User Management

Libraesva ESG users can manage and access the system.

With Libraesva ESG you can enable per-user quarantine and the system will create user accounts to enable access to quarantine settings and messages. ESG supports per-user account spam score settings.

Account Roles

Libraesva ESG has six type of users, with different roles, as follows:

- Administrator User
- Read-only Administrator
- Quarantine Administrator
- Domain Administrator
- Read-only Domain Administrator
- Quarantine Domain Administrator
- Multi Domain Administrator
- Normal User

Administrator

This user has full rights, can see all email traffic going through the appliance and can access all configuration parameters. This is the only account that can add other users, either Administrators, Domain Administrators or Users. Spam scores settings for the "admin" user will be used as default spam scores levels for the appliance and will be inherited from all users without any custom explicit setting.

Read-only Administrator

The "read-only" administrator one can only read information but cannot make configuration changes.

Quarantine Administrator

The "quarantine" administrator is a "read-only" administrator that can also manage the

quarantine and release messages.

Domain Administrator

The Domain Administrator account can see and manage all the email traffic for its own domain. It can manage spam, white/black list and run reports for all users that belongs to its domain. This account can set spam scores levels for its domain; if not the ones from the admin account will be used. This account can also set a Privacy Passwords for domain, if this configuration was enabled in System Preferences. Not other appliance settings are available to this user.

Read-Only Domain Administrator

The "read-only" domain administrator can only read information about the domain configuration but cannot make configuration changes.

Quarantine Domain Administrator

The "quarantine" domain administrator is a "read-only" administrator that can also manage the quarantine and release messages.

×**NOTE**: domain admin username must be expressed as contoso.com

Multi Domain Administrator

The Multi Domain Administrator account is a Domain Administrator with on all associated Domain Administrator users.

Normal User

Regular Users can access their own messages and manage their own spam as well as editing its own white/black lists. Each user can schedule its quarantine digest report delivery and customize its spam scores levels; if not, the ones from the Domain Administrator will be used.

Users account can be of four types:

- Local users, created and stored on the appliance database, either manually or by text import. An auto user creation feature is available to let ESG create users automatically upon the first email is received by the system.

- LDAP users, imported and synchronized with a remote LDAP server, password will NOT be stored on ESG.

- POP3 users, automatically created after each successful user login with the associated

POP3 server. Password will NOT be stored on ESG.

- IMAP users, automatically created after each successful user login with the associated IMAP server. Password will NOT be stored on ESG.

Account Management

The Administrator has User Management access with full control over all accounts. Domain Admin and Normal Users can only manage their own user account. Multi Domain Administrator can manage associated Domain Admin users. The User Management screen looks as follows:

The first two options a the top of the page, available to the administrator user only, allows to limit user's functionalities:

Users can change their own Spam Settings
Set this to No will NOT permit Normal Users to change their own spam score levels. If set to Yes you will permit users to disable their own spam checks or change their own spam score levels.

Users can teach Antispam only from Safe Learn Net
This option sets the appliance behavior when receiving a learn command from a user. These learning commands allows you to release a quarantined message, to teach Bayesian engine or

to whitelist/blacklist the email sender.

Since the learn link is added to each email as a signature, it can be clicked from multiple sources (PC, mobile, …) and also from different users, as the sender may have access to the link on reply. For security reasons you may want to limit these functionalities only if originating from your internal network, or give wide access but requiring a user confirmation if the request originates form an untrusted network.
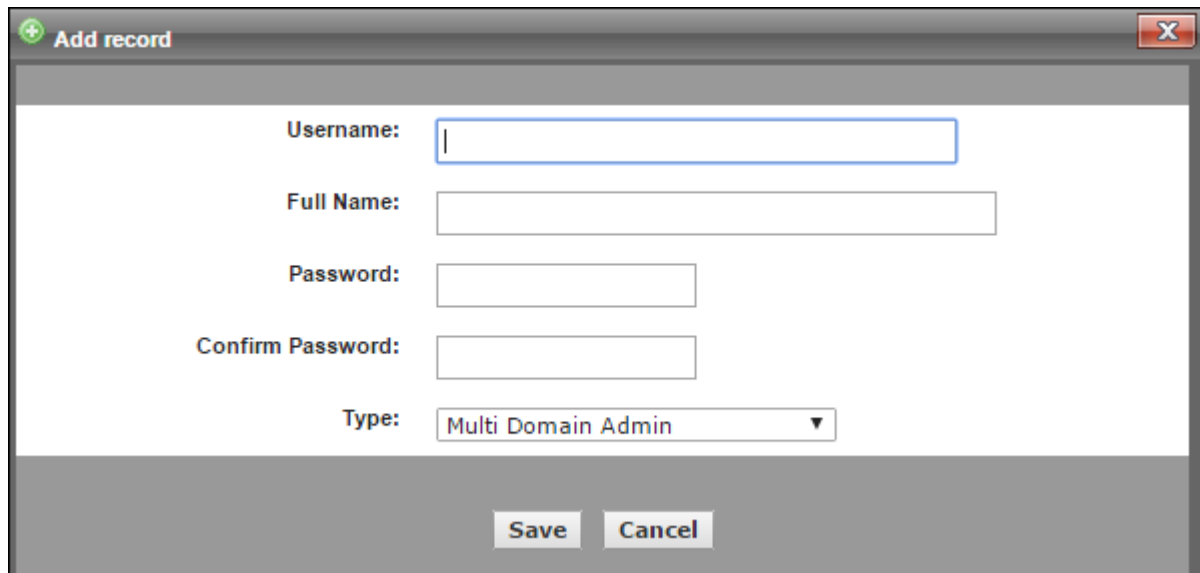
It has three settings available:

1. Yes, Warning: Closed system, the request will be processed only if originates from a trusted networks and message confirmation is sent to the user before processing the request.

2. Yes, Silent: Closed system, he request will be processed only if originates from a trusted networks and no confirmation message is sent and the request is processed silently.

3. No: Open system, the request will be processed also if originates from a untrusted networks and no message will be sent.

×**NOTE:** safe learn networks are defined in the "Safe Learn Networks" tab and aren't related in any way to the Relay Trusted Network
Other options available on the **User List** screen are:

- New – To manually add a new local user

- Search

- Export – To export selected entries to XML, CSV or print records

- Delete Selected

- Delete ALL Entries

- Text Import – To import users from a text file, read later on

- LDAP Import – To imports users from LDAP, read later on

- Digest Report Schedule – To schedule Digest Report for selected users

The **Multi Domain Admins Tab** allows creation of multi domain admins:

Multi domain admins are local users. When a multi domain administrator is created you can associate any existing Domain Admin user.

×**NOTE:** You must first create all single Domain Admins you want to group under a Multi Domain Administrator

The **LDAP Synchronization** Tab allows to configure LDAP Sets to authenticate users, see section below.

The **Auto Populate Users** Tab gives the options to create local users accounts automatically for those domains that have a Valid Recipient verification policy defined (this to avoid invalid users creation). Users are created after the first mail is received by the system, on a daily basis.

This feature is very handy to have the system to automatically set Quarantine Digest reports to all users that are receiving emails without having the need of manually configuring the users. A random password will be set. Users can reset it through the Forgot Password link on the login page.

Local Accounts Creation

Local accounts are users saved on local database. That means all user informations, passwords included, are stored locally on Libraesva ESG appliance. Local accounts will have the same functionalities as LDAP accounts.

You can create local accounts in two ways:

1. By manually adding each user clicking on button **New**

2. By importing a list of accounts from a text file

Text File should be formatted as follows:

- One user per line in the format: Email Address,User Password,User Full name
- Fields are comma separated. Email Address will be used also as Username

User accounts will be created and daily quarantine report will be automatically set as active for all users imported.

×**NOTE:** the Text Import procedure offers you to send a notification email to imported user. Local users can also be created by the Auto Populate Users function.

LDAP Accounts Creation

LDAP accounts are users imported from a remote LDAP Server. All user information are stored on Libraesva ESG except the user password that remains on the LDAP Server.

The first thing you need is an LDAP Set defined, next you can use it for Account Creation.

To use your defined LDAP Set to synchronize users, select menù *System->User Management->LDAP Synchronization* and **Edit** LDAP Properties:
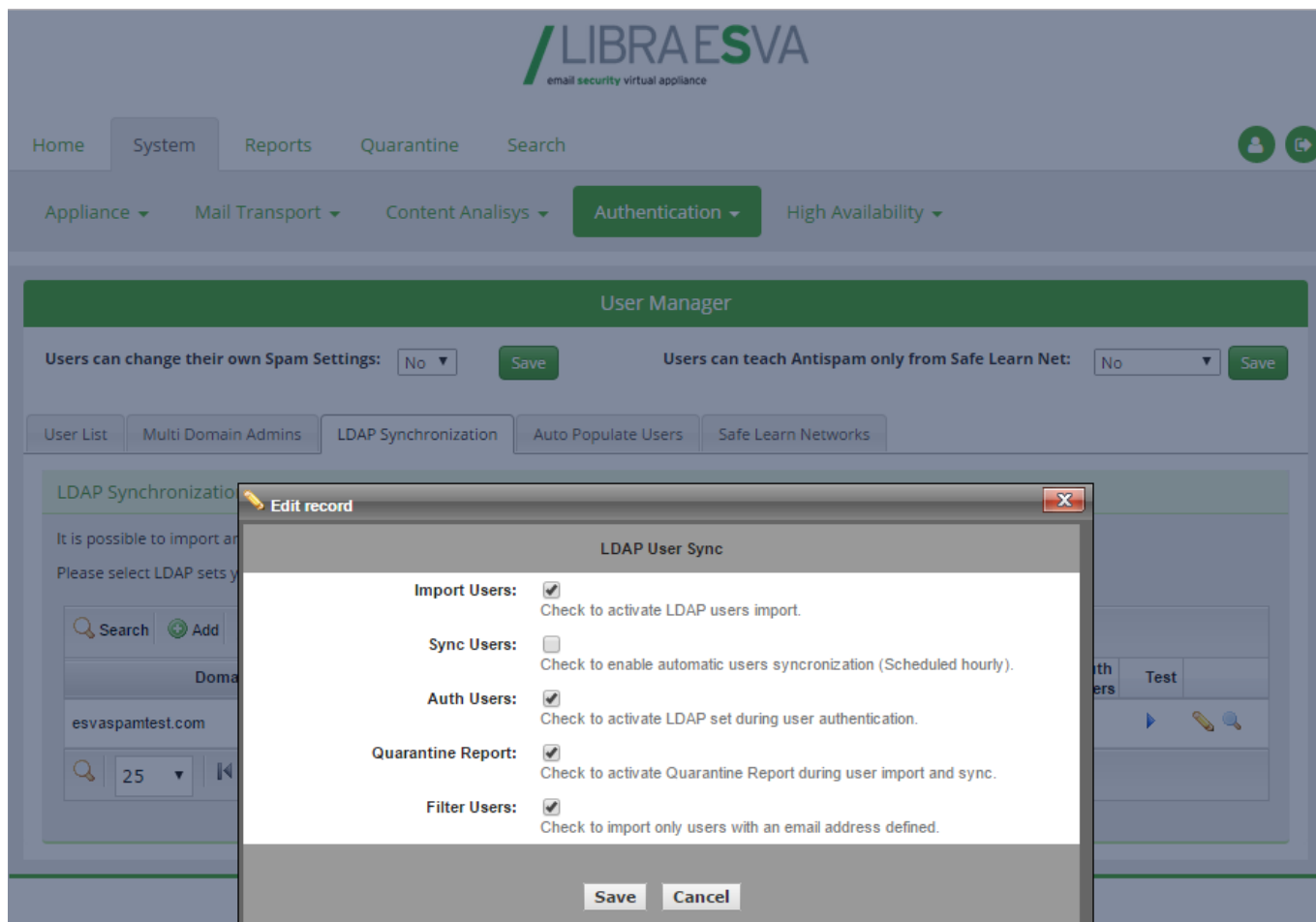
From this screen you can choose LDAP use and preferences regarding your Users.

When importing users from LDAP you have the option to:

- Keep user list in sync with LDAP Server (fixed hourly schedule)

- Authenticate users against your LDAP, to give them Libraesva ESG web access to their quarantine

- Set automatically, for each newly imported users, the Quarantine Digest Report delivery

- Filter out users without a valid email address, as probably you won't deal with them in Libraesva ESG
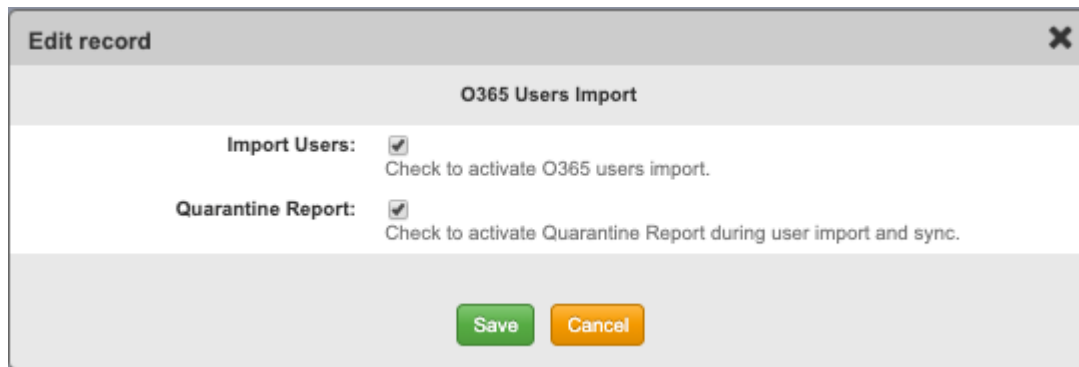
Once you set your preferences simply press the button **LDAP Import** and Libraesva ESG will do the query to import users.

×**NOTE:** you can Test your settings by clicking on the test icon to check result set before doing final import.

O365 Accounts Creation

Once you have created O365 connector, you'll be able to modify two parameters:

- Import Users

- Quarantine Report: activate quarantine report for all imported users

×**NOTE:** you can Test your settings by clicking on the test icon to check result set before doing final import.

×**NOTE:** group aliases will be added as alias of any component of the group once imported.

POP3 Account Creation

POP3 Users are users that authenticate through a POP3 Server verification method.

If a domain has as authentication scheme the POP3 method, each user that successfully authenticates will be created. This user is equivalent to the above LDAP user as no password is stored locally on ESG. All other user preferences are editable. There is no way to force a POP3 user import, as the POP3 Server do not offer such a feature.

IMAP Account Creation

IMAP Users are users that authenticate through an IMAP Server verification method.

If a domain has as authentication scheme the IMAP method, each user that successfully authenticates will be created. This user is equivalent to the above LDAP user as no password is stored locally on ESG. All other user preferences are editable. There is no way to force a IMAP user import, as the IMAP Server do not offer such a feature.

Account Features

Each user account can have the following properties:

1. **Spam Checks** enabled or disabled

2. **Spam Score** and **Hi Spam Score** personalization

3. **Quarantine Actions**, to customize the Quarantine Report Actions

4. **Quarantine Msg Preview**, allow message body Preview from Quarantine Report

5. Quarantine Digest Report, with up to **4 schedules per day**

6. **Email Aliases**, to have a consolidated view of messages and Digest Report

To set the first five feature edit the user account properties:

Quarantine Actions

It's possible to customize the quarantine report actions on a per user basis.

- **Self Release –** The user can self release it's own quarantined messages:

E-mail Quarantine Report for: ████ @ █████

Nelle ultime 24 ore hai ricevuto 4 e-mails che sono state messe in quarantena, come sotto riportato. Tutti i messaggi in quarantena sono automaticamente eliminati 35 giorni dopo la data di ricezione.

L`elenco sotto riportato è ordinato per punteggio di Spam crescente. Eventuali falsi positivi è più probabile che siano quindi in cima all`elenco.

- Virus = mail con contenuti infetti, non è possibile rilasciarla!
- Bad Content = mail con contenuti non permessi
- Infected = mail con script pericolosi nel contenuto , non è possibile rilasciarla!
- Spam = mail considerata spam
- Blacklisted = il mittente è presente nelle blacklist del servizio antispam

Received	From	To	Subject	Score	Reason	Action	Preview
02/09/15 15:55:30	██@████.it	davide████ ██@lib...	Re: INTERNAL_SPAM_TE...	5.85	Spam	[Release] [Rel.& Whitelist]	[View]
02/09/15 15:55:30	██@████.it	davide████ ██@lib...	Re: INTERNAL_SPAM_TE...	5.85	Spam	[Release] [Rel.& Whitelist]	[View]
02/09/15 15:55:29	██@████.it	davide████ @lib...	Re: INTERNAL_SPAM_TE...	5.85	Spam	[Release] [Rel.& Whitelist]	[View]
02/09/15 15:55:30	██@████.it	davide████ @lib...	Re: INTERNAL_SPAM_TE...	6.64	Spam	[Release] [Rel.& Whitelist]	[View]

- **Mark for Release –** The user can only request a message release to the administrator/domain administrator:

E-mail Quarantine Report for: ████ @█████

Nelle ultime 24 ore hai ricevuto 4 e-mails che sono state messe in quarantena, come sotto riportato. Tutti i messaggi in quarantena sono automaticamente eliminati 35 giorni dopo la data di ricezione.

L`elenco sotto riportato è ordinato per punteggio di Spam crescente. Eventuali falsi positivi è più probabile che siano quindi in cima all`elenco.

- Virus = mail con contenuti infetti, non è possibile rilasciarla!
- Bad Content = mail con contenuti non permessi
- Infected = mail con script pericolosi nel contenuto , non è possibile rilasciarla!
- Spam = mail considerata spam
- Blacklisted = il mittente è presente nelle blacklist del servizio antispam

Received	From	To	Subject	Score	Reason	Action	Preview
02/09/15 15:55:30	██@███.it	davide████ ██@lib...	Re: INTERNAL_SPAM_TE...	5.85	Spam	[Ask to Release]	[View]
02/09/15 15:55:30	██@████.it	davide████ ██@lib...	Re: INTERNAL_SPAM_TE...	5.85	Spam	[Ask to Release]	[View]
02/09/15 15:55:29	██@████.it	davide█████.@lib...	Re: INTERNAL_SPAM_TE...	5.85	Spam	[Ask to Release]	[View]
02/09/15 15:55:30	██@███.it	davide████ @lib...	Re: INTERNAL_SPAM_TE...	6.64	Spam	[Ask to Release]	[View]

×**NOTE:** the request details will be shown in the quarantine management in the admin panel.

- **No release –** The user is not allowed to self-release or ask to release messages from within the digest report:


Quarantine Msg Preview:

If enabled, the user has the message view option enabled. This feature requires user credentials on the Libraesva ESG web interface.

E-mail Quarantine Report for: ████████ @ ████████

Nelle ultime 24 ore hai ricevuto 4 e-mails che sono state messe in quarantena, come sotto riportato. Tutti i messaggi in quarantena sono automaticamente eliminati 35 giorni dopo la data di ricezione.

L`elenco sotto riportato è ordinato per punteggio di Spam crescente. Eventuali falsi positivi è più probabile che siano quindi in cima all`elenco.

- Virus = mail con contenuti infetti, non è possibile rilasciarla!
- Bad Content = mail con contenuti non permessi
- Infected = mail con script pericolosi nel contenuto , non è possibile rilasciarla!
- Spam = mail considerata spam
- Blacklisted = il mittente è presente nelle blacklist del servizio antispam

Received	From	To	Subject	Score	Reason	Preview
02/09/15 15:55:30	██@████it	davide██████@lib...	Re: INTERNAL_SPAM_TE...	5.85	Spam	[View]
02/09/15 15:55:30	██@████it	davide██ `@lib...	Re: INTERNAL_SPAM_TE...	5.85	Spam	[View]
02/09/15 15:55:29	██@████it	davide██████@lib...	Re: INTERNAL_SPAM_TE...	5.85	Spam	[View]
02/09/15 15:55:30	██@████it	davide██████@lib...	Re: INTERNAL_SPAM_TE...	6.64	Spam	[View]

To assign additional email address (**aliases**) to an user account press the [**+**] icon next to each account entry in the User list:

and add new email addresses. If the email address is added as active, then will be included in the user Quarantine Digest Report, otherwise not.

×**NOTE:** LDAP Users, will benefit of automatic alias association
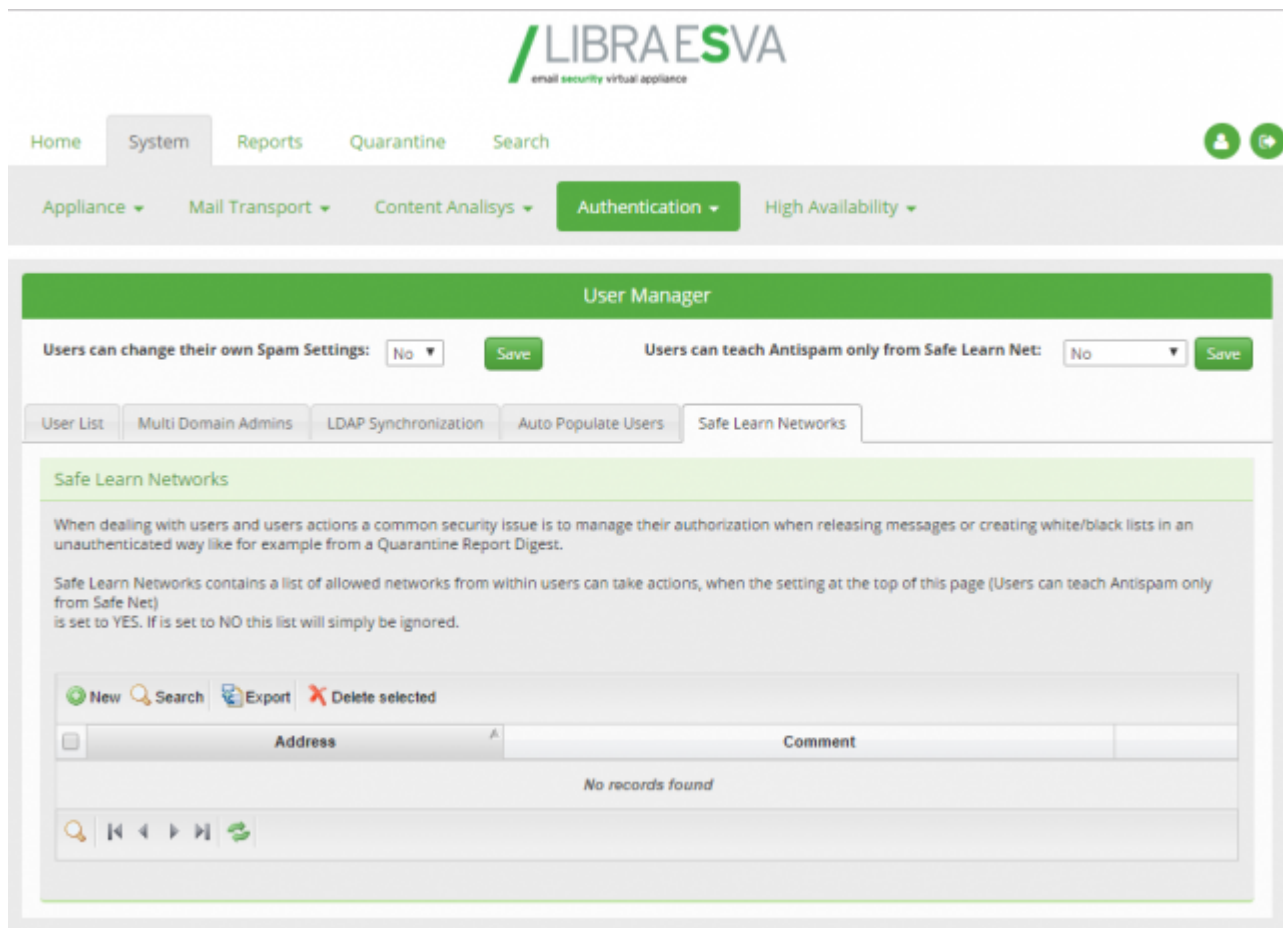
AutoPopulate

This feature allows auto user creation based on unique recipient addresses that received at least one email. Auto populated users are handy as Libraesva ESG will auto-configure the Daily Quarantine Report. User are created as local users. User auto creation is scheduled daily.

×**NOTE:** this feature can be enabled only for domains with a recipient verification defined.

Safe Learn Networks

This table allows to specify host/networks from within you authorized message interactions via Digest Report.

This is a security feature and can be explained in details as follows:

- **User can teach only from Safe Learn Net: No**
  Table entries are ignored and un-authenticated links from Digest Report are always accepted

- **User can teach only from Safe Learn Net: Yes, Silent**

  Un-authenticated links from Digest Report are validated agains this table entries and if the client making the request is not found the request will be silently dropped

- **User can teach only from Safe Learn Net: Yes, Warning**

  Un-authenticated links from Digest Report are validated agains this table entries and if the client making the request is not found the system will send a confirmation email to the intended recipient

Authorized devices

From the Quarantine settings an administrator can enable passwordless authentication for the users. When this feature is enabled, the user can generate a secure cookie on his device, which contain a secret token generated on the server; this way, the user can access LibraEsva whenever he needs to, without the need of a manual authentication.
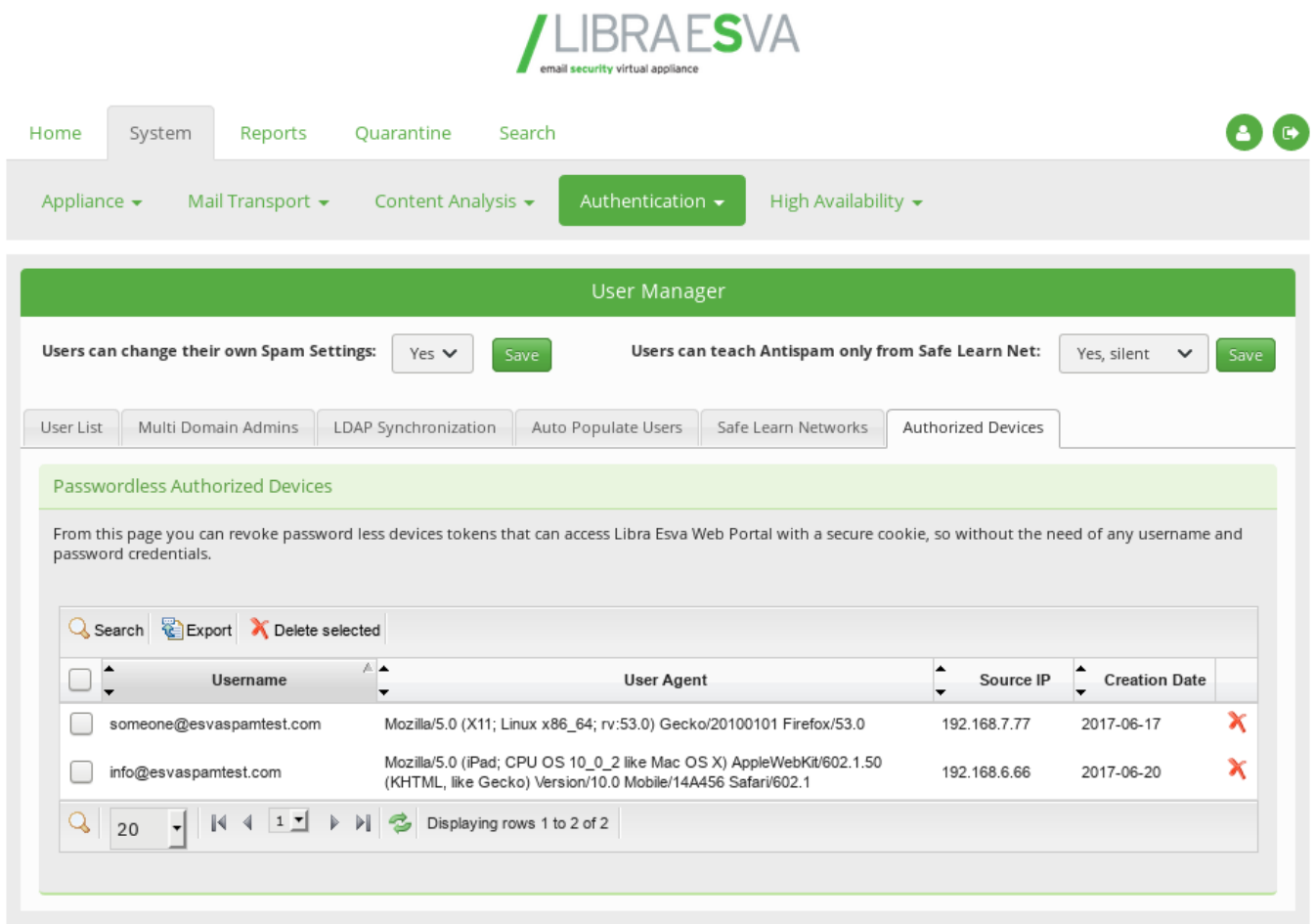
From this page you can see all active token on Libraesva ESG as well as some details of the owner, like the IP and the User Agent.

To revoke a token just remove a record here and the cookie will be disabled immediately.