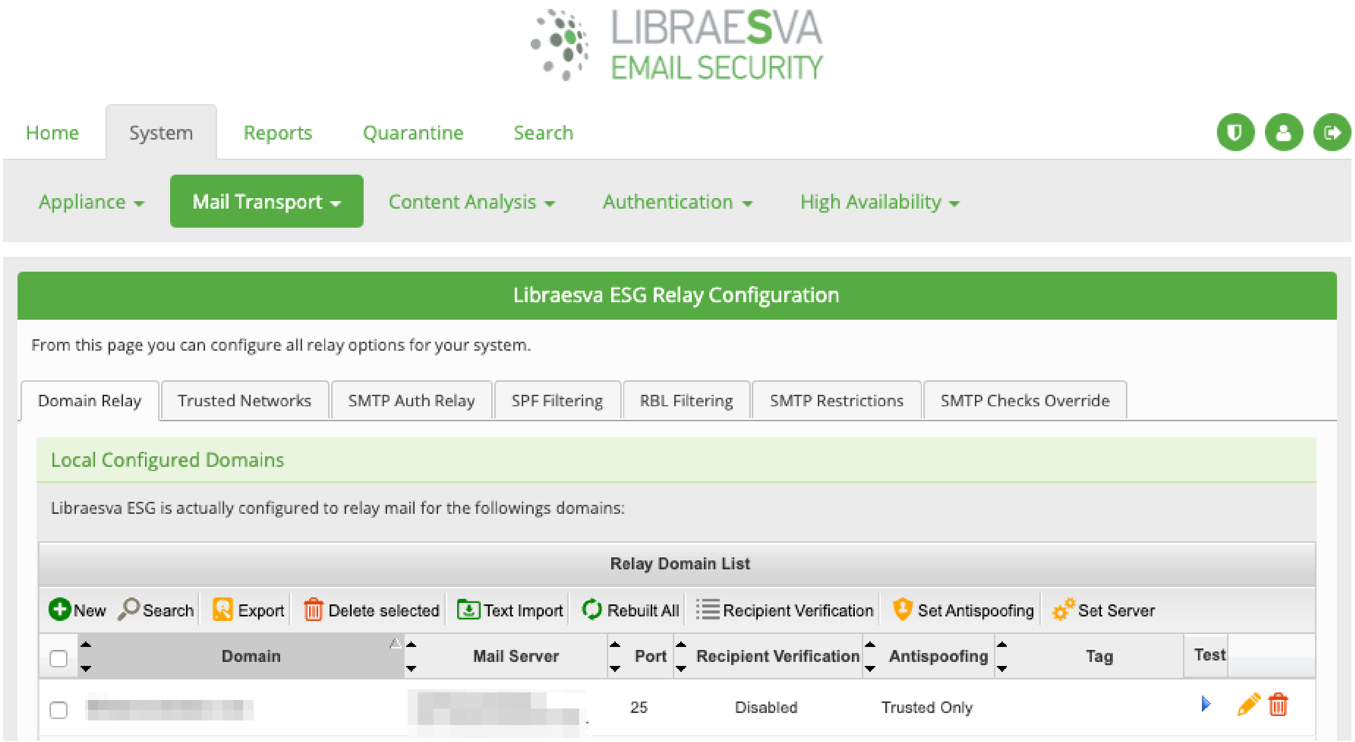
How to Set up a Domain Relay

Usually the First step configuring ESG is to define domains for which the email gateway will accept emails: we have a domain, “ourdomain.it”, and we want ESG analyze e-mail traffic and deliver clean messages to our mail server, “mail.ourdomain.it”

To do this simple task we can use the web interface:
System-> Relay Configuration -> Domain Relay



Libraesva ESG Relay Configuration

From this page you can configure all relay options for your system.

Local Configured Domains

Libraesva ESG is actually configured to relay mail for the followings domains:

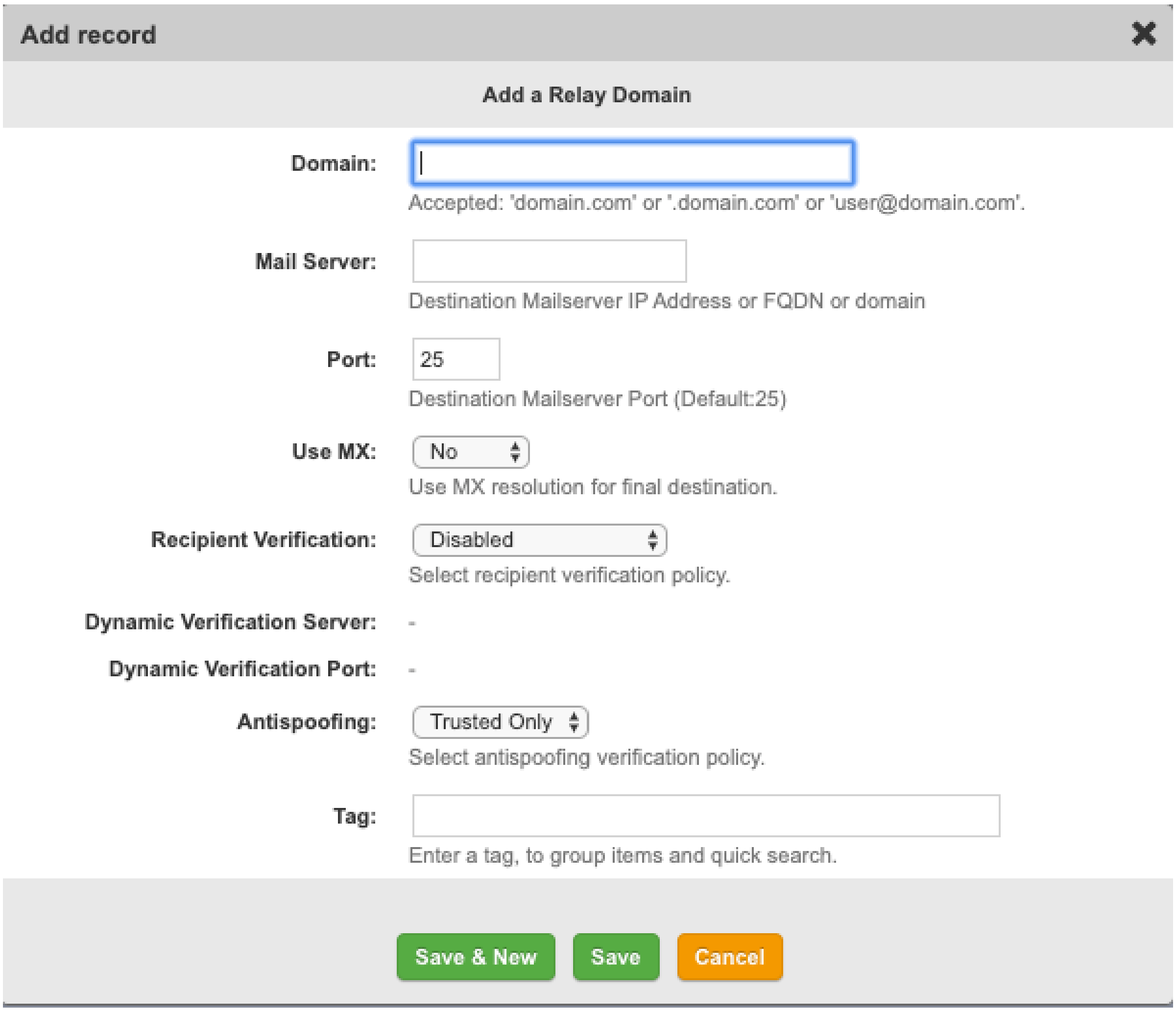
Relay Domain List

□	Domain	Mail Server	Port	Recipient Verification	Antispoofing	Tag	Test
□	[redacted]	[redacted]	25	Disabled	Trusted Only		

We hit the “New” button and start to fill form fields.

Domain: **ourdomain.it”**
(Cannot be empty!)
Mail Server: **mail.ourdomain.it”**
Destination Mailserver IP Address or FQDN or domain
Port: **25**
Destination Mailserver Port (Default:25)
Use MX: **NO**
Use MX resolution for final destination.
Recipient Verification: **Disabled**
Select recipient verification policy. (Disabled/Valid Recipient List/ Dynamic Verification)
Domain Antispoofing: **Disabled**

Select antispoofing verification policy. (Disabled/ Enabled)



Add record ✖

Add a Relay Domain

Domain:
Accepted: 'domain.com' or '.domain.com' or 'user@domain.com'.

Mail Server:
Destination Mailserver IP Address or FQDN or domain

Port: 25
Destination Mailserver Port (Default:25)

Use MX: No
Use MX resolution for final destination.

Recipient Verification: Disabled
Select recipient verification policy.

Dynamic Verification Server: -

Dynamic Verification Port: -

Antispoofing: Trusted Only
Select antispoofing verification policy.

Tag:
Enter a tag, to group items and quick search.

Domain, **Mail Server** and **Port** are pretty easy to understand. “**Use MX**” is a bit complex because it make possible to manage situation where you need to forward mail flow to a Cluster of Mail Servers. *(I will explain this case further in this document).* Usually you can leave it to “NO”.

Recipient address verification is useful to block mail for undeliverable recipients. This can help to prevent the mail queue from filling up and prevent un-necessary load for the engine.

- **Disable** option simply do nothing. Every mail, existing or forged by spammer, will be accepted and analyzed.
- **Dynamic Verification.** A live recipient probe, a RCPT TO, will be sent to destination mail server. If a recipient probe fails, then ESG rejects mail for the recipient address. If a recipient probe succeeds, then ESG accepts mail for the recipient address. To improve performance address verification results will be cached into a persistent database. It works good with Zimbra, Domino and many OpenSource MailServer. Exchanges need antispam agents to be installed. In every case you have to test if your server support

"rcpt to" return codes. (Just send a mail to goofy@mydomain.it and watch if it get rejected ad a not existent recipient).
Pros: it's easy if your server support it. *Cons:* ESG will depends from MailServer, if it became unreachable ESG won't be able to do recipient address verification anymore (and will accept everything).

- **Valid Recipient List.** We got a local list of all email address that ESG use to accept or drop a message. *Cons:* if a recipient is not on the list will be dropped. *Pros:* ESG is fully independent and, especially on Geografical Cluster, will always works as expected. We got tree way to fill up the list: *Manually* (one address by one), using a *TXT File* (every line an address) or by *LDAP Sync* (most complete and automatic solution).

Domain Antispoofing. smtp protocols do not provide mechanisms for authenticating the source or destination of a message. This means that is vulnerable to spoofing attacks when extra precautions are not taken to verify the identity of the sending host. To avoid someone spoof your domain you can enable this feature . Pay attention to set up in Trusted Network every Ip that need to deliver email using your domain.

USE MX: Cluster Option.

If you need to set up ESG to deliver email to a MailServer cluster (more than one Ip or hostname) you can use a DNS and its MX definition. Typically an internal DNS configurated to list in MX fields all the Cluster MailServer. Defining a DNS Conditional Forwarder ESG will dynamically ask to which mail server deliver.