



# Setup guide for DeepL Single Sign-on (SSO)

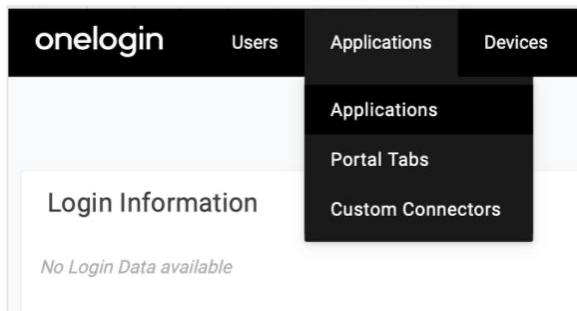
## OneLogin OpenID

### 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

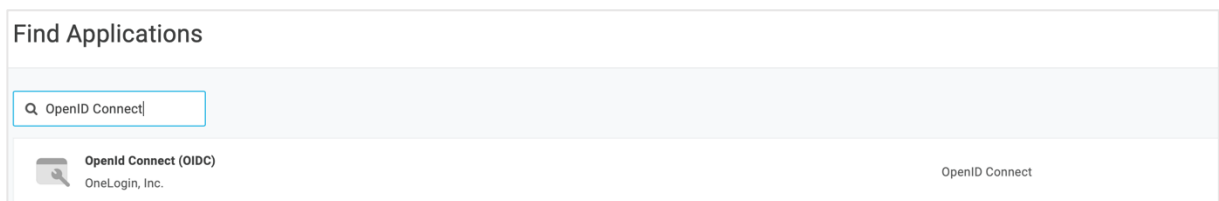
1. Open your OneLogin administration page and open the *Applications* section on task bar and click on *Applications*



2. Click on *Add App*



3. Search for *Openid Connect (OIDC)* and click on it



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


App Listing / Add OpenId Connect (OIDC) Cancel Save


**Configuration**

**Portal**

Display Name  
OpenId Connect (OIDC)

Visible in portal

Rectangular icon  
  
Upload an icon with an aspect-ratio of 2.64:1 as either a transparent .PNG or .SVG

Square icon  
  
Upload a square icon at least 512x512px as either a transparent .PNG or .SVG

Description  
200 characters

## 2) Set the configurations

1. Click on *Configuration* on the left-hand bar

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

Enter the Redirect URI:  
`https://w.deepl.com/auth/realms/prod/broker/ALIAS/endpoint` (*replace ALIAS with your chosen company DOMAIN*)

Applications / OpenId Connect (OIDC) More Actions Save

**Configuration**

**Application details**

Login Url  
`https://ALIAS.deepl.com`

Redirect URIs  
`https://w.deepl.com/auth/realms/prod/broker/ALIAS/endpoint`

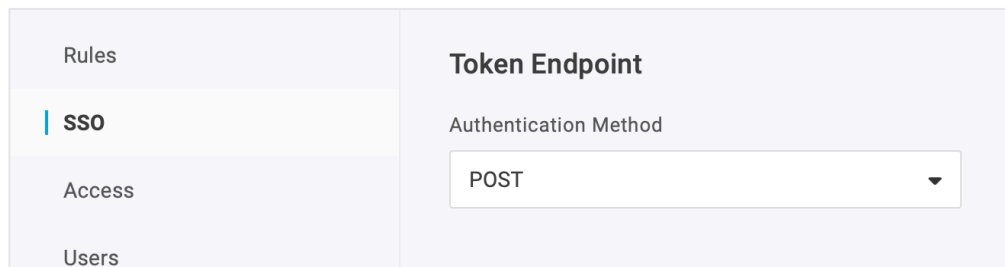
After the user is authenticated we only allow redirects back to entries on this comma (or new-line) separated list of uris, and HTTPS is required. http://localhost is permitted for development purposes only and should not be used in production.

Post Logout Redirect URIs

After the user is logged out by OIDC we only allow redirects back to entries on this comma (or new-line) separated list of uris, and HTTPS is required. http://localhost is permitted for development purposes only and should not be used in production.

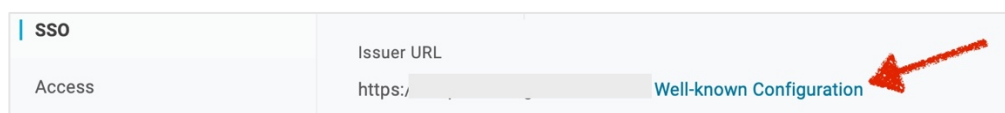
### 3) Get the endpoints, the client ID and secret value

1. Click on SSO on the left-hand bar
2. Set Authentication Method to *POST*



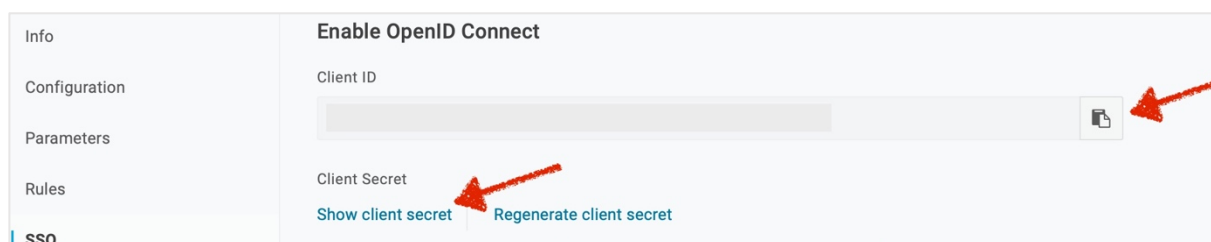
The screenshot shows a sidebar on the left with 'SSO' selected. The main content area is titled 'Token Endpoint' and contains a dropdown menu for 'Authentication Method' which is currently set to 'POST'.

3. Get the Endpoint IRL from *Issuer URL* and use it to [set up SSO in your DeepL account](#)



The screenshot shows the 'Issuer URL' field with a red arrow pointing to the 'Well-known Configuration' link. The URL is partially obscured by a grey box.

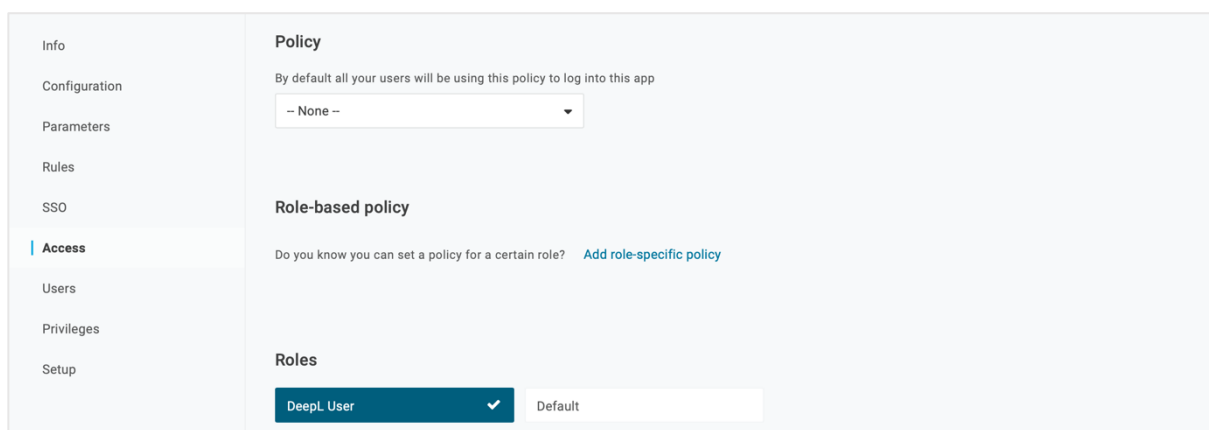
4. Copy the *Client ID* and the *Client Secret* and paste them in your SSO set up



The screenshot shows the 'Enable OpenID Connect' configuration page. The 'Client ID' field has a copy icon (red arrow) and the 'Client Secret' field has a 'Show client secret' button (red arrow) and a 'Regenerate client secret' button.

### 4) Enable DeepL Pro for your users

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



The screenshot shows the 'Access' configuration page. The 'Policy' section has a dropdown menu set to '- None -'. The 'Role-based policy' section has a link 'Add role-specific policy'. The 'Roles' section has a dropdown menu set to 'DeepL User' and a 'Default' button.

