

[Home](#)
[System](#)
[Reports](#)
[Quarantine](#)
[Search](#)

U

P

G

Appliance ▾
Mail Transport ▾
Content Analysis ▾
Authentication ▾
High Availability ▾

Libraesva ESG Relay Configuration

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

Domain Relay
Trusted Networks
SMTP Auth Relay
SPF Filtering
RBL Filtering
SMTP Restrictions
SMTP Checks Override

Local Configured Domains

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

Relay Domain List							
+ New 🔍 Search 📄 Export 🗑 Delete selected 📄 Text Import 🔄 Rebuilt All ⚙ Recipient Verification 🛡 Set Antispoofting ⚙ Set Server							
☐	Domain	Mail Server	Port	Recipient Verification	Antispoofting	Tag	Test
☐	365demonstration.com		25	Valid Recipient List	Trusted Only		▶ 📝 🗑
☐	EsvaRbl.com		25	Disabled	Standard (SPF) esvarbl		▶ 📝 🗑
☐	esvaspamtest.com		25	Disabled	Standard (SPF) spamtest		▶ 📝 🗑
☐	libraesva.com		12725	Valid Recipient List	Standard (SPF)		▶ 📝 🗑
☐	not-spam@libraesva.com		12725	Disabled	Standard (SPF)		▶ 📝 🗑
☐	sink@esvaspamtest.com		12725	Disabled	Standard (SPF) spamtest		▶ 📝 🗑

🔍

⏮ ⏪ ⏩ ⏭
1
🔄
Displaying rows 1 to 6 of 6

The screenshot shows the 'Add a Relay Domain' dialog box in the Libraesva Email Security interface. The dialog contains the following fields and options:

- Domain:** A text input field with a red error message 'Cannot be empty!' below it.
- Mail Server:** A text input field with the description 'Destination Mailserver IP Address or FQDN or domain' below it.
- Port:** A text input field containing '25' with the description 'Destination Mailserver Port (Default:25)' below it.
- Use MX:** A dropdown menu set to 'No' with the description 'Use MX resolution for final destination.'
- Recipient Verification:** A dropdown menu set to 'Disabled' with the description 'Select recipient verification policy.'
- Dynamic Verification Server:** A text input field containing a hyphen '-'.
- Dynamic Verification Port:** A text input field containing a hyphen '-'.
- Antispoofing:** A dropdown menu set to 'Trusted On' with the description 'Select antispoofting verification policy.'
- Tag:** A text input field with the description 'Enter a tag, to group items and quick search.'

At the bottom of the dialog are three buttons: 'Save & New' (green), 'Save' (green), and 'Cancel' (orange). The background interface shows a sidebar with 'Domain Relay' and 'Trusted Net' tabs, and a list of domains including esva.co.uk, libra.it, libraesva.com, and newdomain2.com.

- **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 antispoofting 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.

Libraesva ESG Relay Configuration

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

[Domain Relay](#)
[Trusted Networks](#)
[SMTP Auth Relay](#)
[SPF Filtering](#)
[RBL Filtering](#)
[SMTP Restrictions](#)
[SMTP Checks Override](#)

Trusted Hosts and Networks

Libraesva ESG is actually configured for relay from the followings trusted networks and hosts:

Trusted Networks/Hosts List		
+ New Search Export Delete selected Apply Settings		
☐	Address	Comment
☐	192.168.1.1	
75 1 Displaying rows 1 to 1 of 1		

Manage Hosted Services

Please check the options below only in case you need to route email **outbound** from Office 365 or Google Suite:

☒ Trust Microsoft Office 365 **ACTIVE**.

[Disable](#)

☒ Trust Google Suite **ACTIVE**.

[Disable](#)

When the above options are enabled Libraesva ESG will automatically manage the IP ranges for Office 365 and/or Google. Updates are performed daily.

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 menu Lists.

SMTP SASL Auth

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

Libraesva ESG Relay Configuration

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

[Domain Relay](#) [Trusted Networks](#) [SMTP Auth Relay](#) [SPF Filtering](#) [RBL Filtering](#) [SMTP Restrictions](#) [SMTP Checks Override](#)

SMTP SASL Accounts

Libraesva ESG is actually configured for relay from the followings authenticated users:

Libraesva ESG SMTP Auth Users

[+ New](#) [🔍 Search](#) [🗑 Delete selected](#)

☐	Username	Password
--------------------------	----------	----------

No records found

🔍 ⏪ ⏩ ⏴ ⏵

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.

Libraesva ESG Relay Configuration

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

Domain Relay | Trusted Networks | SMTP Auth Relay | SPF Filtering | RBL Filtering | SMTP Restrictions | SMTP Checks Override

SPF Service Configuration

Libraesva ESG can do SPF Checks at SMTP level. Please configure desired actions.

HELO REJECT ? HELO check rejection policy.

MAIL FROM REJECT ? Mail From rejection policy.

Save & Apply

Sender Domain SPF Checks Exception List

+ New Search Export Delete selected

☐	Sender Domain	Comment	
☐	example.com	Skip SPF for this domain	

75 1 Displaying rows 1 to 1 of 1

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

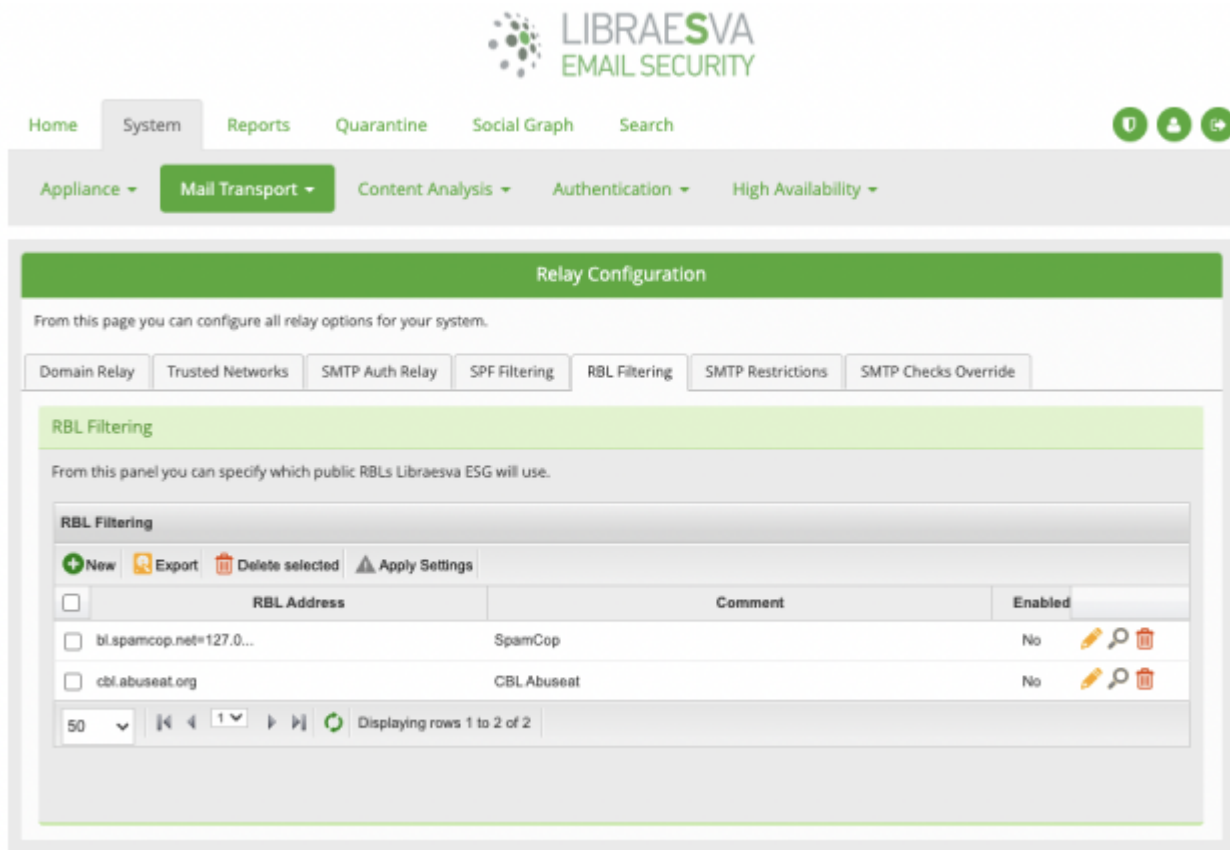
Reference:

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.



The screenshot shows the Libraesva Email Security web interface. The top navigation bar includes links for Home, System, Reports, Quarantine, Social Graph, and Search. Below this is a secondary navigation bar with tabs for Appliance, Mail Transport (selected), Content Analysis, Authentication, and High Availability. The main content area is titled "Relay Configuration" and contains a sub-section for "RBL Filtering". This section includes a table with columns for RBL Address, Comment, and Enabled. Two entries are listed: "bl.spamcop.net=127.0..." with comment "SpamCop" and "cbl.abuseat.org" with comment "CBL Abuseat". Both are currently disabled. The interface also features buttons for New, Export, Delete selected, and Apply Settings, along with pagination controls at the bottom.

RBL Address	Comment	Enabled
☐ bl.spamcop.net=127.0...	SpamCop	No
☐ cbl.abuseat.org	CBL Abuseat	No

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.

Libraesva ESG Relay Configuration

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

Domain Relay Trusted Networks SMTP Auth Relay SPF Filtering RBL Filtering SMTP Restrictions SMTP Checks Override

Connection Restrictions

This option rejects the request when the client IP address has no address->name mapping.

☒ RevDNS Filtering **ACTIVE.**

Disable

HELO Restrictions

These options restrict what hostnames clients may send with the HELO (EHLO) command.

☒ Require Fully Qualified Hostname **ACTIVE.**

Disable

☒ Require Resolvable Hostname **ACTIVE.**

Disable

SENDER Restrictions

These options restrict what sender addresses this system accepts in MAIL FROM commands.

☒ Require Fully Qualified Domain Names **ACTIVE.**

Disable

☒ Reject Unknown Sender Domain **ACTIVE.**

Disable

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.


LIBRAESVA
 EMAIL SECURITY

Home
System
Reports
Quarantine
Search

Appliance ▾
Mail Transport ▾
Content Analysis ▾
Authentication ▾
High Availability ▾

Libraesva ESG Relay Configuration

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

Domain Relay
Trusted Networks
SMTP Auth Relay
SPF Filtering
RBL Filtering
SMTP Restrictions
SMTP Checks Override

SMTP Checks Override

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

SMTP Checks Override List

New
 Export
 Delete selected

☐	IP Address	Comment	
☐	192.168.1.1	arrow class	
☐	192.168.1.2		
☐	192.168.1.3	MX libraesva.com	

▾

▾

Displaying rows 1 to 3 of 3

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!