

Panda Security

Email Protection

Administrator's Guide

Version 4.5.1



Contents

1. Introduction to Email Protection.....	4
1.1 What is Email Protection?.....	5
1.2 Functionalities.....	5
2. Email Protection interface.....	6
2.1 Administrator Access.....	7
2.2 Administrator panel.....	7
2.2.1 Note.....	7
2.3 Administration.....	8
2.3.1 Creating and editing passwords.....	8
2.3.2 State.....	8
2.3.3 Domains.....	12
2.3.4 Users.....	15
2.3.5 Users with basic filtering.....	17
2.3.6 Signup mode.....	18
2.3.7 Multiple administrators.....	23
2.3.8 Actions Audit.....	24
2.3.9 Archive.....	25
2.4 Filtering.....	28
2.4.1 Lists.....	28
2.4.2 Anti Virus.....	30
2.4.3 Anti Spam.....	32
2.4.4 Virus quarantine.....	34
2.4.5 Trusted lists.....	35
2.4.6 Filtering mode.....	36
2.4.7 Rules engine.....	38
2.4.8 Email logs.....	42
2.4.9 NDR Validation.....	46
2.4.10 Anti email spoofing.....	48

2.5 Personalization.....	50
2.5.1 Automatic messages.....	50
2.5.2 Reports of administrators.....	53
2.5.3 Logo.....	55
2.5.4 Language.....	56
2.6 Settings.....	57
2.6.1 Company data.....	57
2.6.2 Administrator data.....	58
2.6.3 Access to panels for end users.....	59
2.6.3.1 Domain setup.....	59
2.6.3.2 Setting by user.....	60
2.6.4 Lists and notices.....	61
2.6.5 Disclaimers.....	64
2.6.6 Synchronization.....	65
2.6.7 Reports.....	67
2.6.8 Notification due to license limit.....	71
2.6.9 Time Zone.....	71
2.6.10 Unsubscribe.....	71
3. Additional functions.....	73
3.1 Panda Notifier.....	74
3.1.1 Technical Specifications.....	74
4. Technical support.....	75

1. Introduction to Email Protection

What is Email Protection?

Functionalities

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, white lists and black lists, greylists, 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.

1.2 Functionalities

Some of the functionalities of Email Protection are:

- Central Setup
- Easy management
- Multilayer anti-spam
- Incoming email backup
- Users registration
 - Manually
 - Imported from file
 - LDAP callout with Alias discovery
 - SMTP callout
- Cluster active-active avoiding any information lost in case of incidence
- Administrators per domain
- Email logs with the possibility of open emails (if you chose this option when you purchase), add senders / IP's to white list / blacklist, classify mails as Valid / Spam
- Trusted lists by User
- Customized filters
- Notification software

2. Email Protection interface

Administrator Access

Administrator panel

Administration

Filtering

Personalization

Settings

2.1 Administrator Access

Email Protection control panel can be accessed using any browser 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 Administrator panel

Email Protection interface is very intuitive and easy to use.

It includes four sections:

- Administration
- Filtering
- Settings
- Help

2.2.1 Note

Some of the postmaster panels are divided into two sections:

- Global setting: you choose certain options which will be applied to all domains.
- Domain settings: you can choose if you want to use the standard option for the whole service (Global) or specific options for a certain domain.

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

- Internet Explorer ® 9
- Mozilla Firefox from 6.x

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 Protection, 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

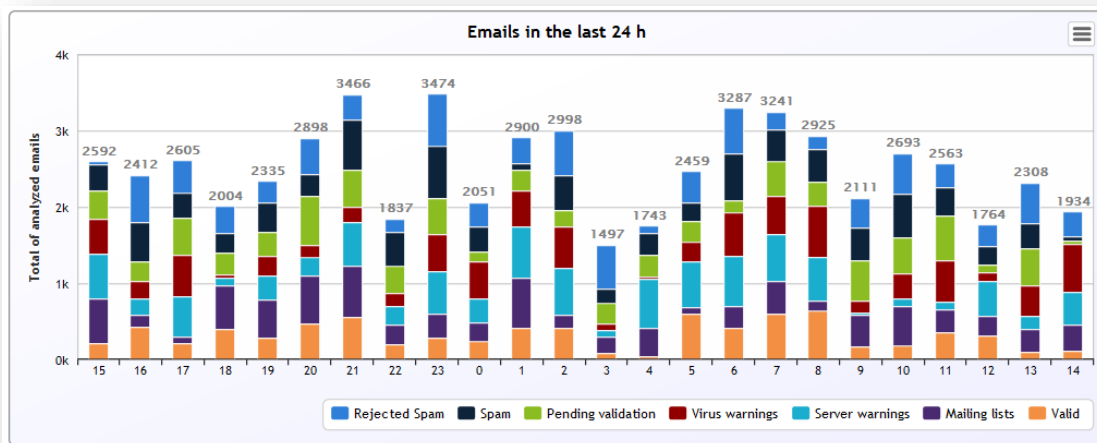
- **Rejected spam:** Number of spam messages rejected by the email Protection due to its high Spam content.
- **Virus:** Number of messages in which a virus has been detected.
- **Valid email:** Number of messages that have passed all the filters and have been delivered.
- The information presented above 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

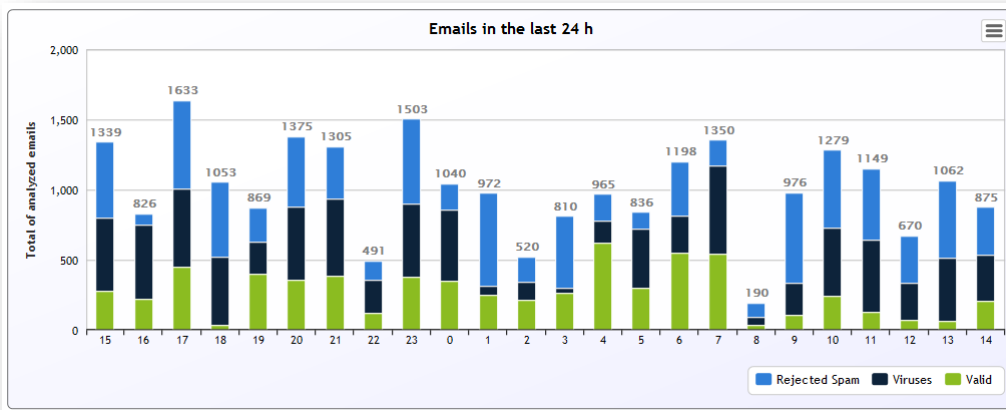
Statistics for incoming mail per hour

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



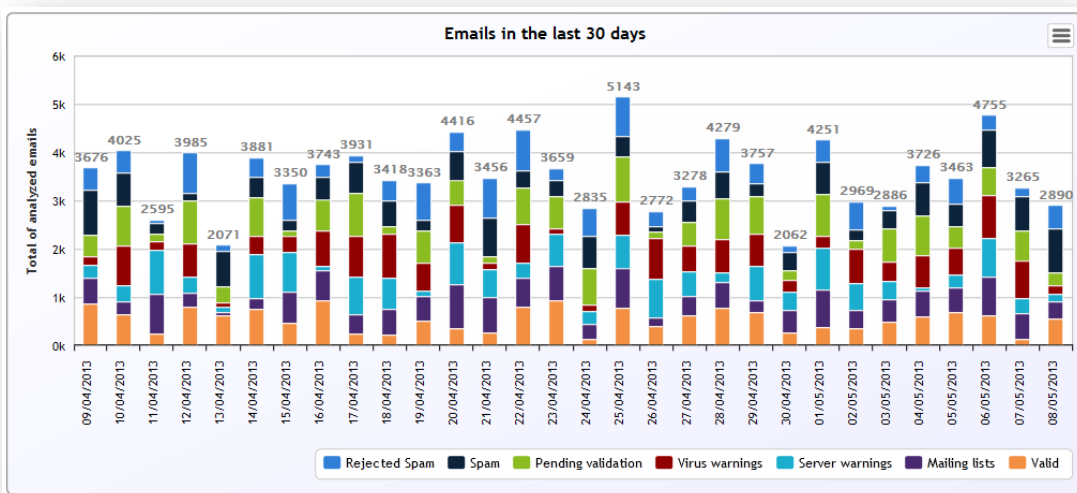
Statistics for outgoing mail per hour

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



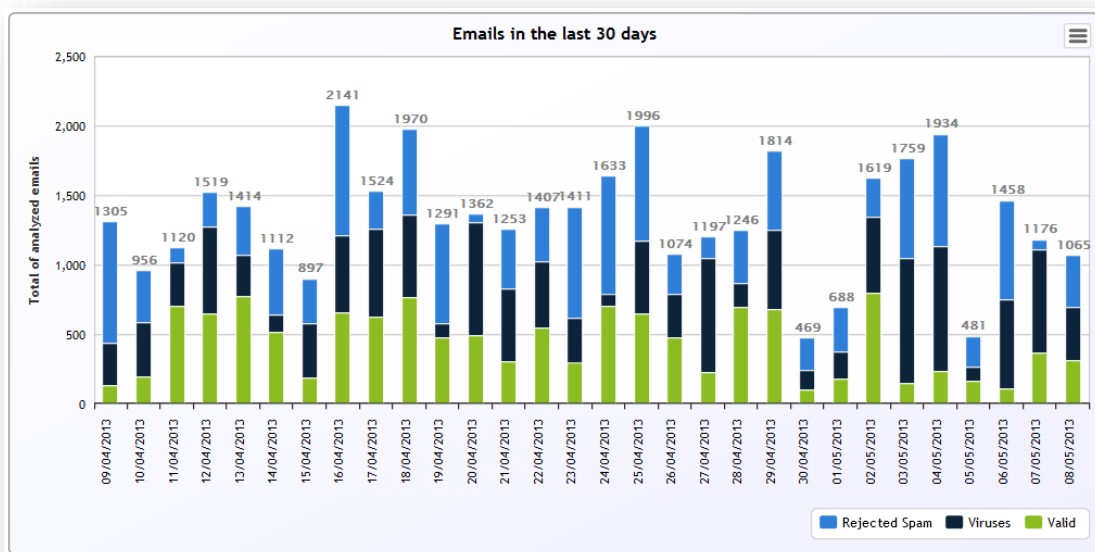
Statistics for incoming mail per day

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

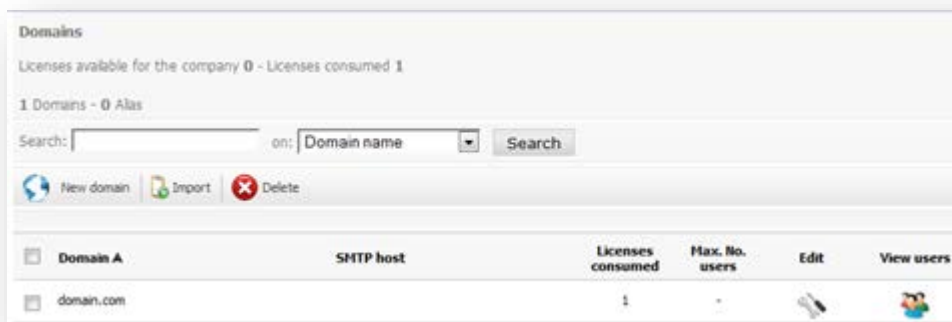


Statistics for outgoing mail per day

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



2.3.3 Domains



This shows the list of domains registered with Email Protection including data such as the target Host SMTP and number of current users. The number of users of a domain can be greater than the number of licenses assigned to the domain, but it cannot be greater than the number of licenses available to the company.

Alias domains¹ appear when clicking on the link *[show alias]* which is showed next to the main domain name.

To edit the domain or see its users, click the corresponding icon.

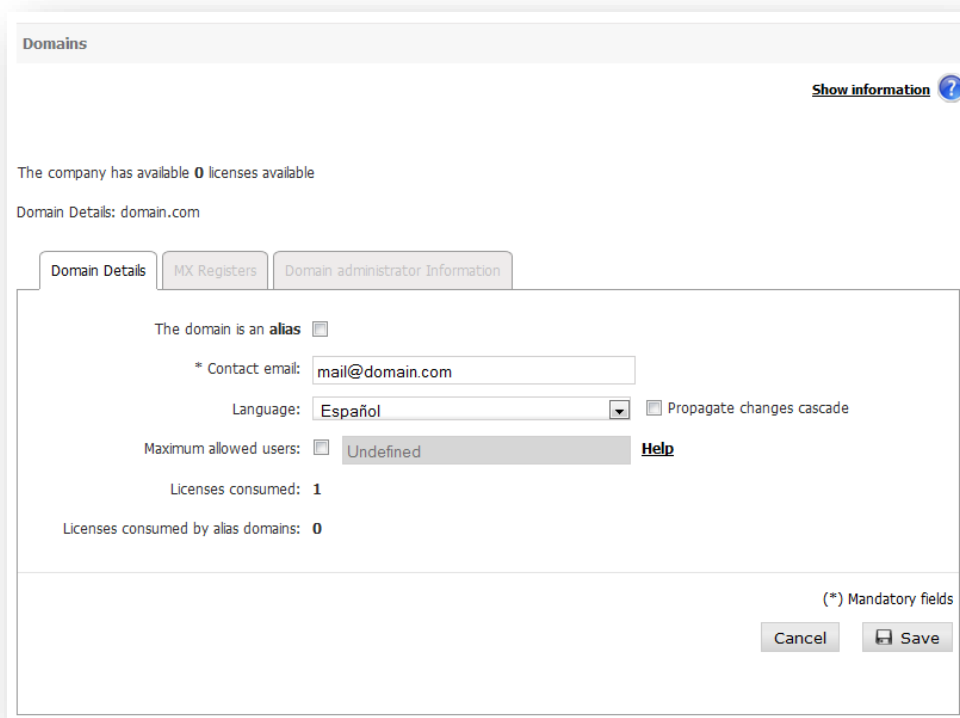
Domains can be searched under the following criteria: "Domain name" and "Alias", selecting one of these options from the selection list in the search form.

¹ An alias domain is a domain created based upon another domain, and by default it has the same accounts from the main domain (it is not necessary to create them). The alias domains only exist in a virtual space and they have no mailbox.

From the “Edit” menu you can create a specific administrator which will have administration rights on the domain.

If the “Access to user panel from listings” option was chosen at hiring time, then an option that allows the domain administrator to access to users panels will appear; it allows the administrator to access to users panels.

If the “View email from panel logs” option was chosen at hiring time, then an option that allows the domain administrator to view the emails from the Email logs.



The screenshot shows a web interface for managing domains. At the top, it says "Domains" and "Show information" with a help icon. Below that, it states "The company has available 0 licenses available" and "Domain Details: domain.com". There are three tabs: "Domain Details" (selected), "MX Registers", and "Domain administrator Information". The main content area shows the following details:

- The domain is an **alias**
- * Contact email:
- Language: Propagate changes cascade
- Maximum allowed users: [Help](#)
- Licenses consumed: **1**
- Licenses consumed by alias domains: **0**

At the bottom right, there is a note "(*) Mandatory fields" and two buttons: "Cancel" and "Save".

To import a domain list, use the following format:

- The import file must contain:
- Domain name
- MX Records (separated by ; if are more than one)
- E-mail contact
- Domain administrator name and last name (1)
- Username (Administrator login) (2)
- Valid password (3)
- Canonical domain (in case of alias domain) (4)

(1, 2, 3 and 4) indicate optional data.

A domain administrator must specify the three fields (1) (2) (3), the absence of one of them will report an error and will not create the domain. An alias domain without an administrator, you must

complete the options (1), (2) and (3) (administrator data) with vacuum, for example: 'alias.com, mx1.com:10; mx2.com:9, user@domain.com,,,, canonico.com'.

Each line of the file should represent a domain.

These files may be .txt or .csv

File structure:

Domain Name, Server MX:Priority, Mail Contact, Domain Admin Name and Last Name[optional], User Name (login)[optional], Password[optional]

For domain ALIAS: Domain Name, Server MX:Priority, Mail Contact, Domain Admin Name and Last Name[optional], user name (login)[optional], Password[optional], Canonical Domain

Final file (example):

dominio.com, servidorMx_1:10;servidorMx_2:20, administrador_empresa@ejemplo.com, Andrés Lopez, andres_lopez, 1234567891

dominioAlias.com,servidorMx_1:10;servidorMx_2:20,administrador_empresa@ejemplo.com, Andrés Lopez, andres_lopez, 1234567891, dominio.com

dominioAliasSinAdmin.com,servidorMx_1:10;servidorMx_2:20,administrador_empresa@ejemplo.com, , , , dominio.com

Important:

- A password is considered valid only if it is not weak
- This process will take several minutes, the result of the import will be notified to the e-mail account provided by the administrator.
- The domain should not have invalid characters
- The Administrator login must be unique
- MX records must be valid
- There may not be missing required fields

Host and servers MX (*the latter for the import of domains*):

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

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

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

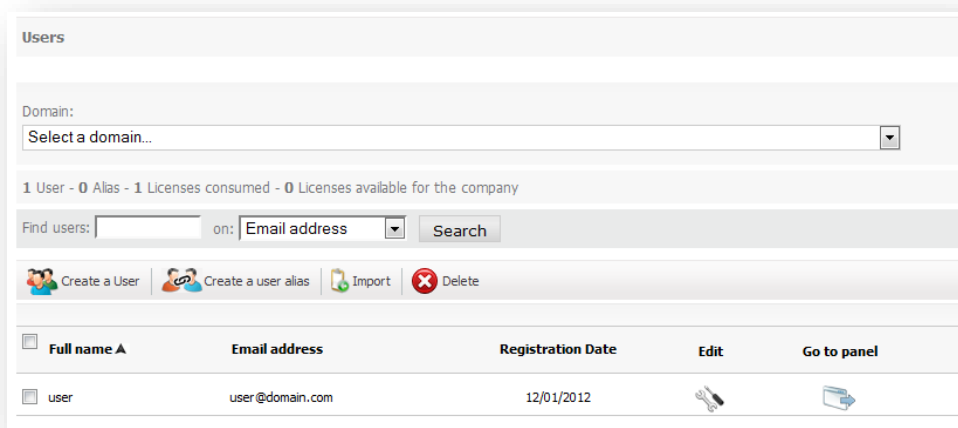
2001:0DB8::1428:57ab

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.

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

From “*Edit*” 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 (optionally including '@domain', if a domain has been selected previously), and the user's password², all separated by commas.

² If the user's password is missing, a new one will be randomly generated to be sent to them in the welcome email.

Each line in the file must represent a user.

These files can be either .txt or .csv

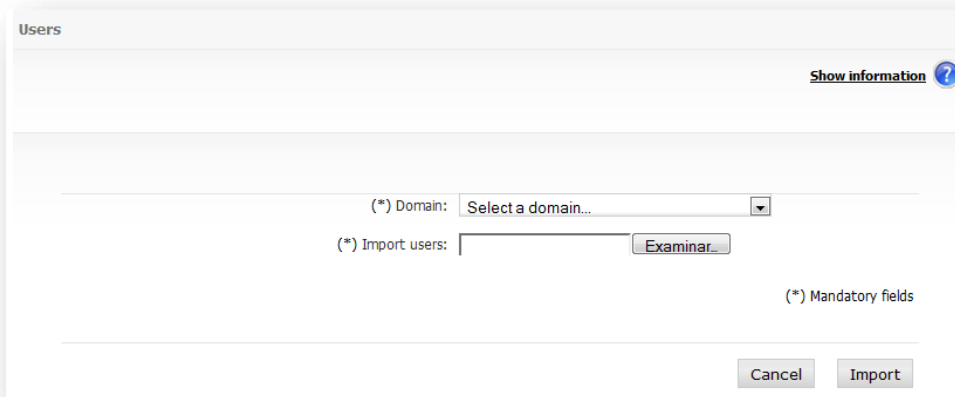
File structure

First name and last name, Email address, Password

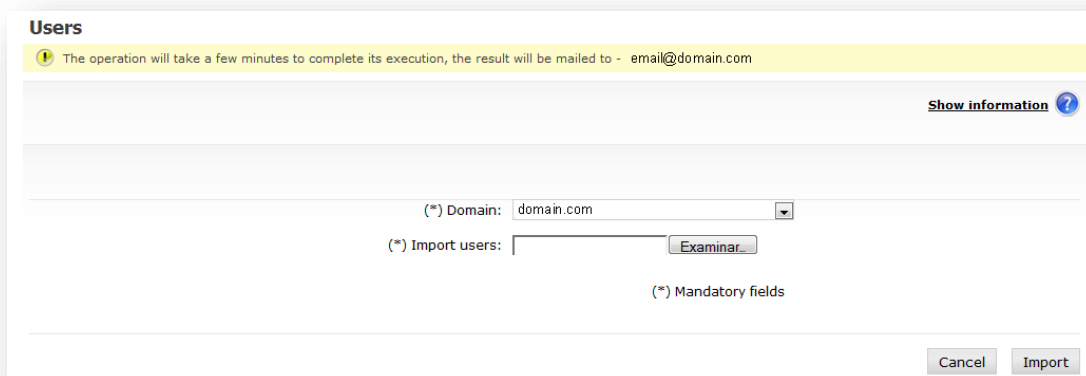
Example

Mike Sanchez, msanchez@example.com, aras249g

Andrew Brown, abrown@example.com, 32kios5



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. The result of the import will be notified by e-mail to the account.



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.



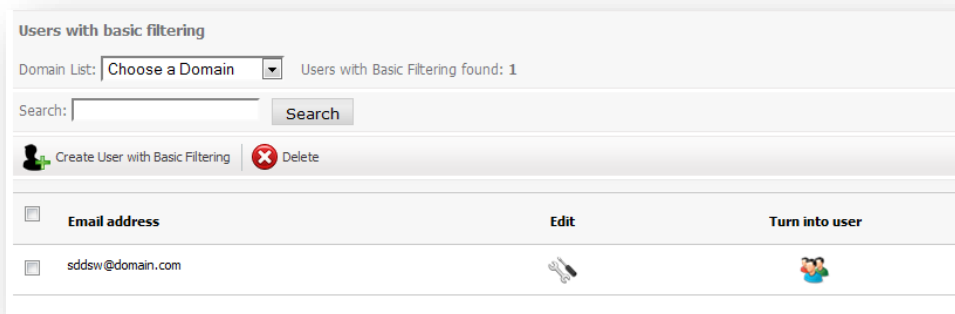
The "Synchronize" button, which is only available when the synchronization mode is set at Manual, allows synchronizing all the domain or company users that have been selected.

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.



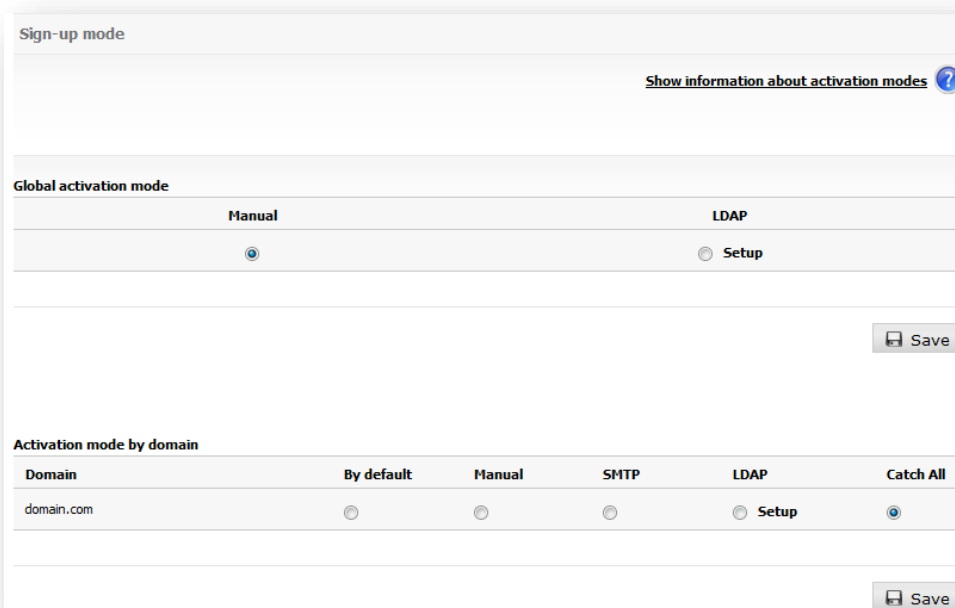
Users with basic filtering can turn to normal users if the administrator thinks it is necessary.

It is important to note that all users must be registered with Email Protection so that their emails shall not be rejected. If you decide to use 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 licenses.

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

Email Protection administrator is responsible for registering each of 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.

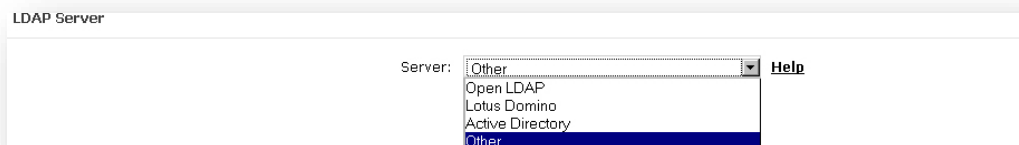
2.3.6.2 Automatic Registration by SMTP callout or LDAP

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 users search in corporate LDAP), 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 checks³. For further information, please contact our Support department.

2.3.6.2.1 Setup of parameters for users search in corporate LDAP

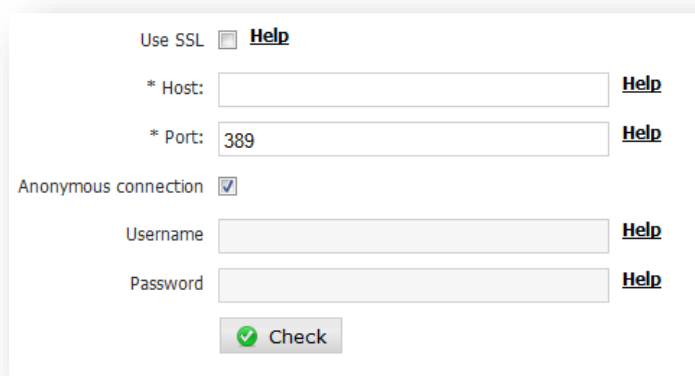
The setup of parameters for user discovery in corporate LDAP, used in the "LDAP registration mode", is divided into the following seven sections:

2.3.6.2.1.1 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.

2.3.6.2.1.2 Connection



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

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

³ SMTP server should only provide an affirmative response just for those domain valid-users.

- Host: Enter the IP address or DNS name of 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

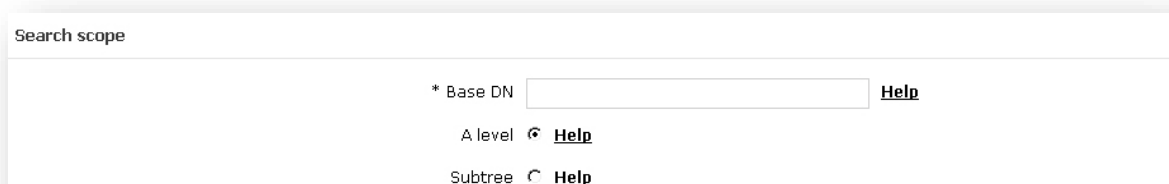
- Port: Indicate TCP/IP port used to connect to LDAP server. There are normally standard ports used by LDAP servers:
 - 389: For normal connections (not secure)
 - 636: For secure connections (SSL)

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

2.3.6.2.1.3 Search scope



The screenshot shows a form titled "Search scope" with three input fields, each followed by a "Help" link:

- * 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 at the level immediately below the Base DN value (not recursive).
- Subtree: specifies that the objects will be searched at the level immediately below the Base DN value (recursive).

Base DN Syntax

In the event the field value contains:

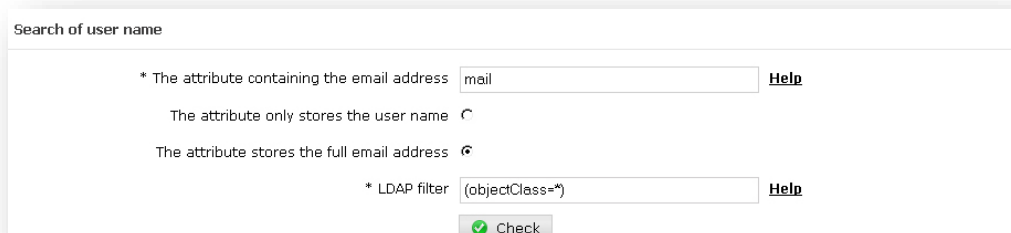
- A space « » (ASCII 32) or numeral «#» (ASCII 35) character at the beginning.
- A space « » (ASCII 32) character at the end.
- Any of the characters: «,» (ASCII 44), «+» (ASCII 43), «"» (ASCII 34), «\» (ASCII 92), «<» (ASCII 60), «>» (ASCII 62) or «;» (ASCII 59)

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

For example, if the value of "Organization Name" (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

2.3.6.2.1.4 Search of user name



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

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

2.3.6.2.1.5 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](#)

Check

If alias search is enabled, the following parameters must be set up:

- Attribute which containing the alias, for example: uid, userId, etc.
- Whether the previous attributes multi-valued. If not, you must specify an alias separator used within this attribute⁴.
- Specify the alias is in the same LDAP object as the email address, in case it is not, you specify the attribute containing the real user object DN (for example: cn, userId).

2.3.6.2.1.6 Groups

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

Groups

Group member(ship)

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

The field is multivalued

Yes

No

Group separators: [Help](#)

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.

⁴ 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 Protection for your entire organization, as well as for certain domains.

There are two types of administrators, for both companies and domains:

- Main administrator
- Secondary administrator

As far as companies are concerned, the main administrator is the only administrator that has been granted privileges to cancel the company or change its access credentials.

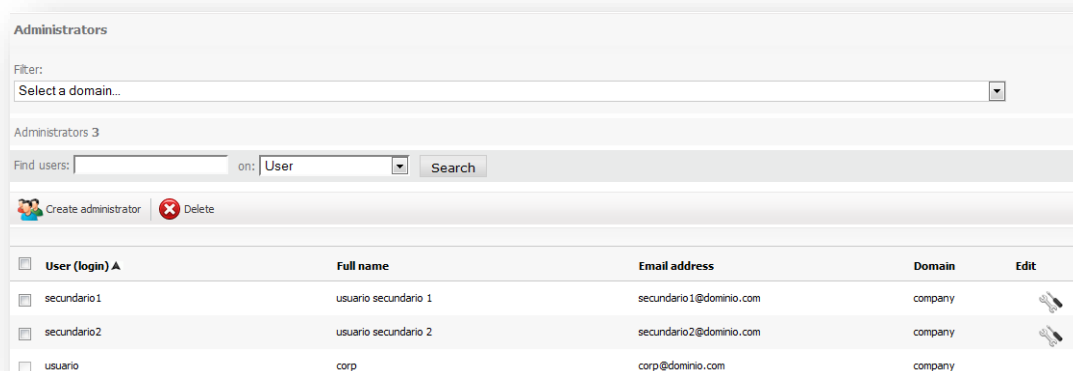
Only one main administrator can be defined for companies or domains.

The following information is required to create an administrator:



- Administrator type
 - Company administrator
 - Domain administrator: In this case, the domain to be administered must be indicated.
- 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 sections:

- Domain administrator: "Management" tab, "Domain" menu option, edition of domain data.
- Company administrator: "Configuration" tab, "Administrator data" menu option.



The screenshot shows the 'Administrators' management interface. At the top, there is a 'Filter:' section with a dropdown menu set to 'Select a domain...'. Below this, it indicates 'Administrators 3'. There is a search bar with 'Find users:' and a dropdown set to 'on: User', followed by a 'Search' button. Below the search bar are two buttons: 'Create administrator' (with a plus icon) and 'Delete' (with a minus icon). The main part of the interface is a table with the following columns: 'User (login) A', 'Full name', 'Email address', 'Domain', and 'Edit'. The table contains three rows of data:

<input type="checkbox"/>	User (login) A	Full name	Email address	Domain	Edit
<input type="checkbox"/>	secundario 1	usuario secundario 1	secundario1@dominio.com	company	
<input type="checkbox"/>	secundario 2	usuario secundario 2	secundario2@dominio.com	company	
<input type="checkbox"/>	usuario	corp	corp@dominio.com	company	

2.3.8 Actions Audit

This functionality provides access to the different registries of the actions performed by all your administrators and end users registered in the system.

Among the types of actions registered, the following are worth mentioning:

- Sign-ups, cancellations and updates of domain data
- Sign-ups, cancellations and updates of domain and company administrator data
- Sign-ups, cancellations and updates of end user data
- Changes to configurations of email filtering
 - Black and white lists
 - Filtering mode
 - Incoming and outgoing email filters
 - Spam marking
 - Classification rules
 - ...
- ...
- The search engine enables you to establish the following filters:
- Type of user that has performed the action: it allows choosing between the following values
 - All
 - Company (company administrators)
 - Domain (domain administrators)
 - End user
- Main category of the action: it allows choosing between the following values
 - Management
 - Filtering
 - Customization
 - Configuration
 - Notifier
 - Webservice
- Specific actions: These depend on the abovementioned filters that have been applied.
- Range of dates in which the action has been performed
 - Start date
 - End date
- Name of the user that has performed the action: when using this option, you must indicate the full username.

The results obtained after performing a search show the following information:

- Name of the action
- Date in which it was performed

- Username (the same one used to login into any of the panels or notifier)
- User type
 - Company administrator
 - Domain administrator
 - End user
- Data related to the action: indicates, for each of the actions, the data used to perform the action.
- Description of the errors that may have been produced during the execution of the action.



By clicking on the "Action", "Date" or "User" columns, the search results can be sorted (ascending or descending) following any of the mentioned criteria.

Actions Audit

Company [v] Filtering [v] (46 of 46 Actions selected) [v]

01/03/2012 [calendar] 22/05/2012 [calendar] User [input] Search

Amount of registries found: 25

Action	Date ▲	User	User type	Data	Warnings / Errors
Add element to Black List	2012-05-21 09:24:31	prueba	Company		Errors found [+]
Add element to Black List	2012-05-21 09:24:44	prueba	Company		Notices [+]

2.3.9 Archive

2.3.9.1 Domains

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

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.

Global settings

	Enabled	Disabled
Company	<input checked="" type="radio"/>	<input type="radio"/>

Domain	Global	Enabled	Disabled
dom1.com	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
dom2.com	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
dom3.com	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

2.3.9.2 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.

Domain:

Archiving configuration: **global settings**. Company configuration: **enabled**

Search: on:

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

2.3.9.3 Search

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

The section «Filters» allows specifying, optionally:

1. Domain on which the search would like to be performed.

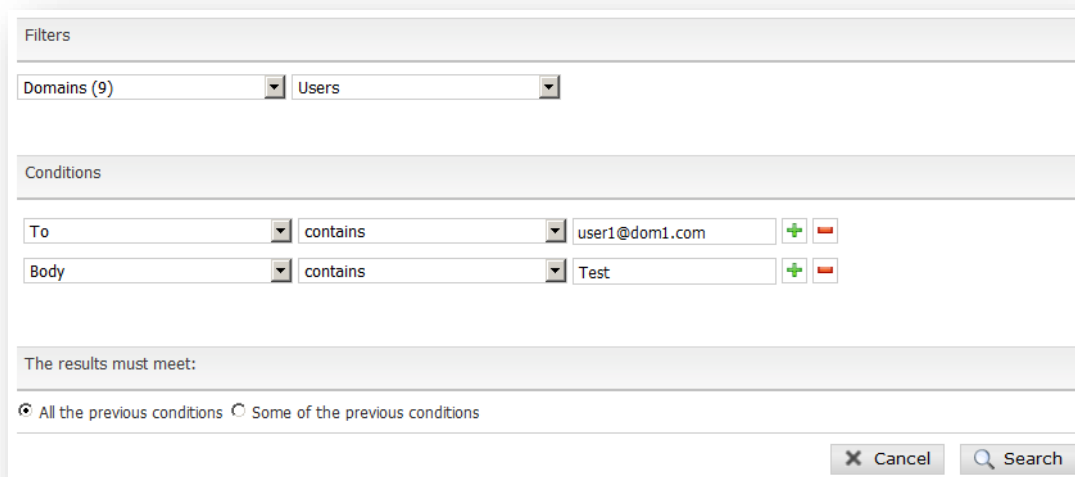
2. User from which emails would like to be obtained. The list of users is only available after having selected a domain.

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
To	<ul style="list-style-type: none"> - contains - does not contain 	All or part of an email addresses.
From	<ul style="list-style-type: none"> - contains - does not contain 	All or part of an email addresses.
Cc	<ul style="list-style-type: none"> - contains - does not contain 	All or part of an email addresses.
Subject	<ul style="list-style-type: none"> - 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	<ul style="list-style-type: none"> - contains - does not contain 	Text to find in the body of the email.
Emails with a date	<ul style="list-style-type: none"> - 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.



2.4 Filtering

In this section you can administer all aspects related to the filtering by Email Protection, applying global settings of 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 company 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 Domains

From here you can activate or deactivate antivirus scanning on domain or enterprise level as well as for inbound and outbound email. 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 activate the virus quarantine (only available for inbound email) you need to have at least one of the available scan engines activated. As a virus is detected in an email, the system quarantines the email and sends a notification to the original recipient of the email. Company administrators will be the only users with access to the quarantined items via the "Virus quarantine" menu available in the "Filtering" tab.

To apply antivirus 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 antivirus scanning 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 antivirus scanning for outbound emails will not be applied.

Incoming email
Outgoing email

ClamAV

Global configuration (applied to all domains)

Domain ▲	ClamAV
dom1.com	Global ▼
dom2.com	Enabled ▼
dom3.com	Disabled ▼

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.

Domain:
Search:
on:

Incoming email
Outgoing email
No. of users: 3

Domain configuration: ClamAV (Enabled)

Name ▲	Log in	ClamAV
User Name 1	u1@dom1.com	Global ▼
User Name 2	u2@dom1.com	Global ▼
User Name 3	u3@dom1.com	Global ▼

2.4.3 Anti Spam

2.4.3.1 Domains

From here you can activate or deactivate spam-filtering for inbound and outbound filtering on company or domain level. 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!

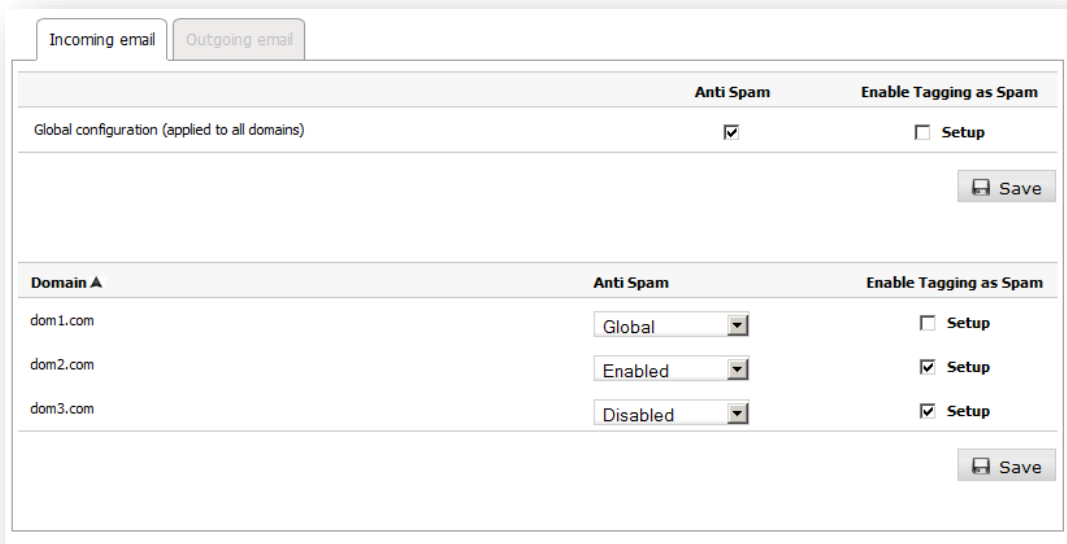
If you deselect anti-spam filtering for a certain scan job, then content filtering will be disabled but connection filtering still applies.

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 the configuration interface for Anti Spam settings. It has two tabs: 'Incoming email' and 'Outgoing email'. The 'Outgoing email' tab is selected. The interface is divided into two sections: 'Global configuration (applied to all domains)' and 'Domain A'.

	Anti Spam	Enable Tagging as Spam
Global configuration (applied to all domains)	<input checked="" type="checkbox"/>	<input type="checkbox"/> Setup
<input type="button" value="Save"/>		
Domain A	Anti Spam	Enable Tagging as Spam
dom1.com	Global	<input type="checkbox"/> Setup
dom2.com	Enabled	<input checked="" type="checkbox"/> Setup
dom3.com	Disabled	<input checked="" type="checkbox"/> Setup
<input type="button" value="Save"/>		

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 RBLs (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.

Default settings are:

- 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.

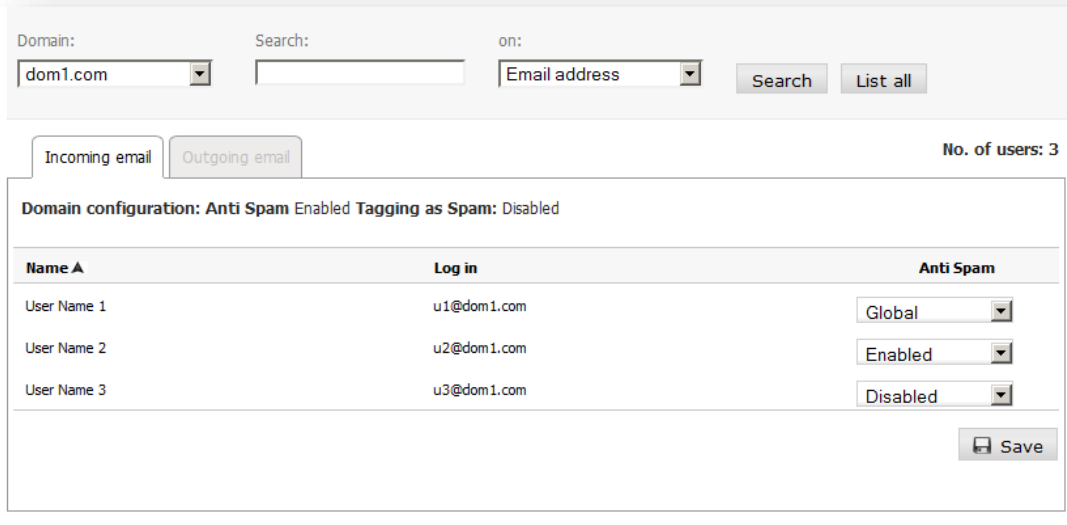
If you deselect anti-spam filtering for a certain scan job, then content filtering will be disabled but connection filtering still applies.

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 autenticate 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 Protection platform (server) as smarthost.
3. Within the SMTP smarthost configuration make sure the SMTP session is autenticated 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 the Panda Email Protection console interface. At the top, there are search filters for Domain (dom1.com), Search, and on: Email address. Below this, there are tabs for Incoming email and Outgoing email, and a 'No. of users: 3' indicator. The main content area displays 'Domain configuration: Anti Spam Enabled Tagging as Spam: Disabled'. Below this is a table with columns for Name, Log in, and Anti Spam. The table lists three users: User Name 1 (u1@dom1.com) with Anti Spam set to Global, User Name 2 (u2@dom1.com) with Anti Spam set to Enabled, and User Name 3 (u3@dom1.com) with Anti Spam set to Disabled. A 'Save' button is located at the bottom right of the table.

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

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 RBLs (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 Virus quarantine

This option allows the administrator to:

- See the emails in the list.
- Download email attachments.
- Delete emails.

The time storage of emails is displayed in the Settings tab, Storing option, Valid Mail.

Virus quarantine

[Show information about virus quarantine](#) 

2 Infected emails

 Delete

<input type="checkbox"/> Sender	Subject	Date	Size
 <input type="checkbox"/> virus2@virus.com	our vacations photos	02/09/2009	1.71 KB
 <input type="checkbox"/> virus@virus.com	look at this	02/09/2009	1.7 KB

2.4.5 Trusted lists


2.4.5.1 Trusted lists by domain

Trust 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.

Trusted lists by domain

[Show information about the trusted list](#) 

Global settings

	Enabled	Disabled
All the domains	<input type="radio"/>	<input checked="" type="radio"/>

Domain setup.

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

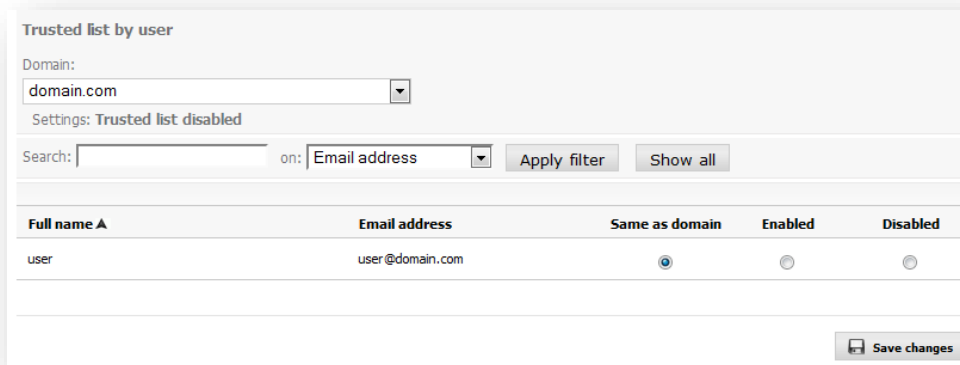
2.4.5.2 Trusted list by user

Trusted lists are automatic white lists customized by user.

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 email addresses of users that Email Protection confirms as safe.

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



2.4.6 Filtering mode

2.4.6.1 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 connection filters, white lists or black lists.

In this case, Email Protection offers two filtering modes:

2.4.6.1.1 Automatic mode

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

The higher the protection level you choose, the greater probability of detecting spam messages. However, some messages are detected as spam when they are not Spam (false positives). A value of five should be enough for a standard user.

2.4.6.1.2 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 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.


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

In the event that the sender is not validated, the recipient can do this manually from your Control Panel from the notifier or the report of blocked email.

The "Propagate in cascade", the configuration applies to all domains and users of the company, domain-level settings apply to all domain users.

Filtering mode by domain

[Show information about the filter configuration](#) 

 The folder **"Email Pending Validation"** in the guaranteed filtering mode is always shown, regardless of the user filtering mode.

Global settings

	Automatic	Guaranteed	
All the domains	<input checked="" type="radio"/> 5 ▾	<input type="radio"/>	<input type="checkbox"/> Propagate in cascade

Spam filtering mode

New Domain	Global	Automatic	Guaranteed	
domain.com	<input checked="" type="radio"/>	<input type="radio"/> 5 ▾	<input type="radio"/>	<input type="checkbox"/> Propagate in cascade

2.4.6.2 Filtering mode by user

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.

Filtering mode by user

[Show information about filter configuration by user](#) ?

! The folder "Email Pending Validation" in the guaranteed filtering mode is always shown, regardless of the user filtering mode.

Domain:

Search: on:

Full name ▲	Email address	Same as domain	Automatic	Guaranteed
user	user@domain.com	<input checked="" type="radio"/>	<input type="radio"/> 5 ▼	<input type="radio"/>

2.4.7 Rules engine

2.4.7.1 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.

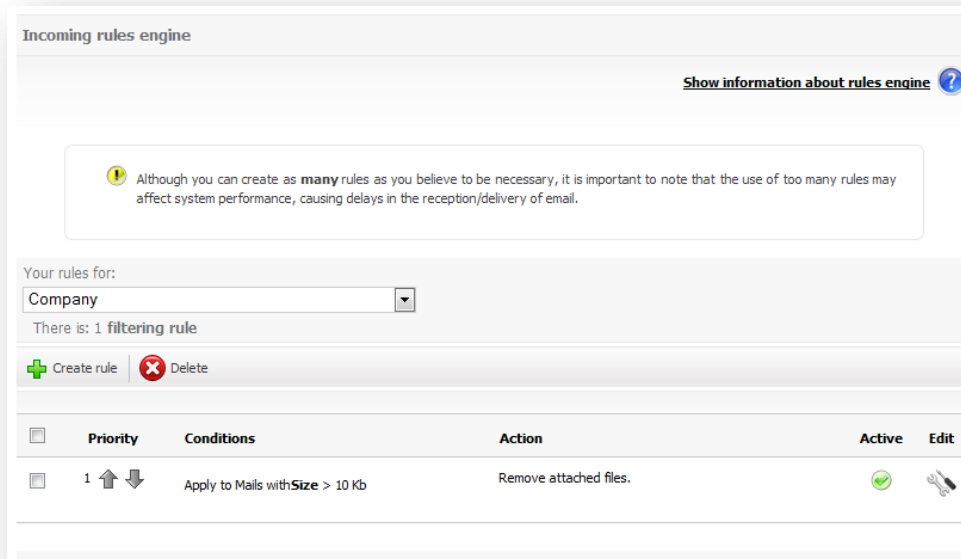
The "send copy to" action sends a copy of the original email to a specified address or to several comma-separated.

The "forward to" action 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.

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

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

2.4.7.2 Outcoming 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.

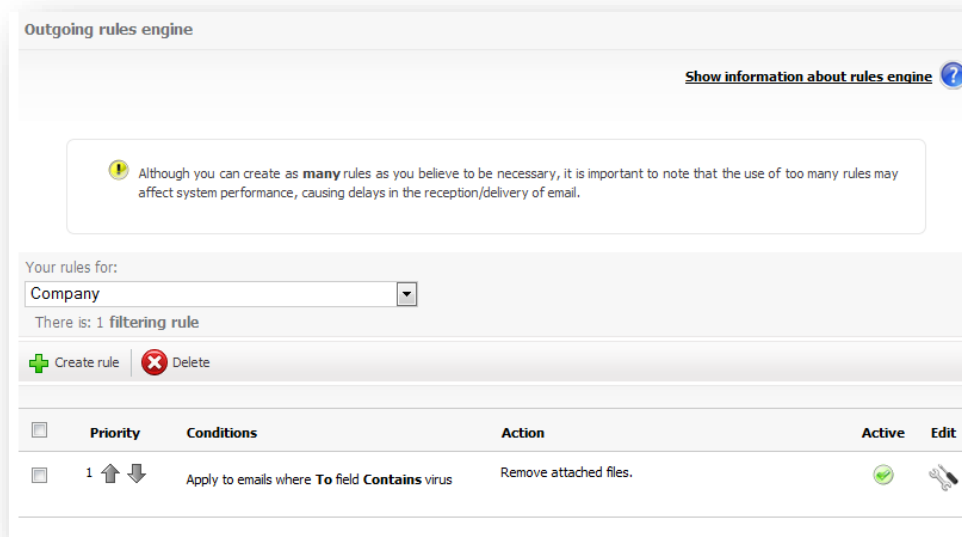
The "send copy to" action sends a copy of the original email to a specified address or to several comma-separated.

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.

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

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

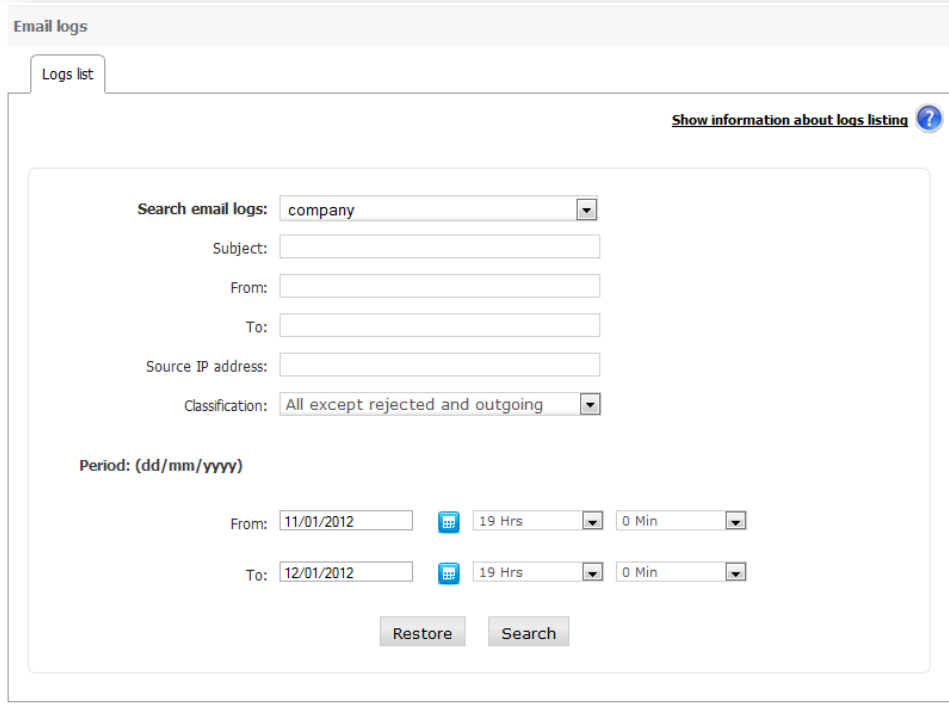
PERL-type common expressions are those supported. For further information on this type of expressions, you may check the following official reference: http://en.wikipedia.org/wiki/Regular_expression#Perl-derived_regular_expressions

2.4.8 Email logs

2.4.8.1 Logs listing

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 screenshot shows the "Email logs" interface. At the top, there is a "Logs list" tab and a link to "Show information about logs listing" with a help icon. The main area contains a search form with the following fields:

- Search email logs:** A dropdown menu with "company" selected.
- Subject:** A text input field.
- From:** A text input field.
- To:** A text input field.
- Source IP address:** A text input field.
- Classification:** A dropdown menu with "All except rejected and outgoing" selected.

Below the search fields, there is a "Period: (dd/mm/yyyy)" section with two rows of date and time selection:

- From:** Date: 11/01/2012, Time: 19 Hrs, 0 Min.
- To:** Date: 12/01/2012, Time: 19 Hrs, 0 Min.

At the bottom of the form, there are two buttons: "Restore" and "Search".

The range of dates to search mail logs will be limited to storage time.


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

- All except rejected and outgoing
- Service warnings

- Virus warnings
- Infected email
- Mailing lists
- Pending validation
- Spam
- Valid
- Valid outbound email
- Rejected incoming email
- Rejected outbound email

Possible statuses⁵ 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"*.
- **Temp error:** An error occurred in the delivery of the email. You can see the cause 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.

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**

⁵ Email log 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)

- 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 to source IP white list: In e-mails from IPs belonging to this list will apply the plug-ins and antivirus, and no content filtering.
- Send source IP Blacklist: Those emails from IPs in this list will be directly rejected.
- 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:

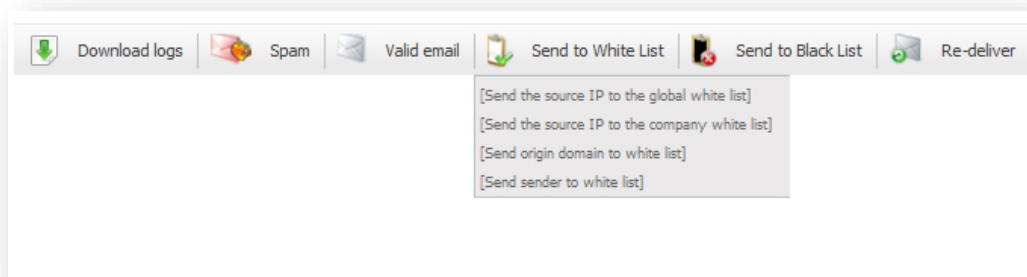
Mass actions allow carrying out different operations on a group of email logs simultaneously. As the process may take several minutes, the result of each operation is notified via email to the contact email that has been configured previously.

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

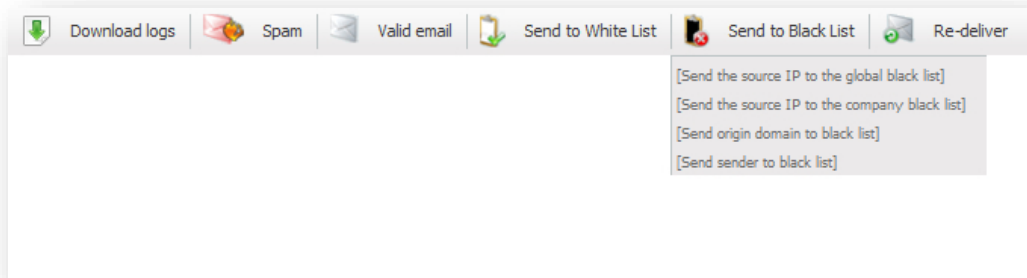
Not all the actions are applicable to all types of emails:

- 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



2.4.9 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.

2.4.9.1 NDR Validation by domain

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

NDR validation by domain

[Show information about NDR validation by domain](#) 

Company setup

NDR Validation

Global configuration (applied to all domains)

Domain A	Global settings	Personalised settings	NDR Validation
domain.com	<input checked="" type="radio"/>	<input type="radio"/>	<input type="checkbox"/>

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*, and 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 incoming emails (the signature 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.


2.4.9.2 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.

NDR validation by user

[Show information about NDR Validation by user](#) 

Domain:

Settings: **global settings**

Search: on:

Full name ▲	Email address	Same as domain	Personalised settings	NDR Validation
user	user@domain.com	<input checked="" type="radio"/>	<input type="radio"/>	<input type="checkbox"/>

2.4.10 Anti email spoofing

This configuration 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 "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, domain or company).

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

2.4.10.1 Anti email spoofing by domain

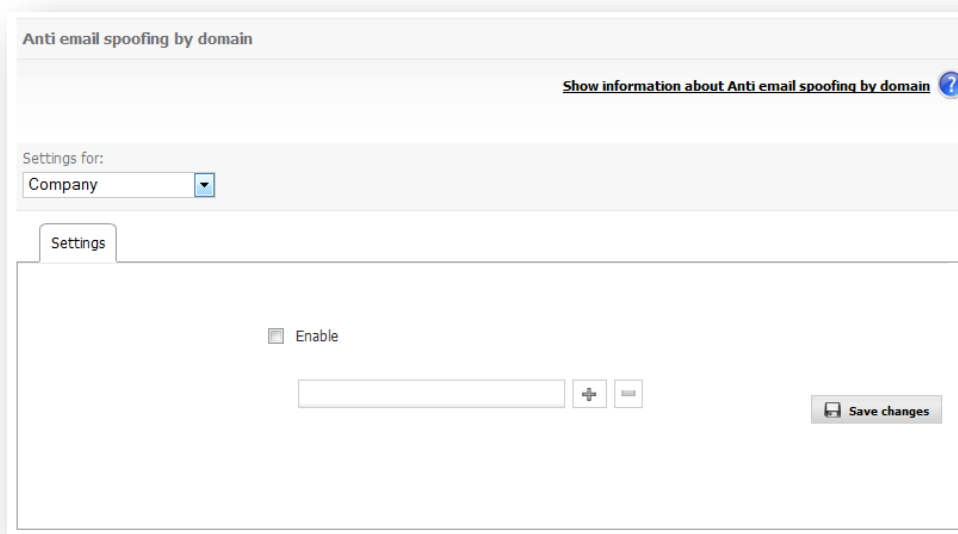
Anti Email Spoofing management by domain will allow you to define configurations which can be applied for all the domains or just for some of them.

This filter is disabled by default settings for the whole company and all its domains.

- **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**.



2.4.10.2 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.

Anti email spoofing by user

Domain:
domain.com

Search: on: Email address

Full name A	Email address	Same as domain	Enabled	Disabled
user	user@domain.com	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

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*.

Welcome message
Blocked Email Report
Guaranteed validation message filtering

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.

Allow the domain administrator to customise the message

Panda Cloud Email Protection Default message

Customise message [Modify](#)

Do not send welcome message

Send without attachment

Send with manual

Send with the file... Ningún a...ccionado

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 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 mail 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 on the link "See templates". Templates can be selected from a drop-down menu.

Welcome message

Blocked Email Report

Guaranteed validation message filtering

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.

Allow the domain Administrator to customise the report

Default message [Preview](#)

Customise message [View templates](#)

Select template

Do not send report

Send daily report

Send weekly report

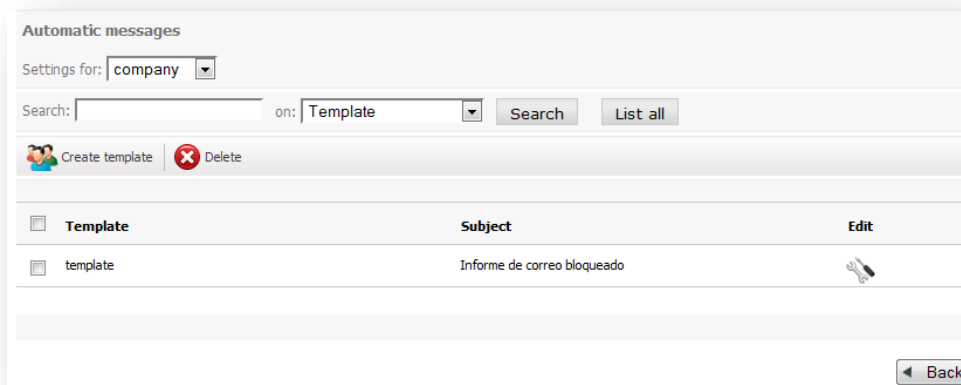
Propagate in cascade

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

2.5.1.2.1 See templates

A new screen appears with the following options:

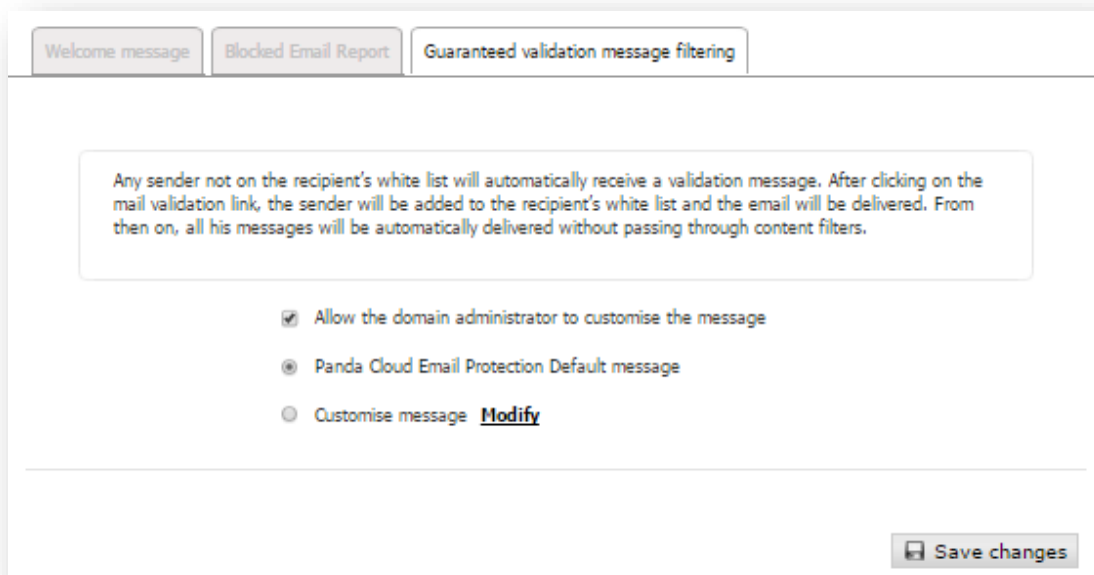
- **Create Template:** This creates a new message based on Email Protection's default message. To create a message you must define the message content and subject. You can also set the name and email address of the message sender. The company's contact email address appears by default and you can select 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 template's name and subject.



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.



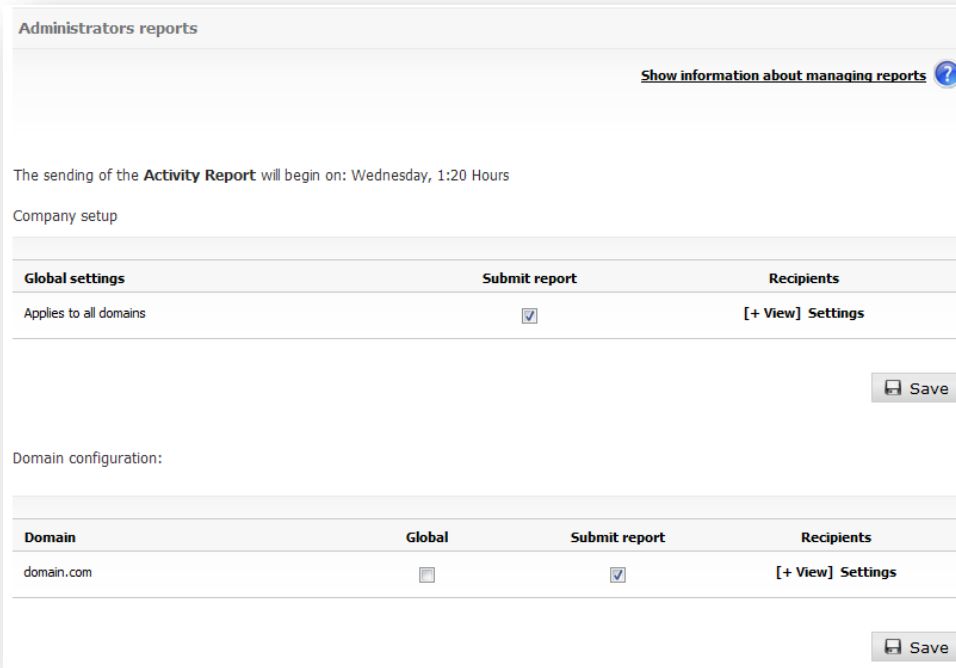
2.5.2 Reports of administrators

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/s:

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

May be set both company level (global settings) and domain level, where sending the activity report is enabled by default.



Administrators reports

[Show information about managing reports](#) 

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

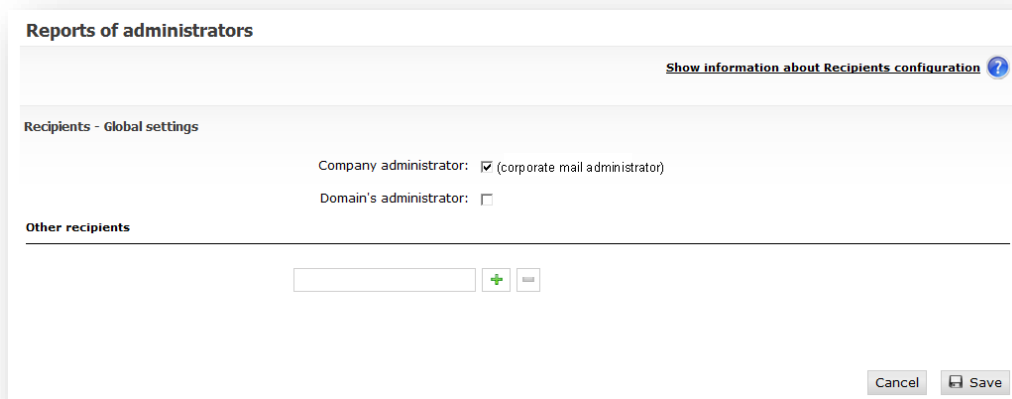
Company setup

Global settings	Submit report	Recipients
Applies to all domains	<input checked="" type="checkbox"/>	[+ View] Settings

Domain configuration:

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

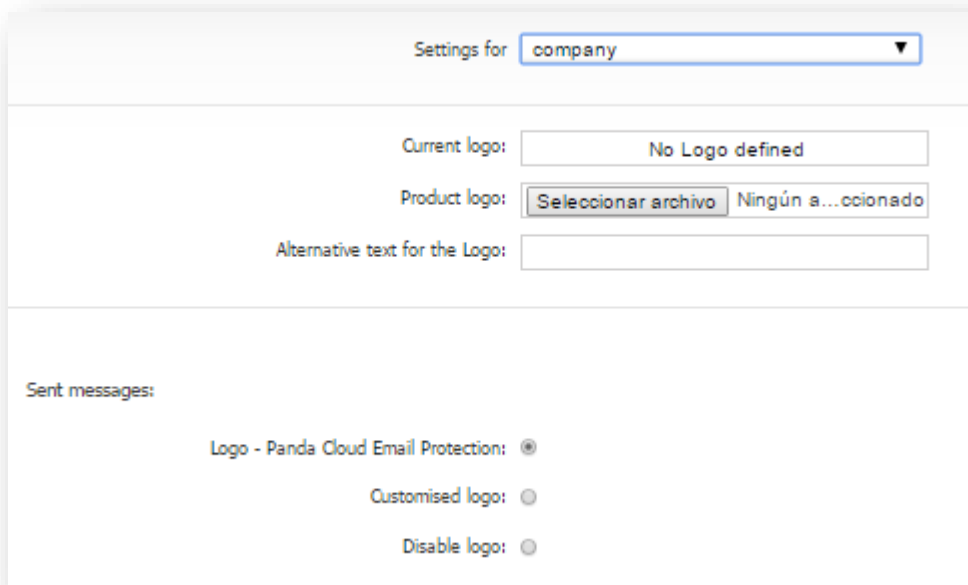
The recipient's setting lets you define the recipients of the activity report globally or for each domain.



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

2.5.3 Logo

The option list "Settings for" will allow you to select the company or the domain settings for the sent messages logos.



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

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 panels through the option "Apply logo change in panels".

Regarding to the sent messages, you can choose among:

- Using the default Email Protection logo
- Using the customized logo ("Customized logo" option)
- Do not use a logo ("Disable logo" option)

2.5.4 Language

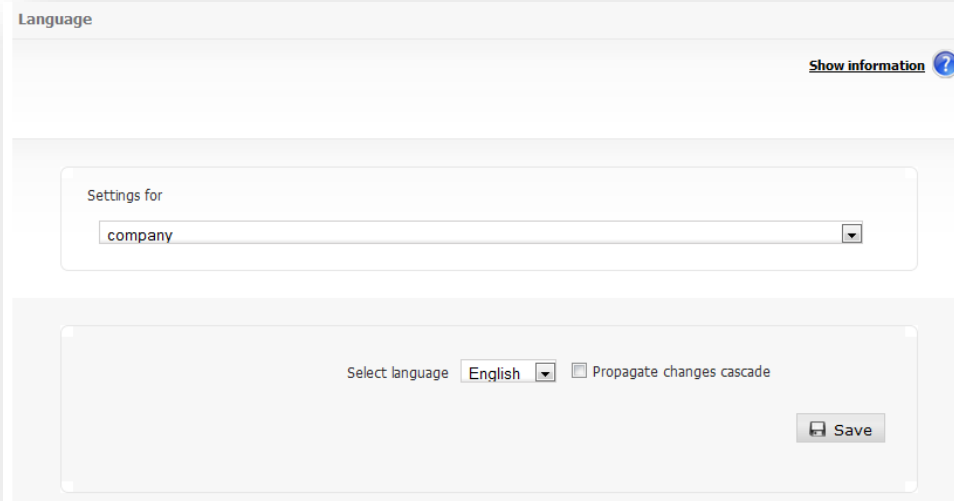
In this section you can choose a language, which will be used for the web panel and the automatic messages. This option is on the tab "Settings".

From this panel is possible to create a domain with a different language from the one used by the company. By default, it appears the company administrator language for each new domain.

The Alias Domains will also have the choice to choose a different language. By default, it appears the same language than de primary domain.

In the creation of users it is possible to select the language although it is selected by default the domain language.

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



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 Company data

This is where information about the company must be entered.

The *Contact email* field indicates the email address from which all messages automatically generated by Email Protection will be sent.

The *Sender of automatic messages* field will be used to send all automatic messages; if this value is absent, then system will use `no-reply@mep.pandasecurity.com`

Company data

* Corp name:

Address:

Address 2:

Postal code:

* Phone number:

Web site address:

* Contact person:

* Contact email:

Sender of automatic messages: [Help](#)

Registration Date: 20/10/2011

Expiration date: 20/10/2012

Licenses purchased: 1

Licenses in use: 1


(*) Mandatory fields

2.6.2 Administrator data

This is where information about the administrator must be entered.

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

Administrator Data

[Show information](#) 

* 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:

2.6.3 Access to panels for end users

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 has been disabled will receive a notification of this situation whenever they try to access.

2.6.3.1 Domain setup


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

Both for the company as well as for each one of the domains which belong to it, the configuration options available are:

- **Global:** The configuration used is the one defined by the higher level: 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 company / domain users will be allowed access to their user panels.

- **Propagate the global configuration in cascade:** Applies the configuration to all domains and users of the company.
- **Propagate the configuration defined for a specific domain in cascade:** Applies the configuration to all users of the selected domain.

Domain setup

[Show information on access to panels](#) 

Global settings

Access to panel for end users

All the domains Propagate in cascade

Access to panel end users

New Domain	Global settings	Personalised settings	Access to panel for end users
domain.com	<input checked="" type="radio"/>	<input type="radio"/>	<input type="checkbox"/> <input type="checkbox"/> Propagate in cascade

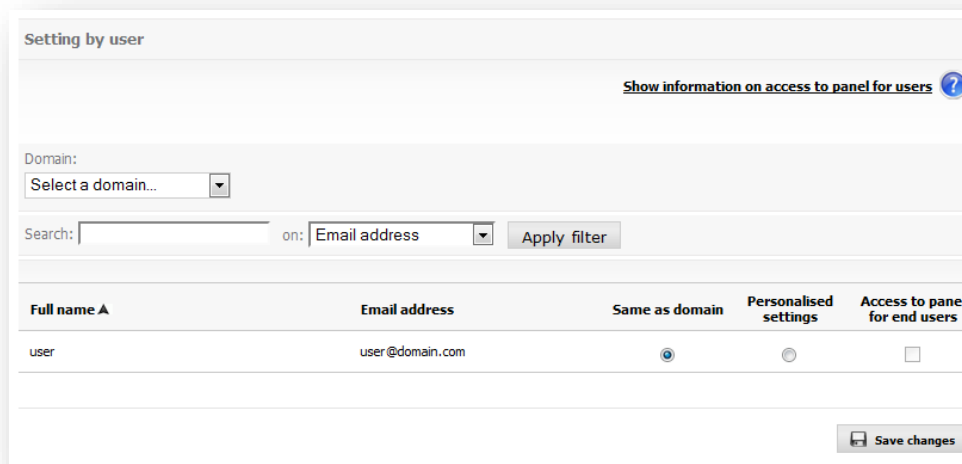
2.6.3.2 Setting by user

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 has been disabled will receive a notification of this situation whenever they try to access.

Allows configuration of the access to panels for end users.

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

- **Same as domain:** The configuration defined for the domain will be 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 be allowed access to their user panel.



2.6.4 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.

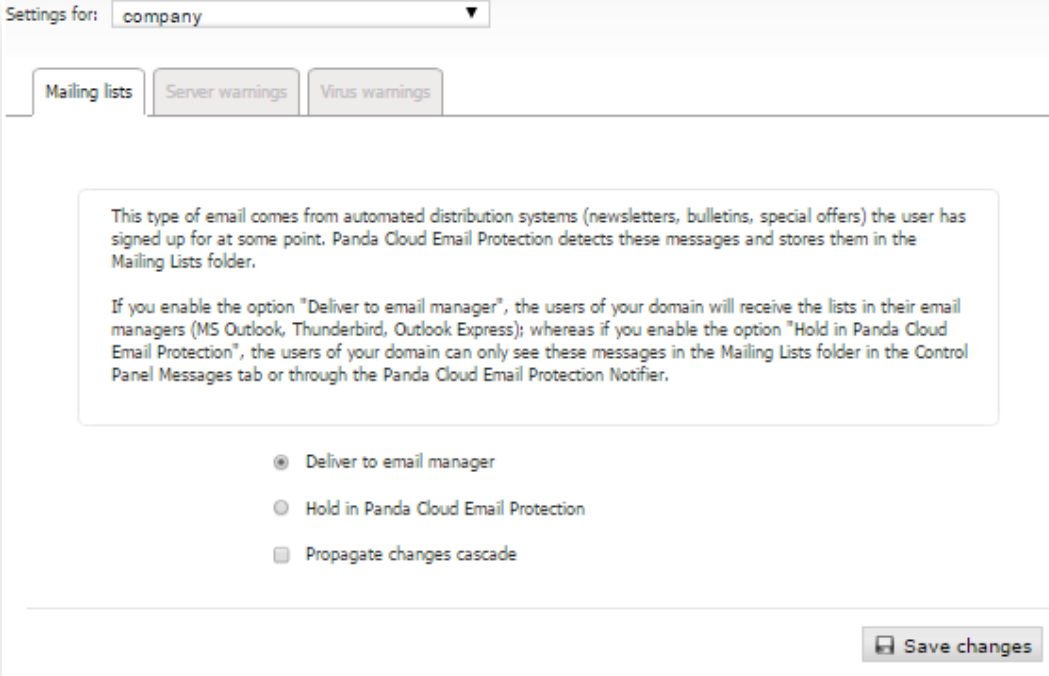
You can decide -for the whole service or for specific domains- whether such emails will be delivered to the end-user, or if they will be saved in separate folders for consultation when required.

2.6.4.1 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 in cascade: It will apply the configuration to every domain and user into the company.



Settings for: 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); whereas if you enable the option "Hold in Panda Cloud Email Protection", the users of your domain can only see these messages in the Mailing Lists folder in the Control Panel Messages tab or through the Panda Cloud Email Protection Notifier.

- Deliver to email manager
- Hold in Panda Cloud Email Protection
- Propagate changes cascade

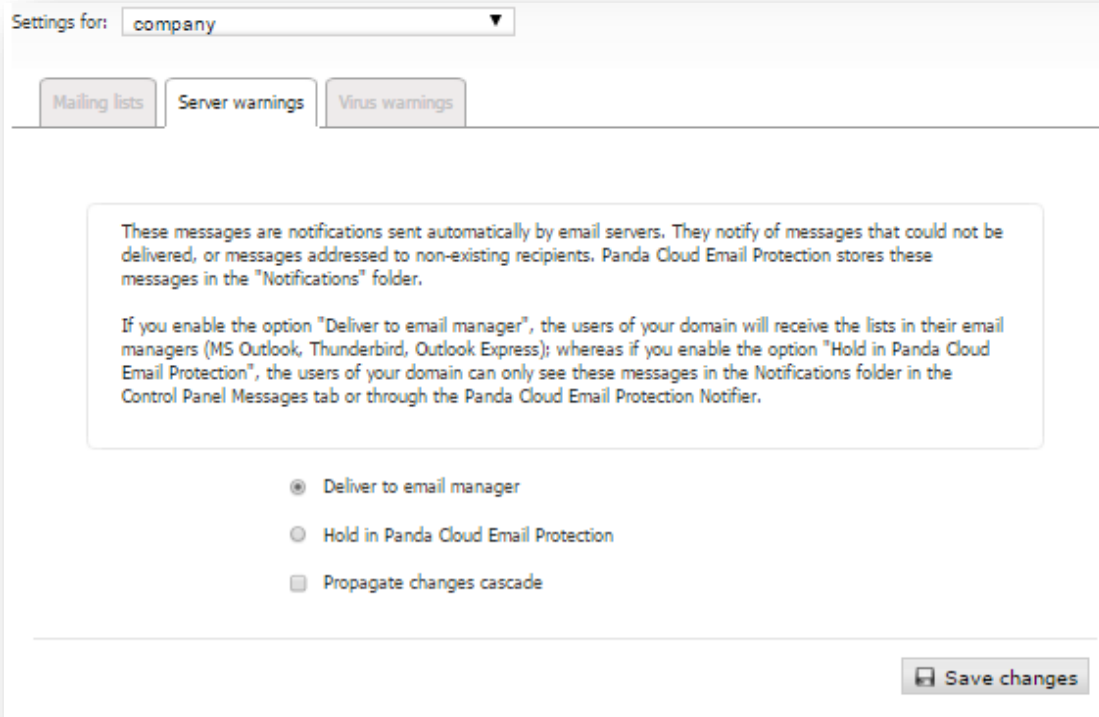
Save changes

2.6.4.2 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. Panda 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 in cascade: It will apply the configuration to every domain and user into the company.



Settings for:

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. Panda Cloud 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); whereas if you enable the option "Hold in Panda Cloud Email Protection", the users of your domain can only see these messages in the Notifications folder in the Control Panel Messages tab or through the Panda Cloud Email Protection Notifier.

Deliver to email manager
 Hold in Panda Cloud Email Protection
 Propagate changes cascade

2.6.4.3 Virus warnings

These emails are notifications sent by Panda Managed Email Protection, reporting the presence of viruses in an email received in your account. Panda 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 in 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

Panda Cloud Email Protection Default message

Customise message [Modify](#)


Allow the domain administrator to customise the message

Deliver/Retain message

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.

2.6.5 Disclaimers

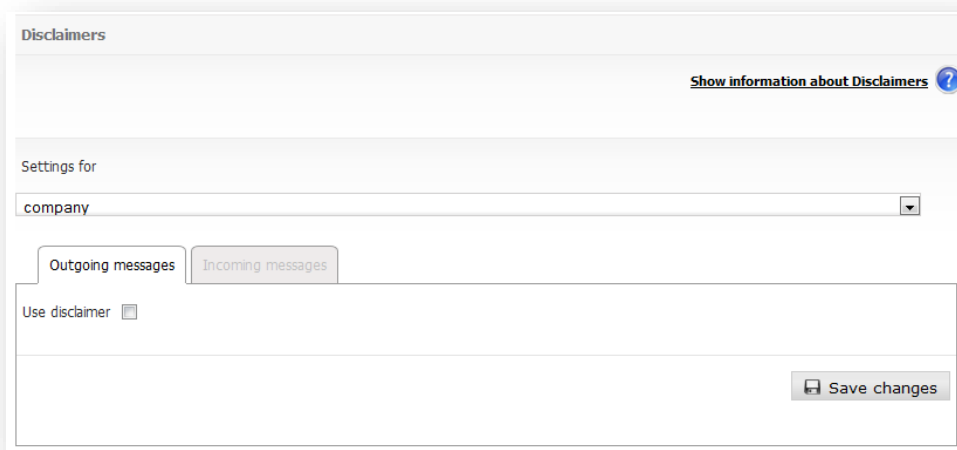
In this section you can set up a text (disclaimer) to be placed automatically at the end of an email, both inbound and outbound email, and you may provide a different setting for each. To include them in outbound mail, it is necessary that outbound email is active and correctly configured through this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



This configuration allows you to:

- Define disclaimers both corporation level and domain level
- Set messages versions both plain text and HTML
- Use a set of variables that will be replaced automatically in every message. For this to work, the disclaimer body must contain the variables in double brackets, as follows:
 - Message arrival date: `[[DATE]]`
 - Message sender: `[[SENDER]]`
 - Message recipient: `[[RECIPIENT]]`

Please note that the use of disclaimers will alter the email content; this could affect those that have been signed through PGP or X.509, making its digital signature non-valid. Email Protection will not be held responsible for any legal implications arising from these modifications.

2.6.6 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

Synchronisation

[Show help about domain synchronisation](#) ?

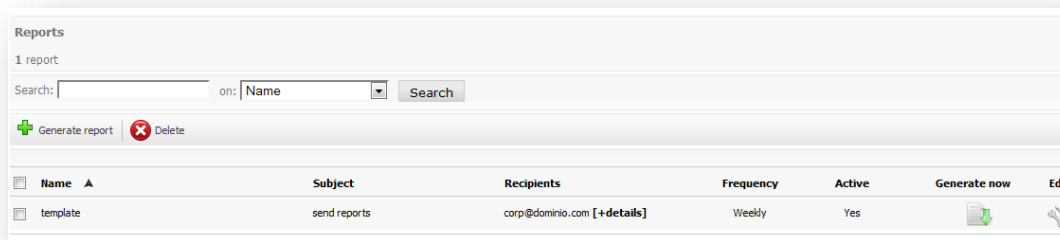
Company setup

	Synchronisation	Synchronisation time	Synchronisation mode	Send synchronisation report
Global configuration (applied to all domains)	<input type="checkbox"/>	Sunday ▾	Manual ▾	<input checked="" type="checkbox"/>

The company has synchronisation: disabled

Domain ▲	Global settings	Personalised settings	Synchronisation	Synchronisation time	Synchronisation mode	Send synchronisation report
domain.com	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	Sunday ▾	Manual ▾	<input checked="" type="checkbox"/>

2.6.7 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 been produced 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/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.

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 most volume of email.
- Top spam addressees: Shows the N users who receive the most spam
- Top virus blocked: 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

Synchronisation [Show information on reports](#) ?

Information for sending the report

Enabled:

(*) Template Name:

(*) Subject:

Domains

All the domains:

Select the desired domains:

Recipients

Company administrator: (user@mail.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:

Filter categories for incoming email

None:

All:

Select those desired:

Valid:

Mailing lists:

Server warnings:

Spam:

Pending validation:

Virus warnings:

Rejected spam:

Graphs on incoming email

Total graphs:

Graph containing the category distribution:

Summary table:

Filter categories for outgoing email

None:

All:

Select those desired:

Rejected spam:

Valid:

Infected email:

Graphs on outgoing email

Total graphs:

Graph containing the category distribution:

Summary table:

(*) Mandatory fields

© 2012 AEGIS Security S.L. | Cloud Email Security 4.0.2.1. Privacy policy and Terms and conditions

2.6.8 Notification due to license limit



- In this section you may define:
 - If you wish to receive notifications due to license limit. The system will notify the configured addresses via email, when the percentage of available licenses for the company is lower than established.
 - Percentage of licenses available that will trigger the notification; it must be a value between 0 and 100.
 - Recipients, up to a maximum of 10 email addresses.

2.6.9 Time Zone

This configuration allows setting the time zone on enterprise level, 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, a domain will have the time zone of the company it belongs to applied and a company will have the time zone the platform that hosts it 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.

2.6.10 Unsubscribe

In order to improve our service, we would appreciate if you please tell us briefly why you have decided to unsubscribe.

Unsubscribe

We would appreciate it if you would briefly indicate the reason why you have decided to unsubscribe. Thank you for helping us to improve our service.

The company **Company**, all of its domains and users will be removed

Reasons:

3. Additional functions

Panda Notifier

3.1 Panda Notifier

The Panda Email Protection Notifier is a utility⁶ which is installed on 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 Panda Email Protection Web console.

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.

⁶ 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.