

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

SAML: OneLogin

#### Table of contents

Requirements <u>1) Create the DeepL SSO app</u> <u>2) Set the Configurations</u> <u>3) Add the Parameters</u> <u>4) Extract the Metadata</u> <u>5) Enable DeepL Pro for your users</u>

#### 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* 



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 the SAML Custom Connector (Advanced) and click on it

Find Applications		
Q SAML Dustom		
SAML Cautom Connector (Advanced)     OneLogin, Inc.	5AML2.0	
SAML Custom Connector (SP Shibboleth) OneLogin, Inc.	SAML2.0	
SAAL Costom Connector (SP Shibboleth + Sign SLO) OneLogin, Inc.	SAML2.0	

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

App Listing / Add SAML Custom Con	nector (Advanced)		
Configuration	Portal		
	Display Name		
	DeepL SAML		
	Visible in portal		
	Rectangular Icon	Square Icon	
	Upload an icon with an aspect-ratio of 2.64:1 as     either a transported _ BVC or _ SVC	Upload a square icon at least 512x512px as     either a transported. DNG or SVO	
	Description 200 characters		

### 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	L should be https://ALIAS.sso.deepl.com (replace ALIAS with yo	our chosen
company DON	MAIN)	

Applications / SAML Custom Connector	or (Advanced)	More Actions - Save
Info	Application details	
Configuration	RelayState	
Parameters		
Rules	Audience (EntityID)	
SSO	https://w.deepi.com/auth/realms/prod	
Access	Recipient	
Users	https://w.deepl.com/auth/realms/prod/broker/ALJAS/endpoint	
Privileges	ACS (Consumer) URL Validator*	
Setup	https://w.deepl.com/auth/realms/prod/broker/ALIAS/endpoint	
	① *Required.	
	ACS (Consumer) URL*	
	https://w.deepl.com/auth/realms/prod/broker/ALIAS/endpoint	
	() *Required	
	Single Logout URL	
	Login URL	
	https://ALJAS.sso.deepl.com	
	① Only required if you select Service Provider as the SAML Initiater.	

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 initia	ator	
Service I	Provider	-
	alD format	
SAML nam	leib loinat	

#### 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	Applications / SAML Custom Connector (Advanced)		More Actions $\mathbf{v}$	Save
info Configuration Parameters	Credentials are  Configured by admin  Configured by admins and shared by all users			
Rules	SAML Custom Connector (Advanced) Field	Value		•
Access	NamelD value	Email		

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

New Field	New Field	New Field
Field name	Field name email O This is the name of the field in the applications API	Field name IsstName ① This is the name of the Field in the application's API
Flags  Include in SAML assertion  Multi-value parameter	Flags Include in SAML assertion Multi-value parameter	Flags  Flags  Flags  Holude in SAML assertion  Multi-value parameter
Cancel Save	Cancel Save	Cancel Save

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

email: Email	firstName: First Name	lastName: Last Name
Edit Field firstName	Edit Field email	Edit Field lastName
Name firstName	Name email	Name IastName
Value First Name 👻	Value Email •	Value Last Name 👻
Plags Z Include In SAML assertion	Flags Sinclude in SAML assertion	Flags C Include in SAML assertion
Cancel Delete Save	Cancel Delete Save	Cancel Delete Save

#### 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 <u>set up SSO in your DeepL account</u>.

Please use the SAML Assertion names as described in Step 3.3

Applications / SAML Custom Connecto	r (Advanced)		More Actions - Save
Info Configuration Parameters Rules SSO Access Users Users Setup	Enable SAML2.0 Sigo on method SAML2.0 X.509 Certificate Standard Strength Certificate (2048-bit) Change Vere Details SAML: Signature Algorithm SHA: 256 SAML: Signature Algorithm SHA: 256 SAML: 2.0 Endpoint (NTTP) https://deepi2.onelogin.com/tust/saml2/http-post/sso/646594fe-a470-4967-b7c8-06408f2b12a9 SLOE Endpoint (HTTP) https://deepi2.onelogin.com/tust/saml2/http-redirect/slo/2417430	6	

## 5) Enable DeepL Pro for your 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

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