



Setup guide for DeepL Single Sign-on (SSO)

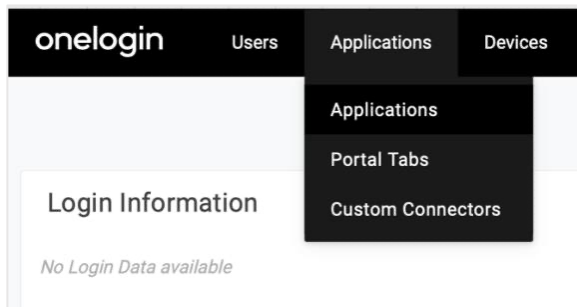
OneLogin SAML

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

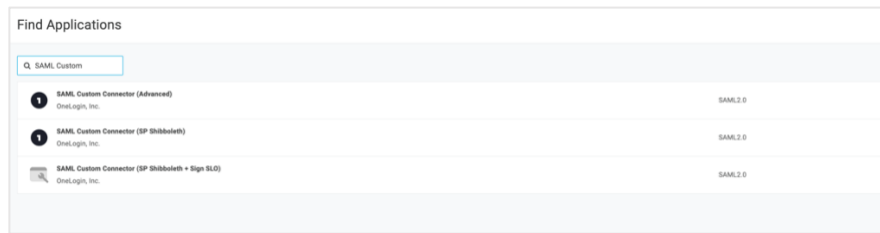
1. Open your OneLogin administration page and open the Applications section on task bar and click on *Applications*



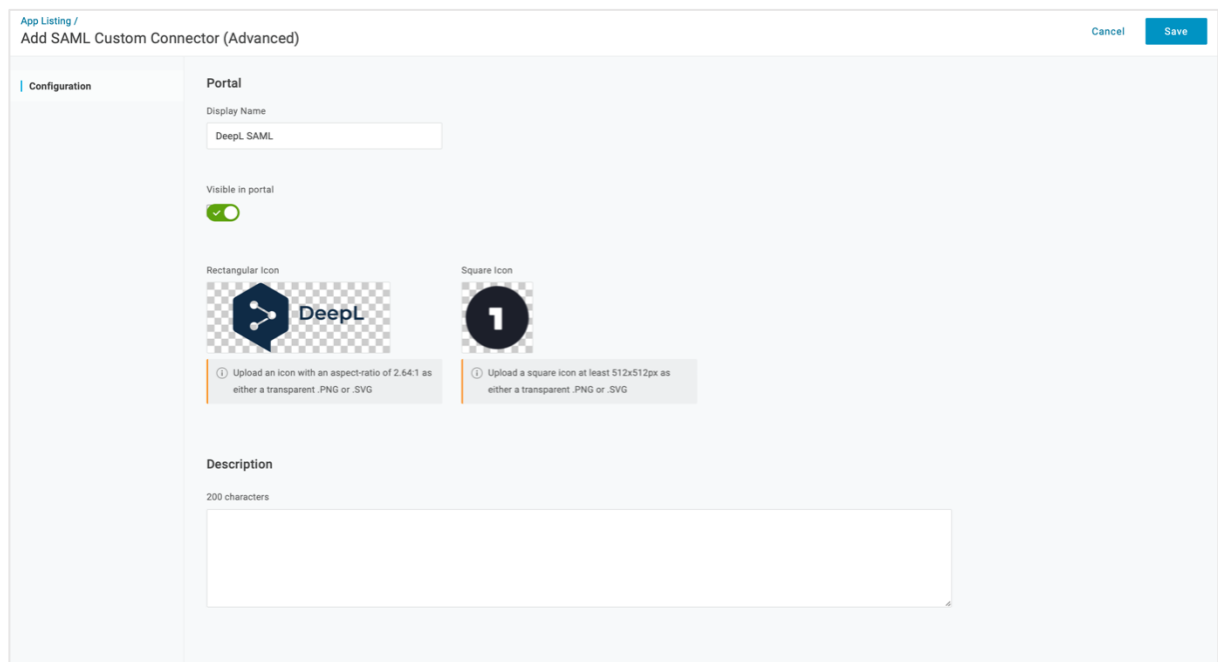
2. Click on *Add App*



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*)

Applications / SAML Custom Connector (Advanced) More Actions Save

Info

Configuration

Parameters

Rules

SSO

Access

Users

Privileges

Setup

Application details

RelayState

Audience (EntityID)

Recipient

ACS (Consumer) URL Validator*

ACS (Consumer) URL*

Single Logout URL

Login URL

*Required.

*Required

Only required if you select Service Provider as the SAML Initiator.

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.

SAML Initiator

Service Provider

SAML nameID format

Email

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

Applications / SAML Custom Connector (Advanced) More Actions Save

Info

Configuration

Parameters

Rules

SSO

Access

Users

Privileges

Setup

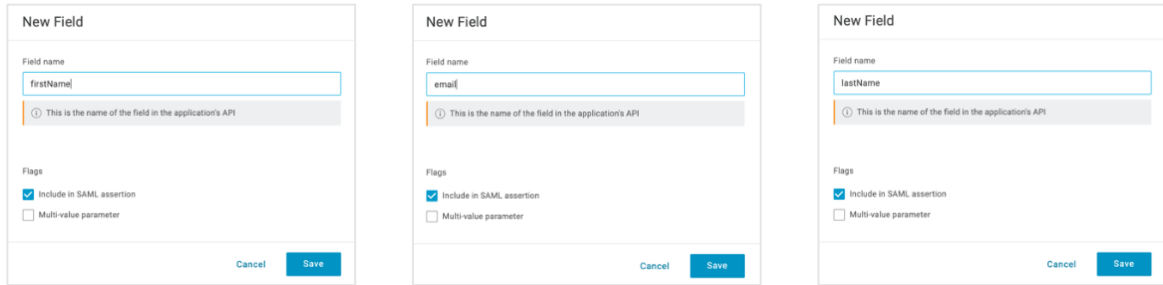
Credentials are

Configured by admin

Configured by admins and shared by all users

SAML Custom Connector (Advanced) Field	Value
NameID value	Email

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



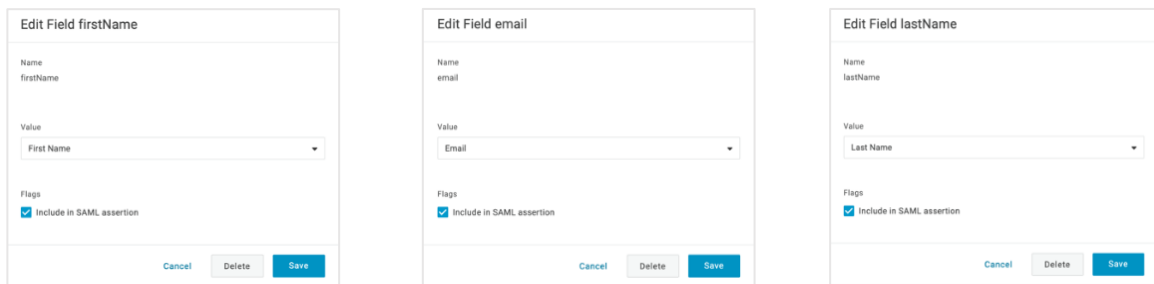
The image shows three 'New Field' forms side-by-side. Each form has a 'Field name' input field and a 'Flags' section. The first form has 'firstName' in the field name and 'Include in SAML assertion' checked. The second form has 'email' in the field name and 'Include in SAML assertion' checked. The third form has 'lastName' in the field name and 'Include in SAML assertion' checked. Each form also has a 'Multi-value parameter' checkbox which is unchecked, and 'Cancel' and 'Save' buttons at the bottom.

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

email: Email

firstName: First Name

lastName: Last Name

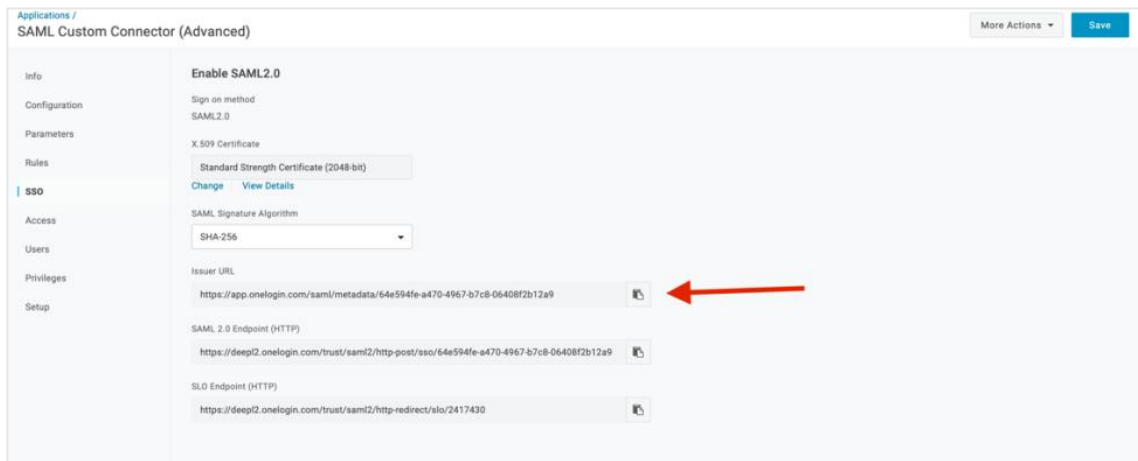


The image shows three 'Edit Field' forms side-by-side. Each form has a 'Name' field, a 'Value' dropdown menu, and a 'Flags' section. The first form has 'firstName' as the name and 'First Name' as the value. The second form has 'email' as the name and 'Email' as the value. The third form has 'lastName' as the name and 'Last Name' as the value. Each form also has 'Include in SAML assertion' checked and 'Cancel', 'Delete', and 'Save' buttons at the bottom.

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](#).

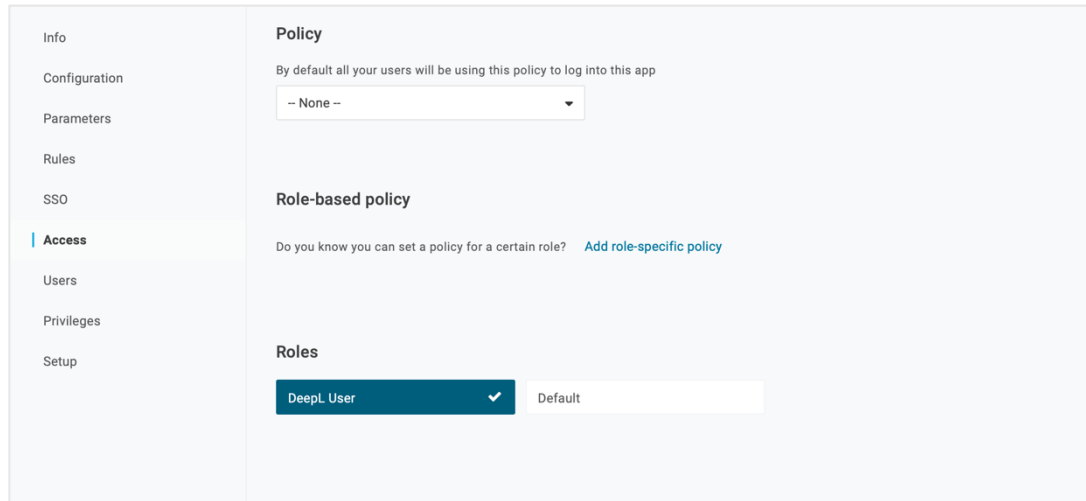
Please use the SAML Assertion names as described in Step 3.3



The image is a screenshot of the 'SAML Custom Connector (Advanced)' configuration page. The left sidebar shows a navigation menu with 'SSO' selected. The main content area is titled 'Enable SAML2.0' and shows various configuration options. The 'Issuer URL' field is highlighted with a red arrow pointing to it. The URL is 'https://app.onelogin.com/saml/metadata/64e594fe-a470-4967-b7c8-06408f2b12a9'. Other fields include 'SAML 2.0 Endpoint (HTTP)' and 'SLO Endpoint (HTTP)'. The 'Save' button is visible in the top right corner.

5) Enable DeepL Pro for your users

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



The screenshot displays a user management interface with a sidebar on the left and a main content area on the right. The sidebar contains the following menu items: Info, Configuration, Parameters, Rules, SSO, Access (highlighted with a blue bar), Users, Privileges, and Setup. The main content area is titled 'Policy' and includes the following sections:

- Policy**: A section with the text 'By default all your users will be using this policy to log into this app' and a dropdown menu currently set to '- None -'.
- Role-based policy**: A section with the text 'Do you know you can set a policy for a certain role?' and a link 'Add role-specific policy'.
- Roles**: A section with a dropdown menu showing 'DeepL User' (selected with a checkmark) and 'Default'.

