Setup guide for DeepL Single Sign-On (SSO)

SAML: Google

Table of contents

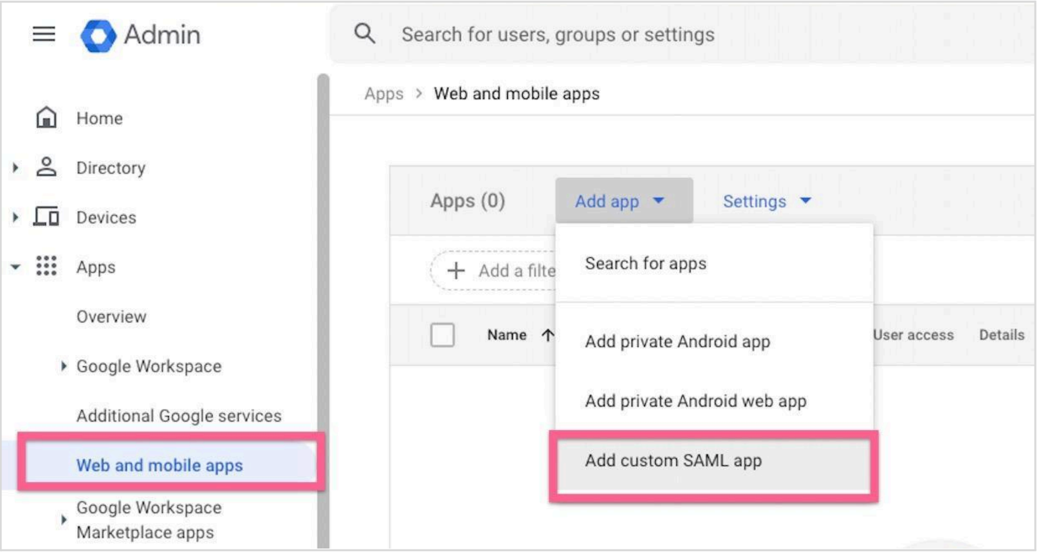
Requirements

- You have administrative permissions to create a custom SAML application within the Google Workspace
- A company domain has been defined for the DeepL environment. For further information please check our Help Center article

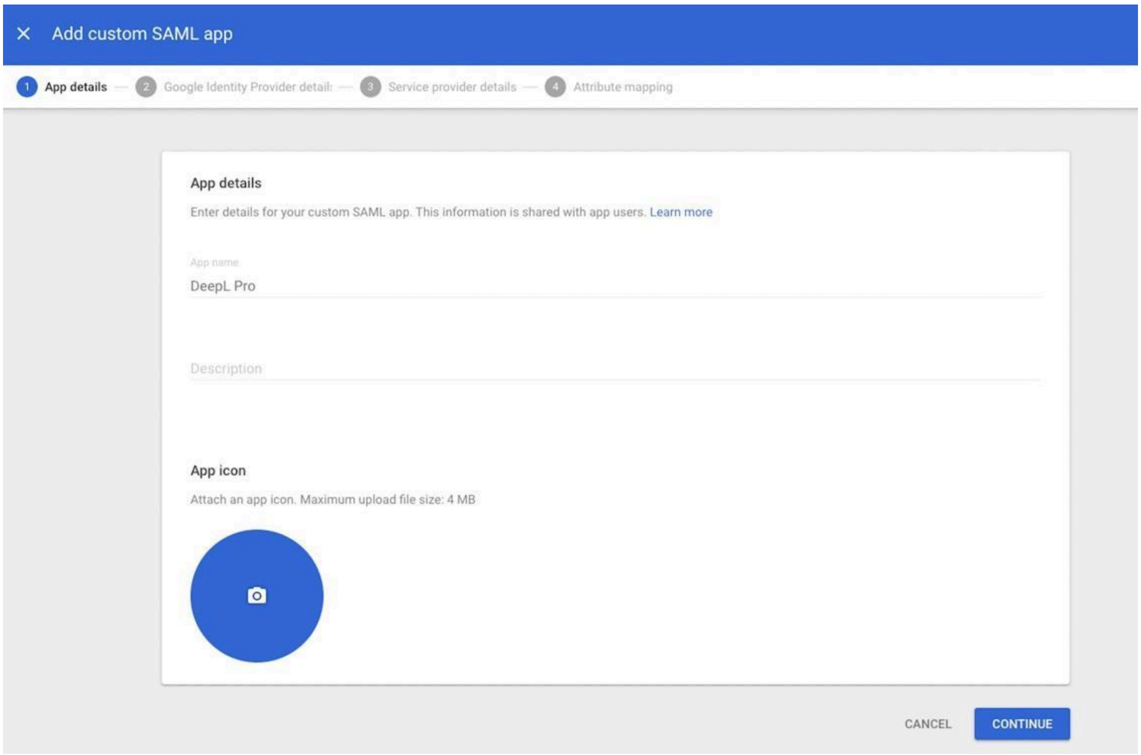
1) Open Google Admin console and add custom SAML app

1. In the Admin console, go to Menu and then *Apps* > *Web and mobile apps*

2. Click *Add App* > *Add custom SAML app*



3. Enter information on the App Details page



App details

Enter details for your custom SAML app. This information is shared with app users. Learn more

App name: DeepL Pro

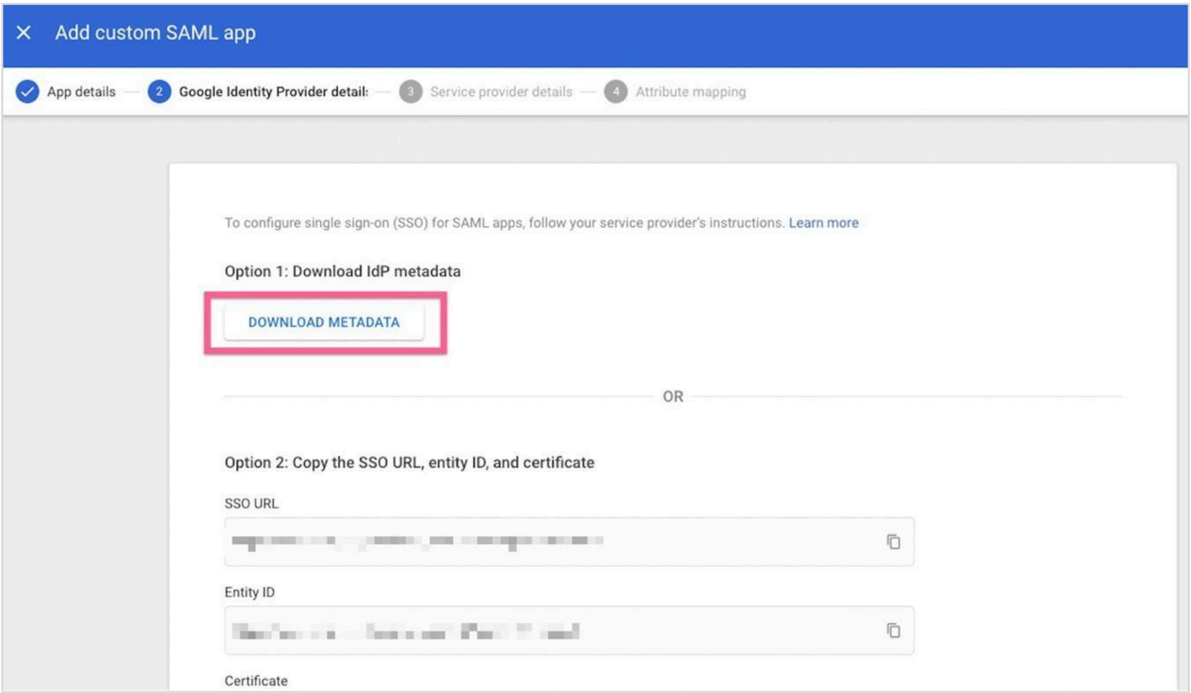
Description

App icon

Attach an app icon. Maximum upload file size: 4 MB

4. Click *Continue*

2) Download the Metadata XML



× Add custom SAML app

✓ App details — 2 Google Identity Provider detail: — 3 Service provider details — 4 Attribute mapping

To configure single sign-on (SSO) for SAML apps, follow your service provider's instructions. Learn more

Option 1: Download IdP metadata

DOWNLOAD METADATA

OR

Option 2: Copy the SSO URL, entity ID, and certificate

SSO URL

[redacted]

Entity ID

[redacted]

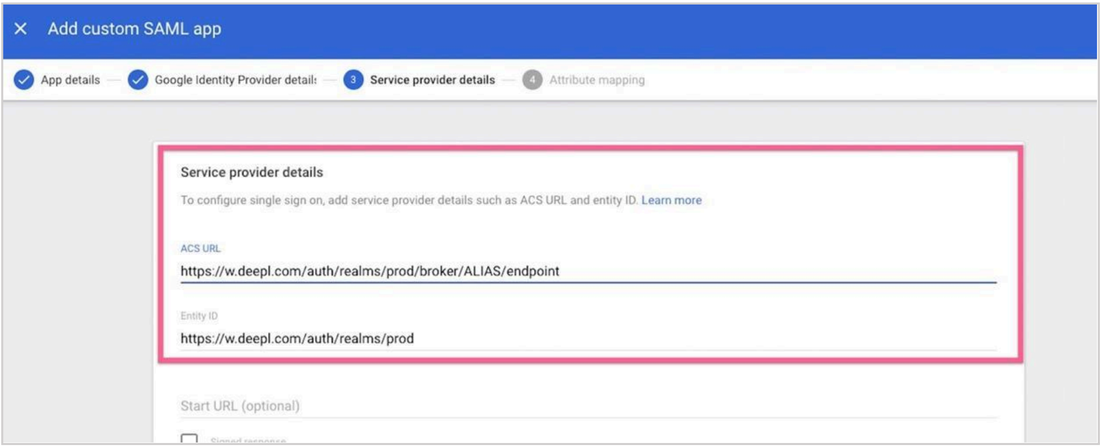
Certificate

3) Configure Service Provider Details

1. Define details:

    - 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 custom SAML app

✓ App details — ✓ Google Identity Provider detail: — 3 Service provider details — 4 Attribute mapping

Service provider details

To configure single sign on, add service provider details such as ACS URL and entity ID. Learn more

ACS URL

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

Entity ID

https://w.deepl.com/auth/realms/prod

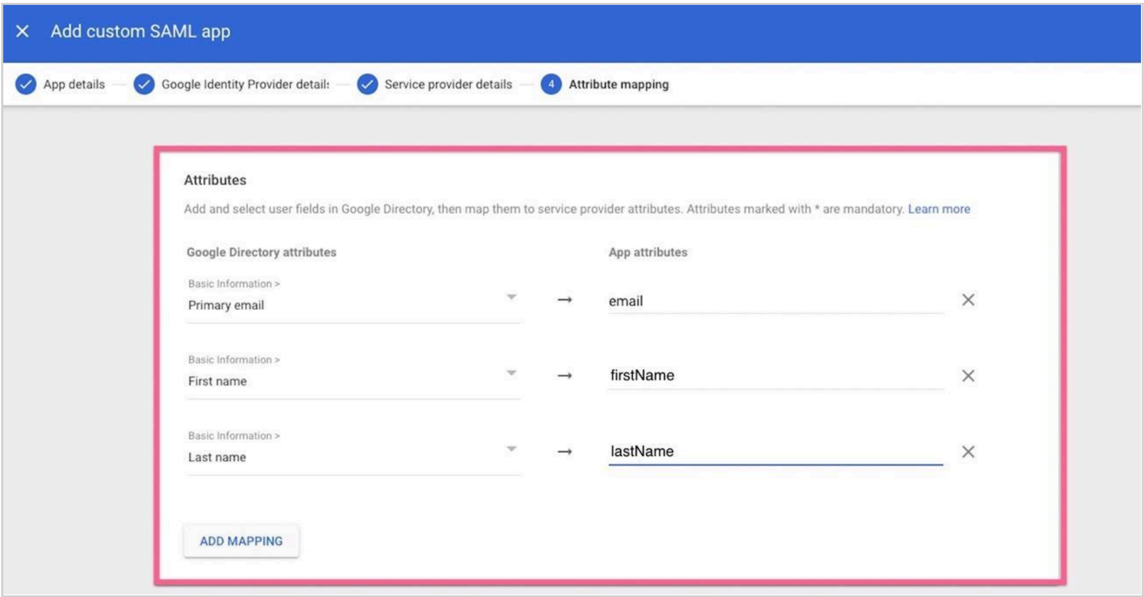
Start URL (optional)

□ Signed response

2. Click *Continue*

4) Claims and Attributes

1. Set the attribute mapping: Primary email, First name and Last name
2. Click *Finish*



Attributes

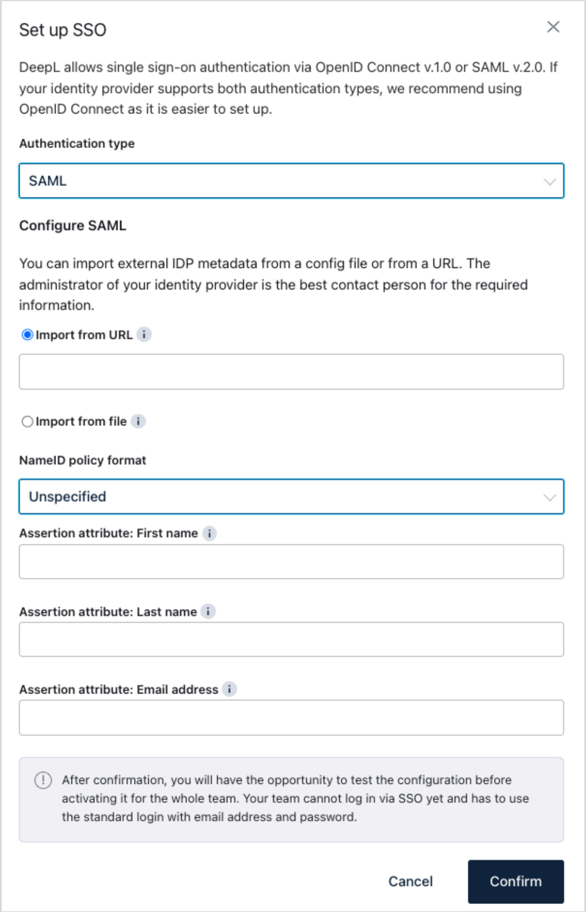
Add and select user fields in Google Directory, then map them to service provider attributes. Attributes marked with * are mandatory. Learn more

Google Directory attributes		App attributes
Basic Information > Primary email	→	email
Basic Information > First name	→	firstName
Basic Information > Last name	→	lastName

5) Provide data

Provide the following data in your **DeepL Account**:

- Select the Authentication type *SAML*
- Upload IdP Metadata XML
- NameID policy format as chosen in Step 3
- Set the attributes firstName, lastName, email



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: Unspecified

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.

6) Turn on your SAML app on Google Workspace

Please refer to the article in Google's Help Center if necessary.