Contents

1 INTRODUCTION TO PANDA CLOUD EMAIL PROTECTION ....................................................... 5

1.1 WHAT IS PANDA CLOUD EMAIL PROTECTION? .......................................................... 5

1.2 FUNCTIONALITIES ........................................................................................................... 5

2 PANDA CLOUD EMAIL PROTECTION INTERFACE ......................................................... 7

2.1 ADMINISTRATOR ACCESS ............................................................................................. 7

2.2 PANDA CLOUD EMAIL PROTECTION INTERFACE .................................................. 7

2.2.1 Note ............................................................................................................................. 7

2.3 ADMINISTRATION ........................................................................................................... 8

2.3.1 Domains ...................................................................................................................... 8

2.3.2 Users ............................................................................................................................ 9

2.3.3 Users with basic filtering .......................................................................................... 10

2.3.4 Signup mode ............................................................................................................. 11

2.3.4.1 Manual Registration ............................................................................................... 11

2.3.4.2 Automatic Registration by SMTP callout or LDAP ............................................... 11

2.3.4.2.1 Setup of parameters for users search in corporate LDAP .................................... 11

2.3.4.2.1.1 LDAP Server .................................................................................................... 11

2.3.4.2.1.2 Connection ...................................................................................................... 12

2.3.4.2.1.3 Search scope ................................................................................................... 12

2.3.4.2.1.4 Search of user name ....................................................................................... 13

2.3.4.2.1.5 Alias search .................................................................................................... 13

2.3.4.2.1.6 Groups ............................................................................................................ 14

2.4 FILTERING ....................................................................................................................... 14

2.4.1 White list...................................................................................................................... 14
2.4.2 Black list

2.4.3 Services per domain

2.4.4 Services per user

2.4.5 Virus quarantine

2.4.6 Trusted lists by domain

2.4.7 Trusted list by user

2.4.8 Filtering mode by domain
   2.4.8.1 Automatic mode
   2.4.8.2 Guaranteed mode

2.4.9 Filtering mode by user

2.4.10 Rules engine

2.4.11 Outbound email filtering by domain

2.4.12 Outbound email filtering by user

2.4.13 Email logs

2.4.14 NDR Validation
   2.4.14.1 NDR Validation by domain
   2.4.14.2 NDR Validation by user

2.4.15 Anti email spoofing
   2.4.15.1 Anti email spoofing by domain
   2.4.15.2 Anti email spoofing by user

2.5 SETTINGS

2.5.1 Company data

2.5.2 Administrator data

2.5.3 Lists and notices
2.5.3.1 Mailing lists ............................................................................................................................ 30
2.5.3.2 Server warnings ...................................................................................................................... 31
2.5.3.3 Virus warnings ...................................................................................................................... 32
2.5.4 Automatic messages .................................................................................................................. 33
2.5.4.1 Welcome message ................................................................................................................ 33
  2.5.4.1.1 Modify message ............................................................................................................... 33
2.5.4.2 Blocked Email Report .......................................................................................................... 34
  2.5.4.2.1 See templates ................................................................................................................ 34
2.5.5 Disclaimers ............................................................................................................................... 36
2.5.6 Logo ........................................................................................................................................ 38
2.5.7 Language .................................................................................................................................. 39
2.5.8 Unsubscribe ............................................................................................................................ 40
¡Error! Marcador no definido.

3 ADDITIONAL FUNCTIONS .............................................................................................................. 40
3.1 NOTIFIER (ONLY FOR PCs) ..................................................................................................... 40
  3.1.1 Technical Specifications ...................................................................................................... 41
3.2 WEBMAIL ................................................................................................................................. 41
1 Introduction to PANDA CLOUD EMAIL PROTECTION

1.1 What is PANDA CLOUD EMAIL PROTECTION?

PANDA CLOUD 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.

PANDA CLOUD EMAIL PROTECTION consists of a multilayer system which combines protection filters and processes using proprietary technologies (PANDA CLOUD 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.

PANDA CLOUD 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 PANDA CLOUD 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
- Administrators per domain
- Email logs with the possibility of open emails (if you chose this option when you purchase), add senders / IP’s to whitelist / blacklist, classify mails as Valid / Spam
- Trusted lists by User
- Customized filters
- Notification software
2 PANDA CLOUD EMAIL PROTECTION interface

2.1 Administrator Access

PANDA CLOUD EMAIL PROTECTION control panel can be accessed using any browser by typing the following URL: https://mep.pandasecurity.com/admin

![Login Panel](image)

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 PANDA CLOUD EMAIL PROTECTION Interface

PANDA CLOUD 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 ® 7 y 8
- Mozilla Firefox 2.X y 3.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 Domains

Domains

<table>
<thead>
<tr>
<th>Domain</th>
<th>SMTP host</th>
<th>No. of users</th>
<th>Edit</th>
<th>View users</th>
</tr>
</thead>
<tbody>
<tr>
<td>newdomain.com</td>
<td>smtp-newdomain.com</td>
<td>1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

This shows the list of domains registered with PANDA CLOUD 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 domains\(^1\) 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.

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

---

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.
2.3.2 Users

It shows the users list and users alias, 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.
When you bought PANDA CLOUD EMAIL PROTECTION, if the option to enter the users panels was chosen, then an icon will be shown from which a panel will be opened, allowing its use as if you were the final user.

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 password¹, all separated by commas.

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

2.3.3 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

<table>
<thead>
<tr>
<th>Domain List: Choose a Domain</th>
<th>Users with Basic Filtering found: 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search:</td>
<td>Search</td>
</tr>
<tr>
<td></td>
<td>View all</td>
</tr>
<tr>
<td>Create User with Basic Filtering</td>
<td>Delete</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Email address</th>
<th>Edit</th>
<th>Turn into user</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:someone@newdomain.com">someone@newdomain.com</a></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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 PANDA CLOUD 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.

¹ If the user's password is missing, a new one will be randomly generated to be sent to them in the welcome email.
These users will not be counted as PANDA CLOUD EMAIL PROTECTION licenses.

### 2.3.4 Signup mode

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

#### Signup mode

<table>
<thead>
<tr>
<th>Global activation mode</th>
<th>Manual</th>
<th>LDAP</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>☐</td>
<td>☐</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Activation mode by domains</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain</td>
</tr>
<tr>
<td>--------------</td>
</tr>
<tr>
<td>newdomain.com</td>
</tr>
</tbody>
</table>

#### 2.3.4.1 Manual Registration

PANDA CLOUD 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.

#### 2.3.4.2 Automatic Registration by SMTP callout or LDAP

PANDA CLOUD 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 PANDA CLOUD EMAIL PROTECTION if they exist or rejecting the email if they do not. If you select SMTP, make sure your email server is set up to perform the checks. For further information, please contact our Support department.

#### 2.3.4.2.1 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:

#### 2.3.4.2.1.1 LDAP Server

---

3 SMTP server should only provide an affirmative response just for those domain valid-users.
In this section you must specify the LDAP server you are using; this allows suggesting certain configuration values already known for your server.

### 2.3.4.2.1.2 Connection

**Connection**

- **Host**: Enter the IP address or DNS name of LDAP server.
- **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)
  - 639: 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`

### 2.3.4.2.1.3 Search scope

**Search scope**

- **Base DN**: A level
- **Subtree**:

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).

2.3.4.2.1.4 Search of user name

Search of user name

* The attribute containing the email address: mail
   - The attribute only stores the user name
   - The attribute stores the full email address

* LDAP Filter: (objectClass=*)

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.

2.3.4.2.1.5 Alias search

Alias search

Enable alias discovery

* Attribute containing the alias

* LDAP Filter

The field is multivalued

Yes
No

Alias separator:

Is the alias the same object as the mailing address?

Yes
No

Attribute containing the object DN of the real user:

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 attribute\(^4\).
- 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).

### 2.3.4.2.1.6 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.

<table>
<thead>
<tr>
<th>Group membership</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Group membership" /></td>
</tr>
<tr>
<td>Attribute that containing groups to which the user belongs: [Text Field] (Help)</td>
</tr>
</tbody>
</table>

The field is multi-valued

<p>| |</p>
<table>
<thead>
<tr>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Yes" /></td>
</tr>
</tbody>
</table>

Group separator: [Text Field] (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.
- Group separator.

### 2.4 Filtering

In this section you can administer all aspects related to the filtering by PANDA CLOUD EMAIL PROTECTION, applying global settings of domains and users.

#### 2.4.1 White list

A white list may include email addresses, domains or IPs at company scope or at global scope. The connection and antivirus filters will be applied to the emails from IPs at company scope, domains or users in white list. No content filter will be applied.

IPs defined at global scope has greater priority than connection filters and no filter will be applied.

Content filters include the bayesian analysis and the rule engine.

---

\(^4\) 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: ? ) @ ! # $ % & * + - / = ^ ` ~ . { | } “
2.4.2 Black list

A blacklist may include email addresses, domains or IPs at company scope or at global scope. Emails from domains or users of the blacklist will be placed in quarantine after passing through connection filters.

Emails from IPs in this list will be rejected.

2.4.3 Services per domain

You can disable PANDA CLOUD EMAIL PROTECTION antivirus and/or anti-spam filters for the domains in the service.

All filters are enabled by default. If you want to disable one of them, select the corresponding checkbox.

If you want to disable the anti-spam filter, there exists a mode in which content filters will not be applied, but connection filters will still be applied.

If the antivirus filter is cancelled, inbound emails will not go through antivirus filter.

If virus quarantine is enabled, then virus filtering will automatically be enabled. If the virus quarantine is enabled, every time an infected email arrives, a notification will be generated and
sent to the user’s email address (and will also be delivered to the user’s email client according to the user’s preferences); the original email will be listed in the “Virus quarantine” menu, available in the “Filtering” tab. The Company administrator will be the only user with access to this option.

Users with disabled filters are still regarded as licenses.

Option Enable Tagged as Spam allows you to tag the mail classified as spam. Following the "Set up" link you will specify where spam tag will be placed, by selecting among:

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

- Insert the tag after the subject: to insert the specified tag at the end (i.e. as a suffix) of mails' subject.
  For example, 'Free Trip [SPAM]'

The setting provided by the system by default is:

- Tag of Spam: [SPAM].

- The tag will be placed before mails' subject.

Enable Tagged as Spam has the following implications:

1. The following "automatic messages" will not be sent to end users:
   1. Welcome message.
   2. Blocked mails' report.
   3. Validation of mails' senders (Guaranteed filtering mode).
   4. Messages of registration by promotion (Registration by promotion mode).

2. Emails will not be stored into users' mailboxes.

3. The "Tagged as Spam" is only compatible with the automatic filtering mode, so the email firewall will work in this mode, even when the domains or users have configured the use of guaranteed filtering mode. 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.

4. If the registration by promotion mode is selected and you begin to use tagged as spam, then registration mode will be forced to "Manual", you can not select this mode when the option of tagged as spam is active.
2.4.4 Services per user

You can disable the PANDA CLOUD EMAIL PROTECTION antivirus and/or anti-spam filters for the users in the service.

All users take their setting from their domains by default, ("Same as domain" option) If you want to disable one of them, select corresponding checkbox.

If you want to disable the anti-spam filter, there exists a mode in which content filters will not be applied, but connection filters will still be applied.

If the antivirus filter is cancelled, inbound emails will not go through antivirus filter.

2.4.5 Virus quarantine

This option allows the administrator to:
- See the emails in the list.
- Download email attachments.
- Delete emails.

**Virus quarantine**

<table>
<thead>
<tr>
<th>Sender</th>
<th>Subject</th>
<th>Date</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:virus@virus.com">virus@virus.com</a></td>
<td>our vacations</td>
<td>06/09/2009</td>
<td>1.71 KB</td>
</tr>
<tr>
<td><a href="mailto:virus@virus.com">virus@virus.com</a></td>
<td>look at this</td>
<td>06/09/2009</td>
<td>1.7 KB</td>
</tr>
</tbody>
</table>

2.4.6 **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 PANDA CLOUD 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**

<table>
<thead>
<tr>
<th>Domain</th>
<th>Global</th>
<th>Enabled</th>
<th>Disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>all-the-domains</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
</tr>
</tbody>
</table>

*Save*
2.4.7 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 PANDA CLOUD EMAIL PROTECTION confirms as safe.

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

trusted list by user

<table>
<thead>
<tr>
<th>Domain:</th>
<th>moedomain.com</th>
</tr>
</thead>
<tbody>
<tr>
<td>Settings:</td>
<td>Trust list disabled</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Full name A</th>
<th>Email address</th>
<th>Same as domain</th>
<th>Enabled</th>
<th>Disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test User</td>
<td><a href="mailto:testuser@moedomain.com">testuser@moedomain.com</a></td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
</tr>
</tbody>
</table>

2.4.8 Filtering mode by domain

Messages are filtered by content to determine whether a message is valid when PANDA CLOUD EMAIL PROTECTION cannot determine whether the sender is a spammer through any connection filters, white lists or black lists.

In this case, PANDA CLOUD EMAIL PROTECTION offers two filtering modes:

2.4.8.1 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.

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

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

**Filtering mode by domain**

<table>
<thead>
<tr>
<th></th>
<th>Automatic</th>
<th>Guaranteed</th>
</tr>
</thead>
<tbody>
<tr>
<td>All the domains</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Spam filtering mode**

<table>
<thead>
<tr>
<th>Domain</th>
<th>Global</th>
<th>Automatic</th>
<th>Guaranteed</th>
</tr>
</thead>
<tbody>
<tr>
<td>domain.com</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>other-domain.com</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2.4.9 **Filtering mode by user**

PANDA CLOUD EMAIL PROTECTION filtering mode can be specified individually for each user.

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

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

- Delete attachments from an email
- Flag an email as Spam or valid
- Move an email to the trash can
- Forward or send a copy of an email to a specified recipient
- Take no action on the 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”.

If the sender of the email belongs to the valid senders’ list (White list), or you select “without anti-spam” from the option “Services by domain” or “Services by users”, content filters will not be applied (anti-spam and Rule Engines)

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 o X.509, making its digital signature non-valid. PANDA SECURITY shall not be liable for any legal consequences arising from these modifications.
If you select “Attached file of size”..., the values specified will be in KB, e.g. 25, means 25 KB; 25000, means 25000 KB (25MB).

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

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

**Visa:** XXXX XXXX XXXX XXXX

**MasterCard:** XXXX XXXX XXXX XXXX

**Maestro:** XXXX XXXX XXXX XXXX

**American Express:** XXXX XXXXXX XXXXX

**Diners:** XXXX XXXXXX XXXX

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

### 2.4.11 Outbound email filtering by domain

Management of outbound email filtering lets you configure PANDA CLOUD EMAIL PROTECTION to enable for outbound mail.

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

This kind of filtering is disabled by default. If you need to enable it, just select the “Outgoing mail filtering” checkbox. If you want to limit the number of recipients for outbound messages, you can enable this feature by selecting the “Use limit of recipients” checkbox. This lets you limit the number of recipients allowed for a single email message, which will be rejected if it exceeds this
value. The use of the recipients limit is disabled by default. Permitted values for this restriction range from 1 to 999.

**Outbound email filtering by domain**

<table>
<thead>
<tr>
<th>Company setup</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Global configuration (applied to all domains)</td>
<td>Outbound email filtering</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Domain setup</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain</td>
<td>Global settings</td>
</tr>
<tr>
<td>domain.com</td>
<td></td>
</tr>
<tr>
<td>other-domain.com</td>
<td></td>
</tr>
</tbody>
</table>

Once the filtering of outbound email is configured in PANDA CLOUD EMAIL PROTECTION, the client’s email server must also be set up to ensure that email is sent through PANDA CLOUD EMAIL PROTECTION.

**2.4.12 Outbound email filtering by user**

Management of outbound email filtering lets you configure PANDA CLOUD EMAIL PROTECTION to enable filtering for outbound mail. You can set up this kind of filtering for individual users.

**Outbound email filtering by user**

| Domain: | domain.com |  |
|----------------|---|
| Search: | Email address |  |
| Full name | Email address | Same as domain | Own settings | Outbound email filtering | Use limit of recipients |
| Test user 1 | test1@domain.com | R | O | | |
| Test user 2 | test2@domain.com | R | O | | |
| Test user 3 | test3@domain.com | R | O | | |
| Test user 4 | test4@domain.com | R | O | | |
2.4.13 Email logs

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

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

Email logs

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 mail
- Rejected outbound mail

Possible statuses 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”.
- 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 ((png) which reflects this situation.

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.

2.4.14 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

---

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)
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.

2.4.14.1 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

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

- **NDR Validation**: enabling this validation implies that PANDA CLOUD 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 PANDA CLOUD EMAIL PROTECTION will not receive notifications from the server or automatic replies if the NDR validation is enabled.

2.4.14.2 NDR Validation by user

Management of NDR validation by user allows each user to enable the NDR Validation. This validation implies that PANDA CLOUD 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 PANDA CLOUD EMAIL PROTECTION, will not receive notifications from the server or automatic replies if the NDR validation is enabled.

**NDR validation by user**

<table>
<thead>
<tr>
<th>Full name</th>
<th>Email address</th>
<th>Same as domain</th>
<th>Own settings</th>
<th>NDR Validation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test User</td>
<td><a href="mailto:testuser@newdomain.com">testuser@newdomain.com</a></td>
<td>@</td>
<td>O</td>
<td>O</td>
</tr>
</tbody>
</table>

### 2.4.15 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).

#### 2.4.15.1 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 nd receiver of the email are firewall protected and they belongs 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*.

**Anti email spoofing by domain**

![Anti email spoofing by domain settings](image)

2.4.15.2 **Anti email spoofing by user**

The anti email spoofing by user will allows 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**

![Anti email spoofing by user settings](image)

2.5 **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 PANDA CLOUD EMAIL PROTECTION can launch messages automatically, etc.

2.5.1 **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 PANDA CLOUD 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**

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Company name</td>
<td>0001847070</td>
</tr>
<tr>
<td>Address</td>
<td></td>
</tr>
<tr>
<td>Address 2</td>
<td></td>
</tr>
<tr>
<td>Zip code</td>
<td></td>
</tr>
<tr>
<td>Phone</td>
<td>1234567890</td>
</tr>
<tr>
<td>Website address</td>
<td></td>
</tr>
<tr>
<td>Contact person</td>
<td>Contact Person</td>
</tr>
<tr>
<td>Contact email</td>
<td><a href="mailto:contact@someemail.com">contact@someemail.com</a></td>
</tr>
<tr>
<td>Sender of automatic messages</td>
<td><a href="mailto:peter@dominon.com">peter@dominon.com</a></td>
</tr>
</tbody>
</table>

(*) Mandatory fields

### 2.5.2 Administrator data

This is where information about the administrator must be entered.

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

**Administrator data**

<table>
<thead>
<tr>
<th>Tab</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>Personal information</td>
<td>* Name and surname: John Doe</td>
</tr>
<tr>
<td></td>
<td>Phone:</td>
</tr>
<tr>
<td></td>
<td>Address:</td>
</tr>
<tr>
<td></td>
<td>City:</td>
</tr>
<tr>
<td></td>
<td>Country:</td>
</tr>
</tbody>
</table>

(*) Mandatory fields

[Save button]
2.5.3 Lists and notices

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

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

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

2.5.3.1 Mailing lists

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

If you enable the option “Deliver to email manager”, the users of your domain will receive the lists in their email managers (MS Outlook, Thunderbird, Outlook Express). However, if you enable the option “Hold in PANDA SECURITY”, the users in your domain will only see these messages in the Mailing Lists folder -in the Control Panel Messages Tab-, or through the PANDA SECURITY Notifier.
2.5.3.2  Server warnings

These messages are notifications sent automatically by email servers. They inform of messages that could not be delivered, or messages addressed to non-existing recipients. PANDA SECURITY 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). However, if you enable the option “Hold in PANDA SECURITY”, the users in your domain will only see these messages in the Notifications folder -in the Control Panel Messages Tab-, or through the PANDA CLOUD EMAIL PROTECTION Notifier.
2.5.3.3  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 SECURITY 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). However, if you enable the option “Hold in PANDA SECURITY”, the users in your domain will only see these messages in the Virus Warnings folder—in the Control Panel Messages Tab, or through the PANDA SECURITY Notifier.
2.5.4 Automatic messages

PANDA CLOUD EMAIL PROTECTION can automatically send three kinds of messages to users:

2.5.4.1 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.

PANDA CLOUD 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.

2.5.4.1.1 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 PANDA CLOUD EMAIL PROTECTION Email Firewall distributions. Before saving the message you can preview it by clicking “Preview”
2.5.4.2  **Blocked Email Report**

This details messages which have been blocked by PANDA CLOUD 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 PANDA CLOUD 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.

### Automatic messages

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The report is sent daily by default, and reports on the messages that have been blocked by Panda Cloud Email Protection. The report lets users retrieve messages classified as spam by mistake, and add their senders to the user's white list. This way, the report becomes a powerful tool to adapt the service to each user's needs.

- Show the domain administrator to customize the report
- Default message: [Preview]
- Customize message: [See templates]

Select template

- Do not send report
- Send daily report
- Send weekly report

[Save changes]

### See templates

A new screen appears with the following options:

- **Create Template:** This creates a new message based on PANDA CLOUD 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.
Automatic messages

Here you can set up different data for the company.

Information for sending the report:

(*) Template Name:

(*) Sender Name:

(*) Sender email address:

(*) Subject:

Through the following form you can edit the content of the templates you have saved, or create new ones.

When creating a message you have the possibility to select the content you want in the report and the one you want to narrow.

Message content:

☒ [ ] user@example.com
☒ [ ] XXXXXX
☒ [ ] XXXXXX
☒ [ ] YYYYYYYY (spam) / ZZZZZZZZZZ (pending validation)

☒ [ ]

☑ [ ]

☑ [ ]

from@example.com subject

from@example.com subject

(*) Mandatory fields
· **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.

### Automatic messages

<table>
<thead>
<tr>
<th>Settings for</th>
<th>company</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search</td>
<td>Template</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Template</th>
<th>Subject</th>
<th>Edit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Report template</td>
<td>blocked email report</td>
<td></td>
</tr>
</tbody>
</table>

### 2.5.5 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:
  
  o Reception date of the message: [[DATE]]
  o Sender of the message: [[SENDER]]
  o 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 SECURITY 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 o X.509, making its digital signature non-valid. PANDA CLOUD EMAIL PROTECTION will not be held responsible for any legal implications arising from these modifications.

2.5.6 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, but it will be automatically edited in order 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 firewall logo
- Using the customized logo (“Customized logo” option)
- Do not use a logo (“Disable logo” option)
2.5.7  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.
3 Additional functions

3.1 Notifier (Only for PCs)

The PANDA CLOUD EMAIL PROTECTIONNotifier is a utility which is installed on the PC and offers complete control of email management.

(*) 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.

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.
3.1.1 Technical Specifications
The notifier works in the following operative systems, Windows 2000 Professional+ and Windows XP Professional+; the operative system must support multiuser.

3.2 Webmail
PANDA CLOUD EMAIL PROTECTION has a webmail service (email reader through the Web browser) on http://webmail.mep.pandasecurity.com. From PANDA CLOUD EMAIL PROTECTION Webmail, you can write emails as you would from any other online email application (Terra, Yahoo, Hotmail...).