Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

MailCleaner FAQ

Introduction

MailCleaner is a Swiss product which is used by several Swiss universities. The product runs on our mail gateways and is managed by the Informatikdienste.

1. Main Features

- You will be provided with a personal quarantine for each of your filtered addresses.
- Messages containing executable attachments such as java scripts and macro-enabled documents will be rejected. To receive this kind of message, the sender must use some file transfer service such as Dropbox, polybox or CIFEX.
- Messages that violate the sender's SPF or DMARC policy will be quarantined or marked as spam.
- Messages that come from hosts found on certain blacklists, will be rejected.

2. Personal Quarantine & Quarantine Reports

- You will receive a daily quarantine report via email. The report may be used to release quarantined messages and provide access to your “Management Center" user interface.
- Quarantined messages will be kept for 30 days.
- Each message listed in the quarantine report will have 3 "action" icons:
    - The "release" icon will deliver a copy of the quarantined message to your mailbox and provide you with a white-listing option .
    - The "preview" icon will display the content of the quarantined message.
    - The "filter adjustment" icon will send a request to the MailCleaner analytical team to inform them that the message should not have been quarantined.
- *Please check your quarantine any time that an expected message fails to arrive.*

3. Management Center

- The Management Center uses the same username and password as your email account.
- If your mailbox is located on the Exchange server, you may ignore the email domain during the login procedure.
- *If your mailbox is not on the Exchange server, then you must select your domain from the pull-down menu.*
- *If you have a “psi.ch” address, then you must select your domain from the pull-down menu.*
- The Management Center, https://mailcleaner.ethz.ch/ may be used to:
    - change the language and frequency of quarantine reports (daily, weekly, monthly, none)
    - group quarantines for multiple addresses into a single quarantine
    - purge quarantined messages
    - choose the SPAM filtering action for your address (quarantine, tag, delete)
    - add sender addresses to your personal blacklist, whitelist, or warnlist

4. Blacklist, Whitelist & Warnlist

- Mail from addresses in your blacklist will be quarantined, tagged, or deleted, depending on your spam filtering preference.
- Mail from addresses in your whitelist will not be filtered for SPAM. The whitelist must be used with caution. See the user manual for more information.
- If a message from an address in your "warnlist" lands in the quarantine, you will receive a warning message.
- Blacklists, whitelists and warnlists may use the "From:" address or the envelope-sender address (from the “Received:” headers).
- The black/white/warn lists may contain addresses or domains.

someaddress@somedomain.com	a sender address
*@somedomain.com$	a sender domain

- Wildcards (*) may be used in blacklist/whitelist/warnlist addresses or domains:

```
philip@*.ac.uk$
werbung@*.com$
*.books.ch$
@ethz.ch
@*.ethz.ch
postgres@id-hdb*.ethz.ch$
```

- If you blacklist a domain, but whitelist an address from that domain, mail from the whitelisted address will be delivered.

5. Spam Messages

- SPAM messages will be quarantined, tagged or deleted, depending on your preferences.

6. Phishing, Malware and Messages with Dangerous Content

- Confirmed malware messages will be deleted or "disarmed" by removing an attachment or link. User preferences will have no effect on these actions.
- Dangerous content such as executable attachments or links to suspicious web sites may be removed from received messages. These messages will be tagged as “{Content?}”. Please contact the Service Desk to get the full text of the message.
- If you have received an AttentionVirus.txt attachment, it will contain the date and Message-ID of the original message. Please include this information when you contact the Service Desk.

7. Messages with Executable Attachments

- Messages containing executable attachments such as java scripts or macro-enabled documents will be rejected. User whitelists will have no effect on these rejections. To receive this kind of message, please ask the sender to use a file transfer service such as Dropbox, polybox or CIFEX.

8. SPF, DMARC and DNS Blacklists

- Messages that violate the sender's SPF or DMARC policy will be tagged as spam or quarantined. Messages from hosts in the SpamHaus blacklist will be rejected.
- https://en.wikipedia.org/wiki/Sender_Policy_Framework
- https://en.wikipedia.org/wiki/DMARC

9. Newsletters

- Many spam messages are now disguised as a newsletter. The “newsletter quarantine” function will quarantine any message that is classified as a newsletter. If you wish to use the “newsletter quarantine” function, you must activate it in the Management Center (Configuration> Address settings> For each message detected as newsletter: retain in quarantine)
- To add the sender to your “newsletter” whitelist and have the newsletter delivered to your mailbox, then click the message-release icon in your quarantine report, or click the "Accept this newsletter" button in your on-line quarantine.
- Note that a message can be classified as a “newsletter” AND “spam”, which means that a message may still land in your quarantine, even if the sender has been added to your “newsletter” whitelist.

10. Reporting Phishing and Malware

- Phishing and malware messages should be reported to phishing@ethz.ch or virus@ethz.ch Please forward the message as an attachment to include the message "headers". Mail sent to these two addresses will open an OTRS ticket. Mail sent to phishing@ethz.ch will also send a copy of the message to the MailCleaner analytical team. Mail sent to the virus@ethz.ch address will be forwarded to the MailCleaner analytical team when appropriate.

11. Reporting Misclassified Messages

- False negatives are "bad" messages that were delivered to your mailbox. False positives are "good" messages that were held in the quarantine or tagged as spam.
- *Misclassified messages (false positives and negatives) should be reported as soon as possible to one of the reporting addresses.*
- A false-negative message may be reported by forwarding the message as an attachment to spam@ethz.ch
- Forwarding the message as an attachment will include the message "headers", which are needed by the analytical team. After you have forwarded a false-negative message to the appropriate reporting address, you may delete the message.
- A **false-positive** message should be reported by clicking the message’s "filter adjustment" icon, or by forwarding the message *as an attachment* to nospam@ethz.ch

12. Why do false-positive messages still land in the quarantine?

- Messages from a particular sender may still land in the quarantine after you requested a filter adjustment. The filter adjustment icon feeds messages to a Bayesian classifier, so you may need to repeat this process over several days.

13. Why do I still receive this spam after I have reported it to MailCleaner?

- You may still receive spam with a particular subject or sender address even after you have reported it. *An effective filtering system requires feedback from its users, so please forward every spam that you receive to the analytical team.* To stop spam-waves, reporting is best done on a daily basis. You may include several spam messages in a single message to spam@ethz.ch

14. Why does ETH internal mail land in the quarantine?

- Mail may come from other servers within our network, but are seen as "external" to the mail filter and are therefore subjected to filtering checks
- ETH servers that only generate automated mail would be candidates for the central whitelist.
- ETH servers that relay mail from external sources would *not* be considered for the central whitelist.
- Contact the Service Desk if the sender address is a candidate for a central whitelist.

15. Why do I receive some tagged messages when I have chosen the quarantine option?

- Your address is included in a mail distribution list that is configured to tag spam messages.

16. Mail Distribution Lists

- Mail distribution lists that receive external mail should be configured as “tag-only”, or should have one address designated to receive quarantine reports, set filter preferences and to release any wrongly-quarantined messages to members of the list.
- The reports-to address may be set in the Management Center (Address settings> Send reports to this address).
- Please contact the Service Desk if you are unable to set the address.

17. When should I submit a ticket to the Service Desk?

- for questions about the use of quarantine reports or your Management Center
- to request the full text of a “disarmed” message
- for questions about missing messages
- to designate an address to receive quarantine reports for a distribution list

18. User Guide

- For more information, please see the MailCleaner User Guide:

http://www.mailcleaner.net/downloads/documentations/mailcleaner_user_manual.pdf
http://www.mailcleaner.net/downloads/documentations/de/mailcleaner_benutzerhandbuch.pdf
http://www.mailcleaner.net/downloads/documentations/fr/mailcleaner_manuel_utilisateur.pdf

Update: Zurich, 14 July 2021