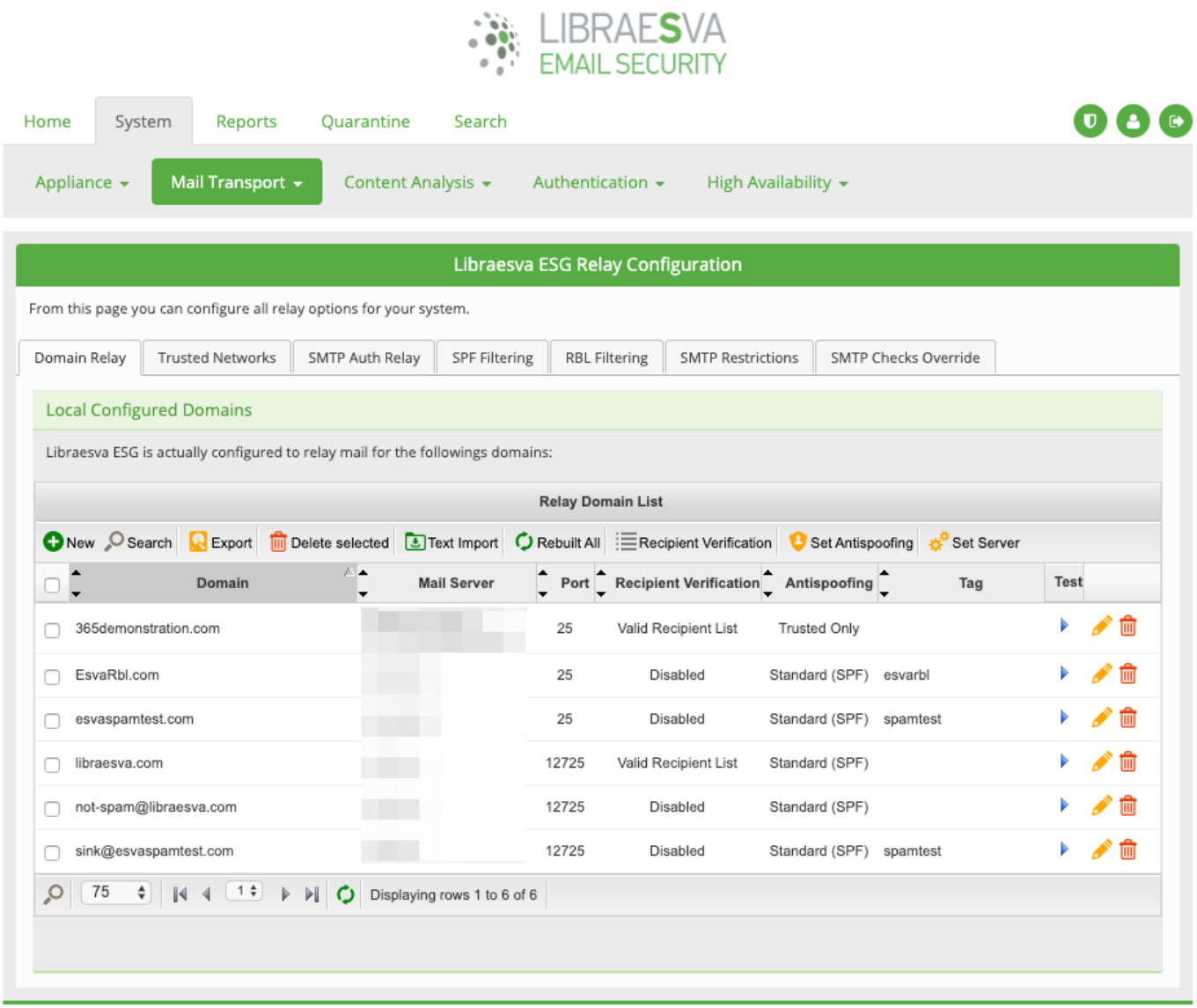
Relay Configuration

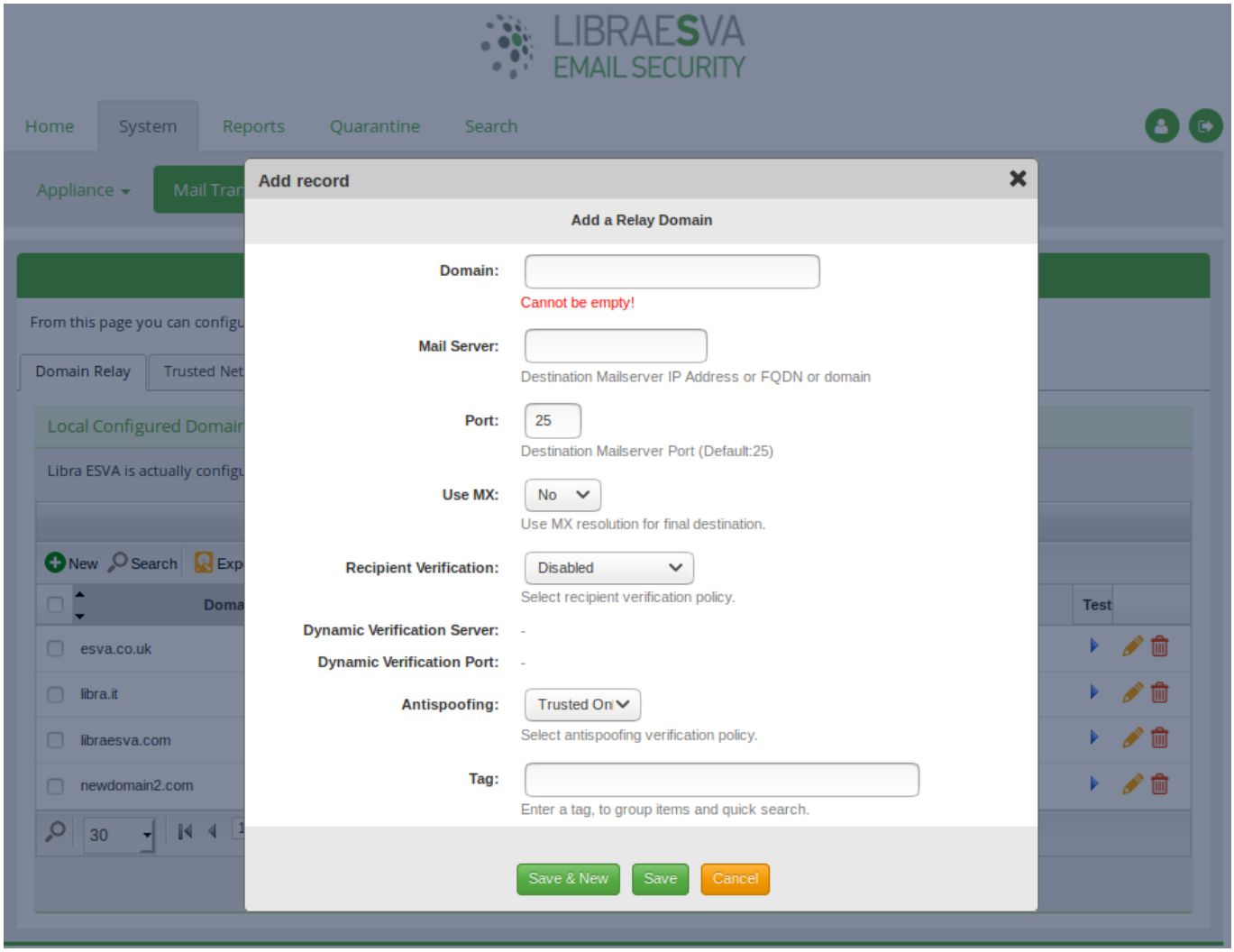
Domain Relay

Libraesva ESG carries out the relay for electronic mail directly to locally configured domains as well as for the computer indicated as belonging to a local IP address.



The first part (**Domain Relay**) serves to configure the email domain considered local by ESG, for which to therefore accept mail.

Libraesva ESG is capable of managing mail for multiple domains, in addition to the one specified during the installation procedure. To add an additional domain press the **New** button and fill in all required informations:



- **Domain:** is the new domain name you want to add. You can specify also a single email to achieve a special route or include all subdomains by inserting a trailing dot before the domain name: *domain.com*
  Subdomain must be declared (i.e. subdomain.example.com)
  You can also add a mail address as a domain to obtain more granular options.
- **Mail Server:** indicates the final destination mail server where Libraesva ESG will forward the scanned email to
- **Port:** the Mail Server port (default 25)
- **Use MX:** use DNS MX resolution of what indicated as Mail Server above to find out final destination
- **Recipient Verification:** select recipient verification policy. (Disabled/ Valid Recipient List /Dynamic Verification)
- **Dynamic Verification Server:** the dynamic verification server address (available only if Dynamic Verification is selected as Recipient Verification method)
- **Dynamic Verification Port:** the dynamic verification server port number (available only if Dynamic Verification is selected as Recipient Verification method)

- **Domain Antispoofing:** select antispoofing verification policy (Standard SPF / Trusted Only)
- **Tag:** label used for massive searches/modifications

Recipient Verification: allows relaying emails only for existent email addresses, and it is a best practice to enable it.

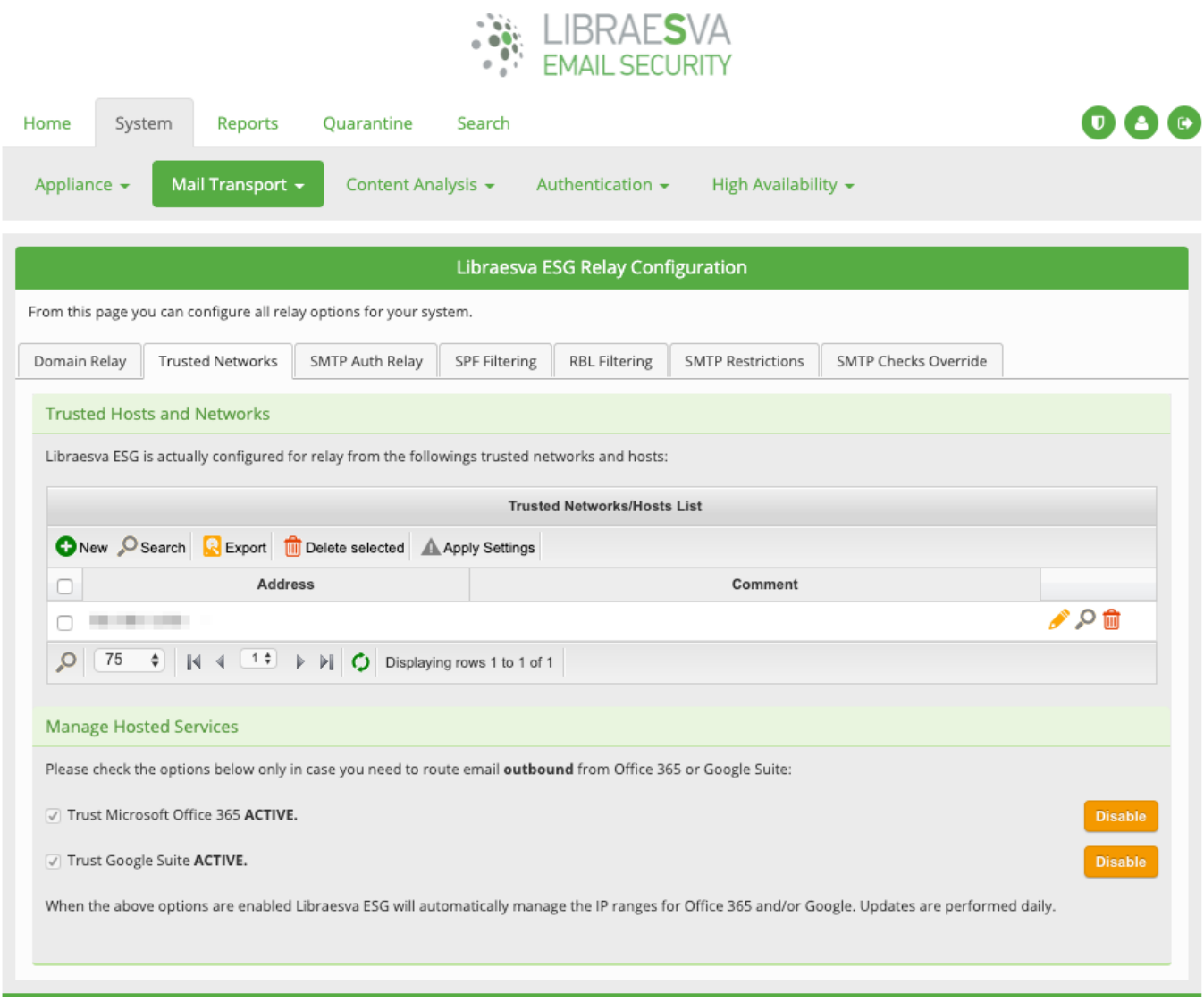
Antispoofing: is a feature that prevent relay of email coming from the domain itself unless the sending server is not present in the following Trusted Networks list. For this reason cross check you added all trusted mail server that are sending email from your domain through Libraesva ESG before enabling this feature.

Test: is a feature that allow to send a mail from Libraesva ESG to the relay server configured for the domain in order to test the email delivery, e.g. before going to production.

×**NOTE:** You can import multiple domains from a text file by clicking **Text Import** button

Trusted Networks

Libraesva ESG allows relay from all Trusted Networks and hosts defined here.

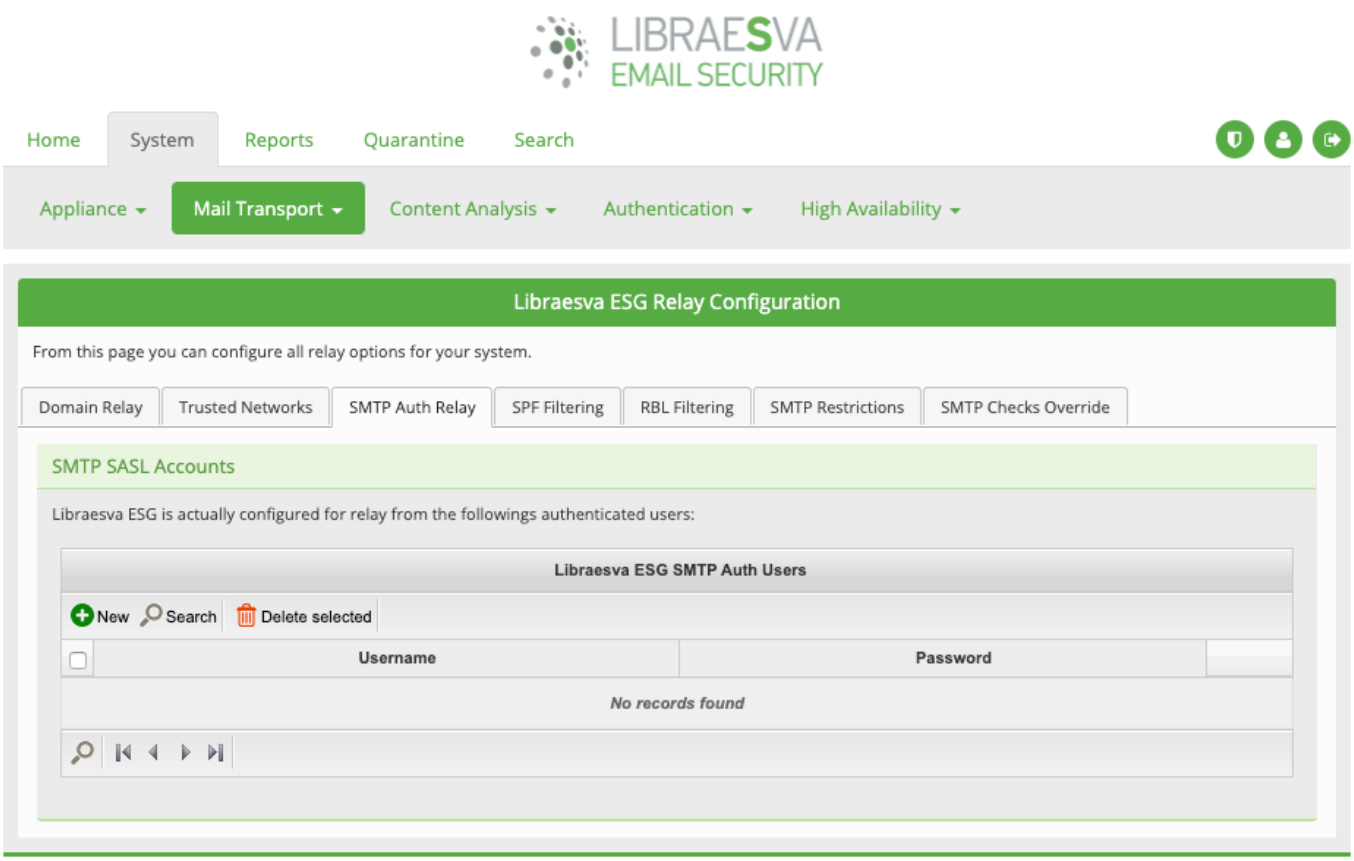


Typically you will add your internal mail server, or any host you want to authorize to send email through Libraesva ESG.

×**NOTE:** This allows only relay and is not a whitelist function. So emails received from these hosts/networks will be analyzed for spam. If you need to whitelist this traffic add in addition a whitelist entry from menù Lists.

SMTP SASL Auth

SMTP Auth Relay allows configuration of credentials for authenticated SMTP sessions, which will be relayed by Libraesva ESG.



Libraesva ESG allows relay from any SMTP authenticated client.

To add an additional user, please provide username and password and click **New** button.
To change password for an existing user simply re-add the same username with the new password.

Authentication ports supported are:

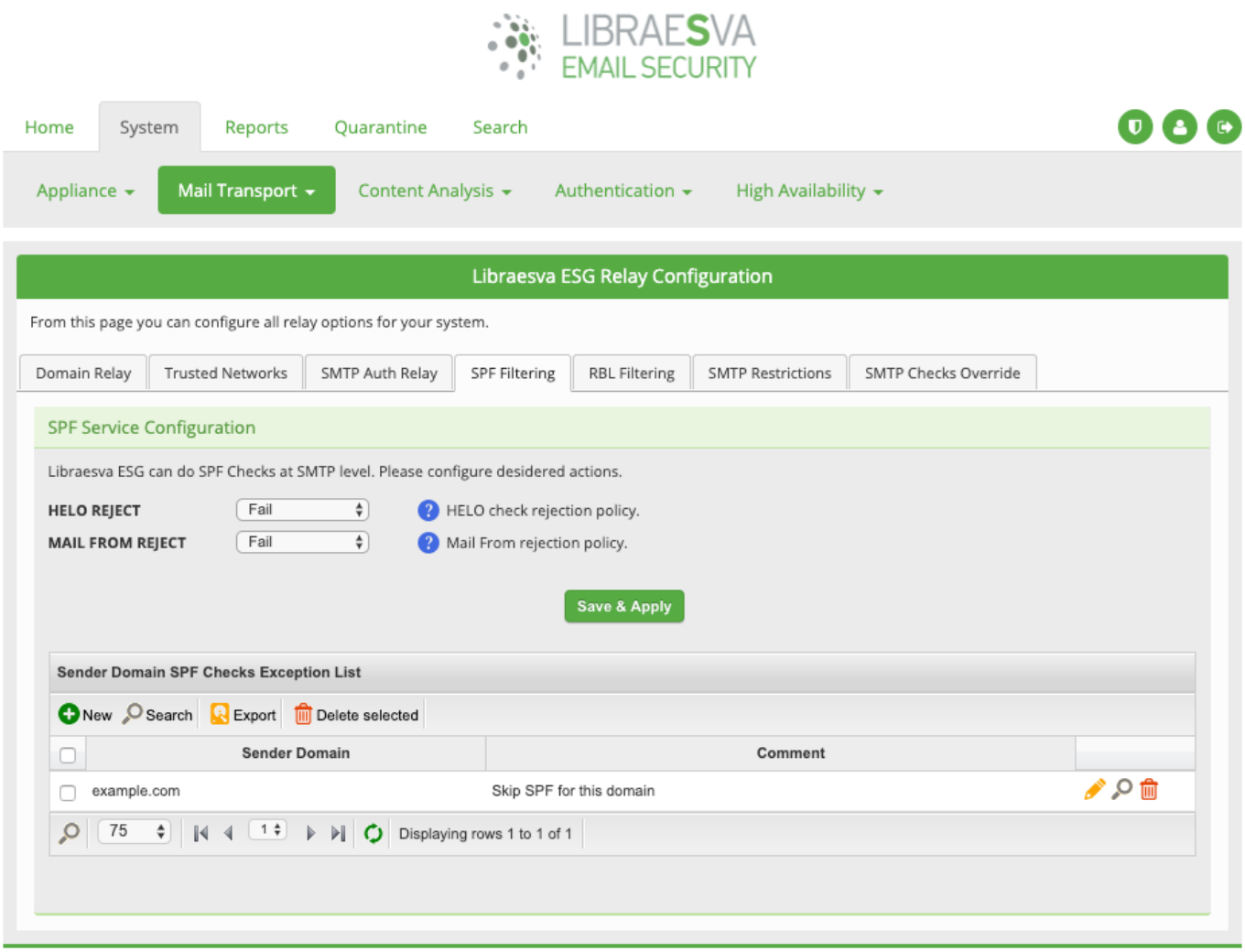
- 25
- 465 (SMTPS)
- 587 (Submission)

×**WARNING:** SMTP Auth passwords are easily intercepted as users share them. We do not recommend creating SMTP Auth sessions.
You can also select LDAP authentication method to verify connections.

SPF Filtering

Libraesva ESG can do SPF (Sender Policy Framework) checks at SMTP level on both HELO

and MAIL-FROM commands.



You can reject mails that will not pass the check. This control can be more or less restrictive, depending on the following options available for both checks:

- **SPF_Not_Pass:** reject mail if SPF Check result is not ‘Pass/None/Tempfail’
- **SoftFail:** reject mail if SPF Check result is ‘Softfail’ and ‘Fail’
- **Fail:** reject mail if SPF Check is ‘Fail’
- **Null:** only reject ‘Fail’ for Null sender (SPF Classic)
- **False**: never reject/defer, append header only

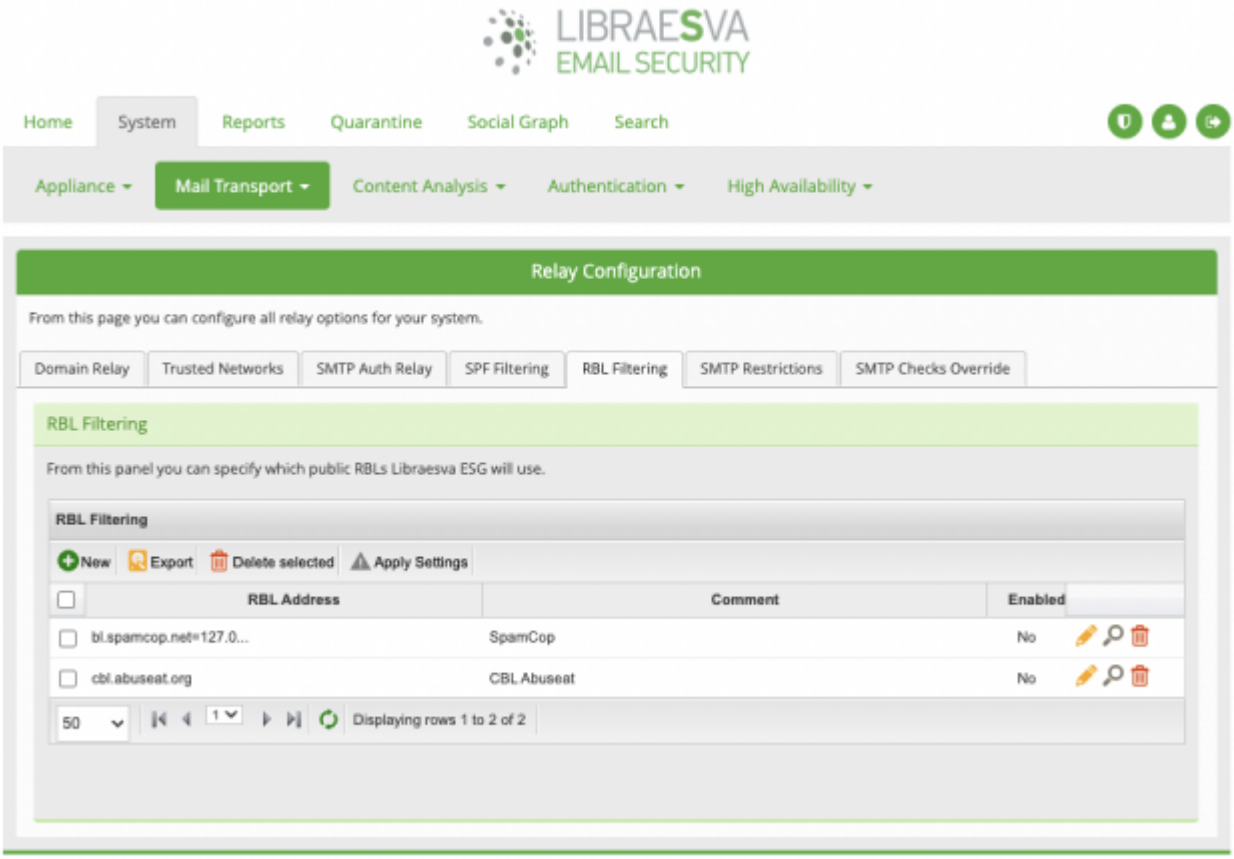
×We recommend action ‘Fail’ on both checks, as the hard fail respects the sender explicit policy. SoftFail will come to some False Positives due to common sender inaccuracy when defining SPF records
Reference:

http://www.openspf.org/RFC_4408#op-result

You can also add SPF Checks exceptions for some sender domains. To do that just add the sender domain in the Sender Domain SPF Checks Exception list.

RBL Filtering

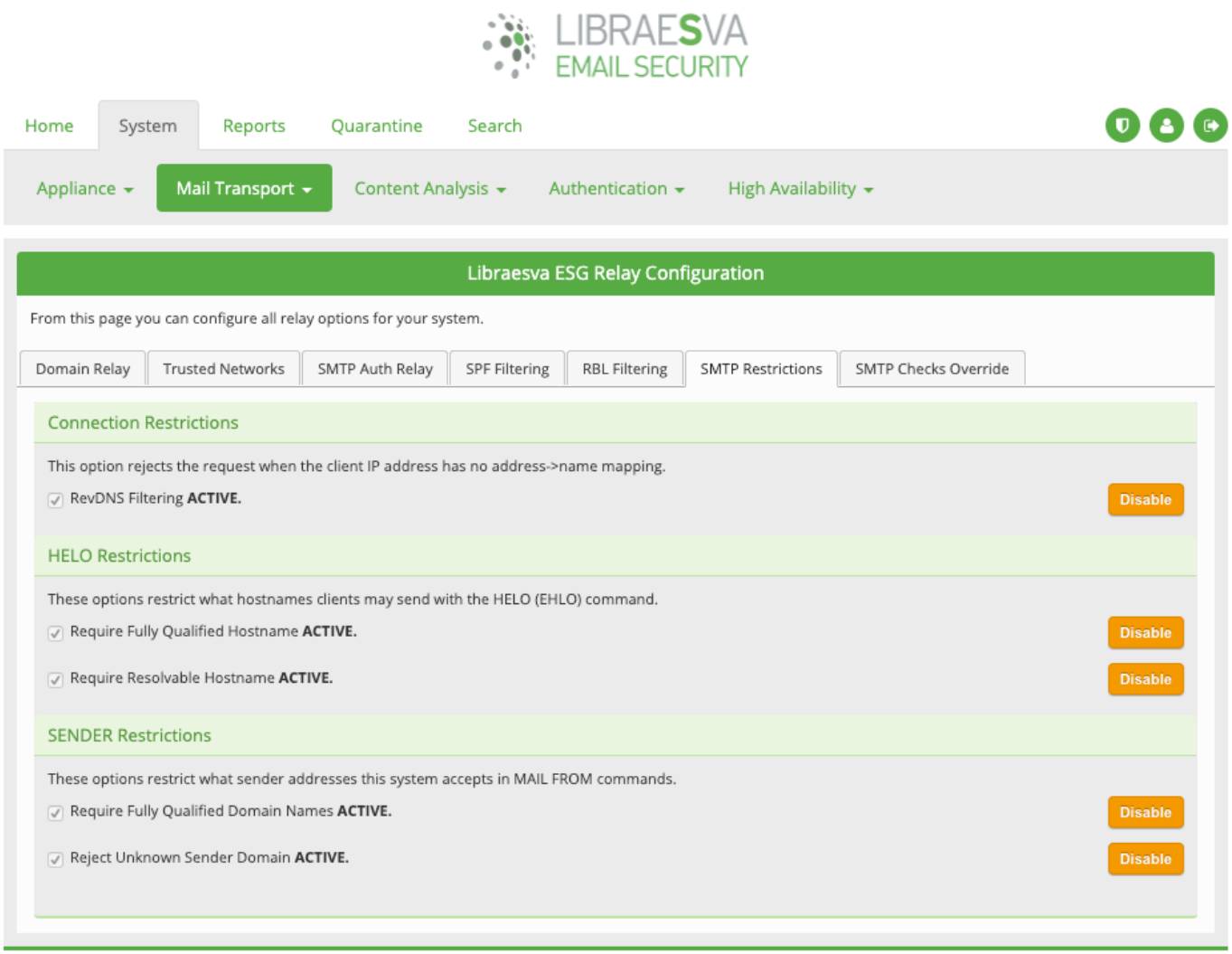
Any antispam filter uses public RBL's to arginate spam. Libraesva ESG makes no exception and from this page you can define which RBL's you want to use.



To add and enable an RBL entry press the New button and specify RBL address.

SMTP Restrictions

From this panel you can configure rejects based on SMTP protocol restrictions.



Connection Restrictions

The RevDNS option rejects the message when the client IP address has no IP address->name mapping.

HELO Restrictions

These options restrict what hostnames clients may send with the HELO (EHLO) command. By default Libraesva ESG require the sender to announce with a FQDN hostname that is correctly registered into a public DNS.

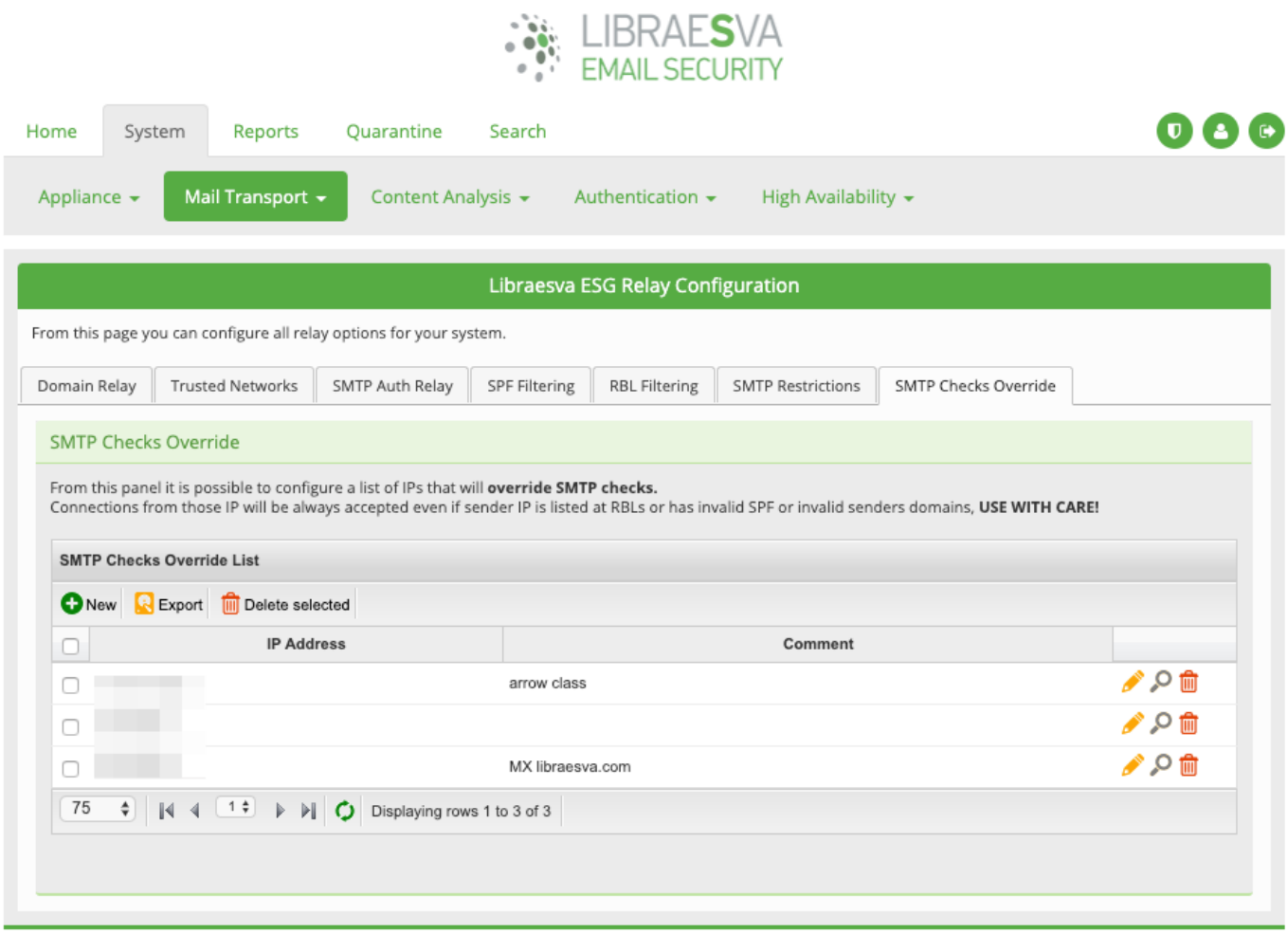
SENDER Restrictions

These options restrict what sender addresses this system accepts in MAIL FROM commands. By default Libraesva ESG require a Fully Qualified Domain Name as sender address and rejects Unknown (ie not in any DNS) Sender Domains.

SMTP Checks Override

From this panel it is possible to configure a list of IPs that will **override SMTP checks.**

This is very handy when a particular sender is blocked by an SMTP check (i.e. RBL Listed, Antispoofing check, SPF, etc.) and you need a permissive rule to allow relay from it's IP.



To add a new exception press New button and specify sender IP and a comment.

×**WARNING:** Connections from those IP will be always accepted even if sender IP is listed at RBLs or has invalid SPF or invalid senders domains, use with care!