

Setup guide for DeepL Single Sign-On (SSO)

SAML: PingOne

Table of contents

Requirements

 Create the DeepL SSO app
 Extract the XML information setting the connection

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

	Authentication	Applications 🛨
	MFA	Q Search (Filter)
	Risk	
. .	Identities	
	Users	
	Groups	
	Populations	
	Attributes	
	Roles	
u	Connections	
	Applications	
	Applications	
	Application Catalog	

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

Add Application		×
Application Name • DeepL SSO		
Description		
	11	
Max Size 1.0 MB		
Application Type		Show Details
Select an option below or can't find what you need	r view the Application Catalog to us in the catalog, consider SAML or C	e a templated integration. If you IDC to get started.
SAML Application	S OIDC Web App	☐ Native
Single-Page	Vorker	
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	

5. Click on the tab Attribute Mapping and add the Attribute Statements firstName, lastName, and email

DeepL				0		×
Overview Co	onfiguration Attribute Map	pings Policies A	ccess			
These mappings associate PingOne user a	ttributes to SAML or OIDC attri	butes in the application	. See Map	ping at	ttributes.	0
DeepL > Edit Attribute Ma	appings					×
If this Application is accessit map the Identity Provider ID Attribute Mapping	ble by users from more tha attribute so the Applicatio	n one External IdP, i n can distinguish us	t is recon ers by th	nmen eir Idf	ded tha	it you + Add
Attributes	PingOne Mapping	s		F	Require	d
saml_subject	User ID	-	°o	:		Î
email	Email Address	-	°o	:		Î
firstName	Given Name	-	°o	:		Î
lastName	Family Name	-	°.	:		i i

- 2) Extract the XML information setting the connection
 - 1. Open the tab *Configuration* and click on *Download Metadata* to receive the Metadata XML file

	DeepL						•	×
		Overview	Configuration	Attribute Mappings	Policies	Access		
Configu	uration details for	r a SAML appli	cation.					
Conn	nection Det	tails						
Down	nload Metadata							
Down	nload Signing C	Certificate						

2. Enable the application

	DeepL				-		:	×
		Overview	Configuration	Attribute Mappings	Policies	Access		
Config	guration details for	a SAML appli	cation.					0

- 3. Provide the following data under set up SSO in your <u>DeepL Account settings</u>:
 - 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 v.2.0. If using C	allows single sign-on authentication via OpenID Connect v.1.0 or SAML your identity provider supports both authentication types, we recommend penID Connect as it is easier to set up.
Authen	ication type
SAML	· · · · · · · · · · · · · · · · · · ·
Config	ure SAML
You car adminis informa	import external IDP metadata from a config file or from a URL. The trator of your identity provider is the best contact person for the required tion.
Impo	rt from URL 🕕
ା _{mpo}	rt from file 🕕
⊂ _{Impo} NameIĽ Email	rt from file 👔 policy format
Impo NameIC Email Assertie	rt from file 👔 policy format on attribute: First name 👔
Impo NamelC Email Asserti	rt from file 1 policy format on attribute: First name 1
Impo Namel Email Assertio	rt from file 👔 policy format
Impo NamelE Email Assertio	rt from file 1 policy format on attribute: First name 1 on attribute: Last name 1
Impo NamelE Email Assertio	rt from file 1 policy format
Impo NamelE Email Assertio Assertio	rt from file 1 policy format on attribute: First name 1 on attribute: Last name 1 on attribute: Email address 1
Impo NamelE Email Assertio	rt from file 1 policy format on attribute: First name 1 on attribute: Last name 1 on attribute: Email address 1