Getting started with Inbound

The Incoming Filtering service on the SpamExperts Hosted Cloud can be started by purchasing our product, or by beginning a free trial.

• Login

To log in to our Control Panel interface you need to go to the control panel, available through your user-account. From here choose your domein and click on the SpamExperst tab.
After you are successfully logged in, you will notice the Control Panel Dashboard and several tables with buttons for all available features.

• Add domain

To add a domain, please read the manual on How to Add a Domain.
If you do not have a specific destination server route to add from the start, the Control Panel will automatically fill in the destination route for you, with a default destination port 25.

• Configure MX records

After setting the destination route, you need to add our **MX Records** in your domain **DNS Settings**, in order to point to the SpamExperts Hosted Cloud routes. See our article on changing your MX Records.
Optionally, after completing this step, you can let the SpamExperts team know you have switched the MX-records, so we can double-check everything is set correctly.

Now you're all done, within 24 hours you should be "Simply SpamFree"!

In case you are not 100% spam free within this timeframe, please read the following Knowledge-base article or contact our dedicated support team.

Getting started with Outbound

The outgoing filtering solution is operating independently from the incoming email solution and can be used to relay outgoing email.

Configuring the SpamExperts side

The first thing you will need to do, is to create an outgoing user. Here you have 3 options:

1. IP authentication
2. Per domain authentication
3. Per user authentication

If you wish to filter an entire server, then the IP authentication will likely be the best and fastest way forward.

Please do note that when you choose an IP authenticated outgoing user, then all traffic from all domains that come from this authenticated IP will be logged on the outgoing user domain that the IP is assigned to.

Per domain and per username authentication works very well when you want to have logging on a per domain or user base. Using this type of authentication requires you to configure your MTA to authenticate with a user and a password for each domain.

Creating the outgoing user

1. Login to the SpamExperts Control Panel via https://cloud.internl.net/
2. Add domain (if using IP authentication it's advised to create a domain specifically for this. For example, you can use your server hostname as the domain. This domain will be used for logging and statistical purposes).
3. Navigate to the newly created domain
4. Click "Manage Outgoing users"

5. Add Outgoing User (If using IP authentication, please add the IP or range of the sending mail server)
6. Edit the Outgoing user settings. Here you can configure the limits, Identification header, and various other settings. More information can be found **here**.

   We would strongly recommend that an Identity header is set for all outgoing traffic. This makes monitoring and taking action against spammers much easier.
7. Click save

Configuring the Abuse address

When using the Outbound filter, its highly recommended to setup an address to receive the abuse reports that are sent when outbound messages are blocked. To do this, please do the following:

1. Click "Outgoing settings"
2. Add abuse address
3. Click save.

Please do note, that the address that is configured should be an address that has no inbound filtering, and not a "freemail" address as these can often cause problems in receiving the reports. More information on the ARF reports can be found here. It's also possible to use other methods of monitoring the outbound spam, if using ARF reports is not possible. For example you may use using API's, CSV reports and/or IMAP. Full details on the options can be found in the following article - Abuse Reporting Format (ARF).
Please do ensure that when spammers are reported in your network, either via ARF reports or other means, that these problem sources (senders, scripts, etc) are dealt with directly.

Configuring outgoing delivery IP (Optional: Local Cloud only!)

By default, the filtering servers will use the primary IP for both inbound and outbound traffic. It's possible to configure specific outbound delivery IP's for your senders. To be able to do this you will need at least 2 IPs per server. This is often very useful if you want to seperate out your traffic for senders. Instructions on how to do this can be found on our Delivery IP management page here.

- # Configuring your domains

Setting up SPF

Hosted Cloud users

Please see here for details

Local Cloud users

We recommend to create a similar DNS hostname as above, however for SPF we would recommend to add all cluster IP's to the hostname, so that if IPs are changed/rotated, no changes are needed to be made to senders SPF records.

```
spf.example.tld > A > Primary IP 1st server

spf.example.tld > A > Secondary IP 1st server

spf.example.tld > A > Tertiary IP 1st server

spf.example.tld > A > Primary IP 2nd server

spf.example.tld > A > Secondary IP 2nd server

spf.example.tld > A > Tertiary IP 2nd server
```

If your sending domains already use SPF, then you simply need to add **"a:spf.example.tld"** to their existing TXT record. If they do not have a SPF record, and you wish to configure this, (and restrict all email to the SpamExperts server), then you can create something like this: **"v=spf1 a:spf.hostname.tld -all"**

Setting up DKIM

If your sending domains already sign with DKIM, then this should not be changed. We will simply forward the DKIM signed messages along to the recipient. If there is no DKIM signing, you can decide to either sign this on your sending MTA, or sign with SpamExperts. It's not obliged to sign with DKIM, however it often helps to "authenticate" as much as possible your senders.Information on how to setup DKIM with SpamExperts can be found here.

Setting up your SMTP hostname

Hosted Cloud users

- Trial users:
- SMTP Hostname: **smtp-trial.antispamcloud.com**
- Port: **587**
- Licensed Users: Please contact **support@spamexperts.com** for your custom SMTP (and SPF) hostname

Local Cloud users:

We would highly recommend to create a DNS round robin type hostname here for redundancy. An example here would be (for a cluster with 3 filtering servers):

```
smtp.example.tld > A > Primary IP 1st server

smtp.example.tld > A > Primary IP 2nd server

smtp.example.tld > A > Primary IP 3rd server
```

Using a setup like this means that if a server would be unreachable, the other configured servers can automatically pick up the traffic. To spread the load across the servers, utilize a low TTL for these records (60-300) for traffic randomization.

Configuring your MTA

Configuring your MTA should be very simple. We have mutiple examples per MTA which can be foundhere. Some mailservers are more versatile than others, so depending on what systems you are using configuration options can be (very) limited.Once your MTA is correctly configured, outbound messages should now be relayed though your SpamExperts filtering server(s).

Additional notes

Connection Limits

The filtering servers by default will accept a maximum of 10 concurrent connections from your servers. This ensures optimal delivery speeds. To prevent your server from getting temporary rejects "421 Too many concurrent SMTP connections from this IP address; please try again later." and queuing the messages, please ensure to configure your MTA to open a maximum of 10 connections concurrently. This will prevent a backlog building up on your server(s).

Available Outgoing Ports

Default outgoing port is 587 (supports STARTTLS which will be automatically employed if the connecting server supports it). Port 465 can be utilized but chances of needing to use this are very rare (please first check with our support team). Optionally a custom port can be opened to accept outgoing email (supports STARTTLS) for Local Cloud users only. In case you wish to use port 25 for outgoing email, you'll need to specify a secondary IP which will be configured to listen to port 25. For custom changes please contact support.

Outgoing License Size

When ordering outgoing licenses, please be aware that 1 IP as a smarthost does not count as one license. We calculate the number of outgoing domains and tally this to your number of outgoing licenses.

Counting Outgoing sending domains

Often when using IP authentication, it's good to see how many outgoing user domains your clients are sending from. It's possible to check and count these via the interface. Please see here on steps to do this.