

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

OpenID: OneLogin

#### Table of contents

Requirements1) Create the DeepL SSO app2) Set the configurations3) Get the endpoints, the client ID and secret value4) Enable DeepL Pro for your users

#### Requirements

• A company domain has been defined for the DeepL environment. For further information please check our <u>Help Center article</u>.

#### 1) Create the DeepL SSO app

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

onelogin	Users	Applications	Devices
		Applications	
		Portal Tabs	
Login Inform	ation	Custom Conne	ctors
No Login Data avail	able		

2. Click on Add App

onelogin	Users	Applications	Devices	Authentication	Activity	Security	Settings	Developers		TM Tore
Application	S								± Download JSON	Add App

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

Find Applications	
Q OpenID Connect	
OpenId Connect (OIDC) OneLogin, Inc.	OpenID Connect

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

App Listing / Add OpenId Connect	t (OIDC)		Cancel	S
Configuration	Portal			
	Display Name			
	OpenId Connect (OIDC)			
	Visible in portal			
	Rectangular Icon	Square Icon		
		and the second s		
		2		
		50000 B		
	<ol> <li>Upload an icon with an aspect-ratio of 2.64:1 as either a transparent .PNG or .SVG</li> </ol>	<ul> <li>Upload a square icon at least 512x512px as either a transparent .PNG or .SVG</li> </ul>		

### 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 👻
Info	Application details	
Configuration	Login Uri	
Parameters	https://ALIAS.deepl.com	
Rules	Redirect URI's	
SSO	https://w.deepl.com/auth/realms/prod/broker/ALIAS/endpoint	
Access		
Users		
Privileges	① After the user is authenticated we only allow redirects back to entries on this comma (or new-line) separated list of urls, and HTTPS is required.	
Setup	http://localhost is permitted for development purposes only and should not be used in production.	
	Post Logout Redirect URIs	

## 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

Rules	Token Endpoint
SSO	Authentication Method
Access	POST -
Users	

3. Get the Endpoint IRL from Issuer URL and use it to set up SSO in your DeepL account

SS0	Issuer URL	4
Access	https:/	Well-known Configuration

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

Info	Enable OpenID Connect
Configuration	Client ID
Parameters	E 🍝
Rules	Client Secret
SSO	Show client secret Regenerate client secret

#### 4) Enable DeepL Pro for your users

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

Info	Policy
Configuration	By default all your users will be using this policy to log into this app
Parameters	- None -
Rules	
SSO	Role-based policy
Access	Do you know you can set a policy for a certain role? Add role-specific policy
Users	
Privileges	
Setup	Roles
	DeepL User 🗸 Default

DeepL Help Center: <u>https://support.deepl.com</u>

DeepL Website: <u>https://www.deepl.com</u>