
Setup guide for DeepL Single Sign-On (SSO)

SAML: PingOne

Table of contents

[Requirements](#)

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

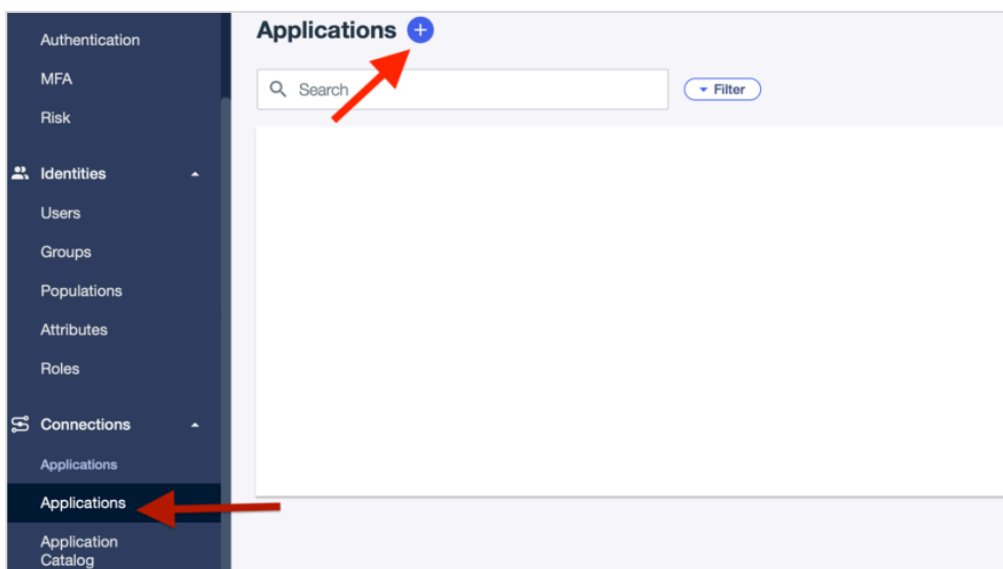
[2\) Extract the XML information setting the connection](#)

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 Ping administration page and open the *Applications* section on the left-hand side
2. Click on "+" to add a new application



3. Name the application DeepL or DeepL SSO, choose SAML Application and click on *configure*

Add Application

Application Name *
DeepL SSO

Description
[Empty text area]

Icon
[Placeholder image]
Max Size 1.0 MB

Application Type Show Details

Select an option below or view the [Application Catalog](#) to use a templated integration. If you can't find what you need in the catalog, consider SAML or OIDC to get started.

SAML Application OIDC Web App Native

Single-Page Worker

Configure **Cancel**

4. Click *Manual Enter* and enter the:

- ACS URL: `https://w.deepl.com/auth/realms/prod/broker/ALIAS/endpoint` (replace *ALIAS* with your chosen company *DOMAIN*)
- Entity ID: `https://w.deepl.com/auth/realms/prod`

Add Application

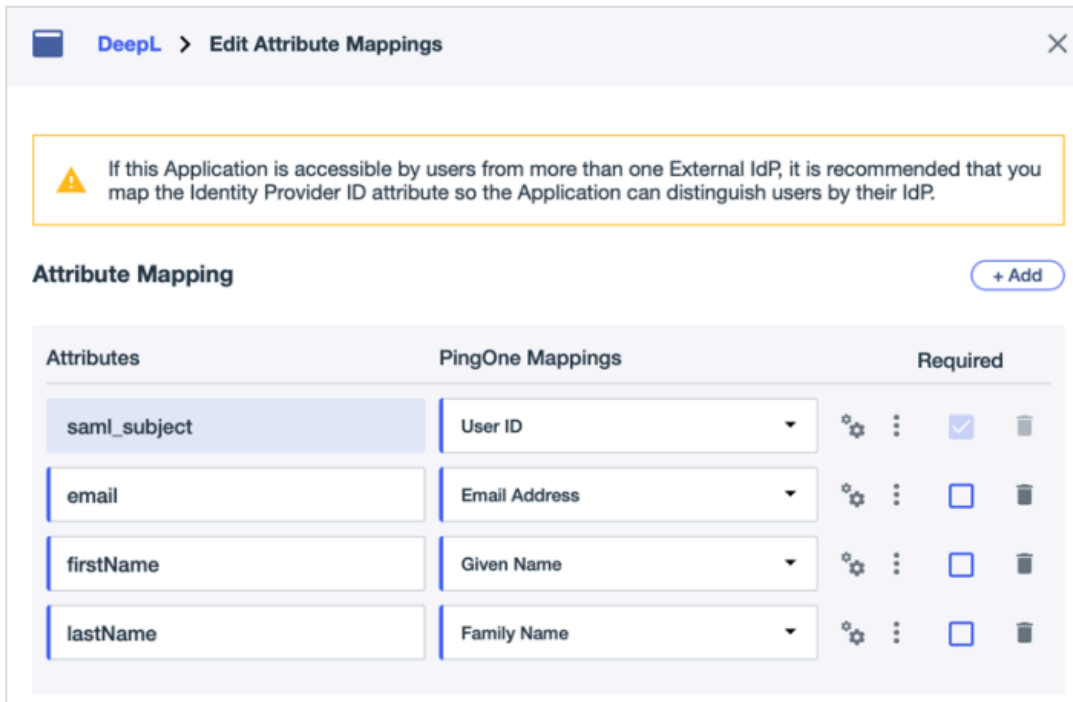
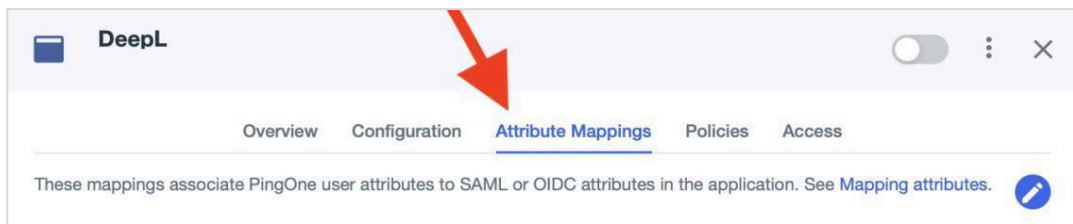
SAML Configuration

Provide Application Metadata
 Import Metadata Import From URL Manually Enter

ACS URLs *
https://w.deepl.com/auth/realms/prod/broker/ALIA...
[+ Add](#)

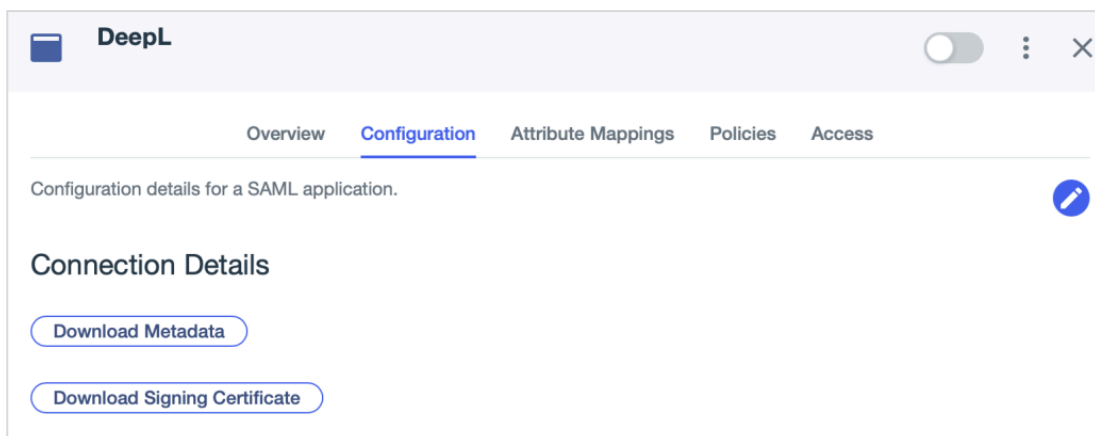
Entity ID *
https://w.deepl.com/auth/realms/prod

- Click on the tab *Attribute Mapping* and add the Attribute Statements *firstName*, *lastName*, and *email*

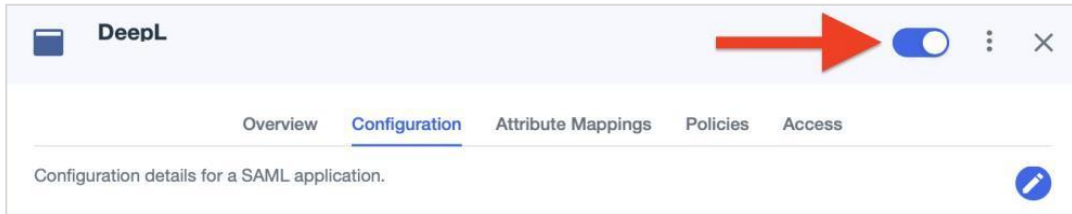


2) Extract the XML information setting the connection

- Open the tab *Configuration* and click on *Download Metadata* to receive the Metadata XML file



2. Enable the application



3. Provide the following data under set up SSO in your DeepL Account settings:

- Choose SAML as Authentication type
- Add the previously saved XML file
- Choose the NameID *persistent*
- Add the attributes as defined in Step 1, point 5

Set up SSO ✕

DeepL allows single sign-on authentication via OpenID Connect v.1.0 or SAML v.2.0. If your identity provider supports both authentication types, we recommend using OpenID Connect as it is easier to set up.

Authentication type

SAML ▾

Configure SAML

You can import external IDP metadata from a config file or from a URL. The administrator of your identity provider is the best contact person for the required information.

Import from URL ?

Import from file ?

NameID policy format

Email ▾

Assertion attribute: First name ?

Assertion attribute: Last name ?

Assertion attribute: Email address ?

! After confirmation, you will have the opportunity to test the configuration before activating it for the whole team. Your team cannot log in via SSO yet and has to use the standard login with email address and password.