

Outgoing filtering

- [How does the outgoing filtering work?](#)
- [How to order and setup outgoing spam filter?](#)
- [Is it possible to activate the option "valid sender address required"?](#)
- [Outgoing mail is quarantined](#)
- [Which SPF record to use with a spam filter?](#)
- [🇪🇸🇪🇸🇪🇸🇪🇸 Cómo configurar el filtro de spam de salida](#)

How does the outgoing filtering work?

Question:

What is outgoing email filter and how it works?

Answer:

The outbound email filtering prevents spam from being unknowingly sent out of your network through a compromised account or script. You can protect your entire network by monitoring all outgoing email traffic, identifying and locking down compromised user accounts. Outgoing filtering helps you to keep your network free of outbound spam and IP addresses away from blacklists.

Out going filter work as follow.

SpamExperts outbound spam and virus filter is a gateway solution. Activation is done via the web interface or by using the API directly. Configuration is done through a smart host setup where all outbound emails from your network are re-routed through the filtering systems, before going out to the internet. The alternative is to authenticate on a per user basis where the filtering systems are directly used as outgoing SMTP servers.

Once configured outgoing e-mails are no longer sent directly to the receiving mail server, but are re-routed via the SpamExperts cluster. If the e-mail is valid, it's forwarded to the final recipient. If it's spam, it is blocked at the cluster.

DEPLOYMENT

The actual filtering of the messages is done on the highly redundant SpamExperts Hosted Cloud. This SaaS solution is fully managed, maintained, and 24/7/365 monitored by SpamExperts.

CONFIGURATION

For new users the outgoing server that should be configured is **683.smtp.antispamcloud.com** on port **587**.

For users that still use the bundled solution of SpamExperts the following outgoing server applies:

outgoing.mail.registrar.eu on port **587**.

Of course the sending server should authenticate itself to the cluster. Authentication can be done on 2 levels: as *domain user* or as *IP user*:

- **Domain user**

For every filter that is created, Openprovider automatically creates a user for outgoing e-mail. Use those data to authenticate at the SMTP server. Now your e-mail will be filtered.

- **IP user**

It is also possible to filter all e-mail from a certain server, for example your shared hosting server. Do this by creating an *IP user*: there is no need to log in with username and password to the SMTP server, as the cluster will accept all connections from the specified IP address. Please note that only a limited number of IP users is available and this number depends on your bundle size.

How to order and setup outgoing spam filter?

Question

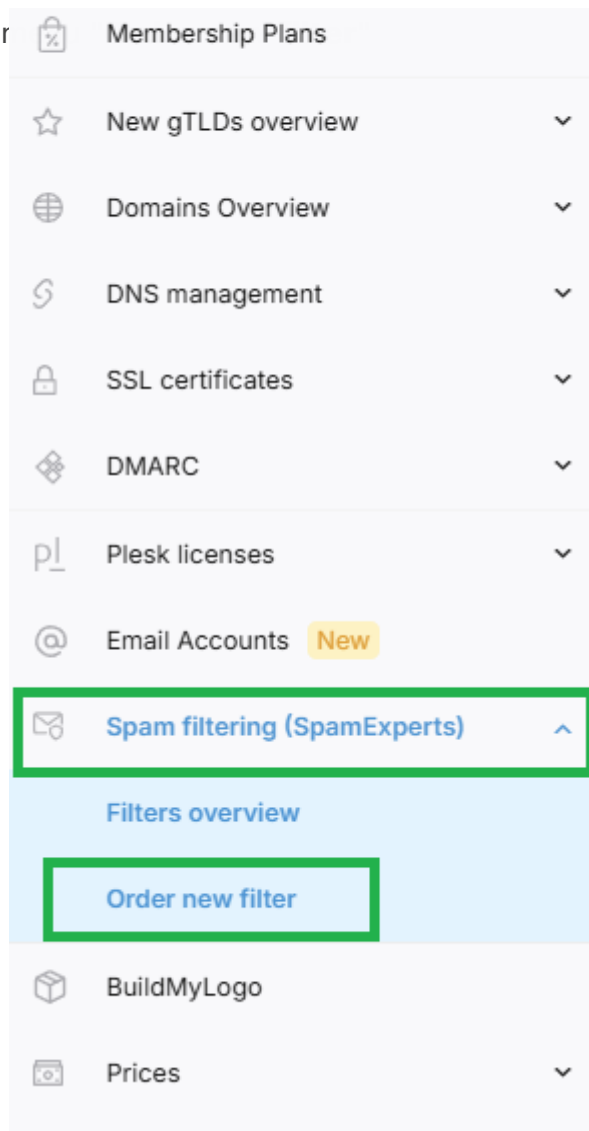
How to order and setup outgoing spam filter?

Answer:

To order a outgoing filter you need to follow the next steps:

1) Navigate to RCP Dashboard (Reseller Control Panel) >> **Spam filtering (SpamExperts)**

2) Click on sub r



3) In the next screen:

- Enter the domain name.
- Select "Outgoing filter"
- Enter mail server address

Fair use policy

Every mailbox that is created beyond the limit of 1000 mailboxes per domain will be invoiced at € 0,10 per month (excl. VAT). The price for e-mail archiving is per 10 GB.

Domain name

☐ Incoming filter — € 1.25

Products

☒ Outgoing filter — € 1.25

☐ E-mail archiving — € 2.99

Monthly payment € 1.25

Mail server

Port

 Add mail server

Aliases

 Add alias

[Back to overview](#)

[Save](#)

4) Save the filter:

To configure your outgoing Spamfilter, you need to use the credentials to login to <https://login.antispamcloud.com> or simply click on the **"Go to spam filter control panel"** button to login directly from Openprovider Control Panel.

Filter details

Products	E-mail archiving Incoming filter Outgoing filter
Destination mail server	testdomainz1909.com:25
Username	
Password	
Expiration date	2025-02-04 07:56:21

Back to overview

Go to spam filter control panel

In the SpamExperts control panel, navigate to **Outgoing > Manage users**

Logged in as: .com | Domain User

Dashboard

General

Reporting

Incoming

Incoming - Protection Settings

Outgoing

Logs

Manage users

Manage identities

Manage

The following selected pas

Page 1 of 1. Total

Us

Page 1 of 1. Total

Add a user

From the manage users page, you can create a new user using using any of three forms of authentication, via IP address or IP range, via user, or via domain. If you don't know which authentication you need, we recommend referring to the SpamExperts knowledge base article [Outgoing Users/Authentication Methods](#).

Note: If the domains are not having a static/fixed IP address for SMTP, use the "**Authenticating Domain**" option.

Manage users ([redacted])

The following users are permitted to send mail through the filtering system. Three types of user exist: an authenticating domain uses the domain name and selected password for SMTP AUTH, an authenticating user uses the username@domain and selected password for SMTP AUTH, and an authorised IP does not require SMTP AUTH (any connections from the IP or IP range are considered authenticated).

To search for a user, just type and press enter

Search

Page 1 of 1. Total items: 1. Items per page: 50

 Username/IP ▲	Auth Type	Automatic unlock
 [redacted]	Authenticating Domain	Not locked

Page 1 of 1. Total items: 1. Items per page: 50

Add a user

Authenticating IP or range (e.g. a smarthost)

Authenticating User

Authenticating Domain

Domain:

Password:

✓ Add ⓘ

To configure your sender policy framework (SPF) you'll be using the "hosted cloud solution" for the Openprovider license the following configurations apply:

- SMTP hostname: **683.smtp.antispamcloud.com** on port **587**
- SPF record "**v=spf1 include:spf.antispamcloud.com -all**"

If you have questions about how to set up a particular mail transfer agent (MTA) the SpamExperts knowledge base article [MTA configuration](#) offers a detailed guide.

For more information about the outgoing spam filter you can read the [knowledgebase article from SpamExperts](#).

Is it possible to activate the option "valid sender address required"?

Question:

Is it possible to activate the option "valid sender address required"?

Answer:

The sender verification is usually off and isn't something that is normally available on the Hosted Cloud.

This toggle is available with the Local cloud but not for general usage with the hosted solution.

Furthermore, it is recommended to only disable sender verification as a last resort, with all other options exhausted. The sender verification is an important anti spam check and should be used for optimal message filtering.

Outgoing mail is quarantined

When an outgoing mail is quarantined, please check the reason. Using the outgoing log search, the mail can be found. Using the "Columns to be displayed" option, you can customize the log output and add "Sub Class" and "Extra Class." These columns will give more information on why the mail is blocked.

Summary row: Columns to be displayed: ⓘ

None ▾ Customise ▾ 🔍

- ☒ Timestamp
- ☒ Sender
- ☒ Recipient
- ☐ Sender hostname
- ☐ Sender IP
- ☐ Sender location
- ☐ Bytes received
- ☐ Bytes sent
- ☒ Main class
- ☐ Sub class
- ☐ Extra class
- ☐ Error class
- ☐ From

If these columns show the class "contains-macro" it means that there is an attachment in the mail that is often used by spammers. Since Spamexperts offers a shared anti-spam solution and want to keep their server reputation healthy, they do not permit any file types that are known to be commonly used by spammers, such as the sending of macros and exe files in attachments.

We recommend end users do not mimic the kinds of behaviour seen by spammers to prevent any unnecessary delays in mail. Possible options are to use password protected zip files for any one off email attachments or any number of other common file transfer solutions if these kinds of files are genuine and shared regularly.

Outgoing quarantined mail can only be released by Spamexperts themselves. If the mail is quarantined for another reason, we can have the mail evaluated and possibly released if you

contact us. Otherwise it's advised to check the error code and adjust the mail accordingly.

Which SPF record to use with a spam filter?

Question

Which SPF record should one use for a spam filter?

Answer

If you want to create an SPF record for your domain when using Openprovider platform you can use the following value.

```
"v=spf1 include:spf.antispamcloud.com -all"
```

If you are still using our older bundled solution, then you can use this SPF record:

```
"v=spf1 a:spf.spamexperts.registrar.eu -all"
```

It includes all our servers and will allow your users to not be flagged as spammers when sending emails.

For more information about the SPF record, please refer to [this article](#).

📧📧📧📧 Cómo configurar el filtro de spam de salida

1. In the control panel, click on "Spam Filters / Add New Filter".
2. On the next screen, add the domain, select "Outbound Filter," and add the mail server. Click Save.

Añadir configuración del filtro de spam

To add a new domain to the spam filter, enter the domain name and the mail servers that should receive the filtered e-mail messages.

More advanced settings can be configured afterwards via the spam filter control panel.

If you use your own nameservers, configure the following MX records for this domain: **mx.spamexperts.com**, **fallbackmx.spamexperts.eu**, **lastmx.spamexperts.net**.

Política de uso

Cada cuenta de correo que se cree pasado el límite de 1.000 cuentas por dominio será facturado a 0,10 € al mes (iva excluido). El precio para espacio de archivo es por 10GB por dominio.

Nombre de dominio

Productos

☐ Filtro de entrada — ₹ 128.41

☐ Filtro de salida — ₹ 128.41

☐ Archiving de correos electrónicos — ₹ 307.15

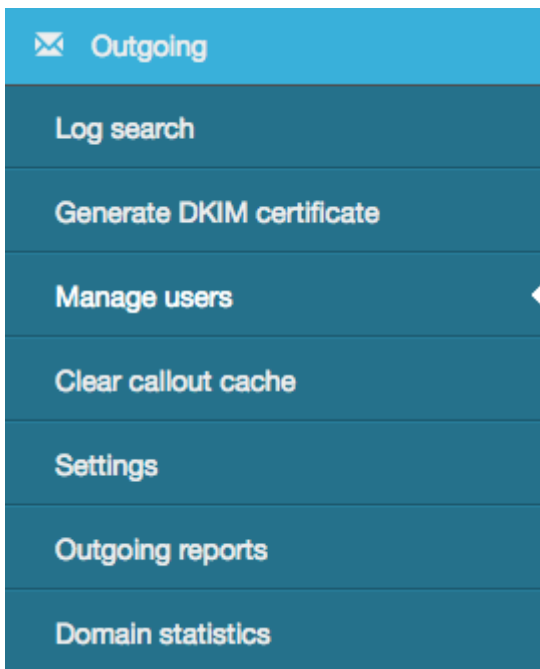
Mensualidad

₹ 0.00

3. Configure your SMTP server credentials by accessing the SpamExpert filter. You can do this by clicking the blue button in the control panel.

[Go to spam filter control panel ↗](#)

- 4) Dentro del panel, en Outgoing, ves a Manage users.



Here you need to configure 1 of the 3 forms of authentication.

Add a user

Authenticating IP or range (e.g. a smarthost)

Authenticating User

Authenticating Domain

We recommend using the Authenticating Domain, where the username will be the domain and where you can set the password.

5) Now you will need to configure the mail server's SMTP to send emails through the filter.

The outgoing server must be configured for **683.smtp.antisipamcloud.com** for port **587** .

For authentication, you must set the username and password.

6) Once this is done, please make sure to update your spf to include spamexperts.

For this, add the following spf:

"include:spf.antisipamcloud.com -all"

or add **:683.submission.antisipamcloud.com** to your existing spf record.