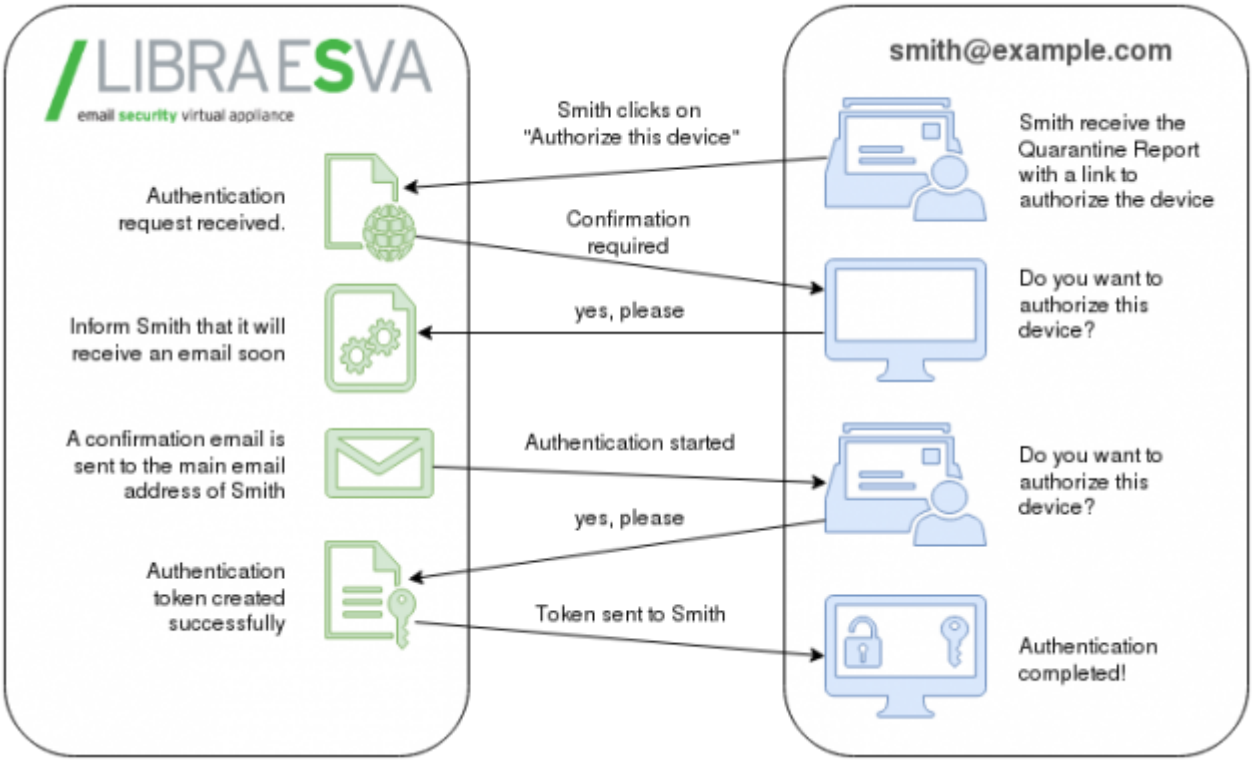
Passwordless authentication

Passwordless authentication

In Libraesva ESG you have multiple method to authorize the user to the web interface: POP3, IMAP, LDAP or a local password are all available for you to configure. The problem with this authentication is that the final user is required to remember the password of his own email — which is usually forgotten — or yet another password saved on Libraesva ESG.

To ease the login process you could enable a passwordless authentication. Despite the name, this method is quite secure and works pretty much like a typical “forgot the password” procedure; the authentication happens not upon clicking on the link inside the quarantine, but upon confirmation from an authentication email sent for this purpose.

How it works



When a user receive the Quarantine Report, it will find a link to authorize his current device. This link does not start immediately the authentication process, but ask for a confirmation to avoid simple mistakes.

An authentication email is then generated and sent to the user, with a link to access Libraesva

ESG without password. To grant the security of this process there are few precautions taken:

- the email is sent to the default address of the user, so there can be no mistake on the recipient
- the authentication is valid for a limited time
- the authentication can be used only once

Once the authentication is done, the user receive a cookie containing a secret token, used to match an authorized session on Libraesva ESG. As long as both ends will share the same secret, the user is able to authenticate without using a password.

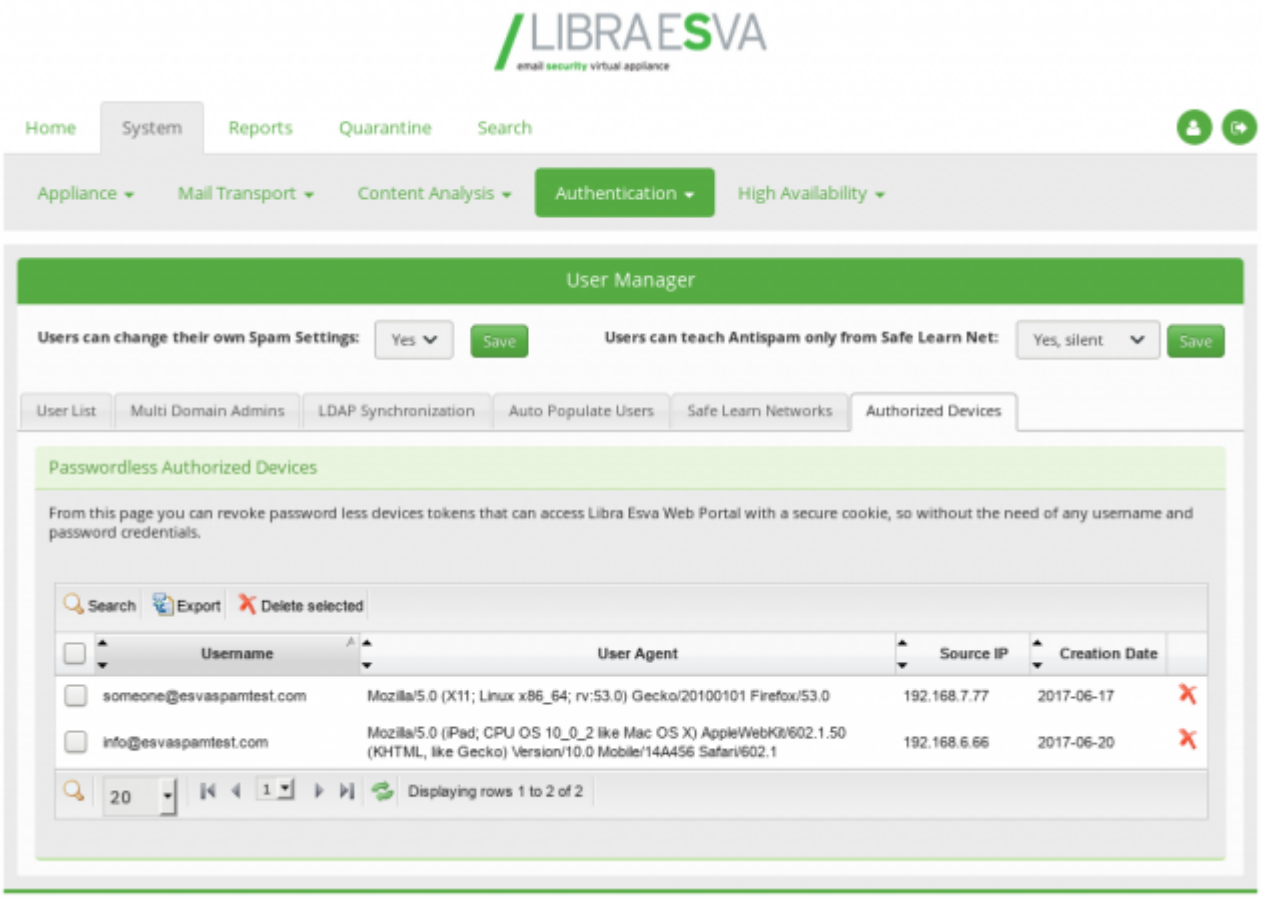
How to enable

Enabling passwordless authentication is pretty straightforward. You only need to access the quarantine settings and set “Permit Passwordless Authentication” to “YES”.

End Users will then have to click on the Passwordless Authentication link embedded in their Quarantine Report to authorize his current device as described above.

Maintenance of authorized devices

The authenticated token has an unlimited lifetime, and it’s up to the user to delete it by manually logout from ESG. But from time to time is the administrator who needs to invalidate the token; this is the case when an employee leave the company, or when a device is lost or otherwise compromised.



From the page **Authorized devices** located in System -> Authentication -> User Management, the administrator has a complete overview of all the token currently enabled, with the creation details: Source IP, creation Date and User Agent.

To un-authorize a token simply delete it. The user will no longer be able to automatically login, until it create a new token.