

# Panda Security Email Protection

Domain Administrator's  
Guide

Version 4.5.1



## Contents

1. Introduction to Email Protection.....	4
1.1 What is Email Protection?.....	5
2. Email Protection Interface.....	6
2.1 Administrator access.....	7
2.2 Email Protection Interface.....	7
2.3 Administration.....	7
2.3.1 Creating and editing passwords.....	8
2.3.2 State.....	8
2.3.3 Domain.....	12
2.3.4 Users.....	13
2.3.5 Users with basic filtering.....	16
2.3.6 Signup mode.....	16
2.3.7 Multiple administrators.....	21
2.3.8 Archive.....	21
2.4 Filtering.....	24
2.4.1 Lists.....	24
2.4.2 Anti Virus.....	26
2.4.3 Anti Spam.....	28
2.4.4 Trusted lists.....	30
2.4.5 Filtering mode.....	31
2.4.6 Rules engine.....	33
2.4.7 Email logs.....	37
2.4.8 NDR Validation.....	41
2.4.9 Anti email spoofing.....	42
2.5 Personalization.....	44
2.5.1 Automatic messages.....	44
2.5.2 Reports of administrators.....	49
2.5.3 Logo.....	50

2.5.4 Language.....	51
2.6 Settings.....	51
2.6.1 Administrator data.....	52
2.6.2 Access to users panel.....	53
2.6.3 Lists and notices.....	54
2.6.4 Disclaimers.....	57
2.6.5 Synchronization.....	58
2.6.6 Reports.....	59
2.6.7 Time zone.....	62
3. Additional functions.....	63
3.1 Panda Notifier.....	64
3.1.1 Technical Specifications.....	64
4. Technical support.....	65

# 1. Introduction to Email Protection

---

What is Email Protection??

## 1.1 What is Email Protection?

Email Protection is a security solution for email based on the concept of software as a service (SaaS). This concept lets companies focus on their core business, freeing them from the management tasks and operating costs associated with traditional security solutions.

Email Protection consists of a multilayer system which combines protection filters and processes using proprietary technologies (Email Protection proactive, trusted lists...) and as standard technologies (IP reputation, Bayesian networks, whitelists and black lists, graylists, traffic shaping...) to ensure maximum effectiveness. By removing spam, viruses and phishing -with more than ten different filters-, it not only reduces the load on the email server but also mitigates productivity problems caused by employees deleting spam.

In addition connection filters, there are two filtering modes: automatic mode and guaranteed mode.

Email Protection has an interface which is intuitive and easy to set up, allowing administrators to rapidly start up the protection components required to ensure the company's security.

# 2. Email Protection Interface

---

Administrator access

Email Protection Interface

Administration

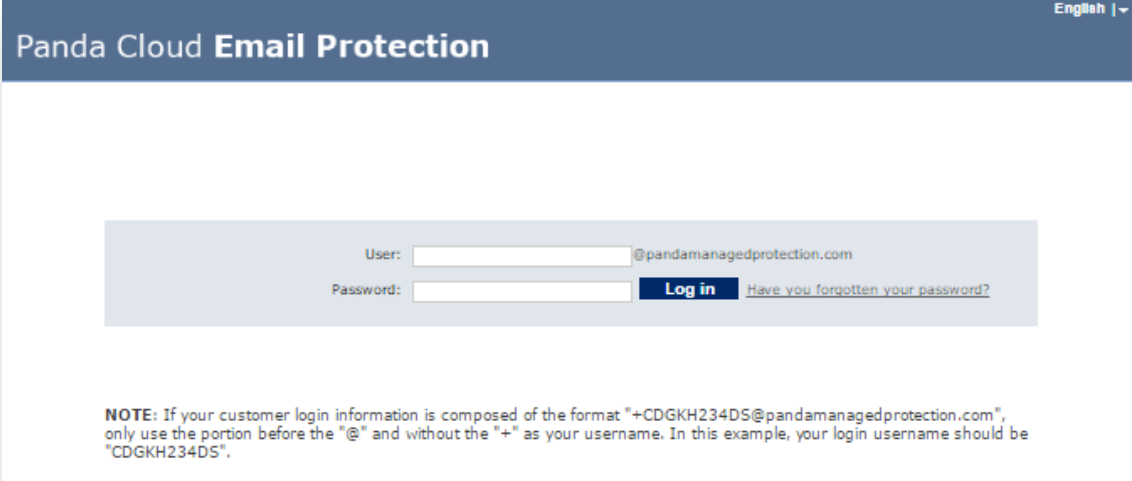
Filtering

Personalization

Settings

## 2.1 Administrator access

The Email Protection control panel can be accessed from any browser by typing by typing the URL assigned by your administrator, adding “/admin/” at the end.



A Web panel will appear where user or administrator credentials must be entered.

If you have forgotten your password, use the “Have you forgotten your password?” option.

## 2.2 Email Protection Interface

The Email Protection interface is intuitive and easy to use.

It includes five sections:

- Administration
- Filtering
- Customization
- Settings
- Help

All the administrator panels have been tested, and they work in the next browsers:

- Internet Explorer ® 9
- Mozilla Firefox from 3.6

The supported screen resolutions are 1024x768 and higher.

## 2.3 Administration

In this section you can administer all aspects related to: users, domains, and registration modes.

### 2.3.1 Creating and editing passwords

In order to help you to choose a secure password, this feature will allow you to check the password security.

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

Note: A password is considered valid only if it is not weak.

### 2.3.2 State

#### State of subscription

- Contracting date.
- Expiration date.
- Amount of licenses consumed.
- Amount of licenses available.

Cloud Email Firewall	
Contracting date	22/02/2013
Expires	22/02/2014
Number of licenses available	83
Amount of active licenses	17

#### Statistics for incoming mail

- **Rejected spam:** Number of spam messages rejected by the email Firewall, whether due to its high Spam content or the connection filters.
- **Spam:** Number of messages classified as spam. They can be checked or recovered using the Administration Panel, User Panel, blocked email report or Notifier.
- **Emails pending validation:** Number of messages from senders that do not yet belong to the white or black lists of recipients using the guaranteed filtering mode.
- **Virus warnings:** Number of messages that inform on the emails in which a virus has been detected.
- **Server warnings:** Number of messages that inform the senders of problems in the delivery of an email.
- **Email lists:** Number of messages classified as email list.
- **Valid email:** Number of messages that have passed all the filters and have been delivered.



- The information presented above is displayed for the following three time periods:
  - **Total** - Statistics covering the last 30 days.
  - **Today** - Statistics for the current day (from midnight onwards).
  - **Last hour** - Statistics for the hour before the current one.

**Summary table of the statistics of Incoming Email**

Reference	Total	Today	Last hour
Rejected Spam	25	0	0
Spam	200	0	0
Email pending validation	83	0	0
Virus warnings	23	0	0
Server warnings	60	0	0
Mailing lists	60	0	0
Valid Email	180	0	0

#### Statistics for outgoing mail

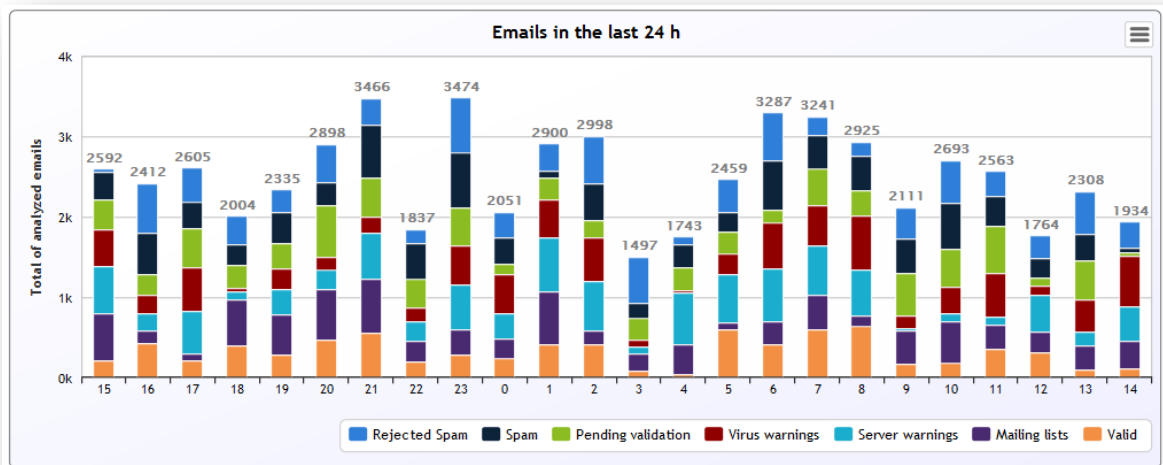
- **Rejected spam:** Number of spam messages rejected by the email Firewall due to its high Spam content.
- **Virus:** Number of messages in which a virus has been detected.
- **Valid email:** Number of messages that have passed all the filters and have been delivered.
- The information presented above is displayed for the following three time periods:
  - **Total** - Statistics covering the last 30 days.
  - **Today** - Statistics for the current day (from midnight onwards).
  - **Last hour** - Statistics for the hour before the current one.

### Summary table of the statistics of Outgoing Email

Reference	Total	Today	Last hour
Rejected Spam	12	0	0
Viruses	3	0	0
Valid Email	60	0	0

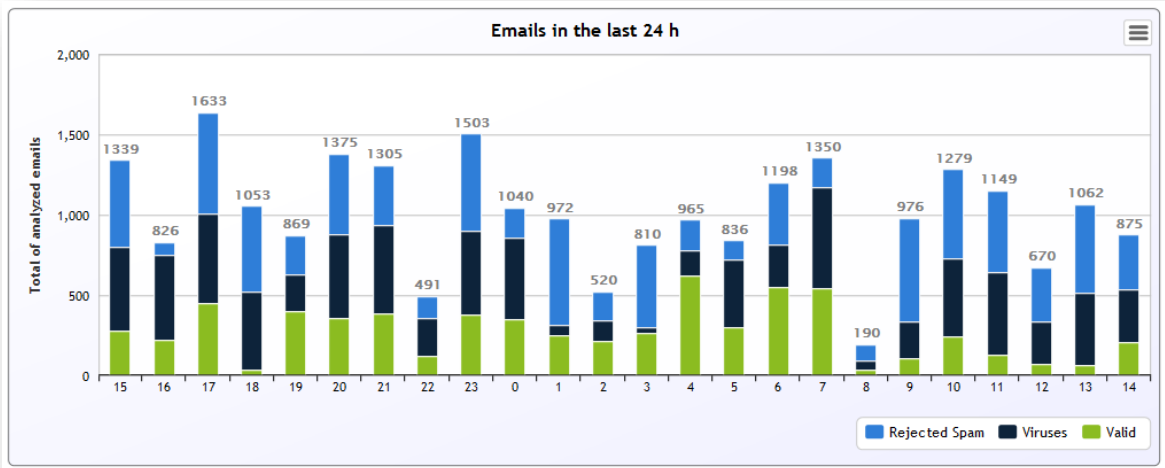
### Statistics for incoming mail per hour

Displays the breakdown of the activity of incoming messages in the last 24 hours of the day.



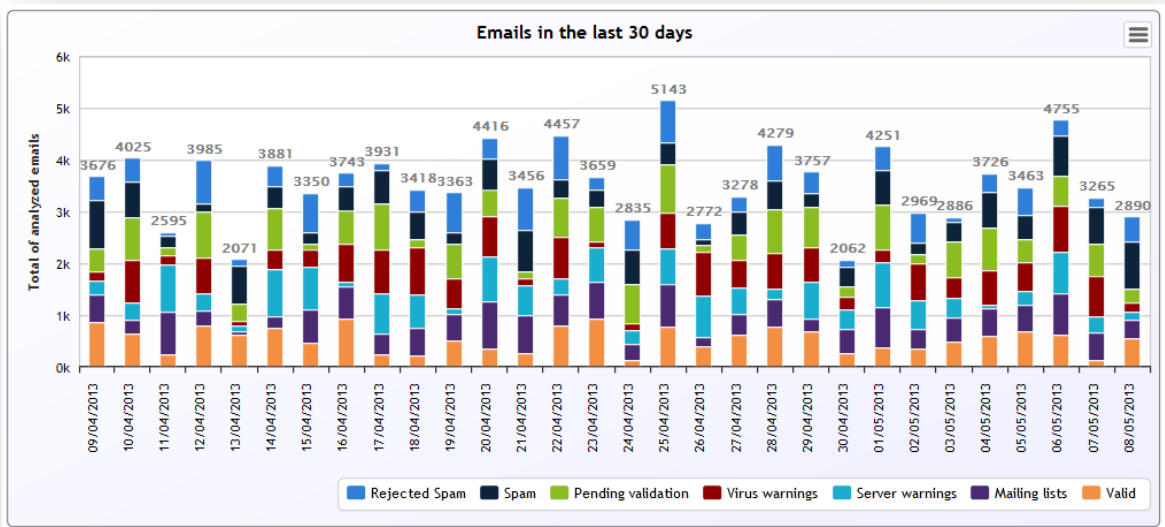
### Statistics for outgoing mail per hour

Displays the breakdown of the activity of outgoing messages in the last 24 hours of the day.



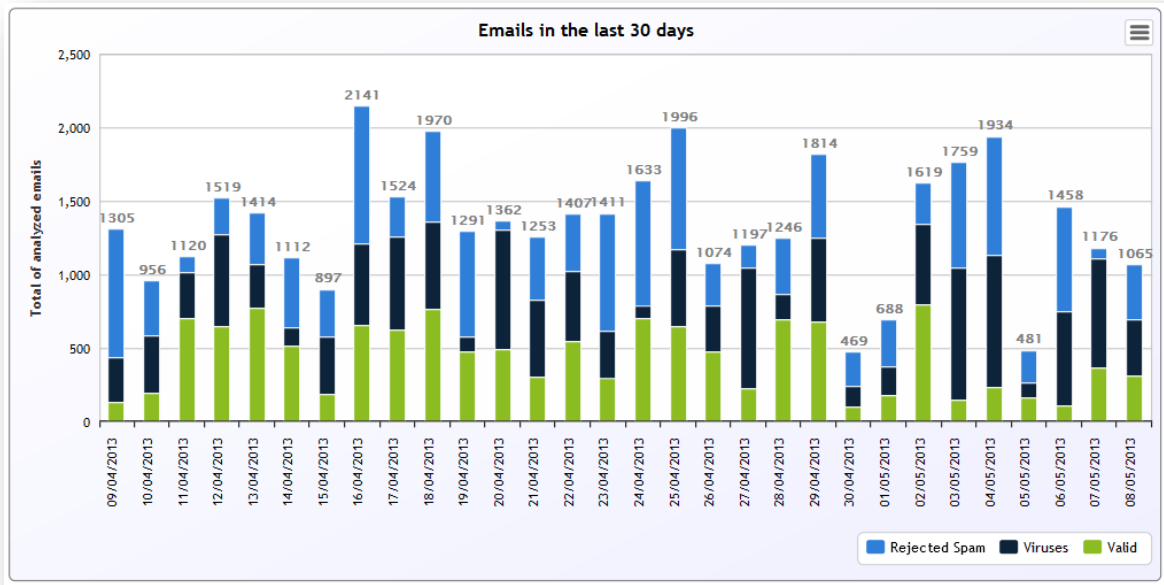
### Statistics for incoming mail per day

Displays the breakdown of the activity of incoming messages in the last 30 days.



### Statistics for outgoing mail per day

Displays the breakdown of the activity of outgoing messages in the last 30 days.



### 2.3.3 Domain

Add as many domains to deliver valid email to as necessary. Email will be delivered to the domain with the lowest priority value. Should delivery fail, the system will try a domain with a higher priority value, and so on.

Domain

[Show information about MX ?](#)

Domain Details: domain.com

\* Contact email:

Outgoing MX

MX host	Priority	+	-	test SMTP
smtp.panda.com	10			

Incoming MX

sentry.domainbank.com : 10
----------------------------

(\*) Mandatory fields

#### HostMX

IP aggregates of both IPv4 and IPv6 types are allowed. Each IPv6 address must be represented in eight groups separated by ":"; each group must contain 4 hexadecimal digits.

It is possible to use compressed IPv6 notation, eliminating the zeroes at the right of each group.

For example:

2001:0DB8:0000:0000:0000:0000:1428:57ab

2001:0DB8:0000:0000:0000::1428:57ab

2001:0DB8:0:0:0:0:1428:57ab

2001:0DB8:0::0:1428:57ab

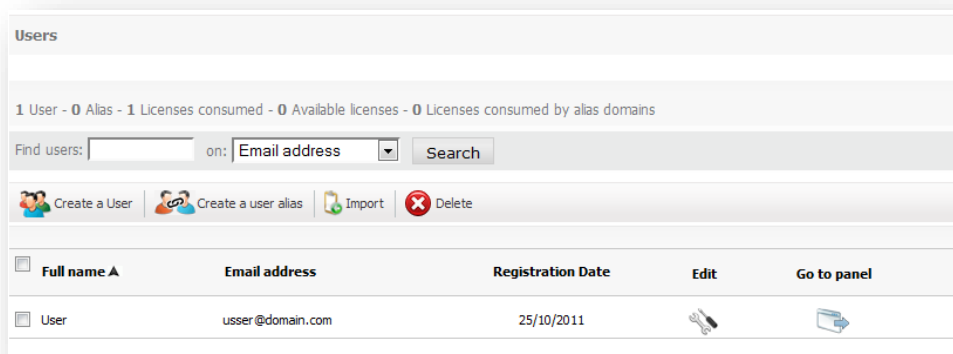
2001:0DB8::1428:57ab

### 2.3.4 Users

This shows the list of users and user aliases, and allows users to be created manually or imported from a file. You can also delete users or user aliases.

You can search for users under the following criteria: Full name, Email and Alias, selecting one of these options from the selection list in the search form.

From the "Edit" menu you can access a form in which the user data can be modified. You can never change its email address.



To import a user list, use the following format:

The file to be imported must include the first and last names of the user, email address (without '@domain'), and the user's password<sup>1</sup>, all separated by commas.

Tips for creating a secure password:

- Lowercase and uppercase letters "a" to "z", except "ñ"
- Numbers 0-9
- Symbols allowed: . -

<sup>1</sup> If the user's password is missing, a new one will be randomly generated to be sent to them in the welcome email.

- Minimum length of 8 characters and maximum of 64 characters

A password is considered valid only if it is not weak.

Each line in the file must represent a user.

These files can be either .txt or .csv

**File structure:**

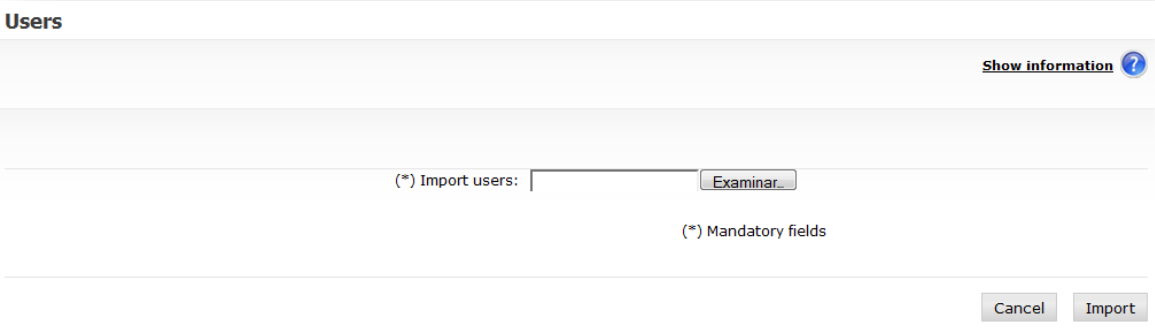
First name and last name, Email address, Password

In the case of email (myuser@mydomain.com) will only be necessary to add the user name (myuser).

**Example:**

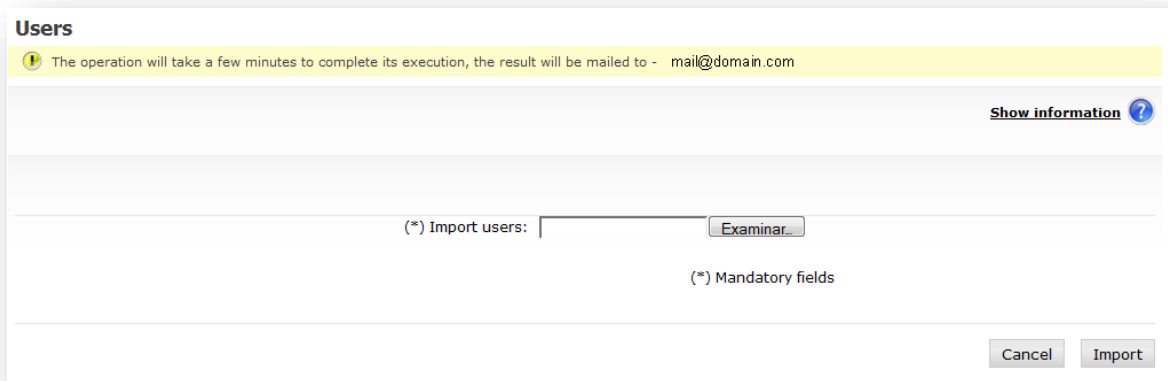
Mike Sanchez, msanchez, aras249g

Andrew Brown, abrown, 32kios5



The screenshot shows a web interface titled "Users". At the top right, there is a "Show information" link with a question mark icon. Below this is a large empty text area for a file upload. Underneath the text area, there is a label "(\*) Import users:" followed by a text input field containing the word "Examiner...". Below the input field, there is a note "(\*) Mandatory fields". At the bottom right of the interface, there are two buttons: "Cancel" and "Import".

The import of users can take several minutes (between 5 and 10 seconds per user) and will be done in the background, so you should not wait for them completing before another action in the system. You will automatically be sent domain administrator email notice of such import.



### 2.3.4.1 Users synchronization

An ignored user is a user that will not be synchronized if the Synchronization mode is active.

The "Go to synchronization mode" button allows viewing those users that:

- Will be ignored by the synchronization process
- Will be deleted by the synchronization process
- Will be updated by the synchronization process

If the manual synchronization mode is active, the synchronization display will only show the users that will be ignored, deleted or updated. If the automatic synchronization mode is active, the synchronization display will only show the users that will be ignored.



The "Synchronize" button, which is only available when the synchronization mode is set at Manual, allows synchronizing all the domain or company users that have been selected.

A user that has been ignored can be added to the synchronization process again by clicking the "Admit" button.

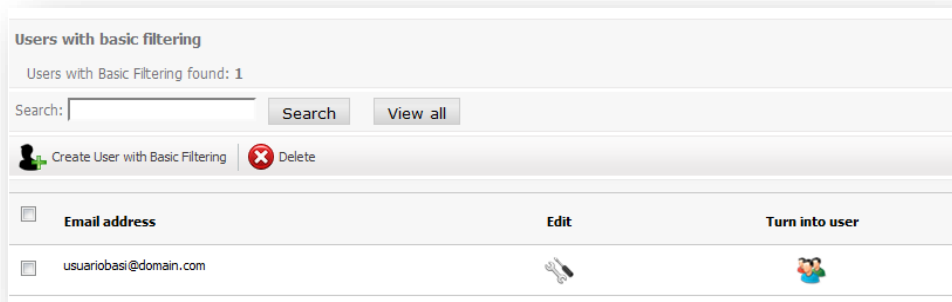


### 2.3.5 Users with basic filtering

Users with basic filtering will receive emails, though only connection filtering will be applied. They will neither have content filtering nor have any kind of quarantine.

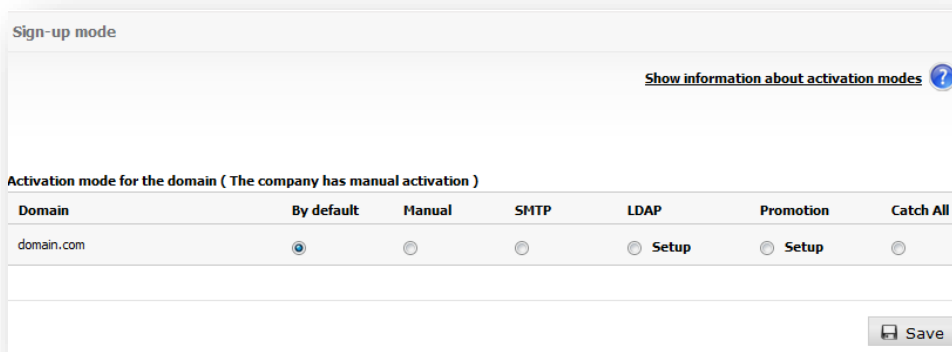
Users with basic filtering can be converted into normal users if the administrator thinks it is necessary. It is important to note that all users must be registered with Email Protection so that their emails are not rejected. If you decide not to use content filters or the user panels, the best option is to create users with basic filtering.

These users will not be counted as Email Protection licences.



### 2.3.6 Signup mode

In order to offer greater flexibility to clients, there are three different ways of registering users.



#### 2.3.6.1 Manual Registration

The Email Protection administrator is responsible for registering each user's account manually. This option is recommended only when a limited number of accounts are to be added. To add an account, go to "Administration" and then to the "Users" menu.



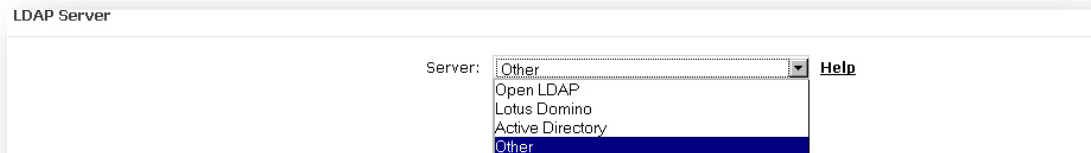
### 2.3.6.2 Automatic registration by SMTP callout or LDAP

Email Protection allows users to register automatically when they start receiving emails. To do this, it checks that recipients' email addresses exist in the end server. These checks can be performed through an SMTP or LDAP server (see Setting up parameters for LDAP user discovery), creating the user in Email Protection if they exist or rejecting the email if they do not. If you select SMTP, make sure your email server is set up to perform the checks<sup>2</sup>. For further information, please contact our Support department.

#### 2.3.6.2.1.1 Setting up parameters for LDAP user discovery

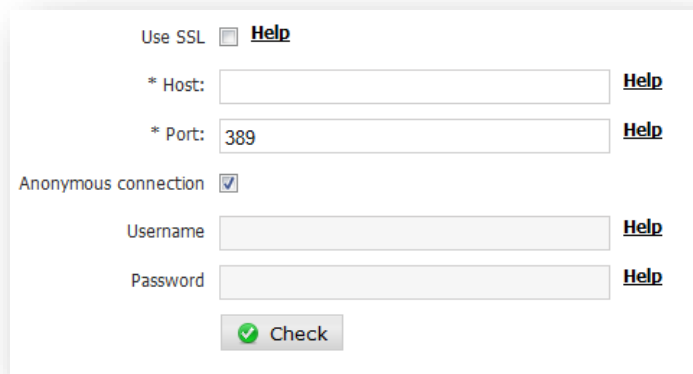
The setup of parameters for user discovery in the corporate LDAP, used in the "LDAP registration mode", is divided into the following seven sections.

#### 2.3.6.2.1.2 LDAP Server



In this section you must specify the LDAP server you are using; this allows suggesting certain configuration values already known for your server.

#### 2.3.6.2.1.3 Connection



In this section you must enter the information required to connect to the LDAP server:

- Use SSL: provides an encrypted connection (Secure Socket Layer).

<sup>2</sup> The SMTP server should only provide an affirmative response for valid users in the domain.

Host: Enter the IP address or DNS name of the LDAP server.

IPs may be used, both IPv4 as well as IPv6 types. Each IPv6 address must be represented in eight groups separated by ":"; each group must contain 4 hexadecimal digits.

It is possible to use compressed IPv6 notation, eliminating the zeroes at the right of each group.

For example:

2001:0DB8:0000:0000:0000:0000:1428:57ab

2001:0DB8:0000:0000:0000::1428:57ab

2001:0DB8:0:0:0:0:1428:57ab

2001:0DB8:0::0:1428:57ab

2001:0DB8::1428:57ab

Port: enter the TCP/IP port used to connect to the LDAP server. There are normally standard ports used by LDAP servers:

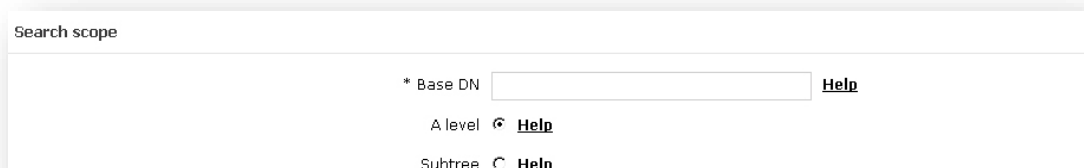
- 389: for normal connections (not secure)
- 636: for secure connections (SSL)

Also you must specify connection information, that is to say, the parameters which will be used to identify the user who will connect to the LDAP server. Based on this information, the server determines the privileges for a specific connection.

If you select "Anonymous connection", you do not have to specify any parameters in this section.

- User's name: It represents a user's DN, for example:  
uid=jperez,ou=People,dc=dominio,dc=com
- Password, for example: supersecret2008

#### 2.3.6.2.1.4 Search scope



The screenshot shows a form titled "Search scope" with the following fields and options:

- \* Base DN:  [Help](#)
- A level:  [Help](#)
- Subtree:  [Help](#)

In this section, specify the search by selecting one of the following values:

- Base DN: In the case of servers with LDAPv3, this field can be left blank in order to connect to the server's *RootDSE*.
- A level: specifies that the objects will be searched for at the level immediately below the Base DN value (not recursive).

- Subtree: specifies that the objects will be searched for at the level immediately below the Base DN value (recursive).

#### Base DN Syntax

In the event the field value contains:

- A space « » (ASCII 32) or numeral «#» (ASCII 35) character at the beginning.
- A space « » (ASCII 32) character at the end.
- Any of the characters: «,» (ASCII 44), «+» (ASCII 43), «"» (ASCII 34), «\» (ASCII 92), «<» (ASCII 60), «>» (ASCII 62) or «;» (ASCII 59)

The character must be an escape character, placing the character «\» (ASCII 92) before it.

For example, if the value of "OrganizationName" (O) is the following: CN=L. Eagle,O=Sue, Grabbit and Runn,C=GB

Then this must be an escape character as given below: CN=L. Eagle,O=Sue, Grabbit and Runn,C=GB

#### 2.3.6.2.1.5 Search of user name

**Search of user name**

\* The attribute containing the email address  [Help](#)

The attribute only stores the user name

The attribute stores the full email address

\* LDAP filter  [Help](#)

In this section, specify the parameters for searching for users in the corporate LDAP:

- The attribute which contains the email address, for example: email, rfc822Mailbox, etc.
- You must indicate if the previously specified attribute contains only the user's name or the whole email address.
- LDAP filter: Specify the most appropriate class to narrow the search field (this affects the performance of the search, as indexes are maintained according to object class). The generic format by default (objectClass=\*) allows the filter to match all LDAP object classes.

#### 2.3.6.2.1.6 Alias search

**Alias search**

Enable alias discovery

\* Attribute containing the alias:  [Help](#)

\* LDAP filter:  [Help](#)

The field is multivalued

Yes

No

Alias separator:  [Help](#)

Is the alias the same object as the mailing address?

Yes

No

Attribute containing the object DN of the real user:  [Help](#)

If “Alias discovery” is enabled, the following parameters must be set up:

- Attribute containing the alias, for example: uid, userId, etc.
- Whether the previous attribute is multi-valued. If not, you must specify an alias separator used within this attribute<sup>3</sup>.
- Specify if the alias is in the same LDAP object as the email address. If not, specify the attribute containing the real user object DN (for example: cn, userId).

### 2.3.6.2.1.7 Groups

**Groups**

Group member(ship)

\* Attribute that containing groups to which the user belongs:  [Help](#)

The field is multivalued

Yes

No

Group separators:  [Help](#)

This configuration is used by the rules engine to determine if a user from a protected domain belongs to a group in the corporate LDAP.

In this section you must specify the information necessary for group membership:

- Attribute which includes the groups to which a user belongs.
- If the field is multi-valued.

<sup>3</sup> You cannot use any character that could be used as part of an email, i.e. numbers from 0 to 9, and the following symbols: ? ) @ ! # \$ % & ' \* + - / = ^ \_ ` ~ . { | } "

- Group separator

### 2.3.7 Multiple administrators

The management of multiple administrators enables you to define the users that will be allowed to manage the email firewall for your domain.

There are two types of administrators:

- Main administrator
- Secondary administrator

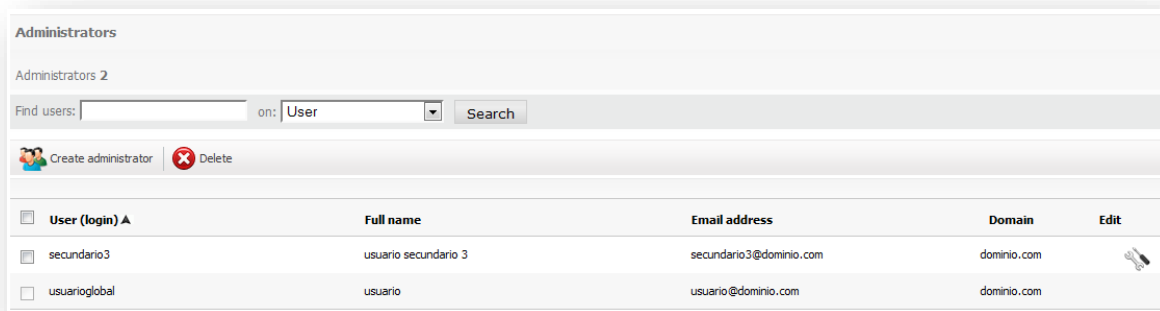
There is only one main administrator for the domain.

The following information is required to create an administrator:

- Full name
- Username: it will be used to login as an administrator
- Password
- Contact email: filtering activity reports will be sent to this email, as well as notifications of the results of actions performed in background mode (e.g. import user function, change of cascade configurations, etc.).

The data of an administrator may be edited or the administrator eliminated only if it is "background" type. The data of a main administrator is edited from the following section:

- "Configuration" tab, "Administrator data" menu option.



### 2.3.8 Archive

#### 2.3.8.1 Domain

If the email archiving system has been contracted, you may decide on the type of configuration that you wish to use for your domain.

The options to «enable» or «disable» the archiving service are applied the moment they are established and those changes do not propagate in cascade to all the lower levels.

**Domain configuration**  
The company has the archiving service **enabled**. [Help](#)

Domain	Global	Enabled	Disabled
dom1.com	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

### 2.3.8.2 Users

If the email archiving system has been contracted, you may decide on the type of configuration you wish to use for each of your users.

You may only «enable» the archiving service if the amount of available licenses allows so.

**Important:** The aliases accounts uses the same configuration defined for the real accounts they refers to. Thus, all the aliases linked to a given account are consuming archiving licenses when archiving service is enabled for such real account.

Archiving configuration for the domain: **global settings**. Company configuration: **enabled**

Search:  on:

Full name ▲	Email address	Same as domain	Enabled	Disabled
User Name	user1@dom1.com	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

### 2.3.8.3 Search

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

The section «Filters» allows specifying, optionally:

1. User from which emails would like to be obtained. The list of users is only available after having selected a domain.

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
<b>To</b>	- contains - does not contain	All or part of an email addresses.
<b>From</b>	- contains - does not contain	All or part of an email addresses.
<b>Cc</b>	- contains - does not contain	All or part of an email addresses.
<b>Subject</b>	- 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.
<b>Body</b>	- contains - does not contain	Text to find in the body of the email.
<b>Emails with a date</b>	- 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.

**Filters**

Users (1)

**Conditions**

To	contains	user1@dom1.com	+	-
Subject	contains	Test	+	-

The results must meet:

All the previous conditions
  Some of the previous conditions

X Cancel
Q Search

## 2.4 Filtering

In this section, you can administer all aspects related to the filtering by Email Protection, applying global settings for domains and users.

### 2.4.1 Lists

#### 2.4.1.1 White list

The White List may contain emails, domains or IPs. Connection filters, the antivirus, the rule engine and no content filters shall be applied to emails from domains or senders included in this list.

The content filter and connection filters shall not be applied to emails from IPs applicable at domain level, although antivirus filters and the rule engine shall be applied. Furthermore, these IPs have a lower priority than those defined in the overall white and black lists.

IPs applicable at global level may not be deleted. These are only displayed for information purposes and may only be managed by system administrators.

On including a sender in a White List or Black List, this sender shall be compared with the Header-From and the Envelope-From.

On sending the sender of an email from the logs to White List or Black List, the Envelope-From is added to them.

The content filters only cover Bayesian analysis.

Email addresses, email domains and IP addresses may be imported.

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



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

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

IP aggregates of both IPv4 and IPv6 types are allowed. Each IPv6 address must be represented in eight groups separated by ":"; each group must contain 4 hexadecimal digits.

It is possible to use compressed IPv6 notation, eliminating the zeroes at the right of each group.

For example:

2001:0DB8:0000:0000:0000:0000:1428:57ab

2001:0DB8:0000:0000:0000::1428:57ab

2001:0DB8:0:0:0:0:1428:57ab

2001:0DB8:0::0:1428:57ab

2001:0DB8::1428:57ab

#### 2.4.1.2 Black list

The Black List may contain emails, domains or IPs. The emails from domains or senders belonging to the black list shall be placed in quarantine after passing the connection filters.

Emails from IPs in this list shall be rejected.

IPs applicable at global level may not be deleted. These are only displayed for information purposes and may only be managed by system administrators.

On including a sender in a White List or Black List, this sender shall be compared with the Header-From and the Envelope-From.

On sending the sender of an email from the logs to White List or Black List, the Envelope-From is added to them.

Email addresses, email domains and IP addresses may be imported.

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

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

IP aggregates of both IPv4 and IPv6 types are allowed. Each IPv6 address must be represented in eight groups separated by ":"; each group must contain 4 hexadecimal digits.

It is possible to use compressed IPv6 notation, eliminating the zeroes at the right of each group.

For example:

```
2001:0DB8:0000:0000:0000:0000:1428:57ab
```

```
2001:0DB8:0000:0000:0000::1428:57ab
```

```
2001:0DB8:0:0:0:0:1428:57ab
```

```
2001:0DB8:0::0:1428:57ab
```

```
2001:0DB8::1428:57ab
```

## 2.4.2 Anti Virus

### 2.4.2.1 Domain

From here you can configure antivirus scanning on domain level for inbound and outbound traffic. The latter will be available only when your company has granted the antivirus-management for outbound email.

By default antivirus-scanning is enabled for all inbound and outbound email. Selected antivirus engines are active on either scan job. If you deselect any of the available scan engines then the antivirus will not be active on any scan job.

To enable the antivirus filter **its necessary** that outbound email gets send via the Email Protection platform (server) where you authenticate with username/password.

1. Activate antivirus filtering for outbound email.
2. Configure your SMTP to use the Email Firewall platform (server) as smarthost
3. Within the SMTP smarthost configuration make sure the SMTP session is authenticated and utilizes the same username/password that is used to connect to the administrator console

Without these settings enabled antivirus scanning for outbound emails will not be applied



Incoming email | Outgoing email

Company configuration: ClamAV (Enabled)

Domain A	ClamAV
dom1.com	Global

Save

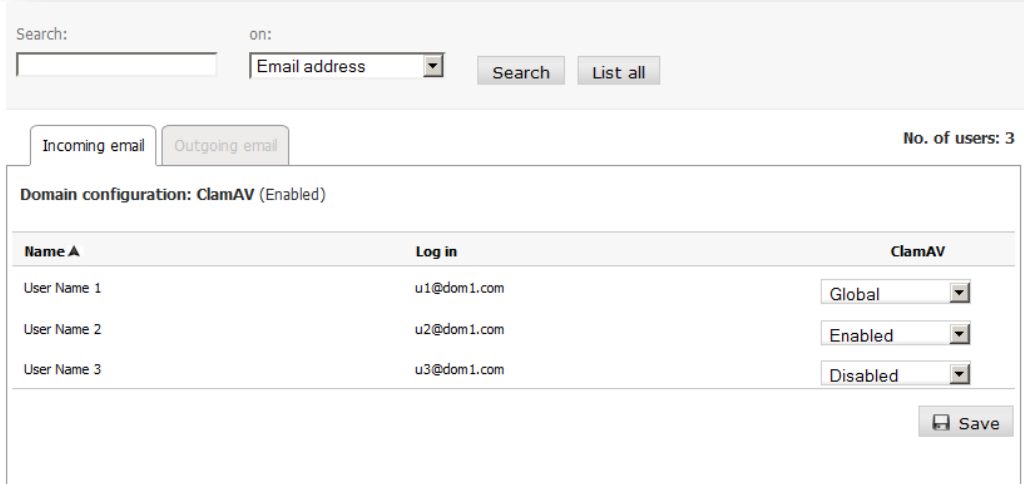
### 2.4.2.2 Users

From here you can configure antivirus scanning on user level as well as for inbound and outbound emails. The latter will be available only when your company has granted the antivirus-management for outbound email.

By default the configuration made on domain level (the domain the user belongs to) gets applied to the user (Global option). This includes the configuration made for either inbound or outbound scanning.

If a specific scan engine or scan job (inbound or outbound) is deselected, then emails will not be filtered by that scan engine!

Please be aware that even if virus-scanning is disabled for specific users this is counted as used license.



Search:  on:  Search List all

Incoming email | Outgoing email No. of users: 3

Domain configuration: ClamAV (Enabled)

Name A	Log in	ClamAV
User Name 1	u1@dom1.com	Global
User Name 2	u2@dom1.com	Enabled
User Name 3	u3@dom1.com	Disabled

Save

### 2.4.3 Anti Spam

#### 2.4.3.1 Domain

From here you can activate or deactivate spam-filtering for inbound and outbound filtering on your domain. The latter will be available only when your company has granted the spam - management for outbound email.

By default spam-filtering is activated for inbound and outbound traffic. Please be advised that the settings made on enterprise level apply to the domain!

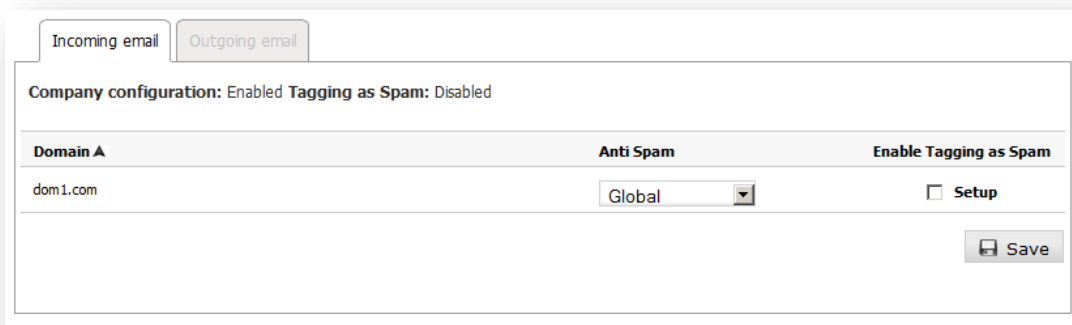
If you deselect anti-spam filtering for a certain scan job, then content filtering will be disabled but connection filtering still applies.

If an outbound email is considered as spam, it will be rejected and reported to the message sender.

To apply anti-spam scanning to outbound email its essential that mails get send via the Email Protection platform where you authenticate via username/password (same password as used to connect to the console):

1. Activate anti-spam filtering for outbound email.
2. Configure your SMTP to use the Email Protection platform (server) as smarthost
3. Within the SMTP smarthost configuration make sure the SMTP session is authenticated and utilizes the same username/password that is used to connect to the administrator console.

Without these settings enabled anti-spam scanning for outbound emails will not be applied.



The screenshot shows a configuration window with two tabs: "Incoming email" and "Outgoing email". The "Outgoing email" tab is selected. At the top, it displays "Company configuration: Enabled" and "Tagging as Spam: Disabled". Below this is a table with three columns: "Domain ▲", "Anti Spam", and "Enable Tagging as Spam". The first row shows the domain "dom1.com", a "Global" dropdown menu, and a checkbox labeled "Setup" which is currently unchecked. A "Save" button is located at the bottom right of the configuration area.

Domain ▲	Anti Spam	Enable Tagging as Spam
dom1.com	Global	<input type="checkbox"/> Setup

**Note:** The service hosts thousands of customers, like all leading email services there exists a possibility that some of our public IP's could become listed by third-party RBL (Reputation Black Lists). We have safeguards in place to prevent this however, in the unlikely event that the IP is added to an RBL, we will do everything necessary to quickly get removed from the RBL. If this happens, customers can minimize the impact to their organisation and the possibility that an outgoing email could be rejected, by temporarily configuring their MTAs to send emails directly to Internet.

Option "Enable Tagged as Spam" is available for inbound email only. If you select configuration you can specify where the tag should be placed:

- Insert the tag before the subject: To insert the specified tag at the beginning (i.e. as a prefix).
- For example, '[SPAM] Free Trip!'.
- Insert the tag after the subject: To insert the specified tag at the end (i.e. as a suffix).

For example, 'Free Trip [SPAM]'

Allowed values for spam tagging are ASCII characters only.

The setting provided by the system by default is:

- Quarantine enabled.
- Tag Spam: **[SPAM]**, **\*SPAM\***, **[Maybe SPAM]**.
- The tag will be placed before mails' subject.

"Enable Tagged as Spam" has the following impact:

1. The following "automatic messages" will not be sent to end users:
  - Welcome message.
  - Blocked mails' report.
  - Validation of mails' senders (Guaranteed filtering mode).
2. The "Tagged as Spam" is only available within the automatic filtering mode, so if any domain or user had guaranteed filtering mode is passed to Automatic. It will be impossible to select the guaranteed mode at any level (company / domain / user) when you have selected the use of tagged as spam.
3. The "quarantine" configuration applies to all emails not just to those classified as spam

#### 2.4.3.2 Users

From here you can configure the anti-spam configuration for inbound/outbound traffic on user level. The latter will be available only when your company has granted the spam -management for outbound email.

By default the configuration made on domain level applies to the end user within this domain (Global option) for inbound and outbound traffic.

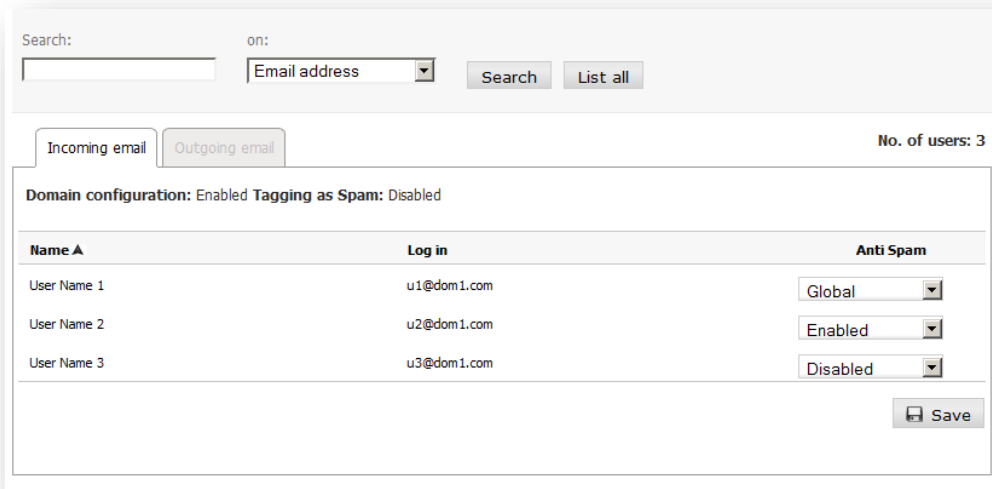
If you deselect anti-spam filtering for a certain scan job, then content filtering will be disabled but connection filtering still applies.

If outbound email is considered as spam, it will be rejected and reported to the message sender.

To apply anti-spam scanning to outbound email its essential that mails get send via the Email Protection platform where you authenticate via username/password (same password as used to connect to the console):

1. Activate anti-spam filtering for outbound email.
2. Configure your SMTP to use the Email Protection platform (server) as smarthost
3. Within the SMTP smarthost configuration make sure the SMTP session is authenticated and utilizes the same username/password that is used to connect to the administrator console.

Without these settings enabled anti-spam scanning for outbound emails will not be applied.



**Note:** The service hosts thousands of customers, like all leading email services there exists a possibility that some of our public IP's could become listed by third-party RBL (Reputation Black Lists). We have safeguards in place to prevent this however, in the unlikely event that the IP is added to an RBL, we will do everything necessary to quickly get removed from the RBL. If this happens, customers can minimize the impact to their organisation and the possibility that an outgoing email could be rejected, by temporarily configuring their MTAs to send emails directly to Internet.

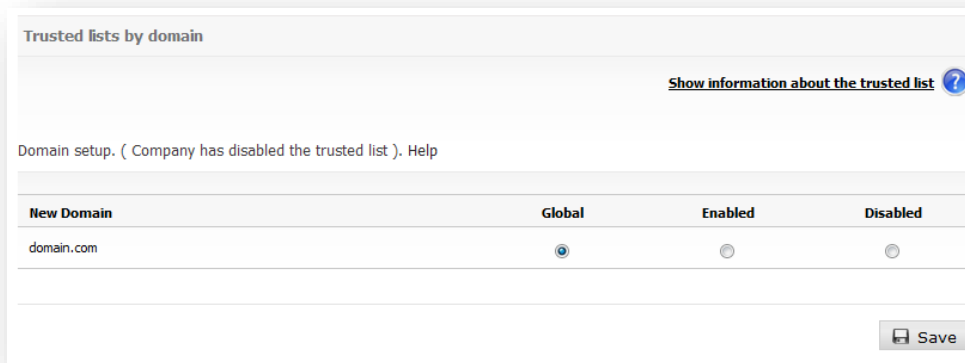
## 2.4.4 Trusted lists

### 2.4.4.1 Trusted lists by domain

Trusted lists are automatic white lists, customized for each domain. This way, filtering is not applied to emails from people with whom legitimate correspondence is maintained. This helps avoid false positives.

These lists are automatically fed with the email addresses of users that Email Protection confirms as safe.

Trusted lists for the whole service or certain domains are enabled or disabled from this panel.



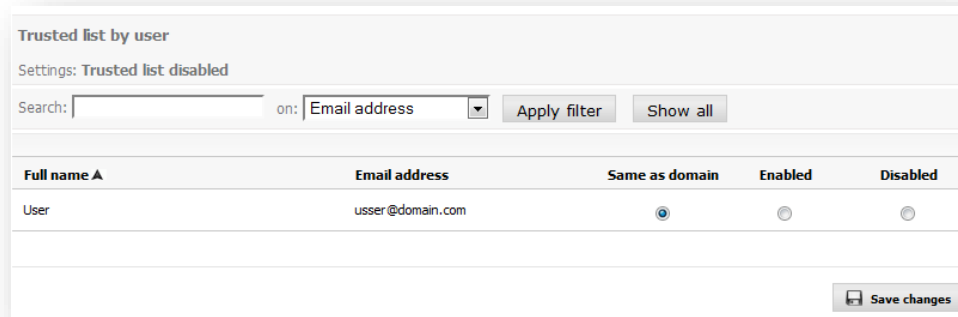
#### 2.4.4.2 Trusted list by user

Trusted lists are automatic white lists customized by users.

This way, filtering is not applied to emails from people with whom legitimate correspondence is maintained. This helps avoid false positives.

These lists are automatically fed with the email addresses of users that Email Protection confirms as safe.

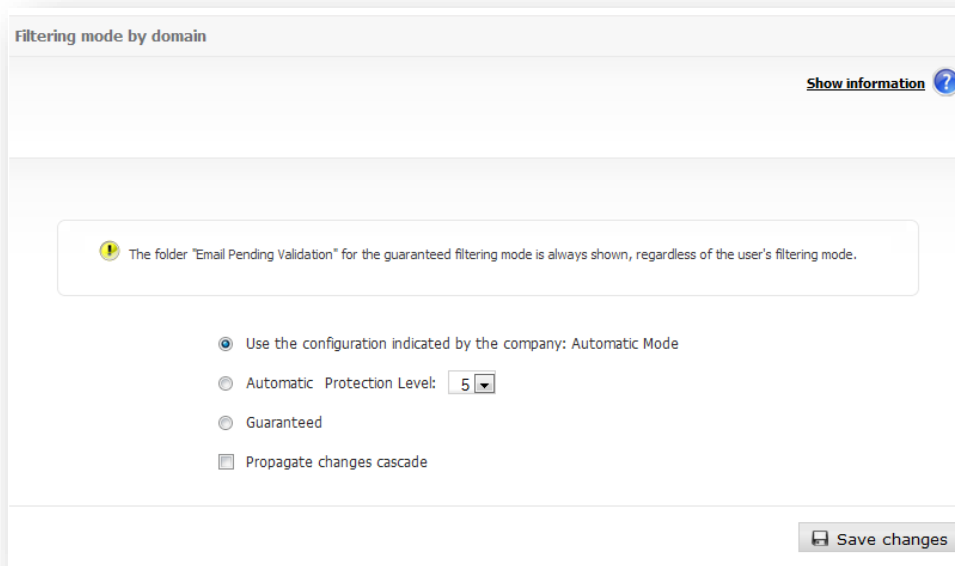
Trusted lists for individual users are enabled or disabled from this panel.



#### 2.4.5 Filtering mode

##### 2.4.5.1 Filtering mode by domain

Messages are filtered by content to determine whether a message is valid when Email Protection cannot determine whether the sender is a spammer through any of the connection filters, white lists or blacklists.



Propagate changes cascade: It will apply the configuration to every user into the domain.

In this case, Email Protection offers two filtering modes:

#### 2.4.5.1.1 Automatic mode

This analyzes and classifies the messages received as valid email or spam according to the score each email gets after being contrasted against more than 600 rules. The higher the score, the greater the probability that a message is spam.

The higher the protection level you choose, the greater the probabilities of detecting spam messages. However, some messages are detected as spam when they are not (false positives).

#### 2.4.5.1.2 Guaranteed mode

This checks and validates the source of the message, verifying whether the senders are included in the user's valid senders list (white list).

Any sender not on the recipient's white list will automatically receive a validation message. After clicking on the email validation link, the sender will be added to the recipient's white list and the email will be delivered. From then on, all messages from that sender will be automatically delivered without passing through content filters.

If the sender is not validated, recipients can do it manually from the control panel, the Notifier or the Blocked Email Report.

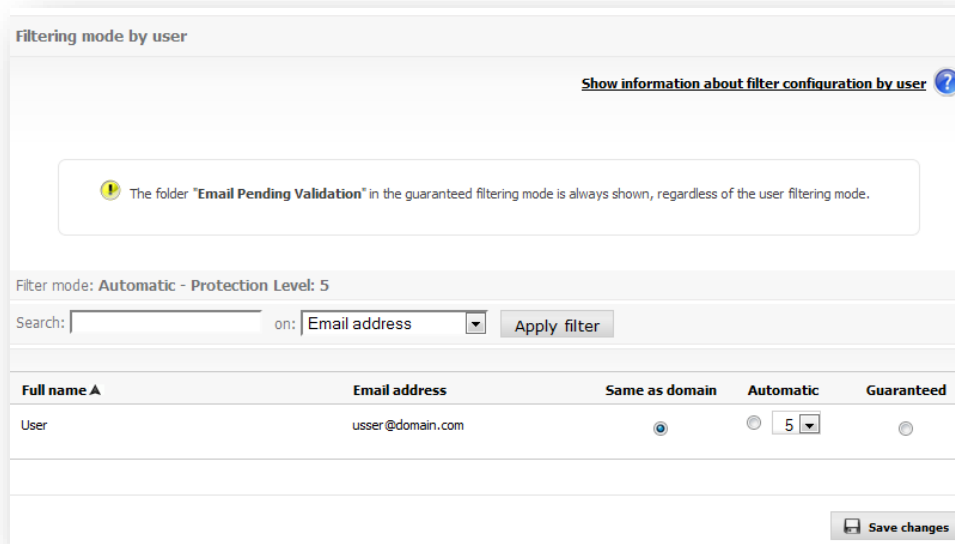
If Guaranteed filtering mode is enabled, then the Anti email spoofing filtering will be disabled at the level where it is applied (user or domain).



### 2.4.5.2 Filtering mode by user

The Email Protection filtering mode can be specified individually for each user.

Refer to the Filtering mode by domain section for further information on filtering modes.



### 2.4.6 Rules engine

#### 2.4.6.1 Incoming rules engine

The filtering rules which you define let you to manage the flow of inbound messages for system users. These rules let you:

- Eliminate files attached to an email message.
- Mark an email message as spam or valid.
- Erases the email instead of keeping it into the trash.
- Forward copy or send an email to one or more recipient.
- Do not perform any actions on email.

To create a rule:

1. Define the criteria (conditions) under which the rule will be applied.
2. Select one or more actions to be applied to the message.
3. You can choose to disable the rule when creating it; the rule will be enabled by default.
4. Finally, click "Create rules".

It is important to mention that the "Forward to" action excludes the remaining actions.

The "send copy to" action sends a copy of the original email to a specified address or to several comma-separated.

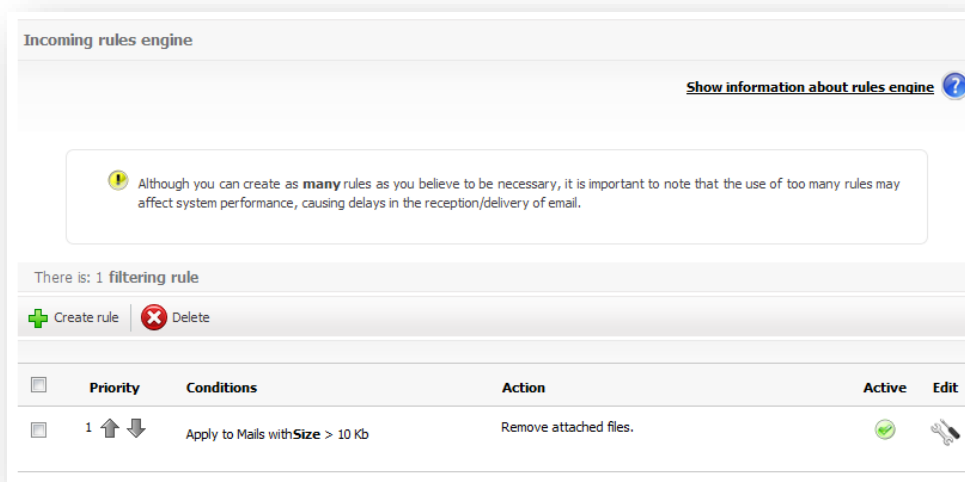
The "forward to" action can not be combined with other actions. The original email is sent to the specified address or to several comma-separated.

Note that the use of "Forward to" excludes all other actions.

If you select "Attached file Mime type", the engine will evaluate the Mime field of the attached file. For **jpg** images, you must enter **image/jpeg**. For **avi**, you must enter **video/avi**, etc.

The **Mail Size** condition refers to the total size of the mail, including attachments.

Note that the use of "delete attached files" will modify the email content; this will affect the emails which have been signed by PGP or X.509, making its digital signature non-valid. Panda shall not be liable for any legal consequences arising from these modifications.



If you select "Attached file of size"..., the values specified will be in KB, e.g. 25, means 25 KB; 25000, means 25000 KB (25MB).

The rule's conditions definition allows you to use URL search patterns into emails body.

It is important to mention that the use of **Contains credit card** allows the recognition of the following credit card formats:

**Visa:** XXXX XXXX XXXX XXXX

**MasterCard:** XXXX XXXX XXXX XXXX

**Maestro:** XXXX XXXX XXXX XXXX

**American Express:** XXXX XXXXXX XXXXX

**Diners:** XXXX XXXXXX XXXX

Although you can create as many rules as necessary, bear in mind that the use of too many rules might impact system performance, delaying email reception/delivery.

Conditions may be defined for attachments that are also evaluated for the content of these files. In compressed files that include other compressed files, the evaluation of the rule will be performed up to the fourth level of compression. Searches in compressed files can be activated when the condition involves the following operators:

- All or part of the name
- Size >
- Size <=

The operator "Contains common expression" can be used for the following fields:

- Subject
- Body

PERL-type common expressions are those supported. For further information on this type of expressions, you may check the following official reference: [http://en.wikipedia.org/wiki/Regular\\_expression#Perl-derived\\_regular\\_expressions](http://en.wikipedia.org/wiki/Regular_expression#Perl-derived_regular_expressions)

#### 2.4.6.2 Outgoing rules engine

The filtering rules that you define allow you to manage the flow of outgoing messages from system users. Using these rules, you can:

- Eliminate files attached to an email message.
- Reject by company policy.
- Accept as valid.
- Erases the email instead of keeping it into the trash.
- Forward copy or send an email to one or more recipient.
- Do not perform any actions on email.

To create a rule:

1. Define the criteria (conditions) under which the rule will be applied.
2. Select one or more actions to be applied to the message.
3. You can choose to disable the rule when creating it; the rule will be enabled by default.
4. Finally, click "Create rules".

It is important to mention that the "Forward to" action excludes the remaining actions.

The "send copy to" action sends a copy of the original email to a specified address or to several comma-separated.

The "forward to" action cannot be combined with other actions. The original email is sent to the specified address or to several comma-separated.

Note that the use of "Forward to" excludes all other actions.

If you select "Attached file Mime type", the engine will evaluate the Mime field of the attached file. For **jpg** images, you must enter **image/jpeg**. For **avi**, you must enter **video/avi**, etc.

The **Mail Size** condition refers to the total size of the mail, including attachments.

Note that the use of "*delete attached files*" will modify the email content; this will affect the emails which have been signed by PGP or X.509, making its digital signature non-valid. Panda shall not be liable for any legal consequences arising from these modifications



If you select "*Attached file of size*"..., the values specified will be in KB, e.g. 25, means 25 KB; 25000, means 25000 KB (25MB).

The rule's conditions definition allows you to use URL search patterns into emails body.

It is important to mention that the use of **Contains credit card** allows the recognition of the following credit card formats:

**Visa:** XXXX XXXX XXXX XXXX

**MasterCard:** XXXX XXXX XXXX XXXX

**Maestro:** XXXX XXXX XXXX XXXX

**American Express:** XXXX XXXXXX XXXXX

**Diners:** XXXX XXXXXX XXXX

Although you can create as many rules as necessary, bear in mind that the use of too many rules might impact system performance, delaying email reception/delivery.

Conditions may be defined for attachments that are also evaluated for the content of these files. In compressed files that include other compressed files, the evaluation of the rule will be performed up to the fourth level of compression. Searches in compressed files can be activated when the condition involves the following operators:

- All or part of the name
- Size >
- Size <=

The operator "Contains common expression" can be used for the following fields:

- Subject
- Body

PERL-type common expressions are those supported. For further information on this type of expressions, you may check the following official reference: [http://en.wikipedia.org/wiki/Regular\\_expression#Perl-derived\\_regular\\_expressions](http://en.wikipedia.org/wiki/Regular_expression#Perl-derived_regular_expressions)

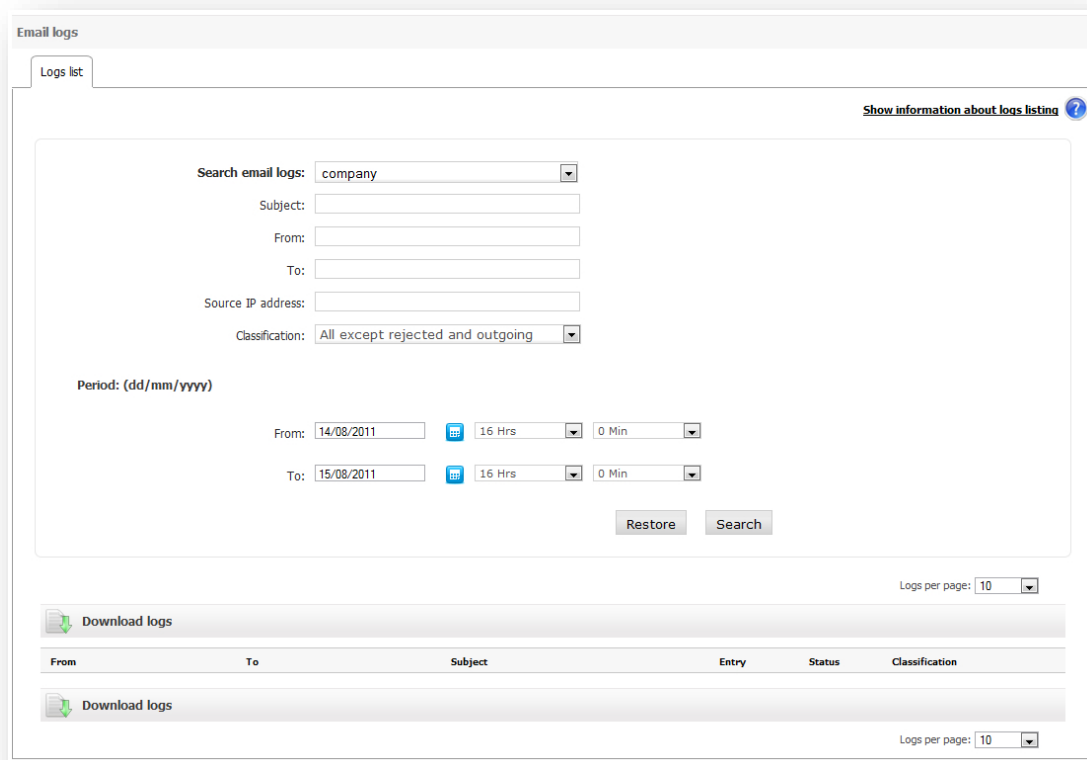
#### 2.4.7 Email logs

The Email logs list lets you see basic details regarding the emails that pass through Email Protection. You can also change the configuration, if this option was selected when buying Email Protection.

Emails can be filtered using any of the fields provided for this purpose or a combination of them.

The classification selection list lets you filter logs by the following categories:

- All except rejected and outbound
- Server warnings
- Virus warnings
- Infected email
- Mailing lists
- Pending validation
- Spam
- Valid
- Valid outbound email
- Rejected outbound email
- Rejected incoming email



The screenshot shows the 'Email logs' interface. At the top, there is a 'Logs list' tab and a link to 'Show information about logs listing'. The main area contains search filters: 'Search email logs' (set to 'company'), 'Subject', 'From', 'To', 'Source IP address', and 'Classification' (set to 'All except rejected and outgoing'). Below these are date and time filters for 'From' (14/08/2011, 16 Hrs, 0 Min) and 'To' (15/08/2011, 16 Hrs, 0 Min). There are 'Restore' and 'Search' buttons. At the bottom, there are 'Download logs' buttons and a 'Logs per page' dropdown set to 10. A table header is visible with columns: From, To, Subject, Entry, Status, and Classification.

Possible statuses<sup>4</sup> for an email are:

- Delivered: The email has been delivered to the recipient.
- Pending: The email is still waiting to be sent, or another delivery attempt is pending due to some kind of recipient error.
- Error: There has been an error in the email delivery. You can see the reason by clicking "More details".
- Temporary error: Some error has occurred in the email delivery; the cause may be seen by clicking on "More details".
- On hold: All emails classified as spam or which, due to user's settings, must not be delivered (virus warnings, server notifications and email lists).
- Processing: the email status has not been determined yet. Wait until the next email logs refresh for the correct email status.
- Deleted: This category is assigned to those messages that has been classified as Viruses and then deleted
- Quarantine: This category is assigned to those messages that has been classified as Viruses and then sent to quarantine.

---

<sup>4</sup> The email logs list shows the current status of any specific email. This means that all previous statuses of an email are not shown (for this reason, an email will only appear once in the log list)

If any changes are made that affect the classification of an email (e.g. moving spam to Valid email, or vice versa), the classification column will also show an icon (🔄) which reflects this situation.

An email may be classified as one of the following values:

- Valid
- Email list
- Server warning
- Spam
- Pending validation
- Virus warning
- Email with virus
- Valid outgoing
- Deleted
- Rejected spam

These classifications are generated by one of the following system components:

- Antispoofing
- Anti-virus system
- Black list
- Email list condition
- Bayesian classifier
- Anti-spam disabled as user with basic filtering
- Email condition pending validation
- Server warning condition
- Auto-generated email
- Rule engine
- RBLw: The sender's IP is in a DNSBL
- RPDS (Recurrent pattern detection system)
- Heuristic classifier
- No filter classifies it and it is valid because nobody says otherwise
- SPFw: The email has been sent from an IP not authorized for this purpose by the administrators of the sending domain
- Trusted list
- Number of recipients exceeded: The number of email recipients exceeds the maximum permitted
- Fixed routing: There are platform policies that have forced this classification

You can also download a file with the logs resulting from a query, or simply, from the default list. This file format is Microsoft® Excel® compatible.

For each email log, depending on its classification and state, the following actions could be available:

- Send origin domain to white list: Emails coming from domains that belongs to this list will be passed through connection and antivirus filters, but none of the content filters.
- Send origin domain to black list: Emails coming from domains that belongs to this list will be sent to the quarantine after pass through connection filters.
- Send sender to white list: Emails coming from senders that belongs to this list will be passed through connection and antivirus filters, but none of the content filters.
- Send sender to black list: Emails coming from senders that belongs to this list will be sent to the quarantine after pass through connection filters.
- Send to valid email: Moves the email from the original folder to valid email folder.
- Send to Spam email: Moves a valid email to the spam folder.
- View email: This option will be available only when the "View email from panel logs" option were chosen at hiring time. It allows viewing the email.
- Resend: Resend the email.

### Mass actions of Email Logs:

Mass actions allow carrying out different operations on a group of email logs simultaneously. As the process may take several minutes, the result of each operation is notified via email to the contact email that has been configured previously.

The actions requested will only have an effect on the logs selected in the current page of search results.

Not all the actions are applicable to all types of emails:

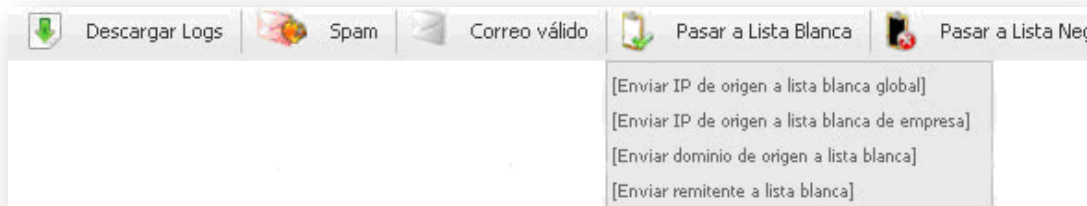
- Re-deliver: only valid emails may be re-delivered.
- Transfer to a White List / Transfer to a Black List: domains, IPs or senders may be included. In order to avoid redundancies in the lists of senders and domains, a sender cannot be added if the domain already exists in the same list. For this reason, when adding a domain to a list, all the email addresses from that domain will be removed from the list.

### Transfer to a White List





## Transfer to a Black List



### 2.4.8 NDR Validation

This validation can be configured from the company administrator panel, at domain level and at user level. These options are found in the "Filtering" tab in the sections "NDR Validation by domain" and "NDR validation by user" respectively.

NDR validation implies that a digital signature (SRS) will be added to all messages sent through our server. This signature is then verified if the message is rejected by the recipient's SMTP server. If this signature is validated, the rest of the filters are applied to the message, but if the signature does not match, the message will automatically be rejected.

Enabling NDR validation for a company, domain or user implies:

- 1 If an email comes with valid SRS encoding, then filtering is applied.
- 2 If an email comes with invalid SRS encoding, it is rejected.
- 3 If an email comes without SRS encoding, it is rejected.

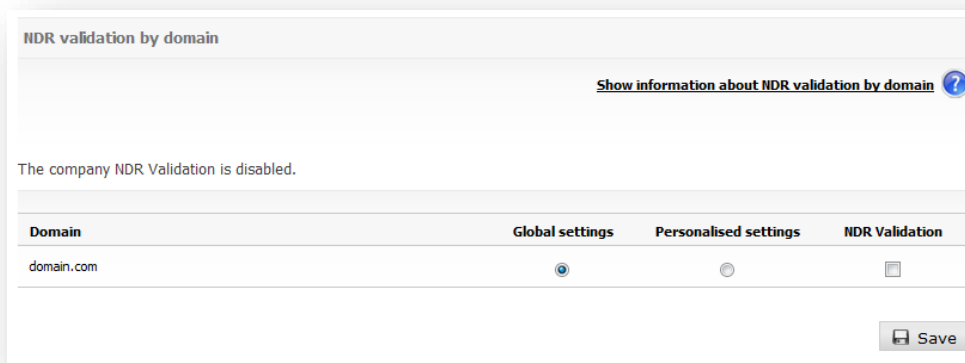
#### 2.4.8.1 NDR validation by domain

Management of NDR validation by domain lets you configure settings for all domains globally or for each domain individually.

This kind of validation is disabled by default, not only for the company but for each domain within it. In order to set it, at company and domain level, select "Own Settings", then click "NDR Validation". If this option is not selected, validation will remain disabled.

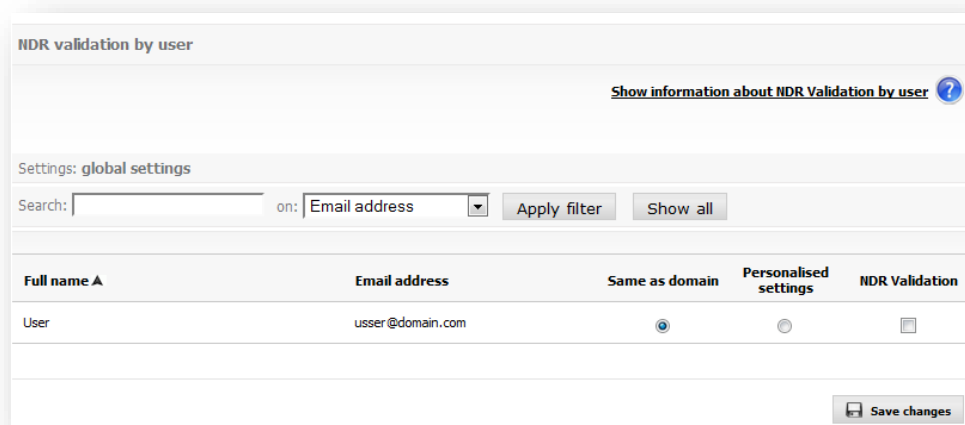
- **NDR Validation:** enabling this validation implies that Email Protection will verify the existence and validity of all digital signatures on rejected inbound emails (the signature that has been added when an authenticated email is sent). This validation prevents spam in the form of spoof non-delivery notices.

Messages which are not sent through Email Protection will not receive notifications from the server or automatic replies if the NDR validation is enabled.



### 2.4.8.2 NDR validation by user

Management of NDR validation by user allows each user to enable the NDR Validation. This validation implies that Email Protection will verify the existence and validity of all digital signatures on rejected inbound emails (the signature that has been added when an authenticated email is sent). This validation prevents spam in the form of spoof non-delivery notices.



The NDR validation configuration for each user is, by default, the same as the domain settings.

Messages which are not sent through Email Protection will not receive notifications from the server or automatic replies if the NDR validation is enabled.

### 2.4.9 Anti email spoofing

This configuration can be configured from the domain administrator panel, at domain level and at user level. These options are found in the "Filtering" tab in the sections "Anti email spoofing by domain" and "Anti email spoofing by user" respectively.

If Guaranteed filtering mode is enabled, then the Anti email spoofing filtering will be disabled at the level where it is applied (user or domain).

IP aggregates of both IPv4 and IPv6 types are allowed. Each IPv6 address must be represented in eight groups separated by ":"; each group must contain 4 hexadecimal digits.

It is possible to use compressed IPv6 notation, eliminating the zeroes at the right of each group.

For example:

2001:0DB8:0000:0000:0000:0000:1428:57ab

2001:0DB8:0000:0000:0000::1428:57ab

2001:0DB8:0:0:0:0:1428:57ab

2001:0DB8:0::0:1428:57ab

2001:0DB8::1428:57ab

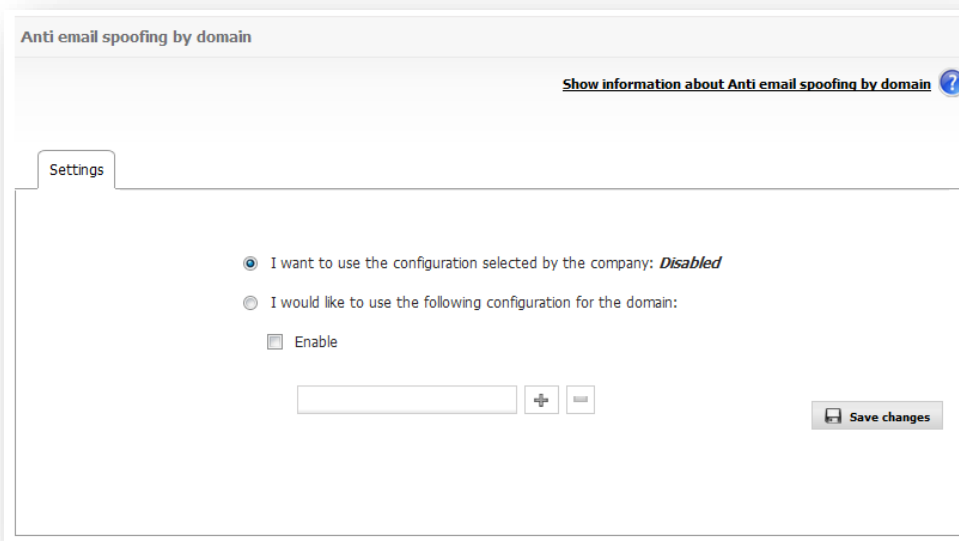
#### 2.4.9.1 Anti email spoofing by domain

This filter is disabled by default settings.

- **Anti email spoofing by domain:** It will check if sender is who he or she claims to be, when the accounts of the sender and receiver of the email are firewall protected and they belong to the same domain. If this filter is enabled, it will not be necessary to add the owned domain to the black list as a preventive spam practice. This kind of practice aims at preventing receiving spam when the sender has supplanted his or her identity with a protected account.

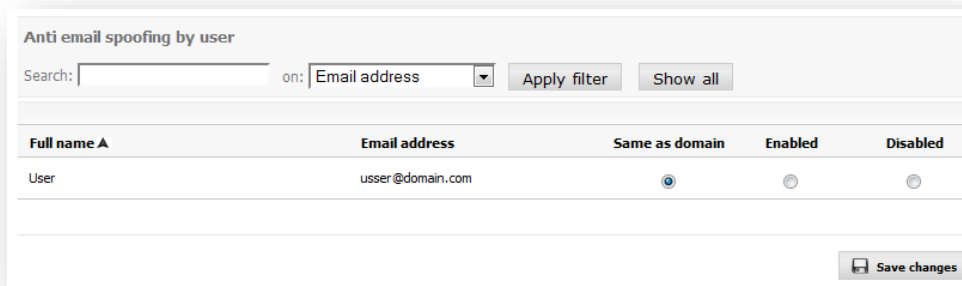
If the test is disabled, or if you want to use the configuration shown by the company for a domain, you will not be able to define the lists of IP addresses authorized to send.

IP addresses included in the **IP addresses list enabled for the email sending** list will not be passed through this filter. If the test is disabled, or if you want to use the configuration shown by the company for a domain, you will not be able to define the **lists of IP addresses authorized to send**.



### 2.4.9.2 Anti email spoofing by user

The anti email spoofing by user will allow you to define, for each user, if you want to activate the anti email spoofing by user. If you enable this feature by user, the filters will be applied TO those emails having a protected account as a sender



## 2.5 Personalization

In this section you can configure:

- Issues that refer to automatic messages: "Welcome message" and "Blocked Email Report".
- Company and domain logo.
- Company and domain administration panel language.

### 2.5.1 Automatic messages

Email Protection can automatically send three kinds of messages to users:

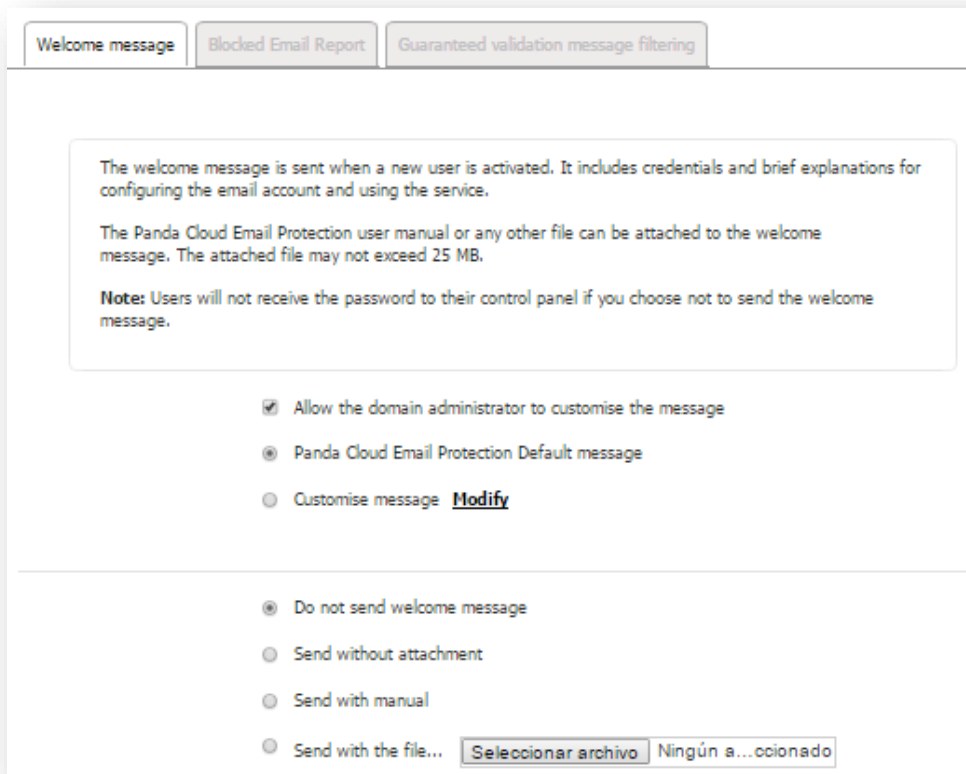
### 2.5.1.1 Welcome message

This is sent only once to each new user of the service. This message explains how to set up email addresses and get the most out of service.

Email Protection User Guide (or any other file) can be attached to the welcome message.

You can customize the welcome message or send the default version. You can customize the welcome message by clicking “*Modify*”.

**Important:** If you decide not to send the welcome message and you are using automatic creation of users, they will not receive the password to access the control panel.



The screenshot shows a configuration interface for the 'Welcome message'. At the top, there are three tabs: 'Welcome message' (selected), 'Blocked Email Report', and 'Guaranteed validation message filtering'. Below the tabs, there is a text box containing the following information:

The welcome message is sent when a new user is activated. It includes credentials and brief explanations for configuring the email account and using the service.

The Panda Cloud Email Protection user manual or any other file can be attached to the welcome message. The attached file may not exceed 25 MB.

**Note:** Users will not receive the password to their control panel if you choose not to send the welcome message.

Below the text box, there are several radio button options:

- Allow the domain administrator to customise the message
- Panda Cloud Email Protection Default message
- Customise message [Modify](#)

At the bottom, there are more radio button options:

- Do not send welcome message
- Send without attachment
- Send with manual
- Send with the file...

#### 2.5.1.1.1 Modify message

You will see a screen with the default text message and subject. Here you can customize the content and subject of the message for the company or for each domain. The default message will be the one that is currently used in Email Protection distributions. Before saving the message you can preview it by clicking “*Preview*”.

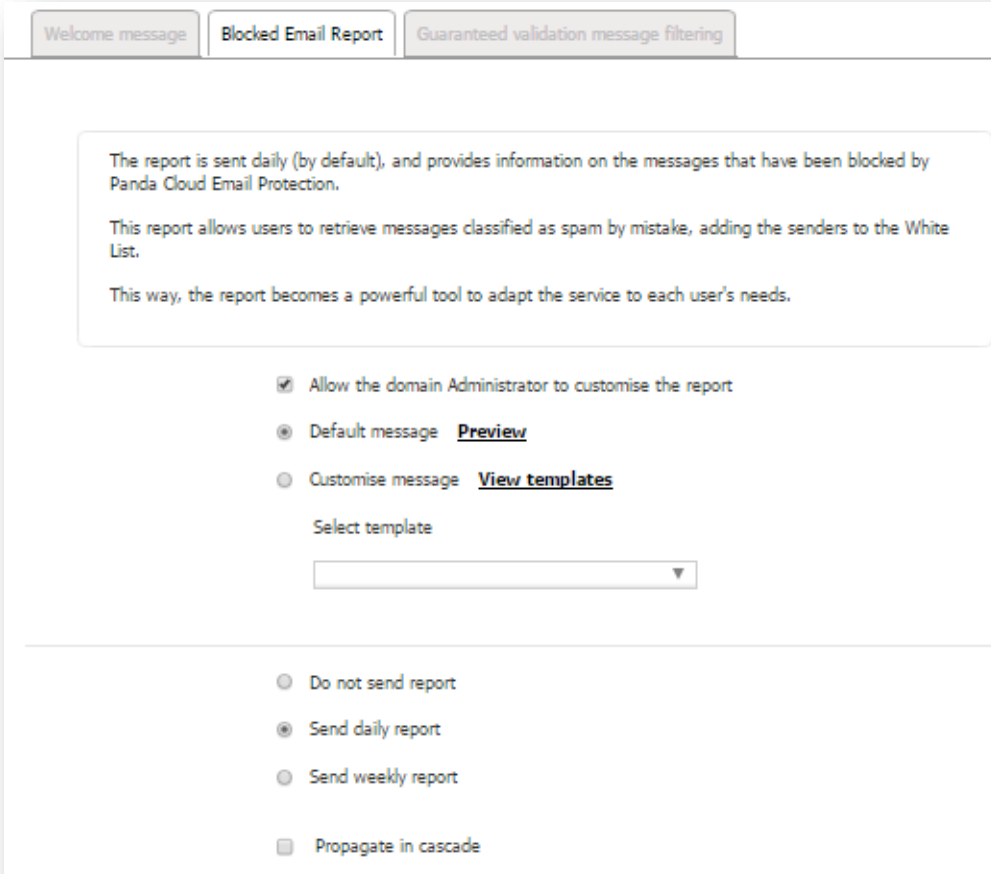
### 2.5.1.2 Blocked email report

This details messages which have been blocked by Email Protection. It also lets you recover email classified as spam and add senders to the white list. You can choose not to send this message or how often you want it to be sent: daily or weekly.

You can choose to send the default Email Protection report or customize the message using a series of templates.

Templates can be requested by clicking the “*See templates*” link. Templates can be selected from a drop-down menu.

**Important:** The customization option must be enabled by the company administrator.



The screenshot shows a configuration window for Email Protection. At the top, there are three tabs: "Welcome message", "Blocked Email Report" (which is active), and "Guaranteed validation message filtering". Below the tabs, there is a text box containing the following information:

The report is sent daily (by default), and provides information on the messages that have been blocked by Panda Cloud Email Protection.

This report allows users to retrieve messages classified as spam by mistake, adding the senders to the White List.

This way, the report becomes a powerful tool to adapt the service to each user's needs.

Below the text box, there are several options:

- Allow the domain Administrator to customise the report
- Default message [Preview](#)
- Customise message [View templates](#)

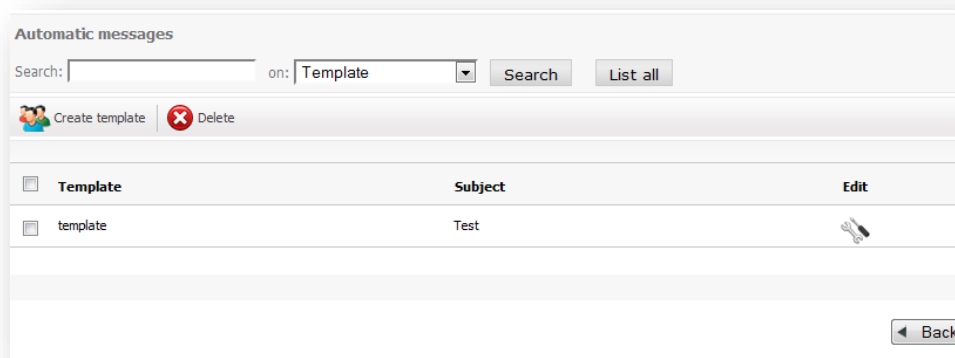
Under the "Customise message" option, there is a "Select template" label and a dropdown menu.

At the bottom of the configuration window, there are four radio button options:

- Do not send report
- Send daily report
- Send weekly report
- Propagate in cascade

**Propagate in cascade:** apply configuration all users.

2.5.1.2.1 See templates



A new screen appears with the following options:

- **Create template:** This creates a new message based on Email Protection's default message. To create a message you must define the message content and subject. You can also set the name and email address of the message sender. The company's contact email address appears by default and you can select the contents you want to appear in the report and those you want to remove.
- You can preview the message before it is saved.
- **Delete:** This deletes the message, subject, sender, and the template. The relationship is 1 to 1 and all the fields are mandatory.
- **Search form:** You can search a template by the template's name and subject.

Automatic messages  
Here you can set up different data for the domain: **domain.com**

Information for sending the report:

(\*) Template Name:

(\*) Sender Name:

(\*) Sender email address:

(\*) Subject:

Through the following form you can edit the content of the templates you have saved or create new ones.  
By modifying or creating a template, you can select the content you want to appear in the report and that which you want to remove.

Message content:

Cuenta protegida: **user@example.com**

Método de filtro para su cuenta en Spam: **XXXXX**

Correos electrónicos bloqueados: **XXXXX**

Correos electrónicos bloqueados: **YYYYYY (spam) / ZZZZZZZZZ (pending validation)**

Le mostramos a continuación el listado de los correos electrónicos que su Firewall de correo ha determinado que no son válidos. Si le interesa alguno de ellos por favor escoja la opción que crea más conveniente para recuperarlos.

\* Opción recuperar: recupera el correo y se lo entrega como válido.

\* Opción recuperar = lista blanca: recupera todos los correos provenientes del remitente indicado que hayan sido bloqueados; además agrega el remitente a su lista blanca para que, en el futuro, los correos provenientes de ese remitente no sean bloqueados.

Correos electrónicos bloqueados

Remitente	Tema	Recuperar	Recuperar + ( )
from@example.com	subject	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Correos electrónicos pendientes de validar

Remitente	Tema	Recuperar	Recuperar + ( )
from@example.com	subject	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Recuerde que, cuando lo desea, puede modificar todos sus datos y configuraciones accediendo, desde su panel de control, a la pestaña Configuración. Para cualquier duda, consulte o sugerencia puede ponerse en contacto con su administrador.

(\*) Mandatory fields

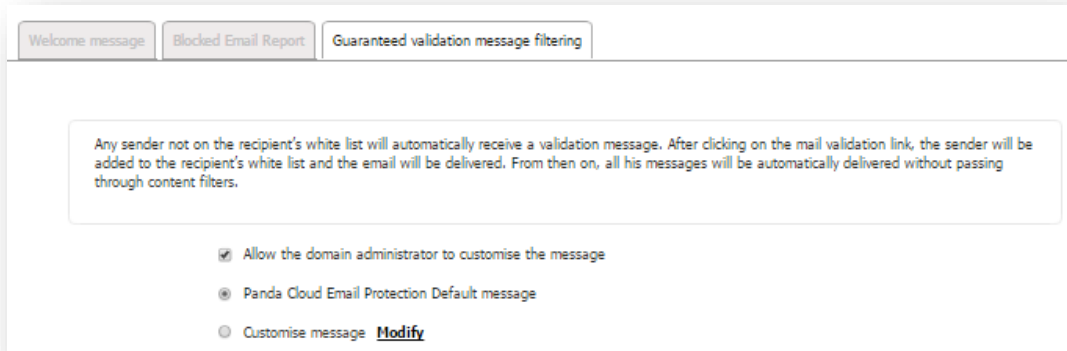
### 2.5.1.3 Guaranteed filtering validation message

Any sender that is not on the white list of the recipient will receive automatically a validation message. After a simple click a link in the validation email, the sender is added to the recipient's



white list and his/her email will be delivered. From that point on, all messages will be delivered automatically without going through the content filters.

You can choose to customize the validation message via the "Custom Message" option; otherwise a default message will be used.



Welcome message | Blocked Email Report | **Guaranteed validation message filtering**

Any sender not on the recipient's white list will automatically receive a validation message. After clicking on the mail validation link, the sender will be added to the recipient's white list and the email will be delivered. From then on, all his messages will be automatically delivered without passing through content filters.

Allow the domain administrator to customise the message

Panda Cloud Email Protection Default message

Customise message [Modify](#)

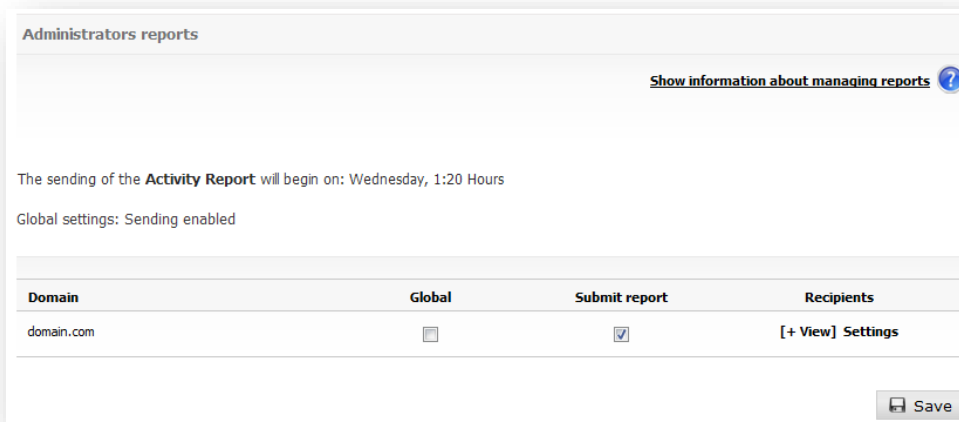
## 2.5.2 Reports of administrators

The management of Management Reports allows you to enable/disable the sending of an activity report and set the recipients.

The management report contains information about your:

- Email Domain.
- Email accounts.
- Email traffic.
- Messages.
- Filter mode.

By default the sending the activity report will be enabled to the domain.



**Administrators reports**

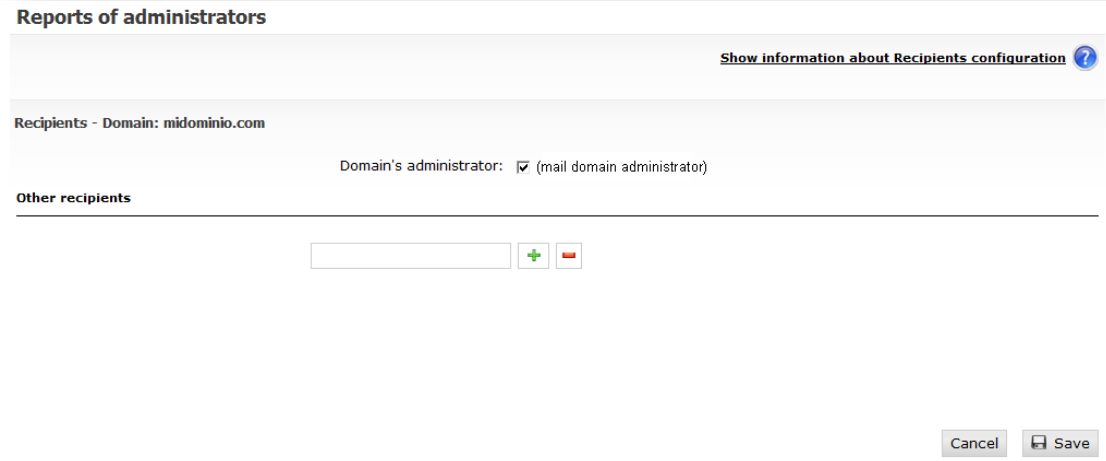
[Show information about managing reports](#) ?

The sending of the **Activity Report** will begin on: Wednesday, 1:20 Hours

Global settings: Sending enabled

Domain	Global	Submit report	Recipients
domain.com	<input type="checkbox"/>	<input checked="" type="checkbox"/>	[+ View] Settings

The target settings allow you to define the recipients of the report.



**Reports of administrators**

[Show information about Recipients configuration](#) ?

Recipients - Domain: midominio.com

Domain's administrator:  (mail domain administrator)

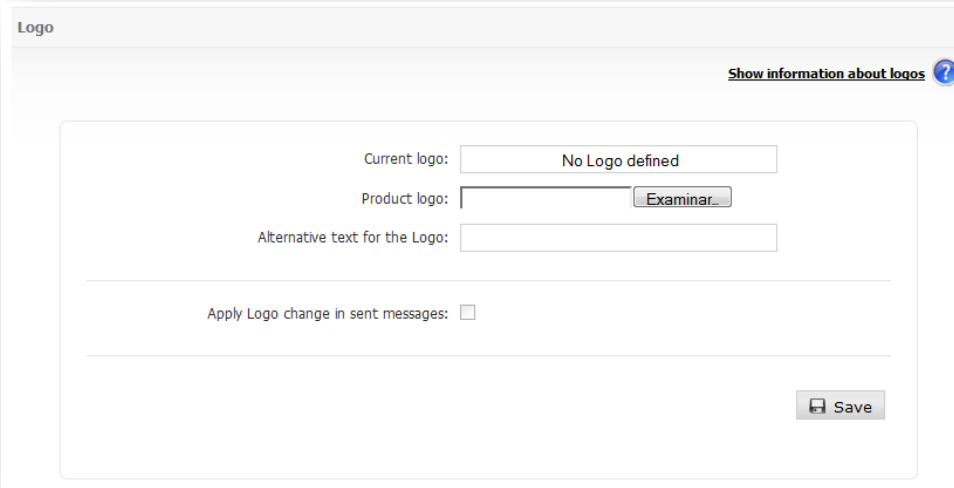
**Other recipients**

It can add up to 10 recipients, and also select (to send report) to domain administrator.

### 2.5.3 Logo

This option lets you select the logo to appear in sent messages.

When selecting the setup of a domain, the logo will be automatically set up. It will be placed in the sent message upper right corner.



**Logo**

[Show information about logos](#) ?

Current logo:

Product logo:

Alternative text for the Logo:

---

Apply Logo change in sent messages:

---

The file can be in any of the following graphic formats: PNG, GIF or JPG. There are no restrictions on the size of the original file, however, it is advisable that the logo is transparent ( PNG) and its format is rectangular, otherwise it will be adapted automatically to be used by the system.

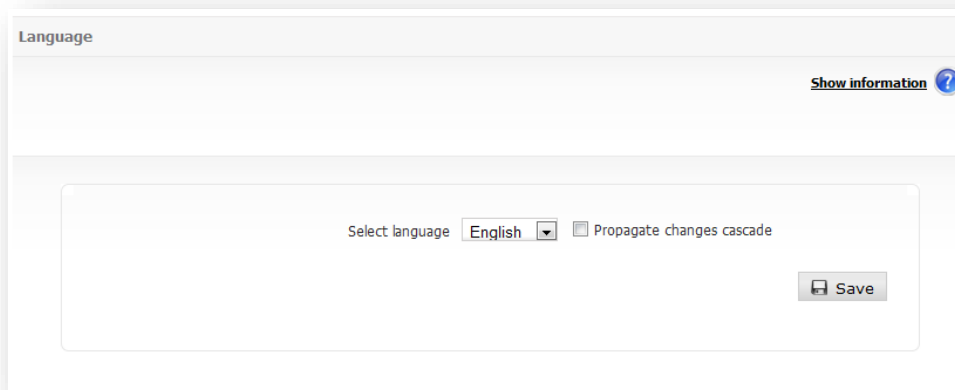


In addition to deleting the current logo, you can enter an alternative text for it.

You can apply the new logos to the sent messages by choosing “Apply logo change in sent messages”.

#### 2.5.4 Language

Here you can choose the language that will be used both for the administration panel and the automatic messages. This option is available in the “Settings” tab, in the “Language” section.



In the domain creation process (from the company administration panel) you can select the domain language from a list (the default value is the company language). Alias domains will inherit, by default, the corresponding main domain language.

Propagate changes cascade: It will apply the configuration to every domain and user into the company.

Both the user creation and the user edit processes allow you to assign a language to the user.

## 2.6 Settings


In this section you can configure system features such as the administrator details, what to do when certain messages in the classification list/server messages/virus warnings are sent or the frequency with which Email Protection can launch messages automatically, etc.

## 2.6.1 Administrator data

This is where information about the administrator must be entered.

You can change the username, password as well as the number of messages per page which will be displayed in the different panels.

### Administrator Data

[Show information](#) 

**Personal Information** | Change Password | Messages per page

\* First name and surname:

Phone number:

Address:

City:

Country:

(\*) Mandatory fields

### Administrator data

**Personal Information** | **Change Password** | Messages per page

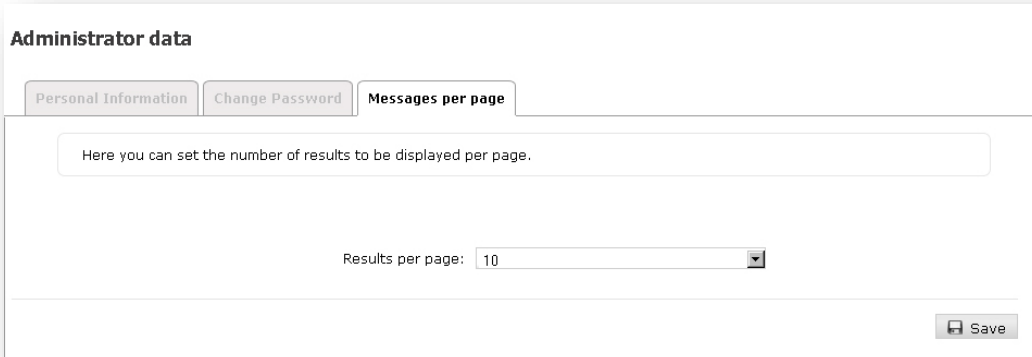
(\*) Username:  [Help](#)

(\*) Old Password:  [Help](#)

(\*) Password:  [Help](#)

(\*) Confirm Password:

(\*) Mandatory fields



**Administrator data**

Personal Information Change Password **Messages per page**

Here you can set the number of results to be displayed per page.

Results per page: 10

Save

## 2.6.2 Access to users panel

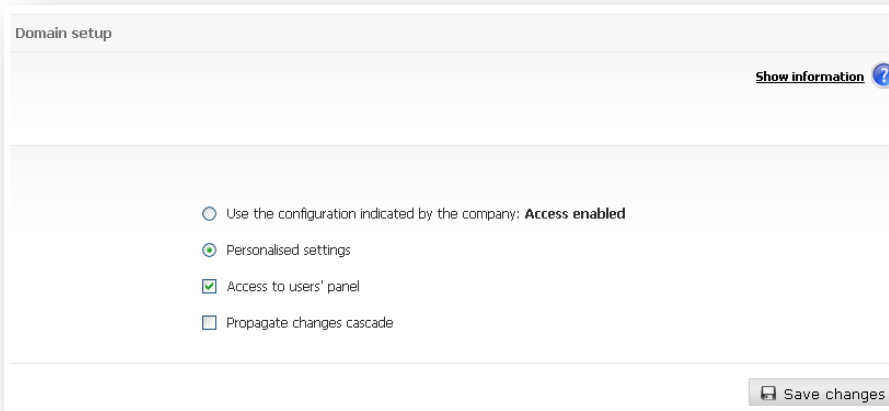
It is possible to determine whether a group of end users can or cannot access the panel. Those users for whom access to the panel was disabled will receive a notice of this situation any time they try to access.

### 2.6.2.1 Settings by domain

Allows configuring access to panels of end users for the domain.

The configuration options available are:

- Global: The configuration defined by the higher level is used: company for the case of the domain and email firewall for the case of the company.
- Own: Allows a configuration other than that specified by the higher level to be applied.
- Access to panel for end users: Indicates that domain users will be allowed access to their user panels.
- Propagate in cascade: Applies the configuration to all users of the domain.



Domain setup

Show information ?

Use the configuration indicated by the company: **Access enabled**

Personalised settings

Access to users' panel

Propagate changes cascade

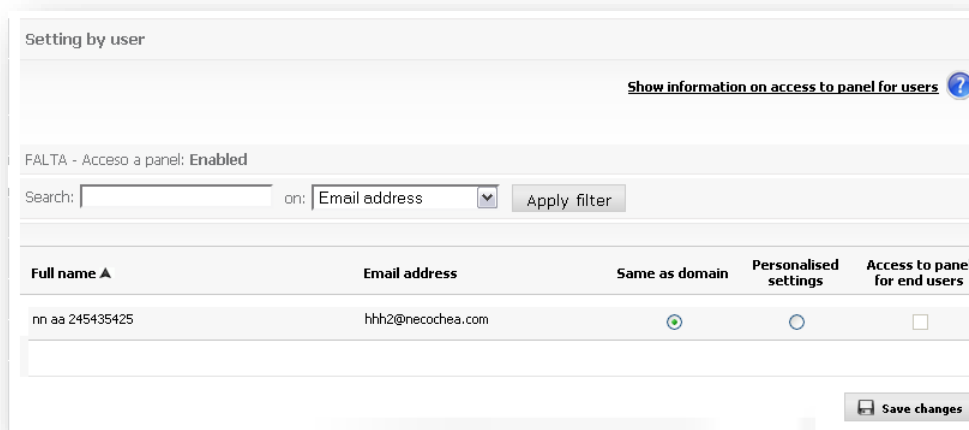
Save changes

### 2.6.2.2 Settings by user

Allows configuration of the access to panels for end users.

For each of the users belonging to the domain selected, the available configuration options are:

- According to domain: The configuration defined for the domain is used.
- Own: Allows a configuration other than that specified by the domain to be applied.
- Access to panel for end users: Indicates if the user will have access permitted to their user panel.



### 2.6.3 Lists and notices

There are certain types of emails which are of no use to most users (although they may be of considerable use to others) or which are often used by spammers as a technique for reaching end-users.

Special menus have been created to decide what to do with email lists, server notices and virus warnings.

You can decide -for the whole service or for specific domains- whether such emails will be delivered to the end-user, or if they will be saved in separate folders for consultation when required.

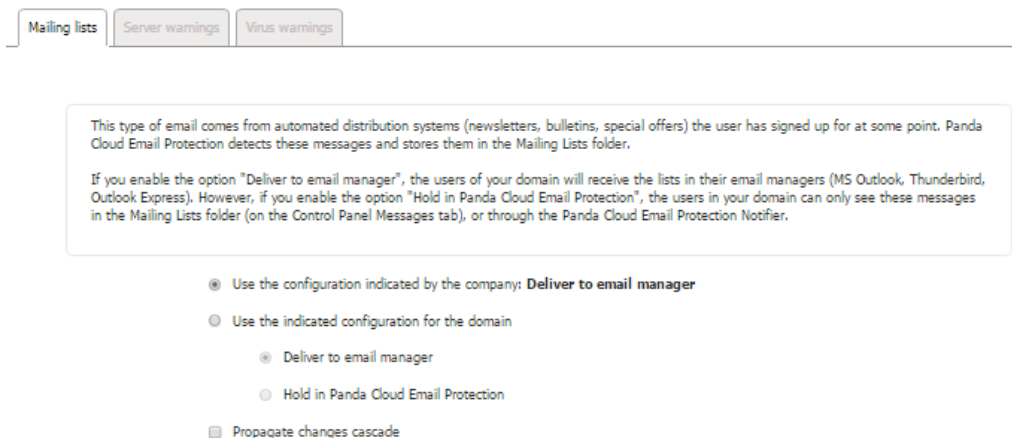
#### 2.6.3.1 Mailing lists

This type of email comes from automated distribution systems (newsletters, bulletins, special offers) the user has signed up to at some point. Email Protection 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, etc). However, if you enable

the option “Hold”, the users in your domain will only see these messages in the Mailing Lists folder - in the Control Panel Messages Tab-, or through the Email Protection Notifier.

Propagate changes cascade: It will apply the configuration to every domain and user into the company.



Mailing lists Server warnings Virus warnings

This type of email comes from automated distribution systems (newsletters, bulletins, special offers) the user has signed up for at some point. Panda Cloud Email Protection 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). However, if you enable the option "Hold in Panda Cloud Email Protection", the users in your domain can only see these messages in the Mailing Lists folder (on the Control Panel Messages tab), or through the Panda Cloud Email Protection Notifier.

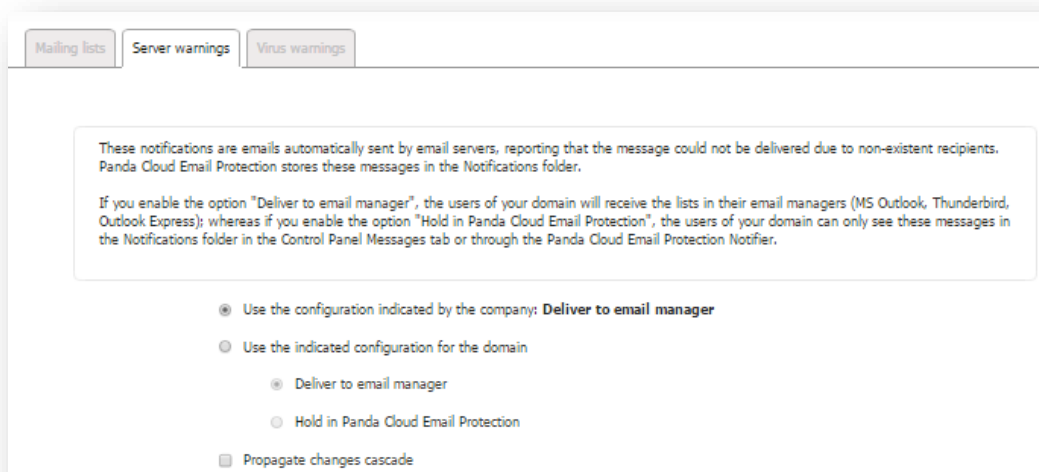
- Use the configuration indicated by the company: **Deliver to email manager**
- Use the indicated configuration for the domain
  - Deliver to email manager
  - Hold in Panda Cloud Email Protection
- Propagate changes cascade

### 2.6.3.2 Server warnings

These messages are notifications sent automatically by email servers. They inform of messages that could not be delivered, or messages addressed to non-existing recipients. Email Protection 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, etc). However, if you enable the option “Hold”, the users in your domain will only see these messages in the Notifications folder -in the Control Panel Messages Tab-, or through the Email Protection Notifier.

Propagate changes cascade: It will apply the configuration to every domain and user into the company.



### 2.6.3.3 Virus warnings

These emails are notifications sent by Email Protection, reporting the presence of viruses in an email received in your account. Email Protection 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, etc). However, if you enable the option "Hold", the users in your domain will only see these messages in the Virus warnings folder -in the Control Panel Messages Tab-, or through the Email Protection Notifier.

Propagate changes cascade: It will apply the configuration to every domain and user into the company.

You can choose to customize the virus warning message from the "Custom Message" option; otherwise a default message will be used.



Mailing lists
Server warnings
Virus warnings

These are notifications sent by Panda Cloud Email Protection reporting the presence of a virus in an email received in your account. Panda Cloud Email Protection 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 Panda Cloud Email Protection", the users of your domain can only see these messages in the Virus Warnings folder in the Control Panel Messages tab or through the Panda Cloud Email Protection Notifier.

**Note:** The cascade configuration shall be applied only to Send/Retain message.

**Define message**

- I would like to use the configuration specified by the company (**Global**): **Default message**
- I would like to use the following configuration for the domain:
  - Panda Cloud Email Protection Default message
  - Customise message [Modify](#)

---

**Deliver/Retain message**

- Use the configuration indicated by the company: **Hold in Panda Cloud Email Protection**
- Use the indicated configuration for the domain
  - Deliver to email manager
  - Hold in Panda Cloud Email Protection
- Propagate changes cascade

**Note:** Spreading changes in cascade will be applied only to Deliver/Hold message.

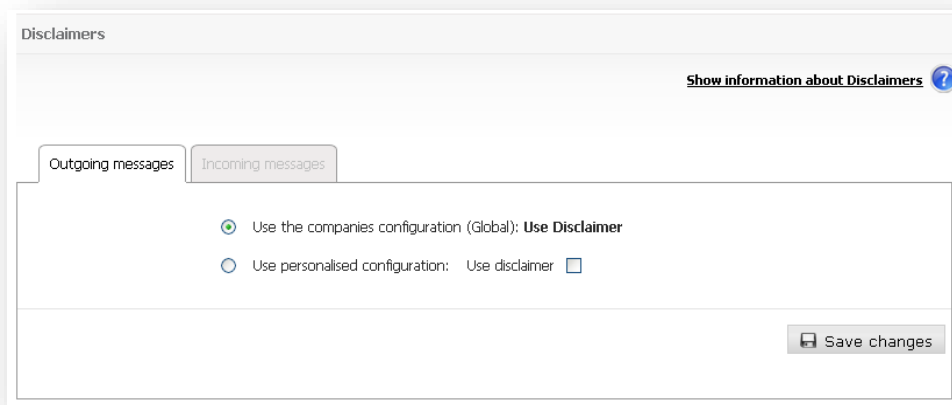
### 2.6.4 Disclaimers

In this section you can set up a text (disclaimer) to be placed automatically at the end of an email, both inbound and outbound email, and you may provide a different setting for each. To include them in outbound mail, it is necessary that outbound email is active and correctly configured through this solution using an authenticated connection.

This configuration allows:

- Define disclaimers at company and domain level
- Establish versions of the message in plain text and HTML
- Use a set of keywords (DATE, SENDER and RECIPIENT) that are replaced automatically for each message. For such replacement, the body of the disclaimer must contain the keywords double brackets, as shown below:
  - Reception date of the message: [[DATE]]
  - Sender of the message: [[SENDER]]
  - Recipient of the message: [[RECIPIENT]]

**IMPORTANT:** The use of disclaimers modifies the email contents, which may affect those who are signed with PGP or X.509, invalidating the digital signature. Panda bears no legal responsibility relating to any side effects caused by these modifications.



### 2.6.5 Synchronization

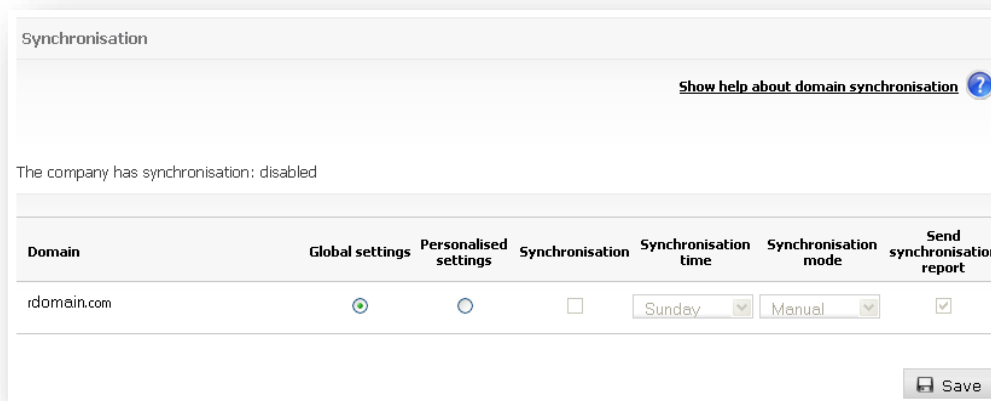
In this section, you can configure user synchronization. This synchronization maintains data coherence between the external repository and Email Protection.

The different settings of the synchronization are:

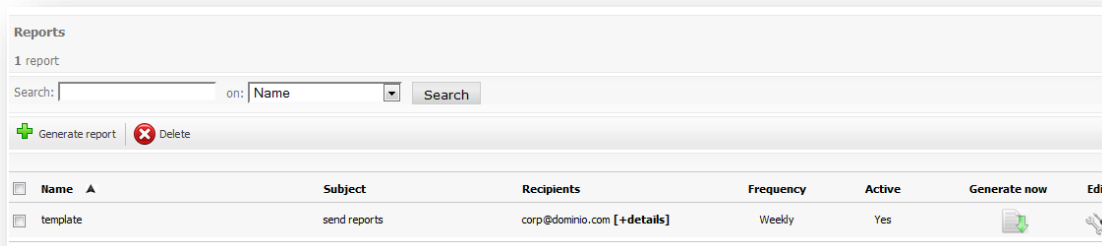
- Synchronization: Allow enable or disable the synchronization process
- Synchronization Execution: Allow Choose how often you run the synchronization process.
- Method of Synchronization: The synchronization mode can be automatic or manual, and is performed by domain.
  - Automatic: Make synchronization without administrator interaction. All users identified are modified or deleted as appropriate.
  - Manual allows the administrator to decide which users will be deleted or changed once the detection of users to synchronize. In this way, users can ignore that are not taken into account by the synchronization process.
  - Sending report Synchronization: If the synchronization process is manual, a report is sent notifying the user domain to modify or delete. After the administrator applies the synchronization, the results are sent in another report. If the synchronization process is automatic, only sends a single domain report timing results.

Global configuration is for the case in which the company administrator decides that the domains have the same configuration as the company. The setting itself is so that each domain has a different configuration for itself.

In the case of a cross-domain alias, the synchronization process generates an email for each of the contact addresses of the primary domains where they are created alias accounts.



## 2.6.6 Reports



During the creation/edition of reports, you must select at least one of the filter categories for both incoming and outgoing email. You may choose not to select filter categories for incoming email provided that at least one filter category of outgoing email has been selected, and vice versa. Likewise, at least one domain must be selected.

If a filter category for incoming/outgoing email is selected, at least one filter graph of incoming/outgoing email must be selected, respectively.

One of the following frequencies may be selected for sending a report:

- Daily: The report is sent on a daily basis and it includes data corresponding to the email flow that has been produced within the range of 0 to 23 hours of the previous day.
- Last 7 days: The report is sent on a daily basis and it includes data corresponding to the email flow that has occurred between the last 7 days and the current day.
- Weekly: The report is sent on a weekly basis and it includes data corresponding to the email flow that has been produced between Monday and Sunday of the last week
- Monthly: The report is sent on a monthly basis and it includes data corresponding to the email flow that has occurred between the first and last day of the month.
- Current month: The report is sent on a daily basis and it includes data corresponding to the email flow that has occurred between the first day of the month and the current day of the same month.

The immediate execution of any report managed from the "Configuration" tab, menu option "Reports" can be requested by clicking the "generate now" button.

The following table summarizes the actions that will be performed when clicking the "generate now" button in accordance with the frequency of the report:

Frequency	Behavior when clicking the "generate now" button
Monthly	The previous month's data will be sent
Daily	The previous day's data will be sent
Weekly	The previous week 's data will be sent
Current month	The data ranging from the first day of the current month to the day before today will be sent
Last 7 days	The data corresponding to the last 7 days counting from yesterday onwards will be sent

Up to 10 addressees may be specified for each report.

The report will be sent by email in PDF format to both the recipients included and the administrator's contact email.

It is possible to create reports by category or predefined reports:

#### **By category**

During the creation/editing of reports, you must select at least one of the filter categories for both incoming and outgoing email. You may choose not to select filter categories for incoming email, provided that at least one filter category of outgoing email has been selected, and vice versa. Likewise, at least one domain must be selected.

If a filter category for incoming/outgoing email is selected, at least one filter graph of incoming/outgoing email must be selected, respectively.

#### **Predefined**

During the creation/editing of predefined reports, you must select at least one of the predefined reports which are available.

The predefined reports available are:

- Top email issuers: Shows the N users who send the most email through the platform.
- Top email issuers by size: Shows the N users who send the most volume of email through the platform.
- Top email addressees: Shows the N users who receive the most email.
- Top email addressees by size: Shows the N users who receive the highest volume of email.
- Top spam addressees: Shows the N users who receive the most spam.

- Top blocked viruses: Shows the N viruses most blocked.

For each of these predefined reports, a limit must be selected for the TOP. The possible values are:

- 10
- 15
- 20
- 30

### Reports

[Show information on reports](#) ?

---

#### Information for sending the report

Enabled:

(\*) Template Name:

(\*) Subject:

---

#### Recipients

Domain administrator:  (domain@dominio.com)

Other recipients:

---

#### Period:

Daily:  (The report will be generated at: 00:30 hours)

Last 7 days:  (The report will be generated every day at: 00:30 hours)

Weekly:  (The report will be generated at: 00:30 hours of Monday)

Monthly:  (The report will be generated at: 00:30 hours of the first day of the month)

Current month:  (The report will be generated every day at: 00:30 hours)

---

#### Report type:

By category:

Predefined:

---

#### Predefined reports:

Top email issuers:  Limit:

Top email issuers by size:  Limit:

Top email addressees:  Limit:

Top email addressees by size:  Limit:

Top spam addressees:  Limit:

Top blocked incoming viruses:  Limit:

Top blocked outgoing viruses:  Limit:

(\*) Mandatory fields

### 2.6.7 Time zone

This configuration allows setting the time zone on domain level and user level individually. The settings can be applied globally or separately on each level. If global is selected a user will have the time zone of the domain he belongs to and a domain will have the time zone of the company it belongs to applied.

End users can select time zones individually. If a configuration is made at this level then management within the console becomes easier as local time is displayed.

The time zone selected on a higher level gets only applied to all users that have not set a time zone on their specific level configured.

# 3. Additional functions

---

Panda Notifier

## 3.1 Panda Notifier

The Email Protection Notifier is a utility<sup>5</sup> which is installed and 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 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 also have the option to access to the same actions from your control panel of Email Protection Web console.

### 3.1.1 Technical Specifications

Notifier works in Windows operating systems (XP, Vista and Windows 7), Mac OS X, Linux x86-64, PowerPC and Linux i386.

---

<sup>5</sup> 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.



# 4. Technical support

---



As Panda client you have several effective options to contact our international support team. Please visit the Panda support website (<http://www.pandasecurity.com/enterprise/support/>) to find your nearest support center and the most convenient contact option for you.



Neither the documents nor the programs that you may access may be copied, reproduced, translated or transferred to any electronic or readable media without prior written permission from Panda Security, C/ Santiago de Compostela, 12, 48003 Bilbao (Bizkaia), SPAIN.

Registered trademarks.

Windows Vista and the Windows logo are trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. All other product names may be registered trademarks of their respective owners.

Panda Security 2017. All rights reserved.