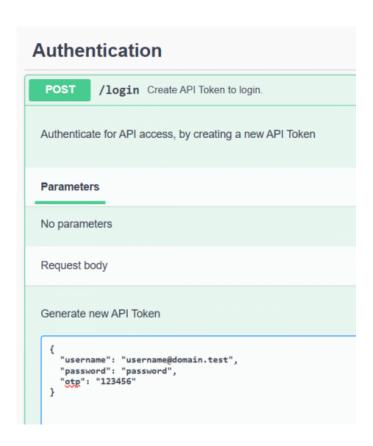# ESG API

The Libraesva Email Security Gateway exposes a set of Application Programming Interface.

APIs are always available, the list of all available APIs can be found inside ESG at path **/api/v2/** after authentication.

Example: *demo.esvacloud.com/api/v2/*

You can interact with APIs directly from the documentation page by authenticating with the "Authorize" button at the top right of the page, this authentication requires a valid **API Token**.

To generate an API Token a login must be performed on the **/api/v2/login** endpoint which will return a valid API Token that can be user do perform other API calls.

The API Token generated will inherit the permission of the User specified to perform the authentication on the /login endpoint if it's a normal User (present in the "User Management -> Users" table).

To perform an API call after the login you must pass the API Token in the "**X-ESG-Auth-Token**".

If the authentication is performed with an **API User** ("User Management -> API Users"), after the initial /login to generate the API Token you have to specify a ESG User to impersonate with the "**X-Switch-User**" header.

In this Header you must specify the **username** of the ESG User to impersonate, the API User performing the call inherits the permission of the specified user for this API call. Not specifying a user will result in a 403 error, the API User has no permission by default and can only perform the /login call.

Below you can see the headers that must be populated when you press the "Authorize" button to perform API calls directly from inside ESG.