



mailcleaner

USER MANUAL

## Important

This manual is for users of the Enterprise and Community version of MailCleaner, but there are many differences between these two versions.

The filtering quality of the Community version is less accurate than the Enterprise version because many modules are supplied without rules and without data:

- Empty Bayesian Bases
- No Machine Learning filters
- Clam Spam Filters empty
- Only free RBL's
- Limited newsletter filtering
- Only free anti-virus
- Support provided only by the community on [forum.mailcleaner.org](http://forum.mailcleaner.org).



mailcleaner

© Fastnet SA – 2022

Reproduction of this manual in whole or in part without the permission of Fastnet SA, St-Sulpice, Switzerland is strictly forbidden. MailCleaner is a trademark of Fastnet SA. All other brands mentioned in this manual are trademarks of their respective owners.

[www.mailcleaner.net](http://www.mailcleaner.net)

1	<b>Introduction</b>	<b>5</b>
2	<b>Quick guide</b>	<b>6</b>
	Quarantine reports	6
	What to do if a message is blocked inadvertently	7
	<i>Viewing the contents of a message</i>	7
	<i>Releasing a quarantined message</i>	7
	<i>Filter adjustment request</i>	8
	<i>Accept this newsletter</i>	8
	What to do if a spam has not been blocked	8
	Improving your knowledge of MailCleaner	9
3	<b>General principles</b>	<b>10</b>
	What you should know about spam	10
	Filtered messages	10
	Principles behind filtering	11
	<i>Internet domains and addresses under protection</i>	11
	Principles behind adjustments	11
	Principles behind spam processing	12
	<i>Quarantine mode</i>	12
	<i>Flag mode</i>	12
	<i>Delete mode</i>	12
4	<b>Management Center</b>	<b>13</b>
	Accessing your Management Center	13
	Setting the language of the interface	14
	The four sections of the Management Center	14
	Logging off the Management Center	14
5	<b>Quarantine section</b>	<b>15</b>
	Selecting the address to be examined	16
	Reviewing the quarantine	16
	Listing quarantined messages	16
	<i>Score Column</i>	17
	<i>Action Column</i>	17
	Quarantine processing tools	17
	<i>Releasing a message</i>	17
	<i>Displaying the contents of a message</i>	18
	<i>Requesting a filter adjustment</i>	19
	<i>Accepting a newsletter</i>	20
	Sorting, selecting and searching messages	21
	<i>Navigating through the quarantine</i>	21
	<i>Sorting the quarantine</i>	21
	<i>Searching for messages</i>	21
	Maintenance tools	22
	<i>Manual purge</i>	22
	<i>Manual quarantine report transmission</i>	23
6	<b>Statistics Section</b>	<b>24</b>
	Selecting the address to analyze	24
	Selecting the period to analyze	24
	Activity Statistics Table	25

<b>7</b>	<b>Help Section</b>	<b>26</b>
<b>8</b>	<b>Configuration Section</b>	<b>27</b>
	Configuring the interface	27
	<i>Language selection</i>	27
	Configuring address settings	27
	<i>Selecting an address</i>	28
	<i>Configuring spam processing modes</i>	29
	<i>Selecting quarantine mode</i>	29
	<i>Selecting flag mode</i>	29
	<i>Selecting delete mode</i>	29
	<i>Configuring error message retention</i>	30
	<i>Configuration of newsletters detection module</i>	30
	<i>Configuring report delivery and format</i>	31
	<i>Selecting the frequency of quarantine reports</i>	31
	<i>Configuring the format of quarantine reports</i>	32
	<i>Applying configuration settings to all addresses</i>	32
	Configuring the quarantine display	32
	<i>Setting the default address</i>	32
	<i>Setting the number of lines to display</i>	32
	<i>Setting the number of days to display</i>	33
	<i>Hiding user-released messages</i>	33
	Configuring an address group	34
	<i>Adding a new address to a group</i>	34
	<i>Removing an address from a group</i>	35
	Configuring the warn list	35
	<i>Adding an address to the warn list</i>	35
	<i>Removing an address from the warn list</i>	35
	Configuring the Allowlist	36
	<i>Adding an address to the Allowlist</i>	36
	<i>Removing an address from the Allowlist</i>	36
	Configuring the Block list	38
	<i>Adding an address to the Blocklist</i>	38
	<i>Removing an address from the Blocklist</i>	38
<b>A</b>	<b>Filter inaccuracies</b>	<b>39</b>
	Managing false positives	40
	Managing false negatives	40
	<i>Managing false negatives with Outlook, Thunderbird, Mail, ...</i>	40
	Appropriate use of the warn and Allowlists	41
	<i>Warn list</i>	41
	<i>Allowlist</i>	42
<b>B</b>	<b>Frequently Asked Questions</b>	<b>43</b>
	Management Center	43
	Spam and quarantine	43
	<i>Quarantined messages</i>	43
	<i>Unblocked spam</i>	44
	<i>Filter adjustment</i>	44
	Viruses and dangerous messages	44
<b>C</b>	<b>Glossary</b>	<b>45</b>

# 1 Introduction

## Welcome to a world where the e-mail you get is the e-mail you want.

MailCleaner is an extremely powerful antivirus and anti-spam system.

Based on the latest generation of filtering technology, MailCleaner does not need to be installed on your computer. Instead, it acts before e-mail messages reach your mailbox, at the highest level of the network infrastructure of your company, organization or ISP. MailCleaner relies on sophisticated rules that are updated daily by the engineers of the MailCleaner *Analysis Center* in response to spammers' ever-changing strategies and the appearance of new viruses. Thanks to MailCleaner'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 MailCleaner works, how it integrates into your e-mail software and how it can be custom fit to your particular needs.

## 2 Quick guide

### Take a couple of minutes to discover how MailCleaner works with your e-mail software.

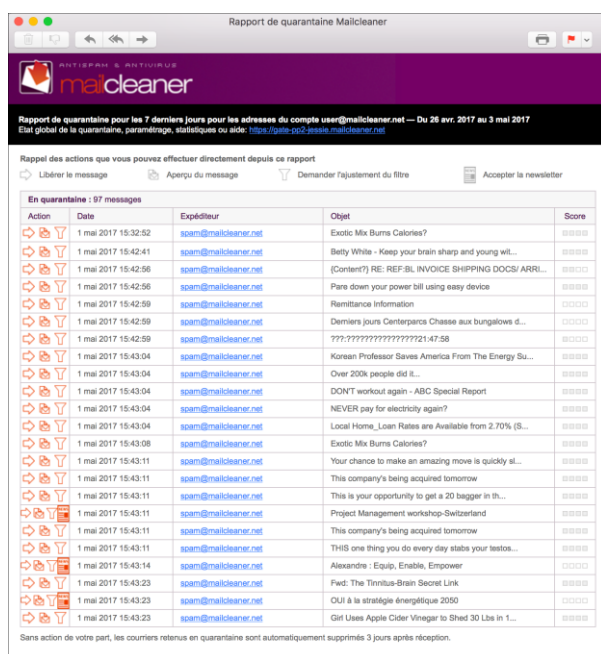
This chapter contains all the necessary information to help you master your new antivirus and anti-spam system in just a few minutes. The default configuration of the MailCleaner filter immediately provides you with maximum protection, so you can rely on MailCleaner from the very start.

MailCleaner requires only minimal attention on your part. It works autonomously to eradicate viruses, identify dangerous content, detect newsletters and remove spam from your e-mail 24 hours a day. MailCleaner works transparently, and you will receive regular *quarantine reports* that will tell you everything about its activity.

### Quarantine reports

As a MailCleaner user, you will be receiving 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 or your Internet Service Provider (ISP). A quarantine report lists all the messages received in a given period that are identified as spam or newsletters. These messages are *quarantined*, meaning that they are retained in a special zone outside of your e-mail system.

Figure 2-1 A typical quarantine report



Action	Date	Expéditeur	Objet	Score
	1 mai 2017 15:32:52	spam@mailcleaner.net	Exotic Mix Burns Calories?	0.0000
	1 mai 2017 15:42:41	spam@mailcleaner.net	Betty White - Keep your brain sharp and young wit...	0.0000
	1 mai 2017 15:42:56	spam@mailcleaner.net	[Content?] RE: REF-BL INVOICE SHIPPING DOCS/ ARR...	0.0000
	1 mai 2017 15:42:56	spam@mailcleaner.net	Pare down your power bill using easy device	0.0000
	1 mai 2017 15:42:59	spam@mailcleaner.net	Remittance Information	0.0000
	1 mai 2017 15:42:59	spam@mailcleaner.net	Derniers jours Centerparcs Chasse aux bungatows d...	0.0000
	1 mai 2017 15:42:59	spam@mailcleaner.net	???-????????????????21-47:58	0.0000
	1 mai 2017 15:43:04	spam@mailcleaner.net	Korean Professor Saves America From The Energy Su...	0.0000
	1 mai 2017 15:43:04	spam@mailcleaner.net	Over 200k people did it...	0.0000
	1 mai 2017 15:43:04	spam@mailcleaner.net	DON'T workout again - ABC Special Report	0.0000
	1 mai 2017 15:43:04	spam@mailcleaner.net	NEVER pay for electricity again?	0.0000
	1 mai 2017 15:43:04	spam@mailcleaner.net	Local Home_Loan Rates are Available from 2.70% (\$...	0.0000
	1 mai 2017 15:43:08	spam@mailcleaner.net	Exotic Mix Burns Calories?	0.0000
	1 mai 2017 15:43:11	spam@mailcleaner.net	Your chance to make an amazing move is quickly sl...	0.0000
	1 mai 2017 15:43:11	spam@mailcleaner.net	This company's being acquired tomorrow	0.0000
	1 mai 2017 15:43:11	spam@mailcleaner.net	This is your opportunity to get a 20 bagger in th...	0.0000
	1 mai 2017 15:43:11	spam@mailcleaner.net	Project Management workshop-Switzerland	0.0000
	1 mai 2017 15:43:11	spam@mailcleaner.net	This company's being acquired tomorrow	0.0000
	1 mai 2017 15:43:11	spam@mailcleaner.net	THIS one thing you do every day stabs your testos...	0.0000
	1 mai 2017 15:43:14	spam@mailcleaner.net	Alexandre - Equip, Enable, Empower	0.0000
	1 mai 2017 15:43:23	spam@mailcleaner.net	Fwd: The Trinitus-Brain Secret Link	0.0000
	1 mai 2017 15:43:23	spam@mailcleaner.net	OUJ à la stratégie énergétique 2050	0.0000
	1 mai 2017 15:43:23	spam@mailcleaner.net	Girl Uses Apple Cider Vinegar to Shed 30 Lbs in 1...	0.0000

During the first few weeks as a new MailCleaner user, you should examine your quarantine reports carefully to make sure that the system does not inadvertently block any legitimate e-mail message that should have been delivered to your mailbox. Such instances are very rare, but not impossible. After a test period, you will have the option to disable the delivery of quarantine reports, depending on whether or not you are interested in reviewing the activity of the filtering system.

## What to do if a message is blocked inadvertently

---

It is possible, although extremely rare, that a message that you want to receive is blocked by MailCleaner. 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 MailCleaner 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 should do:

- release the message from the quarantine to allow it to reach your mailbox;
- notify the MailCleaner Analysis Center 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 MailCleaner vocabulary.

If you are unsure about the nature of the message that has been blocked, you can view its contents before deciding whether it should be released or not via the MailCleaner Management Center.

**Note:** The MailCleaner *Analysis Center*, located on our premises, is composed of a team of highly specialized engineers whose role is to guarantee the highest possible quality of filtering in response to global spam traffic, emergence of viruses and filter adjustment requests emanating from users worldwide.

### Viewing the contents of a message

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

**Figure 2-2** Message preview icon



### Releasing a quarantined message

- Click on the message release icon next to the message of interest.
- A copy of the blocked message is sent to your mailbox.

**Figure 2-3** Message release icon



### Filter adjustment request

- Click on the filter adjustment request icon next to the message of interest.
- Confirm your request.
- A *filter adjustment request* is sent to the *Analysis Center* along with a copy of the blocked message. You will not be notified of any corrective measures taken by the MailCleaner *Analysis Center*.

**Figure 2-4** Filter adjustment request icon



### Accept this newsletter

- Click on the newsletter icon next to the message of interest.;
- A copy of the blocked message is sent to your mailbox and the newsletter is now accepted.

**Figure 2-5** Newsletter icon



**Note:** If you use any of the preceding tools available in the quarantine report, your browser will open a new window or a confirmation dialog box.

## What to do if a spam has not been blocked

---

If a spam slips undetected through the MailCleaner system, the differences between this spam and a legitimate e-mail message are likely very small. In such a situation, MailCleaner 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 should request a *filter adjustment* to fine tune MailCleaner detection rules.

To manually notify the MailCleaner *Analysis Center* received spam:

- Select the received spam in the list of messages.
- Resend the message using the resend function of your e-mail software.
- Type in or paste the e-mail address for *filter adjustment requests* obtained previously.
- A *filter adjustment request* is sent along with a copy of the unwanted message.
- You may then delete the spam.
- No confirmation will be sent to you, but your request will be taken into account in the continuous filter adjustment process.



**Important:** Do not forward the contents of the spam message using the copy and paste function. Doing so will prevent the transmission of the long header in the original message which is needed to properly analyze the spam. Regardless of your e-mail software or operating system (PC or Mac), you should only use the *Resend* function (or its equivalent) to send your *filter adjustment request*.

## Improving your knowledge of MailCleaner

---

After mastering the basics, you will undoubtedly want to learn more about customizing MailCleaner to precisely fit your needs.

This manual will answer all of your questions

We wish you a pleasurable experience with MailCleaner.

# 3 General principles

**A powerful anti-spam shield.  
State of the art technology.  
Made in Switzerland.**

## 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.

MailCleaner is an efficient and indispensable tool that makes sure your e-mail system does what it is supposed to do.

## Filtered messages

---

MailCleaner filters four types of unwanted messages:

- **Viruses.** MailCleaner simply deletes viruses without sending any alerts to the recipient.
- **Dangerous content.** Your e-mail administrator must filter dangerous content as a preventive measure. Examples of such content include attachments with executable scripts (.exe) or links to suspicious web sites. MailCleaner removes potentially harmful content and delivers the remainder of the message to your mailbox along with a note explaining how to ask your administrator to send you the complete message.
- **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. As you will see in the following sections, MailCleaner offers you three different modes for handling incoming spam.
- **Newsletters.** MailCleaner offers you the possibility to retain unwanted newsletters in quarantine.

## Principles behind filtering

---

MailCleaner 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.

MailCleaner verifications belong to different categories: statistical (for example, repeated occurrences of specific terms or concepts), explicit (the sending server may be in a blocklist 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*

MailCleaner analyzes all incoming mail for all Internet domains that are under its protection. This basic setting is configured when MailCleaner is installed by your e-mail administrator or your ISP. 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 MailCleaner.

For example, MailCleaner will filter *john@company.com* and *john@enterprise.com* if the two domains *company.com* and *enterprise.com* have been put under its protection.

## Principles behind adjustments

---

A protection appliance such as MailCleaner 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 MailCleaner and has been delivered to your mailbox.
- A message that should have reached you was classified by MailCleaner 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.

MailCleaner offers you simple solutions to manage all of these situations. You will find all the necessary information in Appendix A of this manual.

## Principles behind spam processing

---

As a precaution, it is not possible to modify MailCleaner 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 (flag) to the message subject.
- In **delete mode**, all spam is irreversibly deleted.

### *Quarantine mode*

By default, MailCleaner 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. MailCleaner will 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, MailCleaner 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.

The subject of a flagged message may be as follows:

*SPAM -- Blue pills very low price*

### *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 MailCleaner may, on rare occasion, incorrectly evaluate an incoming message as spam and erase what is in fact a legitimate message.

# 4 Management Center

**Your dedicated web space to consult your quarantine and customize MailCleaner.**

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

## Accessing your Management Center

The MailCleaner Management Center can be accessed like any standard web site, using your favorite web browser.

The Management Center address usually has the following format:

*https://mailcleaner.yourdomain.com*

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 (MailCleaner uses the same authentication data as your e-mail system).
- Click on OK.

**Figure 4-1** The authentication zone

ANTISPAM & ANTIVIRUS  
mailcleaner

User name:  @mydomain.com

Password:

Submit

© www.mailcleaner.net

Once your input is validated, you are directed to the MailCleaner 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 MailCleaner.

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 MailCleaner 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: MailCleaner 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 MailCleaner.

## 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.

# 5 Quarantine section

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

Every address filtered by MailCleaner has an associated *quarantine* which contains messages identified as spam.

If you have only one e-mail address, MailCleaner provides you with a single *quarantine*.

If you have several e-mail addresses, *quarantines* are managed by MailCleaner 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 your e-mail administrator. You can release a quarantined message at any point prior to the end of the retention period.

**Figure 5-1** The quarantine list in the Management Center

Please enable the newsletter module (Published on 2016/11/15): You can block any unwanted newsletter by enabling the newsletter module [here](#). Detected newsletter will be present in your usual report and can be whitelisted directly from it.

Address displayed: user@mailcleaner.net  All addresses  All addresses

Q Sender:  Subject:  Search

In quarantine: 97 messages (sorted by date)

	Date	Sender	Subject	Score
	Yesterday 3:43:23 PM	spam@mailcleaner.net	Fwd: The Tinnitus-Brain Secret Link	
	Yesterday 3:43:23 PM	spam@mailcleaner.net	OUI à la stratégie énergétique 2050	<input type="button" value="Accept this newsletter"/>
	Yesterday 3:43:23 PM	spam@mailcleaner.net	Girl Uses Apple Cider Vinegar to Shed 30 Lbs in 1 Month: INCREDIBLE	
	Yesterday 3:43:14 PM	spam@mailcleaner.net	Alexandre : Equip, Enable, Empower	<input type="button" value="Accept this newsletter"/>
	Yesterday 3:43:11 PM	spam@mailcleaner.net	This company's being acquired tomorrow	
	Yesterday 3:43:11 PM	spam@mailcleaner.net	THIS one thing you do every day stabs your testosterone to deadly levels!	
	Yesterday 3:43:11 PM	spam@mailcleaner.net	Your chance to make an amazing move is quickly slipping away	
	Yesterday 3:43:11 PM	spam@mailcleaner.net	This company's being acquired tomorrow	
	Yesterday 3:43:11 PM	spam@mailcleaner.net	Project Management workshop-Switzerland	<input type="button" value="Accept this newsletter"/>
	Yesterday 3:43:11 PM	spam@mailcleaner.net	This is your opportunity to get a 20 bagger in the market very fast	
	Yesterday 3:43:08 PM	spam@mailcleaner.net	Exotic Mix Burns Calories?	
	Yesterday 3:43:04 PM	spam@mailcleaner.net	DON'T workout again - ABC Special Report	

© www.mailcleaner.net

**Note:** If you configure MailCleaner 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 MailCleaner, 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 MailCleaner, 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 MailCleaner.

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 MailCleaner.
- 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 MailCleaner:

- 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 MailCleaner (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.

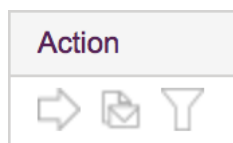
## Quarantine processing tools

---

Three quarantine processing tools offer the following actions:

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

**Figure 5-3** Processing tools icons



### Releasing a message

In rare cases, 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.

**Figure 5-4** *Icon to release a message*



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

### *Displaying the contents of a message*

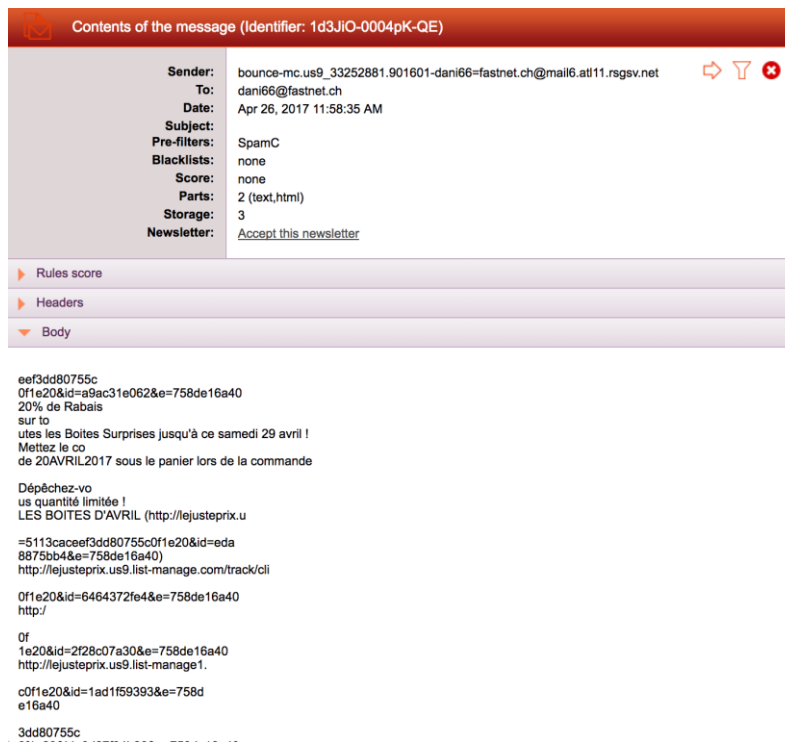
To display the contents of a message:

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

**Figure 5-5** *Message preview icon*



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.

**Figure 5-6** Preview window

### Requesting a filter adjustment

On very rare occasions, MailCleaner may block a message that you wish to receive. If this occurs, it is imperative to send a *filter adjustment request* to the MailCleaner *Analysis Center*.

**Figure 5-7** Filter adjustment request icon

A *filter adjustment request* is processed by the engineers at the MailCleaner Analysis Center within one working day. The rules that were applied to the message are analyzed and modified to render the filter more tolerant towards the sender or format of the blocked message. This procedure is implemented in small incremental steps to prevent creating weak zones in the MailCleaner filter. It is therefore possible that subsequent messages from the same sender are still blocked. In such situations, it may be necessary to repeat the *filter adjustment request* procedure two or three times to obtain the desired outcome.

**Important:** It is possible that a particular spam or unsolicited message has attracted your attention and that you wish to start receiving future messages from its sender (for example, this may be a newsletter that you did not subscribe to but found to be of interest). In such a case you should also make an *adjustment request*. The *Analysis Center* engineers will examine this request and may ask you to create a *warn list* entry instead of implementing a specific exception in MailCleaner.

To make a *filter adjustment request*:

- Click on the corresponding icon.
- Confirm your request.
- You will be notified within one working day about the corrective measures taken by the MailCleaner *Analysis Center*.

### *Accepting a newsletter*

If a message has been quarantined and identified as a newsletter, you can decide to accept it permanently.

**Important:** Once accepted, the newsletter will be accepted as long as you do not delete this information in the allowlist section of the configuration.

To accept a newsletter:

- • *click on the "Accept this newsletter" button*
- • *the blocked message is then allowed to reach your mailbox and the newsletter will now be allowed.*

*Figure 5-8 The button for accepting newsletters*

**Accept this newsletter**

**Note:** once a newsletter is authorized, the "Accept this newsletter" button will be italicized to indicate that this newsletter is authorized.

## 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, MailCleaner 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:

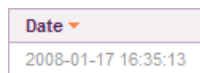
- Simply click on the page links located at the bottom of the list, a display which is similar to a search engine.

### *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.


**Figure 5-9** The active sorting column displays a 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).

**Figure 5-10** Search fields


 Sender:  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, MailCleaner 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 your e-mail administrator.

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.

**Figure 5-11** *Manual purge of the 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*

MailCleaner 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.

**Figure 5-12** *Manual quarantine report transmission*

 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.

## 6 Statistics Section

### Are you a favorite target for spammers? MailCleaner 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 MailCleaner.

#### Selecting the address to analyze

If you have only one e-mail address that is examined by MailCleaner, 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.

**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

MailCleaner 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.

**Figure 6-1** Selecting the period for your statistics

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 MailCleaner 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.

# 7 Help Section

**Are you wondering which configuration is best for you?  
The online help will provide you with the answer.**

The online help includes a summarized version of this manual along with questions frequently asked by MailCleaner users worldwide.

It also includes the following resources:

- e-mail addresses for manually sending filter adjustment requests;
- a downloadable copy of the latest version of this manual in PDF format;
- a glossary;
- support information.

# 8 Configuration Section

**MailCleaner 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 *Allow list*.

**Note:** The *Address groups*, *Warn list* and *Allowlist* sections are not necessarily present in your configuration menu. These options depend on global settings that are managed by your e-mail administrator or ISP.

## 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 MailCleaner.

### *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 MailCleaner 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.

**Figure 8-1** The different options in the Address Settings section

Address:

---

For each message detected as spam:

retain in quarantine  
 deliver with subject keyword:   
 immediately delete

---

Retain error messages

---

For each message detected as newsletter:

retain in quarantine  
 deliver

---

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 MailCleaner 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 MailCleaner 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 *Systemically 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 of 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 *Systemically 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.

### *Configuration of newsletters detection module*

If you select the *Remember quarantine* checkbox, messages identified as newsletters will be blocked in Quarantine.

In this mode, the identified messages can then be released from the email report or from the quarantine.

Note that an email can be recognized as "newsletter" and, at the same time, as "spam". The two notions are separated and an email can be quarantined as spam although the user has authorized it as a newsletter.

When you authorize a newsletter in your quarantine, it adds automatically the sender to the allowlist with a specific tag. This does not affect spam filtering. Never add the sender of a newsletter manually to the allowlist but only use the *"Accept this newsletter"* buttons in the report or quarantine interface.

**Tip:** We strongly recommend activating this function. This greatly improves the feel of the filtering quality.



### *Configuring the format of quarantine reports*

MailCleaner 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 different 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 your e-mail administrator 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 MailCleaner 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 MailCleaner inspects every single e-mail address that belongs to an Internet domain that is placed under its protection by your e-mail administrator or ISP. MailCleaner 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 MailCleaner 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 MailCleaner.

### *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.
- MailCleaner 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.

## Configuring the warn list

---

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

If a sender's e-mail address is added to the MailCleaner warn list, you will be notified immediately each time a message that appears to originate from this smtp 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 MailCleaner filter. Instead, try first to submit a *Filter Adjustment Request* to help MailCleaner 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 MailCleaner.

### *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 MailCleaner.

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

## Configuring the Allowlist

---

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

**Note:** The Allowlist applies only to the envelope-sender visible in the "Received:" headers ("mail from:" of the smtp session)

**Note:** Allowlist is applied before the Block list

The Allowlist contains e-mail addresses of trusted senders whose messages will not be blocked under any circumstances. The Allowlist should be used sparingly, only if the reason for the filtering cannot be eliminated.

In a case where a spammer or a virus spoofs a Allowlisted 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 MailCleaner filter. Instead, try first to submit a *Filter Adjustment Request* to help MailCleaner identify the source of the inaccuracy and take corrective measures if necessary.

### *Adding an address to the Allowlist*

To add a sender's address to the Allowlist:

- 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 Allowlist*

To remove one or more addresses from the Allowlist:

- 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 Allowlist 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.

**Note :** For more information on the syntax of warn, Block and Allowlists have a look to our online

knowledge base

## Configuring the Block list

---

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

**Note:** The Blocklist applies only to the envelope-sender visible in the "Received:" headers ("mail from:" of the smtp session)

The Blocklist allows you to specify addresses of senders for which emails will be quarantined in all cases. The Blocklist should be used only for very short periods of time and for specific cases.

This way of doing is a measure that does not increase the overall improvement of MailCleaner. You should always first choose to do a filter adjustment request so the reasons for the inaccuracy of the filtering can be understood and, if necessary, lead to a global fix.

### *Adding an address to the Blocklist*

To add a sender's address to the Blocklist:

- 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 blocked without being analyzed.

### *Removing an address from the Blocklist*

To remove one or more addresses from the Blocklist:

- 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 Blocklist 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.

**Note :** For more information on the syntax of warn, Block and Allowlists have a look to our online knowledge base

# A Filter inaccuracies

**No filter is perfect.**

**But with your help, MailCleaner may aim at perfection.**

The filtering system implemented by MailCleaner relies on automated and systematic controls that cannot match the quality of human analysis. As a result, MailCleaner may occasionally lack precision. For example, this may occur if there are no mathematically detectable differences between a spam and a legitimate message, or when specific exceptions must be handled.

Three typical scenarios are shown in the table below.

Case	Description	Solution
False positive	A message that you wanted to receive was blocked by MailCleaner.	You may easily <i>release the message</i> and let it reach your mailbox.  At the same time, MailCleaner should learn to be more tolerant towards messages originating from this sender. It is likely that the format of this message or some specific words in its contents triggered an anti-spam measure within MailCleaner. You should request a <i>filter adjustment</i> from the quarantine.
False negative	A spam has managed to bypass all the controls and was delivered to your mailbox.	A new filter rule must be added to MailCleaner. You should request a <i>filter adjustment</i> from your e-mail software.
Individual exception	An unsolicited message with spam-like characteristics (such as a commercial offer or a newsletter) has been blocked by MailCleaner. You are, however, interested in its content and would like to receive future communications from the sender.	After reviewing a <i>filter adjustment request</i> , the Analysis Center engineers may ask you to declare an exception for this sender by including the address in a Warn list or a Allowlist.

## Managing false positives

---

In very rare cases, a message that you would like to receive is instead quarantined (this is called a false positive). A false positive may be caused by different factors, such as a particular format of the e-mail message or a compromised reputation of the mail server used to send the message. It does not mean that MailCleaner is malfunctioning, but simply that the system acts cautiously when encountering unusual characteristics of an e-mail message that cannot be correctly interpreted by a simple scan of the message contents.

If a message is quarantined erroneously, you may easily release it. Simply click on the release icon in the Message Center or the quarantine report.

**Figure A-1** Message release icon



If you encounter a false positive, request a *filter adjustment* so that MailCleaner will be more tolerant towards the sender or format of the blocked message.

**Figure A-2** Filter Adjustment Request icon



## Managing false negatives

---

If a spam slips undetected through the MailCleaner system (a false negative), the differences between this spam and a legitimate e-mail message are necessarily very small. In such a case, MailCleaner chooses to deliver the message to your mailbox. It is better to receive spam on an exceptional basis than to miss a potentially important message.

If you receive spam, you should ask for a *filter adjustment* to reinforce MailCleaner detection rules.

### **Managing false negatives with Outlook, Thunderbird, Mail, ...**

All *filter adjustment requests* resulting from unwanted spam must be sent manually to a specific e-mail address at the MailCleaner *Analysis Center*.

**This address is defined by your e-mail administrator or ISP. It cannot be found in this manual.** To obtain this address, click on the *Help* section of the Management Center and then on *Filter Adjustment Request*. Copy the e-mail address as it will be needed in the subsequent steps.



To manually report a false negative:

- Select the received spam in the list of messages.
- Redirect the message using the *resend* or *forward as attachment* function of your e-mail software.
- Type in or paste the e-mail address for *Filter Adjustment Requests* obtained previously.
- A *filter adjustment request* is sent along with a copy of the unwanted message.
- You may then delete the spam.
- No confirmation will be sent to you, but your request will be taken into account in the continuous filter adjustment process.

**Important:** Do not forward the contents of the spam message using the copy and paste function. This may prevent the transmission of the long header in the original message which is needed to analyze the spam. Regardless of your e-mail software and of your operating system (PC or Mac), you should only use the *Redirect* function (or its equivalent) to send your *filter adjustment request*.

## Appropriate use of the warn and Allowlists

---

The warn list and the Allowlist alter the filtering activity of MailCleaner for e-mail senders that are considered trustful.

**Normally, you should never have to add any addresses to either of these two lists.** There are only two possible exceptions:

- You actually wish to receive spam or similar content from a particular sender, for some specific reason.
- Because of strict confidentiality issues, it is not appropriate for you to request a *filter adjustment* for the sender, which necessitates the transmission of a copy of the blocked message.

### **Warn list**

If a sender's e-mail address is added to the MailCleaner warn list, you will be notified immediately each time a message originating from this e-mail address is blocked by the system. The warn list can almost be considered to be a combination between the *flag* and *quarantine* operating modes.

The quarantined message may be released directly using the received notification.

**Note:** If you have chosen *flag mode* or *delete mode* to process spam messages, adding addresses to the warn list will have no effect.

### ***Allowlist***

Messages whose sender address is in the Allowlist are directly delivered to your mailbox, without being filtered for spam. Viruses and dangerous content are still filtered.

**Note:** It is preferable to use the warn list and not the Allowlist.

# B Frequently Asked Questions

## Simple answers to common questions

### Management Center

---

#### **What is the Management Center?**

The Management Center is your personal MailCleaner space that is accessible via an Internet browser. It gives you access to your quarantine and lets you configure MailCleaner settings according to your specific needs.

#### **How do I access the Management Center?**

The Management Center address usually has the following format: *https://mailcleaner.mycompany.com* (replace *mycompany.com* with your domain name). If in doubt, ask your e-mail administrator to give you the correct address.

#### **Where can I get my user name and password?**

For any given address filtered by MailCleaner, your user name and password are the same as those used for your e-mail account in your standard e-mail software.

### Spam and quarantine

---

#### **What is a quarantine ?**

A quarantine is an isolated zone outside of your mailbox which retains messages identified as spam.

#### ***Quarantined messages***

#### **A legitimate message has been mistakenly quarantined. What should I do?**

Release the message to allow its delivery to your mailbox and request a *filter adjustment* from within the *quarantine*.

#### **Why did MailCleaner quarantine a message that I was supposed to receive?**

Such a situation may occur if the message was relayed by a mail server that may temporarily have a compromised reputation, caused for example by spammers that use it as a spam relay. Alternatively, a specific, unusual format of the message may have triggered an anti-spam rule. It does not mean that MailCleaner has malfunctioned, but simply that the system acts cautiously when encountering unusual characteristics of an e-mail message that cannot be correctly interpreted by a simple scan of the message contents.

#### **How do I release a message?**

Click on the arrow icon located on the same line as the message to release it. This can be done either in the quarantine report or within the Management Center.

**I have released a message, but it is still displayed in the quarantine. Is this normal?**

A released message is kept in the quarantine in case you need to release it again in the future. It is displayed in italics to indicate that it has been released.

**What do I do to stop receiving quarantine reports?**

You may change the frequency at which quarantine reports are sent, or disable this option, in the *Configuration* section of the Management Center. If you choose to disable reporting, you will need to visit your Management Center to consult your quarantine.

**Unblocked spam****A spam has not been filtered. What should I do?**

Use your e-mail software to request a *Filter Adjustment* which will reinforce the filter rules.

**Why did MailCleaner let a spam reach my mailbox?**

Some spam messages manage to slip through the filter because none of the mathematical analyses carried out at the time were able to differentiate it from legitimate e-mail. It is therefore very important that you report this error to the MailCleaner *Analysis Center*, which will then reinforce the relevant filter rules. In borderline situations, MailCleaner chooses to deliver the message to your mailbox, since it is better to receive spam on an exceptional basis than to miss a potentially important message.

**Filter adjustment****What is a filter adjustment?**

A filter adjustment results from a request that you decide to make when you encounter a legitimate mail that is wrongfully quarantined, or a spam message that is wrongfully delivered to your mailbox. In the first case, MailCleaner will relax a rule to be more tolerant towards a specific sender or format. In the second case, MailCleaner becomes more strict.

**What happens when I request a filter adjustment?**

A copy of the message is sent to the MailCleaner *Analysis Center*. The message is examined by MailCleaner engineers and the filter may be corrected. The measures taken by the *Analysis Center* are communicated to you within one working day.

**Viruses and dangerous messages**

---

**How does MailCleaner handle viruses?**

Viruses are eliminated without any notification.

**What do you mean by dangerous content?**

Dangerous content is the type of content that your e-mail administrator must filter as a preventive measure. Examples include attachments with executable scripts (.exe) or links to suspicious web sites. MailCleaner removes dangerous content and delivers the remainder of the message to your mailbox along with a note explaining how to ask your administrator to send you the complete message.

**How do I know that a message included dangerous content ?**

The subject of such a message includes a keyword – usually « {DANGEROUS CONTENT} » – as well as an attached document explaining how to release it.

**How do I obtain this dangerous content from my e-mail administrator ?**

Follow the instructions in the message attachment. To receive the retained content, you must provide the ID of the message that was blocked. If your administrator believes that the original attachment poses a genuine threat, he or she may refuse to forward it to you.

# C Glossary

**Authentication**

A process that verifies that the true identity of a person matches the identity claimed by this person. Successful authentication in MailCleaner is necessary for a user to access his or her quarantine.

**Analysis Center**

A team of specialized engineers working at the MailCleaner headquarters whose role is to guarantee at all times the best possible quality of filtering in response to global spam traffic, virus activity and adjustment requests from MailCleaner users worldwide.

**Dangerous content**

Suspicious content found in a message that has been filtered out as a preventive measure by your ISP or e-mail administrator.

**Domains under protection**

All of the Internet domains examined by the same instance of MailCleaner (examples: company.com, enterprise.com).

**False negative**

Spam that has not been identified as such by the MailCleaner filter. All false negatives should be reported to the *Analysis Center* to take corrective action.

**False positive**

A legitimate message considered as spam by MailCleaner. All false positives should be reported via a *filter adjustment request*.

**Fastnet SA**

The nice folks who are the authors of MailCleaner. They are just the opposite of spammers. Fastnet headquarters are in St-Sulpice, Switzerland.

**Filter Adjustment Request**

A voluntary action on the part of a user in case a legitimate message is blocked or spam is delivered to your mailbox. In the first case, filter adjustment will render MailCleaner more tolerant towards a particular sender or format. In the second case, MailCleaner will reinforce its filter. *Filter adjustment requests* are handled by the MailCleaner *Analysis Center*.

**Filter rule**

A mathematical and statistical analysis of specific characteristics of a message in order to determine whether it should be considered as spam.

**ISP**

Internet Service Provider, a company providing access to the Internet and offering e-mail services.

**Management Center**

A private Internet zone where you can inspect incoming quarantined messages and configure different MailCleaner options.

**Plug-in**

An extension that can be added to a preexisting software application. The MailCleaner plug-in for Microsoft Outlook simplifies the process of notifying of false negatives.

**Quarantine**

An isolated area outside of your mailbox for storing messages identified as spam.

**Quarantine report**

An automatically generated periodic report which lists all blocked messages and which provides tools to inspect their content and to release quarantined messages if necessary.

**RBL**

Realtime Blockhole List. RBLs maintain lists of servers in real time known to send spam. Using RBLs is very simple in principle: If an incoming message is sent by an RBL-listed server it is considered a priori as spam. The difficulty in using RBLs is the need to continuously verify that they are reliable.

**Releasing a message**

User action that releases a quarantined message so that it can reach the recipient's mailbox.

**Retention period**

Period of time during which a quarantined message may be consulted. When the retention period expires, the message is automatically deleted.

**Score**

A quarantine indicator that offers a weighted, numerical estimation that a message is spam or not.

**SMTP**

Simple Mail Transfer Protocol. A protocol used to send electronic mail.

**Spam**

An electronic message that is unwanted by the recipient, but without any dangerous content. Also called "junk mail".

**Spoofing**

E-mail address spoofing is a spammer's strategy where the sender of a message is forged in an attempt to disguise spam as a legitimate message from another sender.

**Switzerland**

Country of origin of MailCleaner, where spam is eradicated with watchmaker's quality and precision.

**Virus**

An intrusive software entity, sometimes included as an attachment to a message, which may alter the integrity of your computer.

**Warn list**

A list of e-mail addresses that are trustworthy and should not generate spam. You will receive a warning if a message sent from a warn list address is blocked by MailCleaner.

**Allowlist**

A list of e-mail addresses that are fully trustworthy. Messages sent from Allowlist addresses will never be blocked by MailCleaner.

**Wow.**

What we hope you will say as a MailCleaner user.