How to Configure Libraesva for Google G-Suite

This article is a guideline to configure Google G Suite, Business and Education editions, with Libraesva ESG.

Inbound Configuration

Google Inbound Gateway

- Log into the Google G Suite Domain Management Portal.
- Navigate to **Apps > G Suite > Settings for Gmail > Advanced settings**
- Find **Inbound gateway** and enter the public Libraesva ESG IP address

×**Note:** Make sure to flag the checkbox “Only let users receive email from the email gateways listed above”. All other email will be rejected.
With this configuration Google will also route internal mail (from your own domain to your own domain) through ESG. This will provide visibility into internal email traffic. In order not to perform spam checks on internal email you can add a whitelist for email from your domain (security checks will still be performed).

If you want internal email to remain within Google and not being routed through ESG read the paragraph “How to bypass ESG for internal email” below.

See also Google official documentation for inbound mail gateway

Add relay to Libraesva Email Security Gateway

To add a domain and forward clean emails to Google Apps, navigate to **System > Settings & Relay Configuration** and select **Domain Relay > New**. Fill in the fields as follows:

- *Domain*: specify your domain, the one you have with Google Apps
- *Mail Server*: **aspmx.l.google.com**
- *Port:*: **25**
- *Use MX*: **NO**.

- *Recipient Verification*: **Dynamic Verification** (or “Disabled” if you enabled a “catch-all address”)
- *Dynamic Verification Server Address*: **aspmx.l.google.com**
- *Dynamic Verification Port*: **25**
- *Domain Anti-spoofing*, set it to **SPF**.

Finally, remember to add the a MX record with hightest priority (less weight) to your ESG appliance to route mail flow through Libraesva ESG.

Outbound Configuration (optional)

This is an optional configuration.

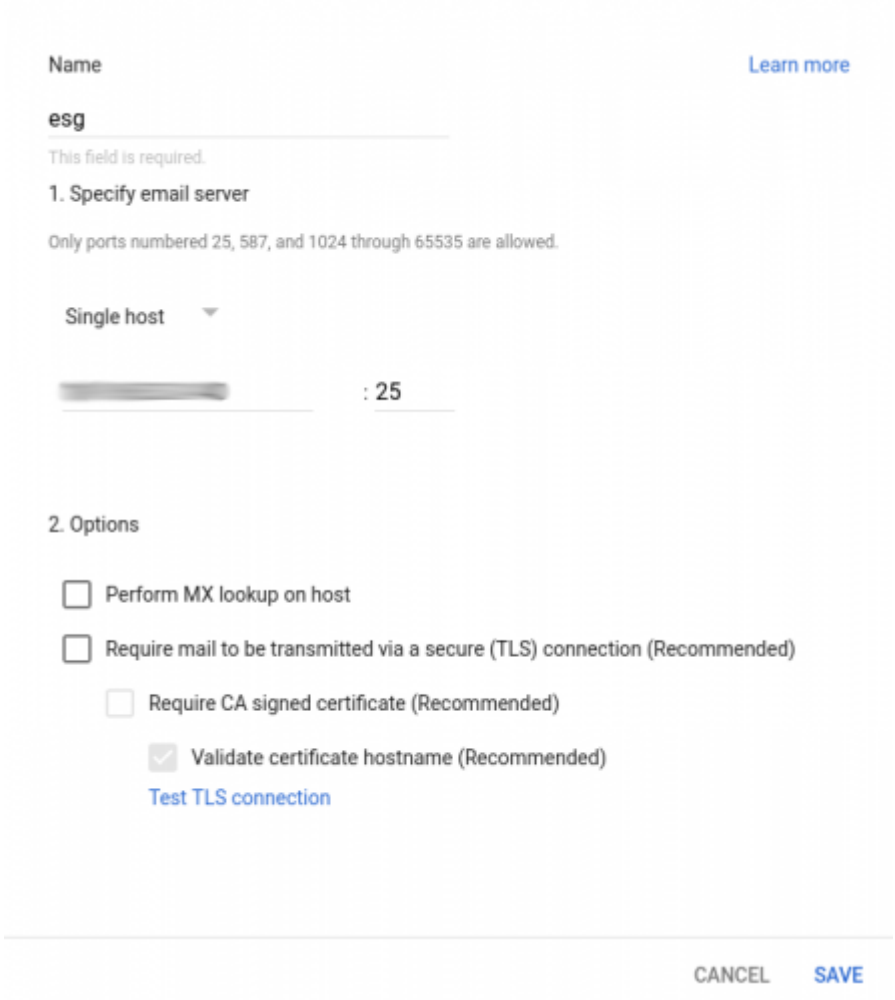
Trust G Suite in Libraesva ESG

To trust Google G Suite and enable outbound mail relay, navigate to **System > Settings > Relay Configuration** and select **Trusted Networks**. Click on the **Enable** button besides Trust Google Suite.

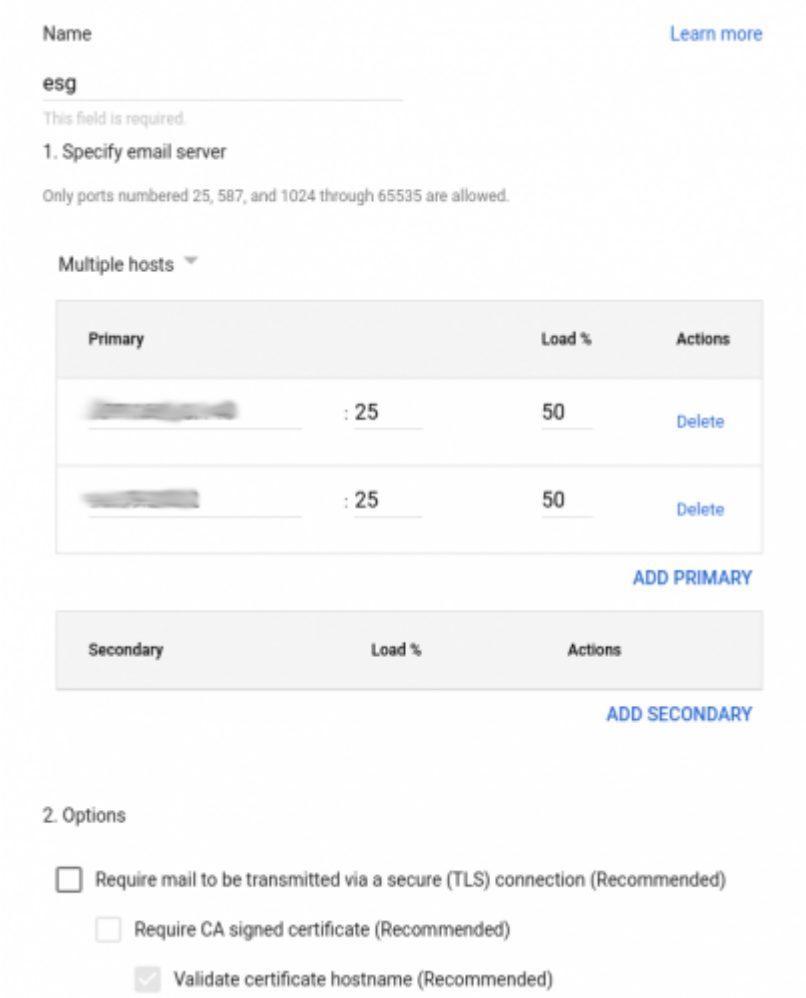
Google Outbound Configuration (step 1 of 2)

- Log into the Google G Suite Domain Management Portal.
- Navigate to **Apps > G Suite > Settings for Gmail > Hosts**
- Click on **ADD ROUTE**
- Give it a name, like **ESG** for example
- Choose **Single Host** if you have a single ESG instance or **Multiple hosts** if you have a cluster
- Enter the ip addresse(s) of your ESG appliance(s) and, in case of multiple hosts, the weight.

This is an example configuration for a single ESG:



This is an example configuration for an ESG cluster:



By unchecking “Require mail to be transmitted via a secure(TLS) connection” you are allowing selef-signed TLS certificates on ESG.

If you wish to check this checkbox make sure that you have a valid non self-signed certificate in use for SMTP on your ESG appliance(s).

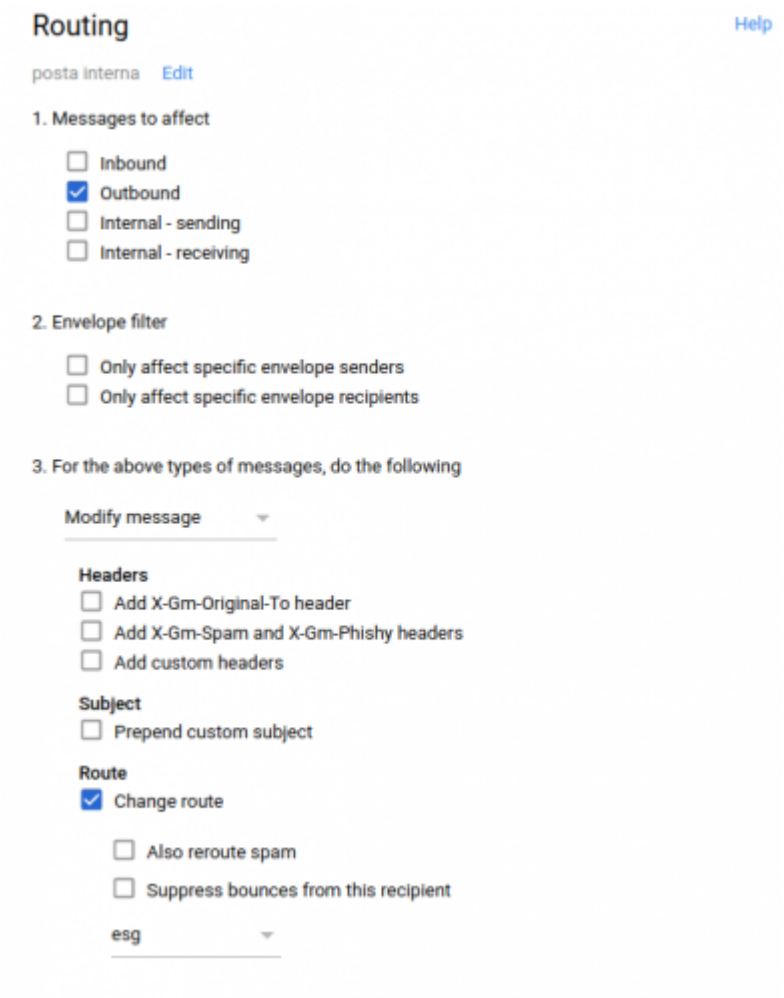
You have just created a host which is not yet in use. In the following step you will use it for an outbound rule.

Google Outbound Configuration (step 2 of 2)

- Log into the Google G Suite Domain Management Portal.
- Navigate to **Apps > G Suite > Settings for Gmail > Advanced settings > Routing**
- Click on **ADD ROUTE**
- Give it a name, like **Outbound route** for example
- Set “Messages to affect” to “Outbound”
- Set the flag “Change route” and choose the host you created at the previous step (ESG).

- Click SAVE

This is how the final configuration looks like:



Click on SAVE at the bottom of the page and your outbound email traffic will route through your ESG.

How to bypass ESG for internal email (recommended)

By default Google routes internal email (from your domain to your domain) to the inbound gateway (ESG).

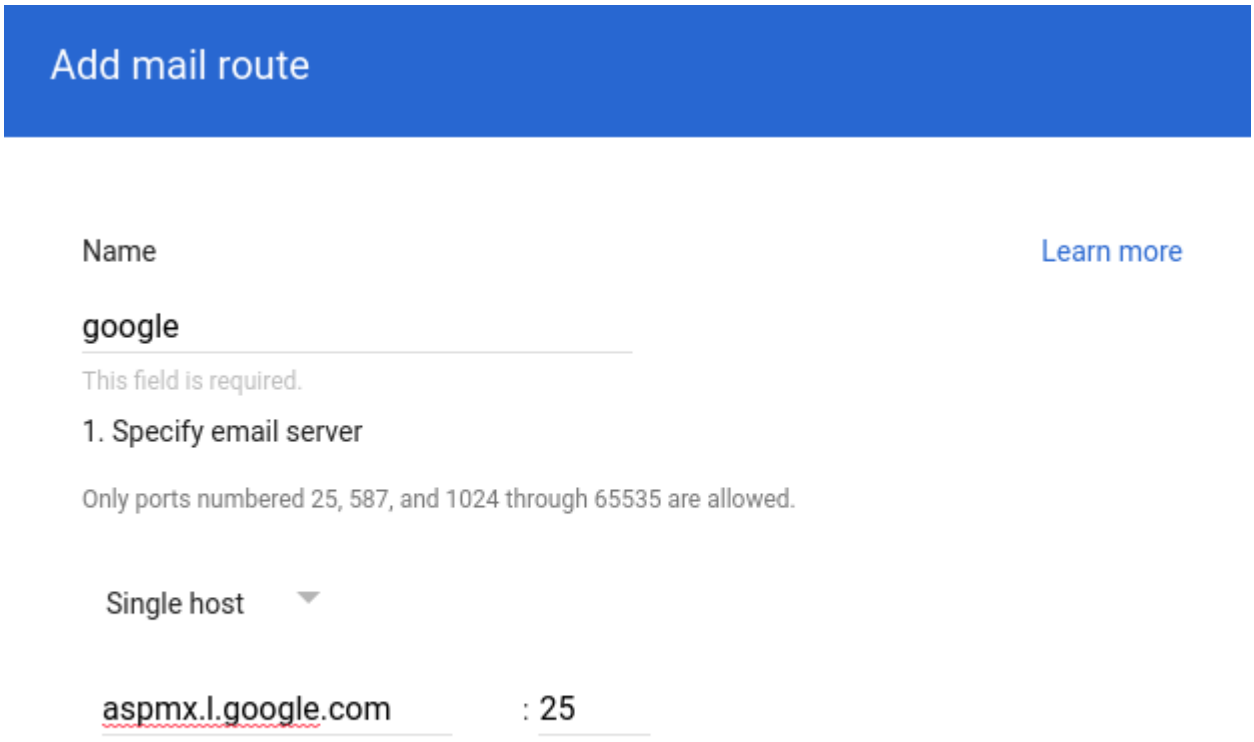
If you prefer to disable spam check for internal traffic, then it’s recommended to not route the traffic via ESG. This is will greatly reduce the pressure on the appliance (e.g. queuing time and storage size). Security checks will still be performed on internal email.

Should you want internal email to remain within Google and not being routed to ESG you must perform the configurations below.

Configuration to bypass ESG for internal email (step 1 of 3)

- Log into the Google G Suite Domain Management Portal.
- Navigate to **Apps > G Suite > Settings for Gmail > Hosts**
- Click on **ADD ROUTE**
- Give it a name, like **GOOGLE** for example
- Choose **Single Host**
- Enter **aspmx.l.google.com**
- Set port to 25
- Click SAVE

This is how the configuration looks like:



Configuration to bypass ESG for internal email (step 2 of 3)

- Log into the Google G Suite Domain Management Portal.
- Navigate to **Apps > G Suite > Settings for Gmail > Advanced settings > Routing**
- Find **Inbound gateway** and click EDIT
- Disable “Reject all mail not from gateway IPs”

An alternative to disabling the “Reject all mail not from gateway IPs” is to add to the Inbound Gateway IPs all the google ip subnets, which can be retrieved from the google’s txt record spf.google.com.

Configuration to bypass ESG for internal email (step 3 of 3)

- Log into the Google G Suite Domain Management Portal.
- Navigate to **Apps > G Suite > Settings for Gmail > Advanced settings > Routing**
- Add a new route with the name like “Internal”
- Under “Messages to affect” select “Internal – sending”
- Under “Envelope filter” select “Only affect specific envelope **recipients**“
- From the dropdown select “pattern match”
- Enter the following pattern replacing yourdomain.com with your domain:
  .*\@yourdomain\.com
  NOTE: this is a regular expression so it is important to keep the backslash.
- Under “Route” check “Change route” and select the route “google” from the dropdown.
- Click on “show options” at the end of the form and check both “users” and “groups”
- Click on ADD SETTING
- Click on SAVE

This is how the configuration looks like:

Route

- [x] Change route
  - [ ] Also reroute spam
  - [ ] Suppress bounces from this recipient

google

2. Envelope filter

- [ ] Only affect specific envelope senders
- [x] Only affect specific envelope recipients

Pattern match

Regexp Learn more

.*\@yourdomain\.com

Test expression