
Setup guide for DeepL Single Sign-On (SSO)

SAML: OneLogin

Table of contents

[Requirements](#)

[1\) Create the DeepL SSO app](#)

[2\) Set the Configurations](#)

[3\) Add the Parameters](#)

[4\) Extract the Metadata](#)

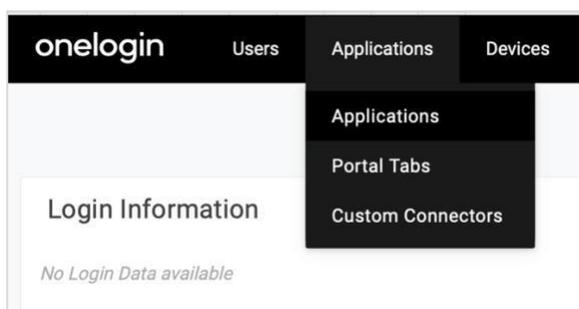
[5\) Enable DeepL Pro for your users](#)

Requirements

- A company domain has been defined for the DeepL environment. For further information please check our [Help Center article](#)

1) Create the DeepL SSO app

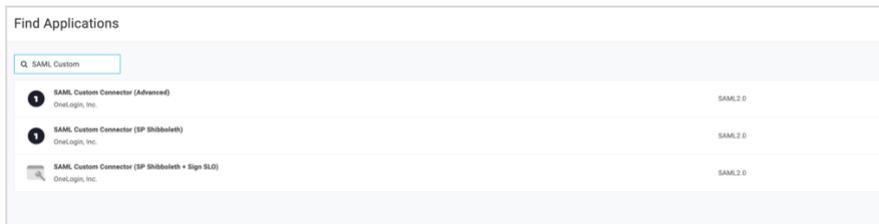
1. Open your OneLogin administration page and open the Applications section on task bar and click on *Applications*



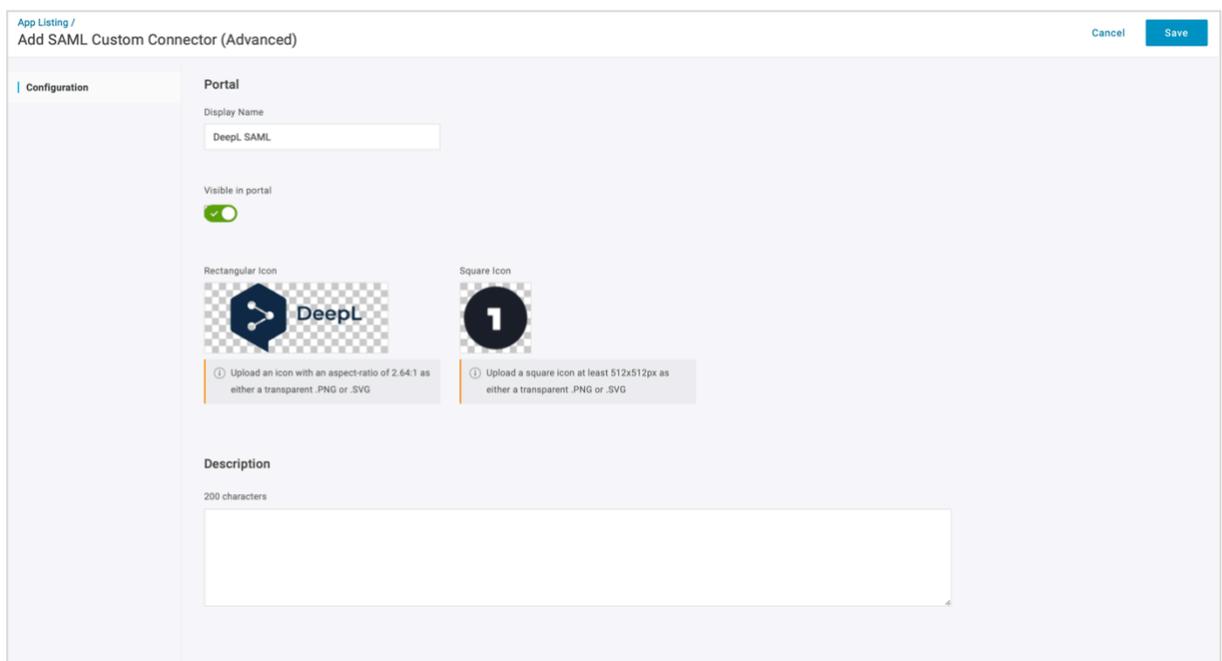
2. Click on *Add App*



3. Search for the *SAML Custom Connector (Advanced)* and click on it



4. Name your DeepL Application, add the logo from our website and click on save



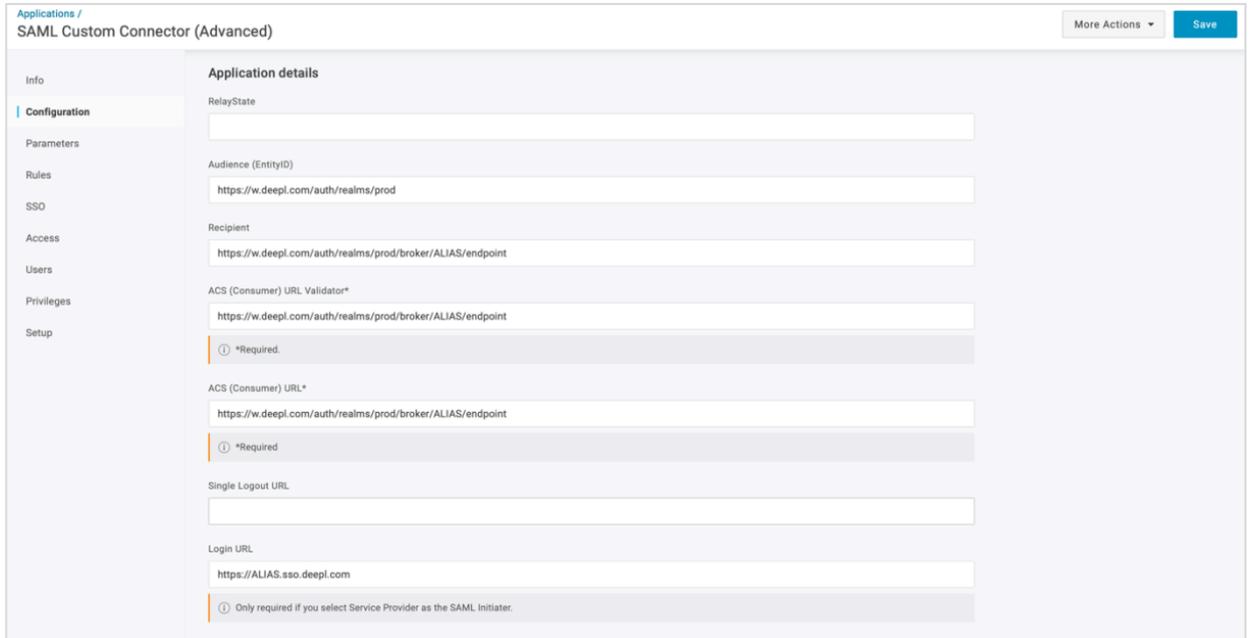
2) Set the Configurations

1. Click on *Configuration* on the left-hand bar
2. Enter the *Audience URL*: <https://w.deepl.com/auth/realms/prod>

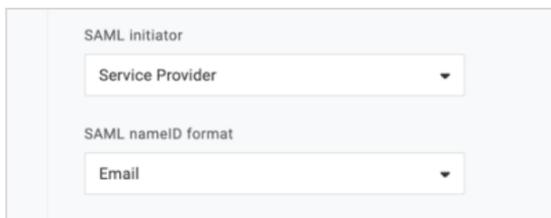
In *Recipient, ACS (Consumer) URL Validator* and *ACS (Consumer) URL* enter:

https://w.deepl.com/auth/realms/prod/broker/ALIAS/endpoint (replace ALIAS with your chosen company DOMAIN)

The login URL should be https://ALIAS.sso.deepl.com (replace ALIAS with your chosen company DOMAIN)

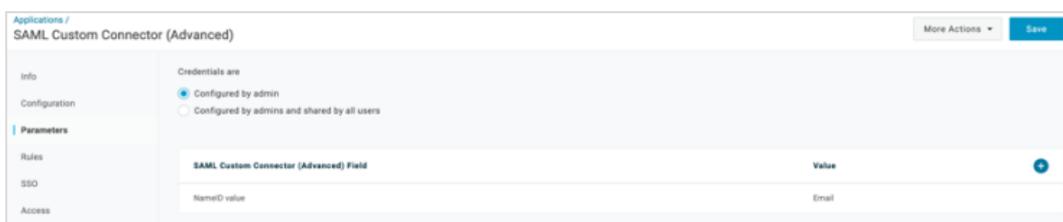


3. Switch the SAML Initiator to *Service Provider* and set SAML nameID format to *Email*. You can leave the remaining as default and click on save in the upper right corner.

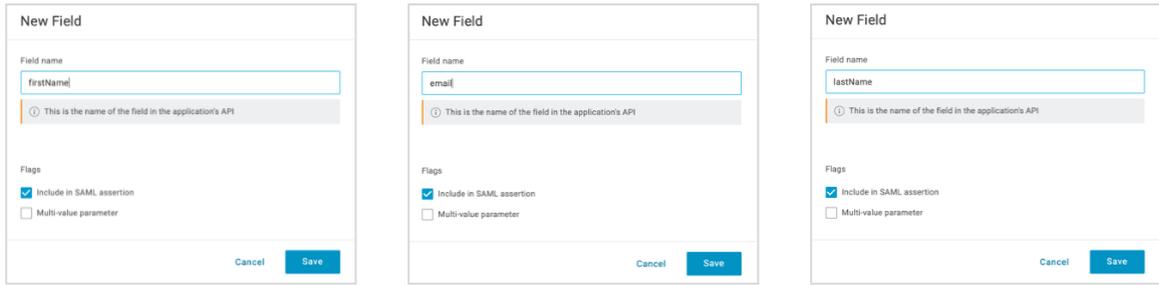


3) Add the Parameters

1. Click on *Parameters* on the left-hand bar
2. Click on the right side on the plus-symbol to add the SAML assertions



3. Add three SAML Assertion with following name *email*, *firstName* and *lastName*

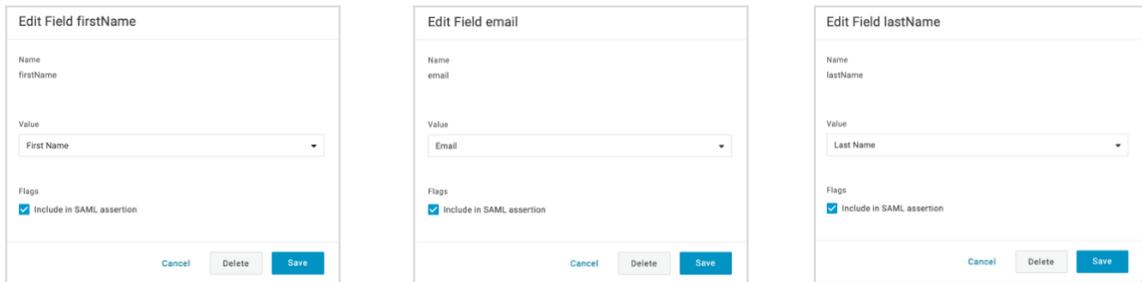


4. Map those parameters to the values and save them:

email: Email

firstName: First Name

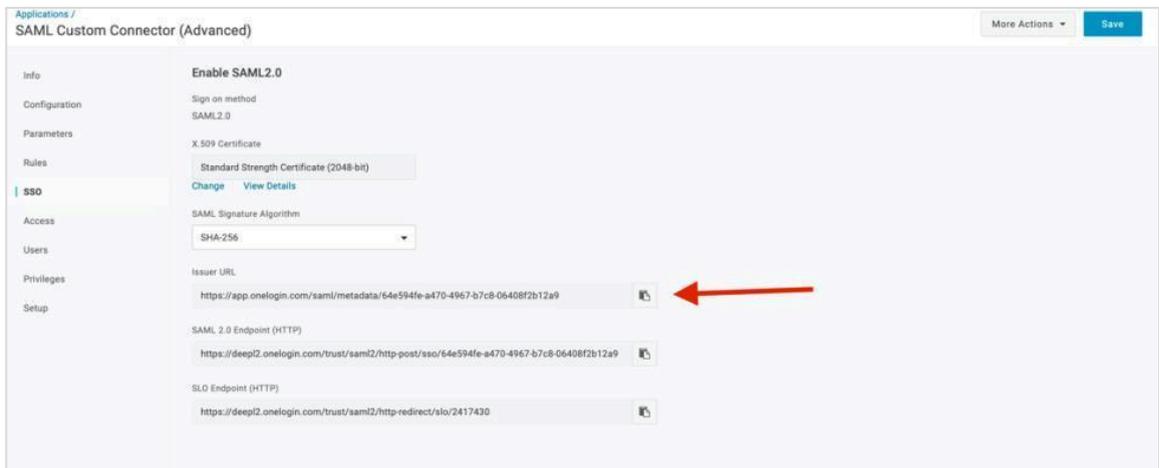
lastName: Last Name



4) Extract the Metadata

1. Click on SSO in the left-hand bar
2. Copy the metadata URL from *Issuer URL* and use it to set up SSO in your DeepL account.

Please use the SAML Assertion names as described in Step 3.3



5) Enable DeepL Pro for your users

Once the SSO connection has been established, you can give access to the dedicated users.

