

Manual



Spamfilter

Table of contents

Introduction	2
Quick guide	3
Quarantine reports.....	3
What to do if a message is blocked inadvertently.....	4
What to do if a spam has not been blocked.....	4
General principles.....	5
What you should know about spam.....	5
Filtered messages	5
Principles behind filtering.....	5
Principles behind adjustments.....	6
Principles behind spam processing	6
Management Center	7
Setting the language of the interface	8
The four sections of the Management Center	8
Logging off the Management Center	8
Quarantine section.....	9
Selecting the address to be examined.....	10
Reviewing the quarantine	10
Listing quarantined messages.....	10
Quarantine processing tools.....	11
Sorting, selecting and searching messages	12
Maintenance tools	13
Statistics Section	14
Selecting the address to analyze.....	14
Selecting the period to analyze	14
Activity Statistics Table.....	15
Configuration Section.....	16
Configuring the interface	16
Configuring address settings	16
Configuring the quarantine display	21
Configuring an address group	22
Configuring the warn list.....	23
Configuring the white list	24
Questions.....	25

Introduction

The spamfilter is an extremely powerful antivirus and anti-spam system. Based on the latest generation of filtering technology, the spamfilter does not need to be installed on your computer. Instead, it acts before e-mail messages reach your mailbox. The spamfilter relies on sophisticated rules that are updated daily by the engineers of Lucrasoft Systems in response to spammers' ever-changing strategies and the appearance of new viruses. Thanks to the spamfilter's unblinking surveillance, you can be assured 24 hours a day that you have the best tool to prevent viral attacks, intrusion of dangerous files and undesirable e-mail messages. This manual will help you understand how the spamfilter works and how it can be custom fit to your particular needs.



Quick guide

“Take a couple of minutes to discover how the spamfilter works”

This chapter contains all the necessary information to help you learn your new antivirus and anti-spam system in just a few minutes. The default configuration of the spamfilter immediately provides you with maximum protection, so you can rely on it from the very start. The spamfilter requires only minimal attention on your part. It works autonomously to eradicate viruses, identify dangerous content and remove spam from your e-mail 24 hours a day.

Quarantine reports

As a the spamfilter user, you can receive a quarantine report for each e-mail address that is protected by the system. Quarantine reports may be sent to you daily, weekly, or monthly, depending on the configuration chosen by your e-mail administrator. A quarantine report lists all the messages received in a given period that are identified as spam. These messages are *quarantined*, meaning that they are retained in a special zone outside of your e-mail system.



Reminder of available actions

Release the message Message preview Request a filter adjustment

In quarantine: 0 messages				
Action	Date	Sender	Subject	Score

Without specific action, quarantined messages will be automatically deleted 90 days after their arrival.

What to do if a message is blocked inadvertently

It is possible that a message that you want to receive is blocked by the spamfilter. This may be caused by different factors, such as a non-standard format of the e-mail message or a compromised reputation of the mail server used to send the message. It does not mean that the spamfilter is malfunctioning, but simply that the system acts cautiously when encountering an e-mail message with unusual characteristics that cannot be correctly interpreted by a simple scan of the message contents. If you encounter such a situation, there are two things you can do:

- Ask for the e-mail to be released so the message from the quarantine will be allowed to reach your mailbox;
- notify Lucrasoft Systems so that the engineers may render the filter more tolerant towards the sender or format of the blocked message.

This is referred to as filter adjustment in the spamfilters vocabulary.

What to do if a spam has not been blocked

If a spam slips undetected through the spamfilter system, the differences between this spam and a legitimate e-mail message are likely very small. In such a situation, the spamfilter chooses to deliver the message to your mailbox. It is better to receive spam on an exceptional basis than to miss a potentially important legitimate message. If you receive a spam message, you could request a *filter adjustment* to fine tune the spamfilter detection rules.

General principles

What you should know about spam

An astonishing 95% of all messages traveling through the Internet are unwanted by their recipients. Spam is the number one enemy of your e-mail system. Spam doesn't just pollute your mailbox. It costs time and money. It takes an average of ten minutes a day to manually clean up a mailbox in the absence of spam filters. This adds up to more than one week of working time per year. Moreover, the thousands of unwanted mail messages that are stored by your company or your ISP also represent a wasteful burden. The spamfilter is an efficient and indispensable tool that makes sure your e-mail system does what it is supposed to do.

Filtered messages

The spamfilter filters three types of unwanted messages:

- **Viruses.** The spamfilter simply deletes viruses without sending any alerts to the recipient.
- **Dangerous content.** Lucrasoft Systems must filter dangerous content as a preventive measure. Examples of such content include attachments with executable scripts (.exe) or links to suspicious web sites. The spamfilter removes potentially harmful content and delivers the remainder of the message to your mailbox.
- **Spam.** Spam does not constitute any technical threat but is simply unwanted, unsolicited e-mail. It can be seen as the electronic version of printed advertisements that fill up your postal mailbox.

Principles behind filtering

The spamfilter operates in a transparent fashion, without slowing down or stopping up the stream of incoming messages. The filtering relies on over thirty quality control criteria. Some criteria concern the potentially illicit aspects of a message, while others focus on issues of trust and confidence of the sending server.

The spamfilter verifications belong to different categories: statistical (for example, repeated occurrences of specific terms or concepts), explicit (the sending server may be blacklisted or the message may have a specific format) or dynamic (the signatures and the volume of received mails are analyzed). A relevance score is calculated mathematically at each step of the analysis. The sum of these scores determines whether the message is classified as legitimate or as spam.

Internet domains and addresses under protection

The spamfilter analyzes all incoming mail for all Internet domains that are under its protection. This basic setting is configured when the spamfilter is installed by your e-mail administrator. You do not need to configure anything. All of the e-mail addresses belonging to the *protected domains*, including redirections, aliases and distribution lists, are handled by the spamfilter.

Principles behind adjustments

A protection appliance such as the spamfilter is capable of filtering out nearly all spam. However, some inaccuracies may occur and specific exceptions may have to be made. Three scenarios are possible :

- A spam has managed to pass undetected through the spamfilter and has been delivered to your mailbox.
- A message that should have reached you was classified by the spamfilter as spam.
- An unsolicited message (commercial information, newsletter, etc.) has attracted your attention and you would like, as a personal exception, to receive future messages from the sender of this message.

Principles behind spam processing

As a precaution, it is not possible to modify the spamfilter features that handle viruses and dangerous content. In contrast, spam can be handled by three different modes:

- In **quarantine mode**, all spam is kept in an isolated zone outside of your mailbox.
- In **flag mode**, spam is delivered to the mailbox but is identified by adding a keyword to the message subject.
- In **delete mode**, all spam is irreversibly deleted.

Quarantine mode

By default, the spamfilter operates in *quarantine mode*. All spam is placed in a quarantine zone located outside of your computer, thus keeping your mailbox as clean as possible. In this mode you may consult a list of the spam that has been blocked and release the messages of your choice. The spamfilter may send you periodical reports that list all the e-mails that have been intercepted.

Flag mode

In *flag mode*, all incoming mail is delivered to your mailbox. However, the spamfilter helps you identify spam by adding a keyword of your choice in front of the subject of the message (for example, {Spam?}). Flagging makes it easy to select all spam using your e-mail software: You may simply sort your messages alphabetically, run a search or even implement an automated rule based on a keyword.

Delete mode

In *delete mode*, spam is immediately and irreversibly deleted. You should choose this mode if you prefer expediency and if you accept the fact that the spamfilter may, on rare occasion, incorrectly evaluate an incoming message as spam and erase what is in fact a legitimate message.

Management Center

“Your dedicated web space to consult your quarantine and customize the spamfilter”

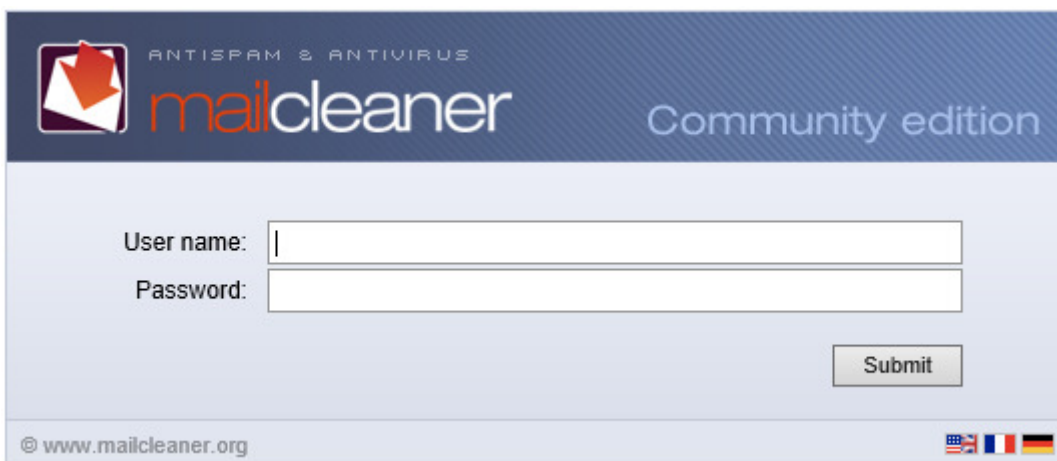
Accessing your Management Center

Note: The address of your Management Center has been given to you by your e-mail administrator.
Contact the person responsible if you have not received this information.

The spamfilter Management Center can be accessed like any standard web site, using your favorite web browser. The Management Center address is: <https://sf.lucrasoft.nl>

The home page displays an authentication zone:

- You may optionally select the language of your choice (click on a flag in the lower right corner) .
- Enter the user name and the password for your e-mail account (the spamfilter uses the same authentication data as your e-mail system).
- Click on OK.



ANTISPAM & ANTIVIRUS
mailcleaner Community edition

User name:

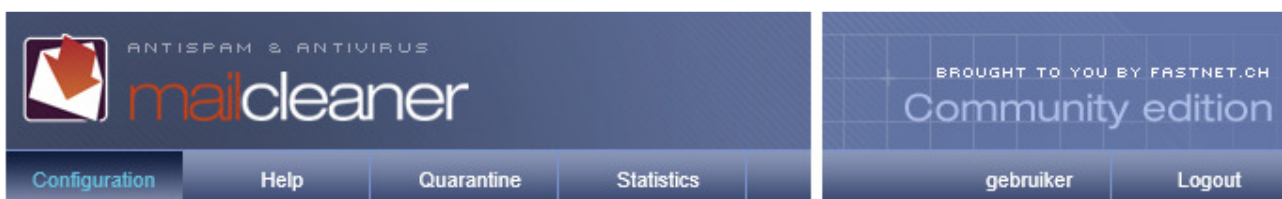
Password:

Submit

© www.mailcleaner.org

Once your input is validated, you are directed to the spamfilter Management Center.

The main navigation bar displays four main sections to the left (*Configuration*, *Help*, *Quarantine*, *Statistics*) and to the right, your user name as well as a *Logout* button.



Setting the language of the interface

When you first access your Management Center, you are invited to set your preferred language. Your choice will apply to all sections of the Management Center and to the quarantine reports that are regularly sent by the spamfilter.

To choose the language:

- Select one of the languages in the list.
- Click on Save to confirm your choice.

Note: If you do not save your changes, the spamfilter Management Center will use the previous configuration upon your next visit.

The four sections of the Management Center

- The Configuration section lets you customize different settings. Customization is optional: The spamfilter is immediately operational using the default settings.
- The *Help* section contains the electronic version of this manual and different help resources.
- The *Quarantine* section lists spam that has been blocked and lets you release messages of your choice.
- The *Statistics* section displays data traffic statistics, including the volume of messages processed by the spamfilter.

Logging off the Management Center

To end your session in the Management Center, simply click on the *Logout* button located on the main navigation bar.

Quarantine section

“To avoid polluting your mailbox, spam messages are held in the quarantine zone”

Every address filtered by the spamfilter has an associated *quarantine* which contains messages identified as spam. If you have only one e-mail address, the spamfilter provides you with a single *quarantine*. If you have several e-mail addresses, *quarantines* are managed by the spamfilter for each address. (However, It is possible to group them in an *address group*.) Quarantined spam messages are automatically and irreversibly deleted after a *retention period* determined by Lucrasoft Systems (default 90 days). You can release a quarantined message at any point prior to the end of the retention period.

ANTISPAM & ANTIVIRUS
mailcleaner
BROUGHT TO YOU BY FASTNET.CH
Community edition

Configuration Help **Quarantine** Statistics gebruiker Logout

Address displayed:
gebruiker@lucrasoft.nl All addresses

Sender: Subject: Search

In quarantine: 0 messages (sorted by date)

Action	Date	To	Sender	Subject	Score
Page 1 of 1					

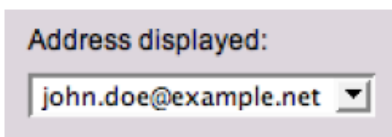
[Manually purge the quarantine](#) [Manually send the quarantine report](#) Messages displayed: 7 last days ([Modify...](#)). Automatic purge after: 90 days

Note: If you configure the spamfilter to operate in flag mode or delete mode, your quarantine list will remain empty.

Selecting the address to be examined

If you have only one e-mail address that is protected by the spamfilter, its corresponding *quarantine* is displayed by default. However, if several addresses have been grouped in the same Management Center, the selection menu located above the list of messages allows you to examine the quarantines for each address. To choose a quarantine associated with a particular address:

- Select the address in the menu.
- The quarantine pages are immediately updated to reflect your choice.



Reviewing the quarantine

During the first weeks of using the spamfilter, carefully inspect the quarantine to make sure that no legitimate messages that should have reached you have been blocked by the system. After these initial checks, it is useful to inspect the quarantine if only to verify that an expected message that has not reached you has not been blocked by the spamfilter.

Such verification can be accomplished in two ways:

- by accessing the *Quarantine section* in the Management Center;
- by examining the *Quarantine reports* that are automatically sent to you at a predefined frequency for each e-mail address that is filtered by the spamfilter.
- The two types of quarantine lists are similar. If you feel comfortable managing one of the lists, you will also feel comfortable managing the other.

Listing quarantined messages

The list of quarantined messages resembles a classic e-mail software interface. The reception date, the sender address and the subject are displayed for each message. Two columns are specific to the spamfilter:

- the *Score* column;
- the *Action* column which contains three different processing tools.

Score Column

The *Score* column contains visual representations of the weighted mean scores of the different analyses carried out by the spamfilter (on a scale of 1 to 4). A higher number of filled squares indicates a higher number of spam criteria.

Action Column

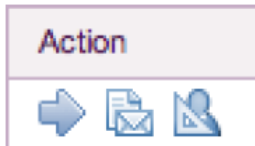
The *Action* column presents the three quarantine processing tools described below.



Quarantine processing tools

Three quarantine processing tools offer the following actions:

- releasing a message;
- displaying the content of a message;
- requesting a filter adjustment.



Releasing a message

You may wish to receive a legitimate message that has been wrongfully quarantined. Releasing such a message results in immediate delivery to your mailbox. A copy of the message is kept in the quarantine should you need to release it again.

Important: The fact that a message is released does not affect the future behavior of the filter. In order to alter a rule, you must make a *filter adjustment request*.

To release a message:

- Click on the corresponding icon.
- The blocked message is sent to your mailbox.



Note: Unless you decide to hide released messages in the quarantine list, they are displayed in italics.

Displaying the contents of a message

To display the contents of a message:

- Click on the date, the message subject or the preview icon.
- The contents of the message are displayed in a new window.



Additional information is available for advanced users, including the long header (extended information about the sender and the outgoing mail server), the applied filter rules, and the associated scores. This information, which is initially hidden, is displayed by clicking on the corresponding triangular buttons.

Sorting, selecting and searching messages

Note: These tools are not available in quarantine reports.

In order to locate a quarantined message that matches specific criteria, the spamfilter includes efficient tools to sort, select and search quarantines.

Navigating through the quarantine

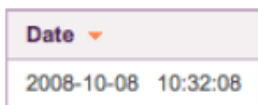
If your quarantine contains a large number of spam messages, the list is paginated using the chosen number of lines per page. To avoid displaying a large number of pages, only the most recent messages are visible by default.

To navigate through the quarantine:

- Simply click on the page links located at the bottom of the list, a display which is similar to a search engine.

Sorting the quarantine

By default messages are sorted by date, with the most recent messages appearing first. If you click on the title of a column, the messages are sorted accordingly. An orange triangle next to the title indicates that the corresponding column is used to sort the quarantine. If the triangle points downwards, the sorting order is decreasing. If the triangle points upwards, the sorting order is increasing. The order may be changed by clicking on the triangle.



Searching for messages

To search for messages sent by a specific sender or containing specific terms in the subject, use the fields displayed on top of the list. The search results take into account the combination of both fields, the sender and the subject (and not the sender or the subject).

To search for a message:

- Enter your criteria in the *Sender* and *Subject* fields (one of the two fields may remain empty) ;
- click on the Search button.
- The list of messages is updated.

To reinitialize the list, click on the link *Display the full quarantine list*.

Maintenance tools

Note: These tools are not available in quarantine reports.

To help with occasional maintenance of your quarantine, the spamfilter includes specific tools to purge the quarantine and manually send quarantine reports.

Manual purge

This option lets you purge a quarantine linked to a specific address. The quarantine is emptied and all blocked messages are deleted. It is not necessary to use this option on a regular basis because messages are deleted automatically after a *retention period* defined by Lucrasoft Systems. This option is only useful if there is a very large number of blocked messages and you wish to remove all spam in a particular quarantine.



[Manually purge the quarantine](#)

To manually purge the quarantine:

- Click on the corresponding icon.
- Confirm your request.
- All blocked messages are irreversibly deleted.

Manual quarantine report transmission

The spamfilter sends quarantine reports to your mailbox(es) on a regular basis, provided that you have not disabled this function. In either case, you may generate a quarantine report manually at any time. This function also allows you to generate a replacement report if you have mistakenly deleted a report that was sent to your mailbox.



[Manually send the quarantine report](#)

To request a quarantine report transmission:

- Click on the corresponding icon.
- Confirm your request.
- A quarantine report is sent to the selected address.



Statistics Section

“Are you a favorite target for spammers? The spamfilter statistics will give you the answer”

In the *Statistics* section, you will find useful information about the number of spam messages, viruses and dangerous content filtered by the spamfilter.

Selecting the address to analyze

If you have only one e-mail address that is examined by the spamfilter, its statistics are displayed by default. However, if several addresses have been grouped in the same Management Center, the selection menu located above the list of messages allows you to display statistics for any individual individual address at will. To select the statistics for a particular address:

- Select the address in the menu.
- The statistics for this address are displayed.

Address displayed:

john.doe@example.net ▼

Note: To obtain a one-page summary of the statistics for all your e-mail addresses, choose *All* in the menu.

Selecting the period to analyze

The spamfilter statistics are calculated using calendar dates to define the period. You have the option to specify the number of days to analyze, or to define start and end dates.

Analyzed period:

7 last days
 From

 to

To select a period for your statistics:

- Choose the number of days to analyze or define start and end dates.
- Click on Refresh.
- The statistics are updated to reflect your choices.

Activity Statistics Table

Activity statistics for each address are displayed in a table. A graphical representation is displayed on the left and precise numerical data are displayed on the right. These include:

- Total number of messages received;
- Number of viruses and dangerous messages;
- Number of spam messages;
- Number of legitimate messages.

In addition to providing you with useful information about the nature of the mail that is sent to you, these statistics verify that the spamfilter operates correctly and illustrate the quality of its filtering system.



Note: Clicking on the graph switches the view from a linear to a pie-chart graph.

Configuration Section

“The spamfilter can be easily customized to fit your needs and your working style”

The Configuration menu contains six sections: Interface, Address groups, Address settings, Quarantine list, Warn list and White list.

Note: The Address groups, Warn list and White list sections are not necessarily present in your configuration menu. These options depend on global settings that are managed by Lucrasoft Systems.

Configuring the interface

The *Interface* section allows you to choose the language used by the Management Center. Your choice is applied to all filtered e-mail addresses and quarantine reports that are generated by the spamfilter.

Language selection

To choose the language of the interface:

- Select one of the languages in the list.
- Click on *Save* to confirm your choice.

Configuring address settings

The *Address Settings* section contains important settings that define how the spamfilter operates globally (for all of your addresses) and individually (independently for each specific address).

The Settings subsection includes four zones :

- address selection;
- spam processing mode for the selected address;
- transmission frequency and format of quarantine reports;
- application and recording of new settings.

Address:

For each message detected as spam:

retain in quarantine
 deliver with subject keyword:
 immediately delete

Retain error messages

Frequency of quarantine reports:

Format of quarantine reports:

Send reports to this address:

Apply settings to all addresses

Selecting an address

If several addresses are grouped in the same Management Center, different settings may apply to each address. For example, you may choose the *quarantine mode* for your main address and a *flag mode* for a second address or an alias.

To select the settings for a specific address:

- Simply select the desired address in the list of available addresses.
- The settings that are displayed are the current settings for that address.

Configuring spam processing modes

After selecting a particular address, you should decide how the spamfilter should process spam sent to that mailbox.

You have three options:

- In **quarantine mode**, all spam is kept in an isolated zone outside of your computer.
- In **flag mode**, spam is delivered to the mailbox but is identified by adding a keyword to the message subject (for example, {Spam?}).
- In **delete mode**, all spam is immediately and irreversibly deleted.

Reminder: The handling of viruses and dangerous content is not affected by this setting; these elements are filtered in a different manner.

Selecting quarantine mode

To apply *quarantine mode* to the selected address:

- Check the option Quarantine messages.
- Click on the *Save* button.

Selecting flag mode

To apply *flag mode* to the selected address:

- Check the option Deliver the message and add a keyword to the subject.
- As an option, you may change the keyword to be inserted in the subject of the message (examples: {Spam?} , UNWANTEDMAIL , JUNKMAIL).
- Click on the *Save* button.

In this mode, all incoming spam is delivered to your mailbox without exception. However, the subject of each message considered to be spam is preceded by the chosen keyword. For example, if the original subject of the message is “*Blue pills very low price*” and the chosen keyword is “{Spam?}”, it will be flagged to become “{Spam?} *Blue pills very low price*”.

Selecting delete mode

To apply *delete mode* to the selected address:

- Check the option Delete the message immediately.
- Click on the *Save* button.

In this mode, all spam is immediately and irreversibly deleted. Choose this mode only after testing the spamfilter in *quarantine* or *flag mode* extensively to determine whether any filter adjustments should be requested.

Configuring error message retention

If you check the option *Retain error messages*, all automated notifications generated by the mail servers of your e-mail recipients will be quarantined. To retain error messages:

- Check the corresponding box (depending on your operating system and your browser, an X, a check mark or a dot should be visible).
- Click on the *Save* button.

Note: The spamfilters *quarantine e-mail delivery error messages* function quarantines the automated warnings generated by the mail servers of your e-mail recipients, such as in the case of invalid e-mail addresses, bounced messages or full mailboxes. This function prevents you from receiving dozens if not hundreds or error messages in case your personal e-mail address is used by a spammer to send mails in your name worldwide (this spoofing is unfortunately a common practice). If your address is spoofed, anti-spam systems that protect e-mail recipients will send rejection notices to your mailbox, a process that can last several days. If your identity is forged and you start receiving large amounts of automated rejection notices, you can enable the *quarantine e-mail delivery error messages* function until the phenomenon subsides. This function should not be enabled permanently. An error message may instantly provide you with useful information, for example if you have mistyped your intended recipient's e-mail address or if the recipient's server is rejecting your message. If such a notification is quarantined, this may prevent you from becoming aware of the problem.

Configuring report delivery and format

If *quarantine mode* is chosen for a particular address, the spamfilter sends a *quarantine report* for this address every day, week or month. You may change the frequency or decide not to receive any reports.

Note: If the chosen mode is different than *quarantine*, the report frequency settings are ignored.

Exception: If you have chosen the option *quarantine e-mail delivery error messages*, a quarantine report will be sent to you when error messages are retained.



Reminder of available actions

Release the message
 Message preview
 Request a filter adjustment

In quarantine: 0 messages				
Action	Date	Sender	Subject	Score
Without specific action, quarantined messages will be automatically deleted 90 days after their arrival.				

Selecting the frequency of quarantine reports

To select the frequency of quarantine reports:

- Select the desired option (daily, weekly, monthly or none) in the displayed list.
- Click on the *Save* button.

Configuring the format of quarantine reports

The spamfilter can generate quarantine reports in two different formats: HTML or raw text. The HTML format offers the best legibility but may be incompatible with older e-mail software applications. If this is the case, you should choose the raw format. To choose the format of quarantine reports:

- Select the desired option (HTML or raw text) in the proposed list.
- Click on the *Save* button.

Applying configuration settings to all addresses

By default, the chosen settings only apply to the selected address. You may, however, decide to use the chosen settings to replace the existing settings of all the e-mail addresses grouped in the Management Center. To apply configuration settings globally:

- Check the option *Apply settings to all addresses*.
- Click on the *Save* button.

Configuring the quarantine display

The options in this section let you customize the way in which the quarantine is displayed in the Management Center.

Setting the default address

If several addresses are grouped in a Management Center, a default address must be chosen. When accessing the Management Center, the first blocked messages to be displayed are for this default address.

To choose the messages that are displayed by default in the quarantine list:

- Select the address of choice in the list of possible addresses.
- Click on the *Save* button.

Setting the number of lines to display

To improve legibility on your computer screen, you may change the number of lines to display on each page of the quarantine list. By default, 20 lines are shown per page.

To set the default number of lines to display on each page of the quarantine:

- Select the number of lines among the options in the list.
- Click on the *Save* button.

Setting the number of days to display

To understand this setting, two points should be clarified:

- The quarantine *retention period* is the period during which spam messages are kept and may be examined. Messages that you do not release during this period are automatically and irreversibly deleted. The retention time is set by Lucrasoft Systems and cannot be modified for individual addresses.
- The *number of days to display* defines a time limit for spam messages to be displayed in the quarantine list. This time filter hides old messages without deleting them (since deletion is handled by the system when the *retention period* has expired).

This setting avoids displaying a large number of pages in the quarantine and allows for more efficient message searches by focusing on a specific time period. The *number of days to display* may be identical to the *retention period*, in which case all currently blocked spam is displayed at all times. To set the number of days to display:

- Select a duration among the options in the list.
- Click on the *Save* button.

Note: The *retention period* and *number of days to display* are visible at all times under the quarantine list.

Hiding user-released messages

A message that has been released is shown in italics in the quarantine list and can also be identified by a specific icon.

You may decide to hide released messages so that the quarantine only shows messages that have never been delivered to your mailbox. To hide user-released messages in the quarantine list:

- Check the option Hide user-released messages.
- Click on the *Save* button.

Configuring an address group

Note: Depending on global spamfilter settings managed by your e-mail administrator, the options below may not be available.

In order to fully understand the concept of an address group, it is important to understand that the spamfilter inspects every single e-mail address that belongs to an Internet domain that is placed under its protection. The spamfilter creates a quarantine zone with its own Management Center for each unique address that is encountered. If you have several personal e-mail addresses that belong to one or more Internet domains under the spamfilter protection (including aliases, redirections, and distribution lists), you may choose for the sake of simplicity and comfort to group all of your addresses in a single, unified Management Center. To do so, you need to select one of your addresses as the main address. This option eliminates the generation of several Management Centers, yet maintains the independence of each address. Thus, different types of processing and quarantine settings may be chosen for each address.

Example: Let's suppose that *john@company.com* and *john@enterprise.com* belong to the same person. It is possible to group these two addresses in the Control Panel used for *john@company.com*. Authentication for this unified Management Center will rely on the user name and password used for the main address *john@company.com*.

Note: In the case of a **distribution list**, only one of its members may declare and manage the list address in the spamfilter.

Adding a new address to a group

To add a personal address to a group:

- Enter the address in the *Add address* field.
- Click on the *Add address* button.
- The new address is temporarily shown in the list in italics.
- The spamfilter sends a confirmation message to the mailbox of the added address.
- Click on the confirmation link in the received confirmation message.
- Configuration options and the quarantine associated with the newly added address can now be accessed from the Management Center of your main address.

Removing an address from a group

To remove one or more addresses from a group:

- Check the box next to each address that you want to remove (depending on your operating system and your browser, an X, a check mark or a dot should be visible).
- Click on the Remove selected addresses button.

- The selected addresses are deleted from the list and their quarantines can no longer be accessed from the Management Center of your main address. They continue to be filtered and may be administered individually using their own Management Centers.

Note: Depending on the global settings chosen by your e-mail administrator, warn list configuration may not be available in your system.

Configuring the warn list

If a sender's e-mail address is added to the spamfilter warn list, you will be notified immediately each time a message that appears to originate from this e-mail address is blocked by the system. You should use this function only in particular situations because it does not help to improve the quality of the spamfilter filter. Instead, try first to submit a *Filter Adjustment Request* to help the spamfilter identify the source of the inaccuracy and take corrective measures if necessary.

Adding an address to the warn list

To add a sender's address to the warn list:

- Enter the address in the field *Add an address*.
- Click on the *Add address* button.
- The new address is shown on the list and you will be notified of all messages received from this address that are blocked by the spamfilter.

Removing an address from the warn list

To remove one or more addresses from the warn list:

- Check the box next to each address that you want to remove (depending on your operating system and your browser, an X, a check mark or a dot should be visible).
- Click on the *Remove selected addresses* button.
- The selected addresses are deleted from the warn list and you will stop being notified about messages received from this address that are blocked by the spamfilter.

Note : It is also possible to disable an address rather than delete it.

Configuring the white list

Note: Depending on the global configuration chosen by your e-mail administrator, the white list configuration settings may not be available in your system.

The white list contains e-mail addresses of trusted senders whose messages will not be blocked under any circumstances. The white list should only be used over short periods of time. In a case where a spammer or a virus spoofs a white listed address, the sender's illegitimate messages will reach your mailbox without being filtered, potentially causing frustration and harm. You should use this function only in particular situations because it does not help to improve the quality of the spamfilter filter. Instead, try first to submit a *Filter Adjustment Request* to help the spamfilter identify the source of the inaccuracy and take corrective measures if necessary.

Adding an address to the white list

To add a sender's address to the white list:

- Enter the address in the field Add an address.
- Click on the Add address button.
- The new address is shown on the list and all messages received from this address will be delivered without being analyzed.

Removing an address from the white list

To remove one or more addresses from the white list:

- Check the box next to each address that you want to remove (depending on your operating system and your browser, an X, a check mark or a dot should be visible).
- Click on the Remove selected addresses button.
- The selected addresses are deleted from the white list and messages received from this address will again be analyzed for the presence of spam.

Note : It is also possible to disable an address rather than delete it.

Questions

If you have any questions left after reading this manual, please feel free to contact us at +31 78 68 11 505 or send an email to support@lucrasoft.nl



Interactive

Websites
E-commerce
App ontwikkeling
Online Visualisatie
E-mailmarketing
Accountview / Unit4 koppeling



Telecom

Swyx in de Cloud
Unified Communications



Systems

Cloud Solutions
IT & Telefonie integratie
Beheer & Support



Software

Depot Software
MainPro
Fleet Planner
Maatwerk ERP oplossingen
Financiële koppelingen

Lucrasoft Systems B.V.

De Zelling 8
3342 GS Hendrik Ido Ambacht
The Netherlands

T +31 (0)78 68 11 505
W www.lucrasoft.nl
E info@lucrasoft.nl

KVK 24482530
IBAN NL48RABO0152384146
BIC RABONL2U