SPAMINA

Cloud Email & Web Security

Cloud Email Firewall

User's Manual

Version 4.3.2-4

Contents

1. Introduction to Cloud Email Firewall

1.1. What is Cloud Email Firewall?

Cloud Email Firewall is an innovative security service which protects company domains and email servers from spam, viruses and phishing attempts (fraudulent email).

To use the service there is basically no maintenance activity required by the administrator. The update of external filters is transparent and executes without any interaction. The email service will continue even in case of a failure (fault tolerance)

Detailed statistical information and configurable reports about email activity are provided. End users can easily access their email from any connection device – no setup by end user required.

Cloud Email Firewall operates as an external filter between the email recipient and sender. It collects/receives messages, filters them before they are delivered and grants email free of threats.

Main benefits:

- Cloud Email Firewall does not slow down computers or mobile devices: filtering is performed via an external server, either as appliance or Cloud Email Firewall's remote servers, and confidentiality is fully guaranteed (validated by "econfia").

- Mobility: It protects your email domain no matter from where you access your mail (your home PC, the office, a cyber-cafe, a PDA or other mobile device, etc.). The solution is continuously updated completely transparent to users (no intervention is required).

- It saves bandwidth by eliminating junk mail, and reduces other risks associated with email.

- It saves users time and effort by preventing them from having to delete unwanted messages that saturate their inboxes.

1.1.1. What makes Cloud Email Firewall different?

Cloud Email Firewall is an application that operates as an external email filter, with the following advantages for users:

- It blocks threats before they can reach your computers.

- It is not a drain on your computers resources: filtering is performed from Cloud Email Firewall.

- It does not only protect computers but also your email accounts: Cloud Email Firewall provides mobility.

- It uses its own trusted lists or dynamic white lists, which minimize the possibility of false positives. .

1.1.2. Is it secure?

Cloud Email Firewall operates as an appliance, setup in a company's data centre, fully independent from the email server or as an email service provider along with your current Internet service provider. Data confidentiality is fully guaranteed:

- All processes are fully automated, with no human intervention or access to the email filter needed.

- The organization is fully compliant with personal data protection legislation, and is subject to continuous external and independent audits.

1.2. How it works

1.2.1. How messages are classified

Cloud Email Firewall runs all email messages through three separate checks to determine if they contain viruses or whether they are junk mail.

1. **Connection filters**: the source of every email received is analyzed to verify whether the sender is reliable or a known spammer.

2. **Antivirus filter**: Checks if a message is infected with a virus. The Message gets deleted and the user can request a detailed report about the infected email.

3. **List filter**: Checks if the sender is included in the valid email lists (white list), if so the message will be delivered to the recipient's inbox. If the sender is included in the non-valid email list (blacklists), the message is retained as spam.

4. **Anti-spam filter**: finally, and for all those messages whose senders are not included in any list, an anti-spam filter is applied, with two operational modes: Guaranteed and Automatic (default).

In Guaranteed mode, messages which are not included in any of the lists will remain pending validation until the sender or recipient validates that message. To make list management easier, Cloud Email Firewall offers the possibility of importing the contact list from your email client. As this your contacts will automatically be white listed and for the future considered as valid.

2. Cloud Email Firewall interface

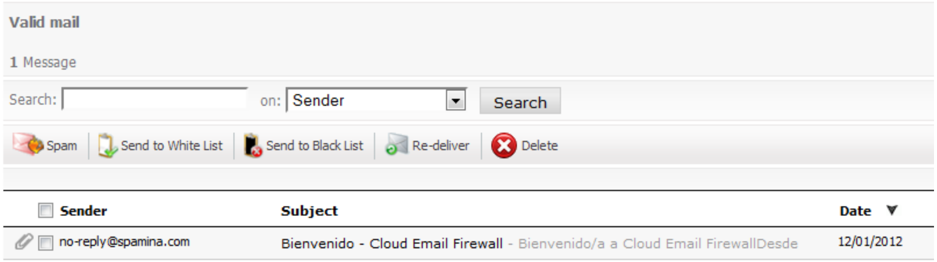
2.1. Cloud Email Firewall Control Panel - User level

SPAMINA Email Firewall users can access a personal control panel via the URL provided by your company where it is possible to find all the information you need about the service provided.

It includes the sections:

- Messages
- Filtering
- Personalization
- Settings

Below screenshot shows filtering options available within the user interface:



Valid mail

1 Message

Search: on: Sender

□ Sender	Subject	Date
□ no-reply@spamina.com	Bienvenido - Cloud Email Firewall - Bienvenido/a a Cloud Email FirewallDesde	12/01/2012

To access the control panel, just enter your email account (user name) and password in the login section of the URL provided by your company or access from the Notifier.

2.1.1. Messages section

2.1.1.1 *Spam*

Emails are saved for as many days as the administrator decides. Once expired, they are sent to the *"Trash can"* and deleted. If you receive a false negative email in this folder, you can recover it by clicking "*Not spam"*.

2.1.1.2 *Valid mail*

Valid email is saved in Cloud Email Firewall for as many days as the administrator decides. Once this period has expired, they are sent to the "*Trash can"*.

False negative messages must be confirmed as Spam so Cloud Email Firewall can provide feedback to the Web.

2.1.1.3 *Mail pending validation*

These are emails from senders that have not been registered by the Cloud Email Firewall sender validation system. This folder "Mail pending validation" for the guaranteed filtering mode is always displayed, regardless of user mode filtering.

2.1.1.4 *Mailing lists*

This email comes from automatic distribution systems (newsletters, news bulletins, sales) to which you may have subscribed. Cloud Email Firewall detects these messages and stores them in this folder.

2.1.1.5 *Virus warnings*

These are notifications sent by Cloud Email Firewall, reporting the presence of a virus in an email you have received in your email account.

2.1.1.6 *Notifications*

These emails are notifications automatically sent by email servers, related to mail which could not be delivered or recipients that did not exist. Cloud Email Firewall places these messages in the *"Notifications"* folder.

2.1.1.7 *Trash can*

Contains messages that have been deleted by the user. This folder is emptied every day.

2.1.2. Filtering section

In order to avoid repetitions of valid and invalid senders and domains, a sender cannot be added if the domain the user belongs to already exists in the same list. Therefore, when adding a domain to a list, all the separate email addresses from that domain will be removed from the list.

2.1.2.1 *White List*

Cloud Email Firewall classifies messages received from senders or domains registered in your White List as valid emails, immediately and without applying any filter.

Email addresses and email domains may be imported.

- The file to be imported must contain elements separated by , (comma), ; (semi-colon) or line break
- Each line of the file may contain several elements separated by the mentioned separators

- The file may be either .txt or .csv
- The maximum number of elements per file is 2000

2.1.2.2 *Black List*

Operates the same way as the White List but has the opposite effect. Every email send from a listed domain or email address will be considered a non-valid sender.

Email addresses and email domains may be imported.

- The file to be imported must contain elements separated by , (comma), ; (semi-colon) or line break
- Each line of the file may contain several elements separated by the mentioned separators
- The file may be either .txt or .csv
- The maximum number of elements per file is 2000

2.1.2.3 *List of senders pending validation*

The List of senders pending validation may contain email addresses.

In order to avoid redundancy in the black lists and white lists, a sender cannot be added if the domain already exists in any of the lists. Meanwhile, when a domain is added to the list, the senders belonging to that domain will be deleted.

2.1.2.4 *Trusted lists*

These are effectively automatic white lists. These lists are automatically created. If an error is detected and there is an invalid entry, it can be sent to the black list.

2.1.2.5 *Filtering mode*

Messages are filtered for spam to determine whether a message is valid or not. When Cloud Email Firewall does not know where the message comes from (messages received from senders or email domains which are not registered in its lists) it applies one of below filtering modes

- Automatic filtering

When Cloud Email Firewall receives an email, it analyzes it and gives it a score according to its characteristics to determine whether it is valid or spam (you can choose the protection level)

The filters applied to your mail can be customized at any time. A valid filter applied by one person may not be valid for another person.

If there is a message that has been mistakenly detected as spam, it can be recovered.

- Guaranteed filtering

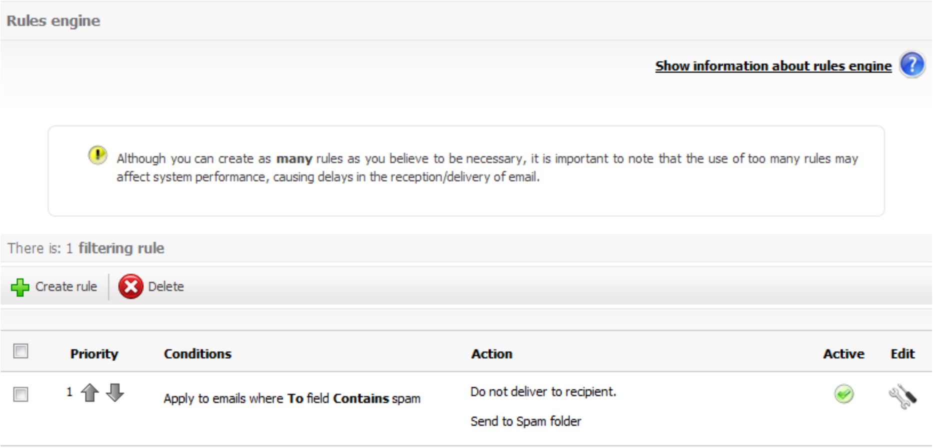
This checks and validates the source of messages, checking whether the senders are included in the valid senders' list (white list)

Any sender not included in the white list will receive a validation message. A simple click will add the sender to your white list and all their future messages will be automatically delivered. Cloud Email Firewall has lists of valid senders and domains (whose messages will only go through the antivirus process) and the invalid ones (which will be considered as junk mail).

2.1.2.6 *Rules engine*

Spamina has provided a rules engine panel for more advanced users where users may create customized rules that will affect email arriving at the User's Cloud Email Firewall level.

Users may change priority for rules using the arrows within the priority column.



Rules engine

Show information about rules engine

Although you can create as **many** rules as you believe to be necessary, it is important to note that the use of too many rules may affect system performance, causing delays in the reception/delivery of email.

There is: 1 **filtering rule**

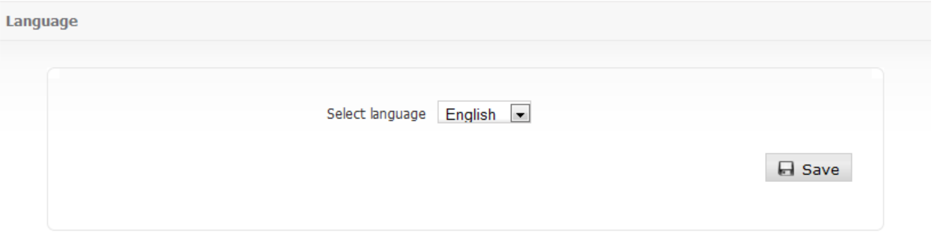
□	Priority	Conditions	Action	Active	Edit
□	1 ⇧ ⇩	Apply to emails where **To** field **Contains** spam	Do not deliver to recipient. Send to Spam folder	✓	

We recommend using the rules engine only if the other service options do not detect certain emails.

2.1.3. Personalization section

2.1.3.1 *Language*

From this menu you can change the language in which the control panel is setup.



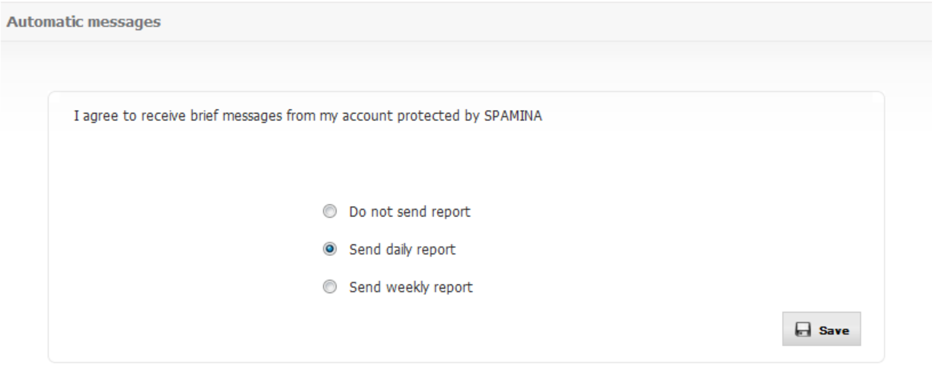
Language

Select language: English

2.1.3.2 *Automated messages*

2.1.3.2.1 Summaries

Cloud Email Firewall sends a summary to all users whose emails are: blocked as spam, pending validation, senders added in the lists, etc. According to the settings of each account, this summary is sent daily, weekly, or never.



Automatic messages

I agree to receive brief messages from my account protected by SPAMINA

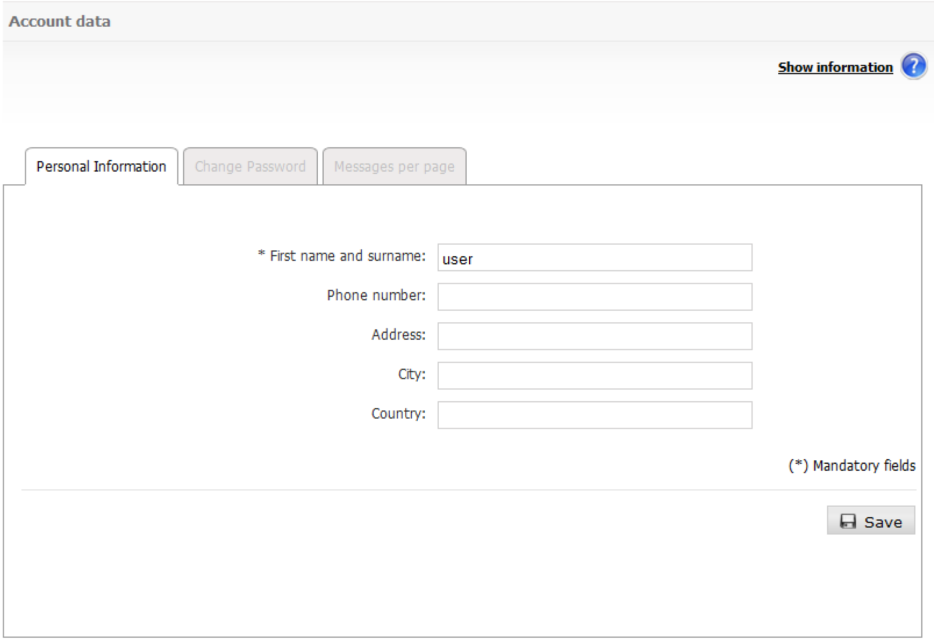
○ Do not send report
● Send daily report
○ Send weekly report

2.1.4. Settings section

2.1.4.1 *Account data*

2.1.4.1.1 Personal information

Here you will find the following account data: First and surname, telephone number, address, city and country (not required fields)



Account data

* First name and surname:	user
Phone number:	
Address:	
City:	
Country:	

(*) Mandatory fields

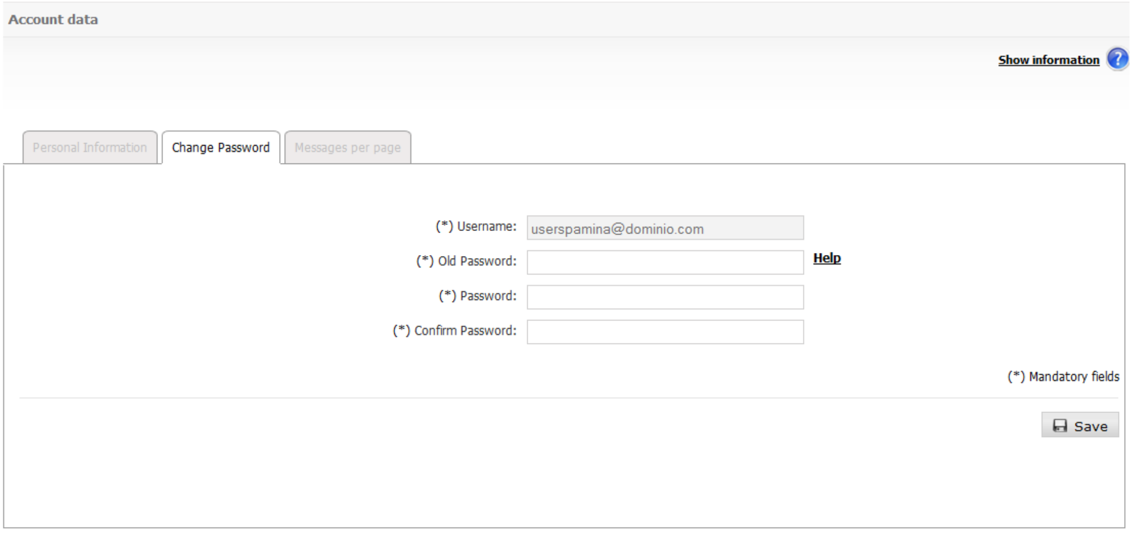
2.1.4.1.2 Password

If you want to change your password you will need to enter your previous password, enter your new password, and enter the new password again.

In order to help you to choose a secure password, this feature will allow you to check if the password is valid or not.

Tips for creating a secure password:

- Lowercase and uppercase letters "a" to "z", except "ñ"
- Numbers 0-9
- Symbols allowed: _ . -
- Minimum length of 8 characters and maximum of 64 characters



Account data

Show information

Personal Information | Change Password | Messages per page

(*) Username: userspamina@dominio.com

(*) Old Password: Help

(*) Password:

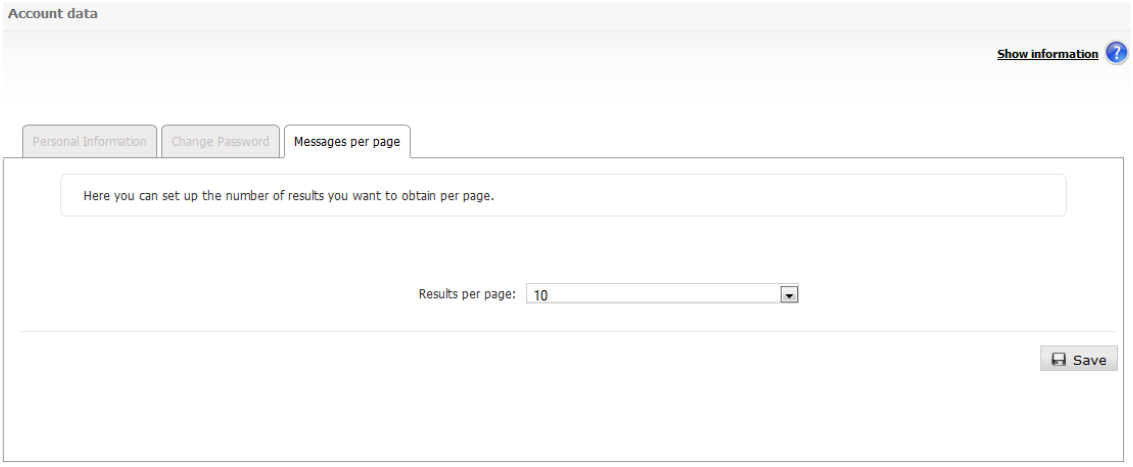
(*) Confirm Password:

(*) Mandatory fields

Save

2.1.4.1.3 *Messages per page*

You can change the number of messages displayed per page in the panel, permitted values are: 10, 15, 20, 50, 75, 100, 200, 500.



Account data

Show information

Personal Information | Change Password | Messages per page

Here you can set up the number of results you want to obtain per page.

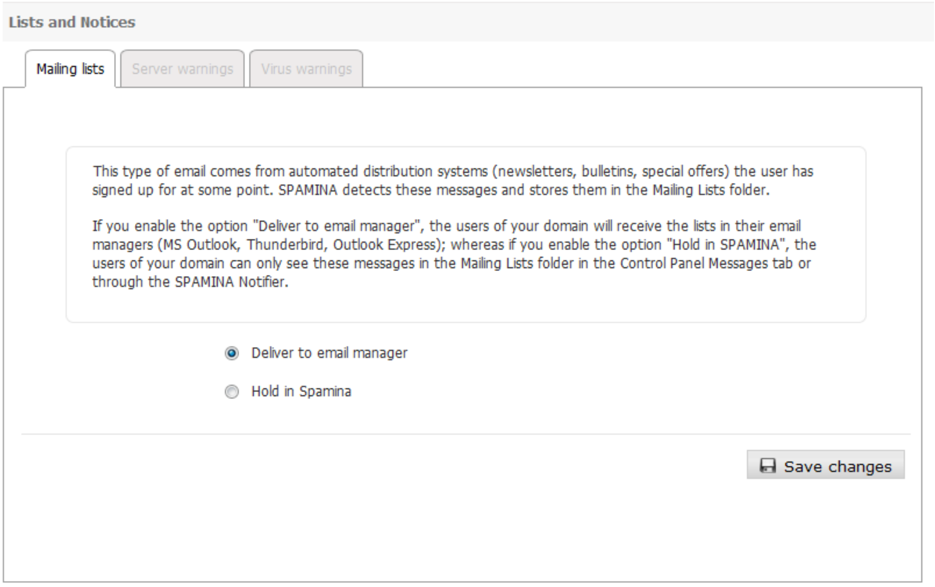
Results per page: 10

Save

2.1.4.2 *Lists and notices*

Mailing lists: This kind of email comes from automated distribution system (newsletters, news bulletins, sales) to which user may have subscribed. Cloud Email Firewall detects these messages, and considers them as valid mail. These emails are delivered to the user's inbox.

If you enable the option "Deliver to email manager", you will receive these messages in your inbox, while if you enable the option "Hold in SPAMINA", you will only see these messages in the "Mailing list" folder within the Cloud Email Firewall control panel.



This type of email comes from automated distribution systems (newsletters, bulletins, special offers) the user has signed up for at some point. SPAMINA detects these messages and stores them in the Mailing Lists folder.

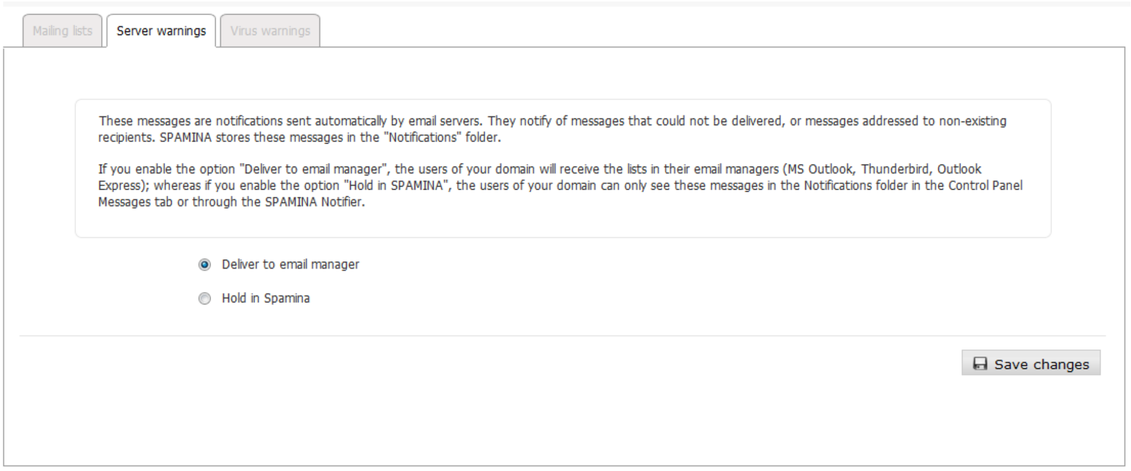
If you enable the option "Deliver to email manager", the users of your domain will receive the lists in their email managers (MS Outlook, Thunderbird, Outlook Express); whereas if you enable the option "Hold in SPAMINA", the users of your domain can only see these messages in the Mailing Lists folder in the Control Panel Messages tab or through the SPAMINA Notifier.

● Deliver to email manager

○ Hold in Spamina

Server warnings: Cloud Email Firewall sends out notifications for emails that could not be delivered or if emails were send to recipients that are not registered within the product. Cloud Email Firewall places these messages in the **Notifications** folder.

If you enable the option "Deliver to email manager", you will receive these messages in your inbox, while if you enable the option "Hold in SPAMINA", you will only see these messages in the "Notifications" folder in the Cloud Email Firewall control panel.



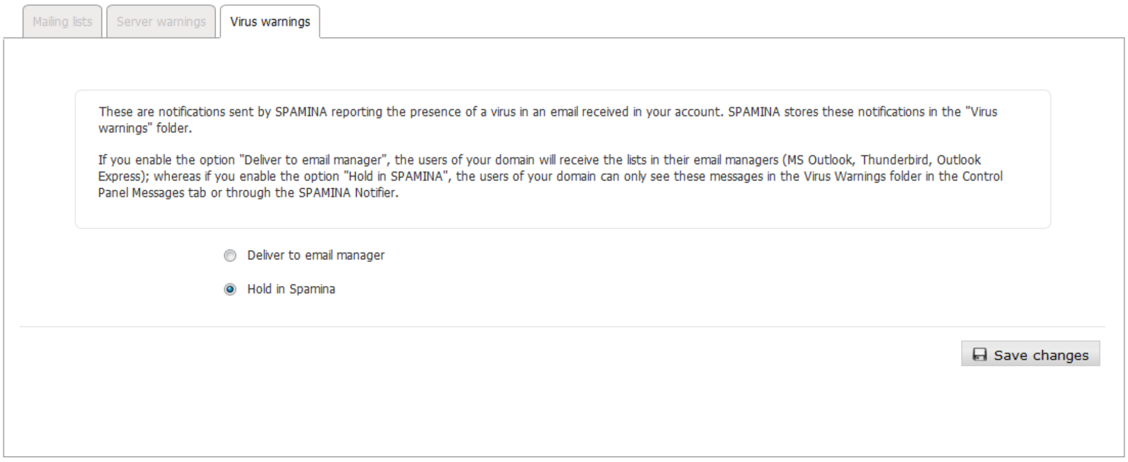
These messages are notifications sent automatically by email servers. They notify of messages that could not be delivered, or messages addressed to non-existing recipients. SPAMINA stores these messages in the "Notifications" folder.

If you enable the option "Deliver to email manager", the users of your domain will receive the lists in their email managers (MS Outlook, Thunderbird, Outlook Express); whereas if you enable the option "Hold in SPAMINA", the users of your domain can only see these messages in the Notifications folder in the Control Panel Messages tab or through the SPAMINA Notifier.

● Deliver to email manager

○ Hold in Spamina

Virus warnings: When you receive a message that contains a virus, Cloud Email Firewall deletes it and sends a notification message to the user mentioning the delivery attempt and the presence of a virus as well as the name of the virus detected.



These are notifications sent by SPAMINA reporting the presence of a virus in an email received in your account. SPAMINA stores these notifications in the "Virus warnings" folder.

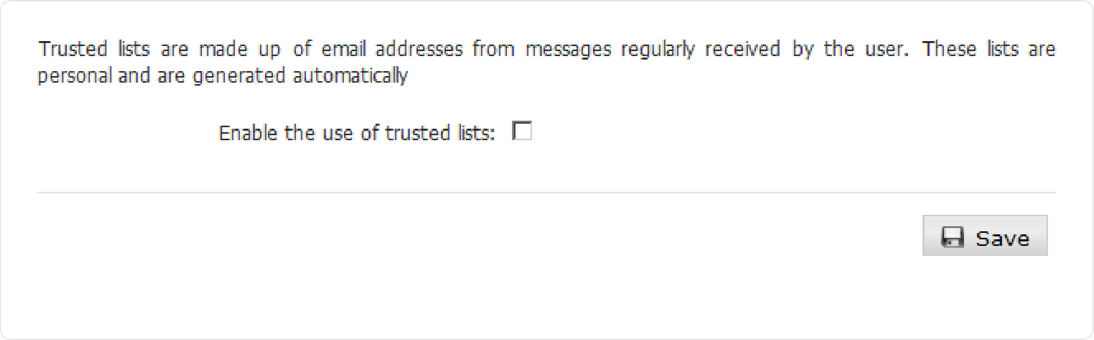
If you enable the option "Deliver to email manager", the users of your domain will receive the lists in their email managers (MS Outlook, Thunderbird, Outlook Express); whereas if you enable the option "Hold in SPAMINA", the users of your domain can only see these messages in the Virus Warnings folder in the Control Panel Messages tab or through the SPAMINA Notifier.

○ Deliver to email manager

● Hold in Spamina

2.1.4.3 *Trusted lists*

Trusted lists include valid email addresses which a user receives. This list is personal and it is automatically generated according to SPAMINA's own protocol.



Trusted lists are made up of email addresses from messages regularly received by the user. These lists are personal and are generated automatically

Enable the use of trusted lists: □

2.1.5. Archive Search

You may use the search interface to perform queries on the archived emails.

In the section «Conditions» you may indicate all the search criteria you wish to use. These criteria may include the fields and operations indicated in the following table:

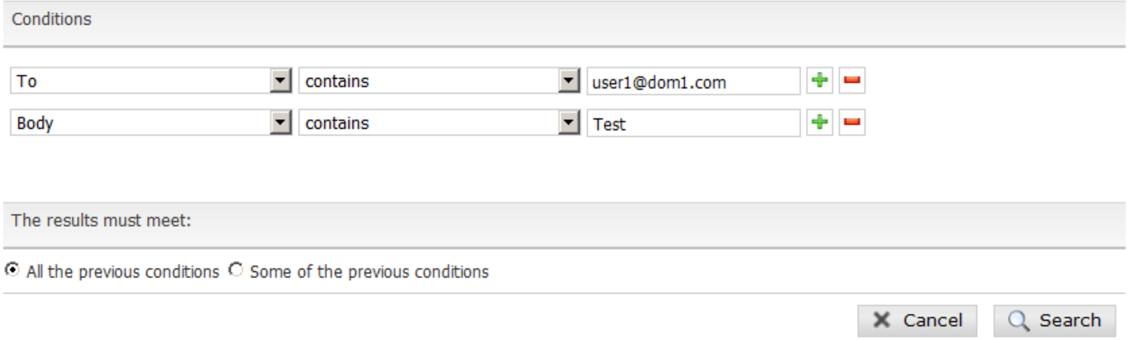
Field	Operation	Value
To	▪ contains ▪ does not contain	All or part of an email addresses.
From	▪ contains ▪ does not contain	All or part of an email addresses.
Cc	▪ contains ▪ does not contain	All or part of an email addresses.

Subject	▪ starts with ▪ does not start with ▪ ends with ▪ does not end with ▪ contains ▪ does not contain ▪ is equal to ▪ is different than	Text to find in the email's subject line.
Body	▪ contains ▪ does not contain	Text to find in the body of the email.
Emails with a date	▪ is equal to ▪ is different than ▪ is equal or higher than ▪ is lower or equal to	Date in which the email was sent.

Finally, you may specify the logical operation that you wish to apply in order to combine the search conditions:

- **All the previous conditions**: The search results will be those that meet all the conditions indicated.

- **Some of the previous conditions**: The search results will be those that meet any of the conditions indicated.



Conditions

To	contains	user1@dom1.com
Body	contains	Test

The results must meet:

● All the previous conditions ○ Some of the previous conditions

3. Additional functions

3.1. SPAMINA Notifier

The Cloud Email Firewall Notifier is a utility[1] which can be installed that offers complete control of email management.

Once installed, a small icon is displayed in the system box which flickers when the service is enabled, and gives different notices: arrival of new emails, virus warnings and undelivered emails. The Notifier has intuitive menus and lets you access all the service options.

It lets you manage messages, by marking them as valid mail, invalid, or by deleting them, as well as considering the filtering mode (Automatic or Guaranteed), and the protection level you require, and let's you manage several mail accounts at the same time. You have access to the same options from within the Cloud Email Firewall web page.

3.1.1. Technical Specifications

The Notifier works in Windows operating systems (XP, Vista and Windows 7), Mac OS X, Linux x86-64, Linux PowerPC and Linux i386; the operative system must support multiuser.

[1] It is an optional program to enhance the use of the external email filter, but it is not necessary to install it to protect an email account.