNotify = BOOL (yes)

Specifies whether or not an administrator should be notified by e-mail on the plug-in termination (including the version update).

UnnotificableVirusesList = STRING (absent)

Specifies a path to the file with the virus list for which the `quarantine` action and sending of notifications may be disabled; if

the name is not specified, such list is considered unavailable. Read p. 3.5 for description of the file format.

UnnotificableAddressesList = STRING (absent)

Specifies a path to the file with the list of addresses for which the quarantine action and sending of notifications may be denied; if the name is not specified, such list is considered unavailable. Read p. 3.4 for description of the file format.

Quarantine = STRING (absent)

A path to the "quarantine" - a directory the infected messages will be placed to.

QuarantineFileNamesMode = STRING (Std)

Sets the mode the new names of files placed to the quarantine directory are created. At present, the following methods are supported:

- `std` — standard. Uses `mkstemp` (template: `%{QuarantineFileNamesPrefix}XXXXXX`)
- `tai` — in TAI format (template: `%sec.%usec.%{QuarantineFileNamesPrefix}XXXXXX`)
- `rand48` — uses `lrand48` (template: `%{QuarantineFileNamesPrefix}XXXXXXXX`)

The `rand48` format can be recommended for heavily loaded systems with incorrectly designed `mkstemp` function (for example, Solaris).

QuarantineFileNamesPrefix = STRING (drweb.quarantine.)

A prefix for quarantine filenames (read above the description of the `QuarantineFileNamesMode` parameter).

3.1.4. Setting up notifications

The notifications rules settings reside in the [VirusNotifications] section.

SenderNotify = BOOL (yes)

AdminNotify = BOOL (yes)

RcptsNotify = BOOL (yes)

Specifies whether or not a sender, an administrator or a recipient should be notified on a virus found in a message.

SenderTemplate = STRING (absent)

AdminTemplate = STRING (absent)

RcptsTemplate = STRING (absent)

Paths to templates of correspondent notifications.

The notification rules denying the check applied as instructed by the program settings are set in the [SkipNotifications] section, in the [ArchiveRestrictionNotifications] section – the rules applied if the breach of restrictions for complexity (size) of an archive happens, in the [ErrorNotifications] section – the rules are applied if the errors during the check occur. The composition, structure and the meaning of the parameters in these sections fully comply with those described above.

3.1.5. Setting up the log file

The log file parameters are specified in the [Logging] section.

Level = STRING (Quiet)

Specifies the information output details level. The following levels are supported:

- Quiet (do not log information)
- Errors (log errors only)

- Alerts (log errors and virus events)
- Info (log errors, virus events and informative notices)
- Verbose (detailed information)
- Debug (debug mode)

The information is output with SyslogPriority and from the SyslogFacility subsystem.

LogFilename = STRING (absent)

A path (including the filename) to the plug-in log file.

LogScanned = BOOL (Yes)

Specifies whether or not the logging of composite objects should be enabled (archives, containers).

MaxLogSize = COUNT (0)

Maximum log file size in kilobytes. By default, it is not limited.

3.1.6. Mail system parameters

The mail system parameters are set in the [Mailer] section.

MailSystem = STRING (CommuniGatePro)

The mail system name should contain the value specified in brackets. The parameter cannot be skipped

SubmitDir = STRING (submitted)

The CommuniGate Pro submitted subdirectory location. The parameter cannot be skipped.

3.2. *Blocked masks list*

3.2.1. Introduction

The blocked masks are used to set the rules on the base of which the plug-in skips without checking some messages depending on a sender's and recipients' addresses.

The rules are set by the `DenyMode` parameter of the configuration file, and the file where the blocked masks are stored is specified in the `DenyList` parameter (read p. 3.1.2).

The lines beginning with `#` are considered commentaries.

There are two versions of the blocked masks file format supported; the first version is reductive, the other possesses more possibilities. The version number may be specified in the first meaningful line of a file as follows

```
[Version=1]
or
[Version=2]
```

By default, the first version is meant.

3.2.2. Second version file format

The file of this version contains lines (entries) of the following format:

```
OPERATION ROLE METHOD MASK
```

OPERATION – it is either `deny`, or `allow` (the first means this entry denies message checking, the second allows it).

ROLE – it is either `from`, or `to`, or `all` (defines whether or not the masks for addresses of a sender, recipients, or for all addresses should be checked).

METHOD may be `exact`, `subst`, `regex` or `cregex`. Specifies if the address matches the MASK field. The `exact` value means an address must strictly correspond to this field. The `subst` value

means, it is sufficient that the MASK is a substring in the address for the address to correspond with it. The `regex` or `cregex` values mean the address should correspond to a regular expression specified in the field. The `exact`, `subst` and `cregex` modes are case-sensitive, the `regex` mode is case-insensitive.

MASK – the line compared with addresses depending on the `MODE` field value. The line should not contain blanks or be included in quotes.

3.2.3. First file format version peculiarities

The entries of this file version look as follows:

```
ACTION MASK
```

The purpose of the fields is similar to the described above. Any entry of the first version can be written as the entry of the second version as follows:

```
ACTION any subst MASK
```

3.2.4. Deny check mode

The following mode sets the message deny check:

1. Let us take a message address (that of a sender and recipients). If no more addresses are available, proceed to item 4.
2. Check the correspondence of this address to the next (following top-down) rule (entry). If no rules left, proceed to item 1. The address corresponds, if the `ROLE` corresponds to the type of the address (address of a sender or a recipient), and the `MASK` field corresponds to the address specified in the `METHOD` field.
3. If the address corresponds to the entry, and the `ACTION` field has the `deny` value, the address will be marked as *denied*. Regardless the value set in the `ACTION` field proceed to item 1. If it fails to correspond, proceed to item 2.

4. If neither address of a message is denied, the message will either be checked or get skipped, depending on the value set in the `DenyByDefault` parameter of the configuration file (read p. 3.1.2). With the `no` value (by default) a message will be checked, otherwise the check is denied.

In other cases the check is allowed or prohibited depending on the value set in the `DenyMode` parameter of the configuration file (read p. 3.1.2). With every value of this parameter, the deny check mode conditions are as follows:

- `byAll` – a check is not performed if all the addresses are denied
- `byOne` – a check is not performed if at least one address is denied
- `bySender` – a check is not performed if a sender's address is denied
- `bySenderAndOneRecipient` – a check is not performed if a sender's address and of at least one recipient are denied
- `byOneRecipient` – a check is not performed if at least one recipient's address is denied
- `byAllRecipients` – a check is not performed if all recipients' address are denied



If the first of the suitable rules (entries) contains the `Allow` action field specified, the address will not be marked as denied (as if neither of rules matches). This allows to set up exceptions from general rules as stated below in example 3.

Example 1.

Deny check of incoming messages for all users except for `asv` with the address from the `.ru` domain:

```
deny to regex ^asv@(.*)\.ru$
```

Example 2.

Deny check of outgoing messages for users of the `drweb.com` domain:

```
deny from regex @(.*)\.drweb\.com$
```

Example 3.

Deny check of messages from the `@company.com` address, except for a user with the `oneuser@company.com` address:

```
allow any exact someuser@any.domain.com  
deny any subst @any.domain.com
```

3.3. Notification templates

The notification templates are plain text messages. The templates on different events addressed to the message sender, its recipient or an administrator, can be included into the plug-in. The names and paths to template files are specified in the program's configuration file. The appropriate parameters of the configuration file are described in p. 3.1.4.

The template bodies may contain macroses (restricted by `$symbols`) replaced by realistic data for the moment the notification is created.

Macroses:

- **`$SENDER$`** - an original message sender's address
- **`$RCPTS$`** - recipients' addresses list

Integration of Dr.Web with CommuniGate Pro for Windows

- **\$SECURE_RCPTS\$** - this macros equals to \$RCPTS\$, if a recipient is one, otherwise, it has the value "Recipients of original message" <#@[]>
- **\$FILTER_MAIL\$** - an address used by the mail filter (will be replaced by the FilterMail parameter value of the configuration file (read p. 3.1.3)
- **\$POSTMASTER\$** - an address notifications will be sent (will be replaced by the AdminMail parameter value of the configuration file (read p. 3.1.3)
- **\$SUBJECT\$** - a message subject (if any, otherwise unknown)
- **\$MSGID\$** - internal sendmail id for a message
- **\$FULLHEADERS\$** - message headers
- **\$ARCHIVE_RECORD\$** - a filename in the quarantine (makes sense in notifications informing on the message placed to the quarantine);
- **\$VIRUS_LIST\$** - a list of the viruses detected.

Example of the notification template delivered to a sender:

Dear User,

The message you sent was infected and
has not been delivered.

Antivirus filter reports:

--- Dr.Web report ---

Following virus(es) has been found:

\$VIRUS_LIST\$

Dr.Web detailed report:

\$DAEMON_REPORT\$

Dr.Web scanning statistic:

\$SCAN_STAT\$

--- Dr.Web report ---

An original message
was storied in archive record named:
\$ARCHIVE_RECORD\$
In order to receive the original message,
please send request to \$POSTMASTER\$,
referring to the archive record name given above.

Another notification template example:

From: DrWeb-DAEMON \$FILTER_MAIL\$
To: \$SENDER\$
Content-Type: text/plain; charset=us-ascii
Subject: Undelivered mail: \$SUBJECT\$

Dear User,
The message with following attributes
has not delivered.

From = \$SENDER\$
To = \$SECURE_RCPTS\$
--- Begin message headers ---
\$FULLHEADERS\$
--- End message headers ---

Antivirus filter report:
--- Dr.Web report ---
Following virus(es) has been found:
\$VIRUS_LIST\$
--- Dr.Web report ---

An original message
was storied in archive record named:
\$ARCHIVE_RECORD\$
In order to receive the original message,
please send request to \$POSTMASTER\$,
referring to the archive record name given above.

Antivirus service provided by Dr.Web Daemon
(<http://www.drweb.com>)

3.4. Denying sending notifications to specified addresses

The plug-in supports an option of blocking notifications to specified addresses (or group of addresses) depending on the role of the address in the message which processing caused generation of a notification. The correspondent addresses and descriptions of their roles are listed in the *blocked addresses file*. The filename and its location are specified as the `UnnotificableAddressesList` parameter values of the configuration file.

The blocked addresses file has a plain text format; lines starting with `#` are considered commentaries. Each meaningful line is a separate entry of the following format:

```
ROLE ADDRESS
```

The **ROLE** field may have the `from`, `to` or `any` values (i.e. the sender's address, recipient's address or any address).

The **ADDRESS** field is an expression used for the search of addresses. The expression should be written in terms of POSIX regular expressions. The expression is case-insensitive. For example, to set `@example.com` as the domain expression, you should write `"@example\.com"`. It is strictly recommended to enclose all expressions in quotes. The NOT operation can be applied to the expression (symbol `!` before the quoted expression), its enabling means notification will not be sent to the address that does not match the expression, if the address matches the expression the search continues. This is useful to set notifications for local users only. The NOT operation for `@example.com` matches the following expression:

```
"@[^e][^x][^a][^m][^p][^l][^\.]^[c][^o][^m]"
```

Example 4.

Do not send notifications to `asv@drweb.com`, if a virus was sent from it, and send notification if a virus was sent to it:

```
from "asv@drweb\.com"
```

Example 5.

Do not send notifications to users from the `example.com` domain, if a virus is sent to them, and send notification if a virus was sent from them:

```
to "@example\.com"
```

Example 6.

Do not send notifications to local users (outside the `mydomain.ru` domain):

```
any !"@mydomain\.ru"
```

3.5. *Setting the plug-in reaction restrictions for specified viruses*

During the virus epidemics there may come a necessity to prohibit sending of notifications and/or place certain types of viruses to the quarantine directory. Such mode is supported in the plug-in. These viruses are listed in the file with blocked viruses. The filename and its location are specified as the `UnnotificableVirusesList` parameter values of the configuration file.

The blocked viruses file has a plain text format; the lines beginning with `#` are considered commentaries.

There exist two versions of the file format. The file format version is indicated in the first meaningful line of the file as

```
[Version=1]
```

or

```
[Version=2]
```

If such a line is missing, the first version is meant.

Integration of Dr.Web with CommuniGate Pro for Windows

Other lines are the entries of the blocking instructions. These entries for version 1 have the following format:

```
TO_ADMIN TO_SENDER TO_RCPTS VIRUSNAME
```

And for version 2 they look as follows:

```
TO_ADMIN TO_SENDER TO_RCPTS QUARANTINE VIRUSNAME
```

The **TO_ADMIN**, **TO_SENDER** and **TO_RCPTS** fields may have the `allow` or `deny` values, i.e. either allow or prohibit sending notifications to an administrator, a sender or recipients of the original message.

The **QUARANTINE** field may have the same values and allow or deny moving a message to the quarantine, if such reaction is specified by other settings of the program.

The **VIRUSNAME** field contains a virus name. All names of viruses should be written in terms of POSIX regular expressions. For example, `HLLM.Generic.95` should be written as `"HLLM\Generic\95"`. It is strongly recommended to enclose all names in quotes.

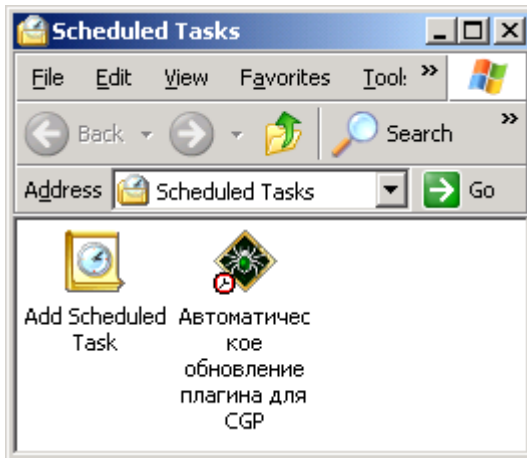


Deny of moving to the quarantine denies also the `redirect` action for the given virus, i.e. redirection of a message.

4. Automatic updating of the virus bases and the plug-in files

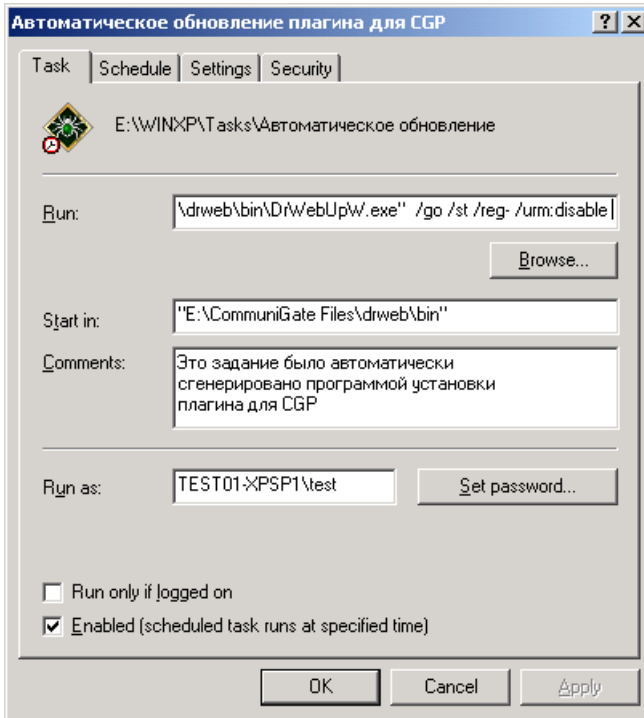
The antivirus module (plug-in) for CommuniGate Pro incorporates the automatic updating module for Windows.

Due to the highly importance of the timely updating of the virus bases, the installation program instructs the system Scheduler to start the automatic updating module in every 30 minutes (pic. 2).



Picture 2. The Scheduler window

You can view and edit, if necessary, the task (pic. 3).



Picture 3. Updating task

The command line launching the task looks as follows:

```
Path\drwebupw /go /st /reg- /urm:disable
```

These parameters provide for a "silent" updating and block unnecessary functions of the automatic updating module.



At present, automatic start of the update is not guaranteed when installing the program under Windows versions prior to Windows 2000. In these cases you should manually set up the automatic start of the updating as it is described in the examples listed above.

The antivirus plug-in detects and loads the updated virus bases automatically, checking the state of the `drwtoday.vdb` "hot" add-on file of the virus base in the intervals set by the `UpdatePeriod` parameter of the configuration file (read p. 3.1.1).

5. Contacts

The Dr.Web antivirus program is in constant development. The latest news on its updates and informative notices are available on the web site:

<http://www.drweb.com>

Sales department: sales@drweb.com

Technical support service:

WWW: <http://support.drweb.com>

e-mail: support@drweb.com

When addressing our technical support the following information which can help to thoroughly examine the case will be greatly appreciated:

- full name and version of Windows
- full name and version of a mail system
- the Dr.Web module version
- configuration files of the module and the applications the Dr.Web module is integrated with
- module's and mail system's log files the Dr.Web module is integrated with