



Setup guide for DeepL Single Sign-on (SSO)

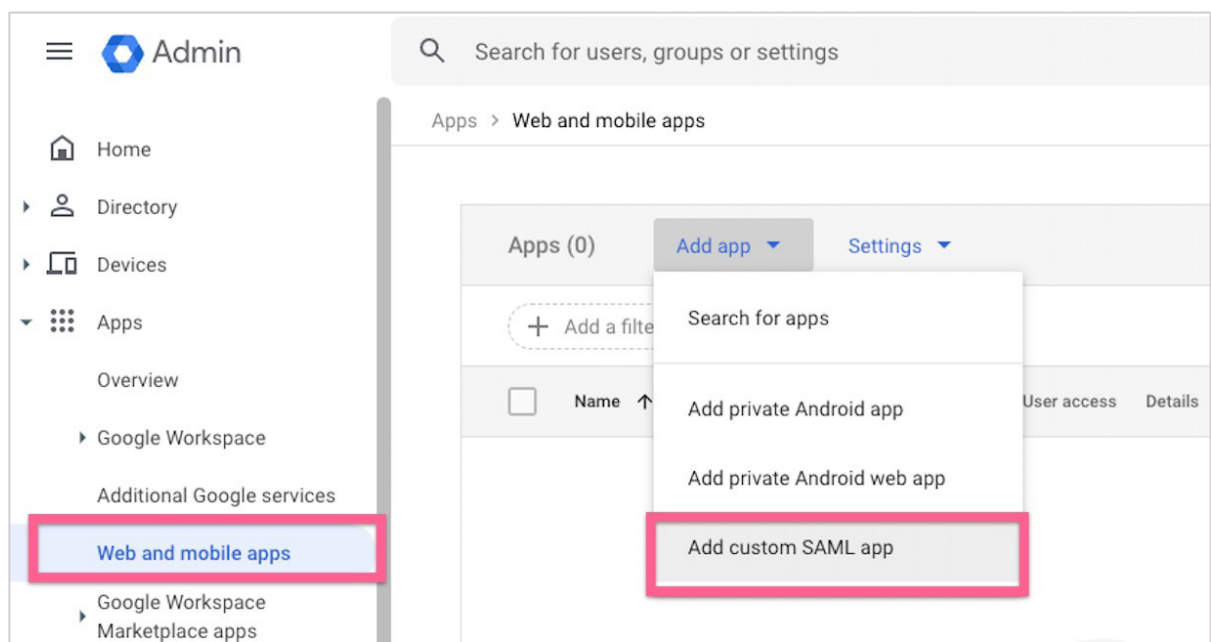
Google Workspace SAML

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

The screenshot shows the 'Add custom SAML app' interface. At the top, there is a blue header with a close button and the title 'Add custom SAML app'. Below the header is a progress bar with four steps: 1. App details (active), 2. Google Identity Provider details, 3. Service provider details, and 4. Attribute mapping. The main content area is titled 'App details' and contains the following fields:

- App name:** A text input field containing 'DeepL.Pro'.
- Description:** A text input field that is currently empty.
- App icon:** A section with the instruction 'Attach an app icon. Maximum upload file size: 4 MB'. Below this is a large blue circular button with a white camera icon, indicating an upload function.

At the bottom right of the form, there are two buttons: 'CANCEL' and 'CONTINUE'.

4. Click *Continue*

2) Download the Metadata XML

The screenshot shows the 'Add custom SAML app' interface at the 'Google Identity Provider details' step. The progress bar at the top shows four steps: 1. App details, 2. Google Identity Provider details (active), 3. Service provider details, and 4. Attribute mapping. The main content area contains the following information:

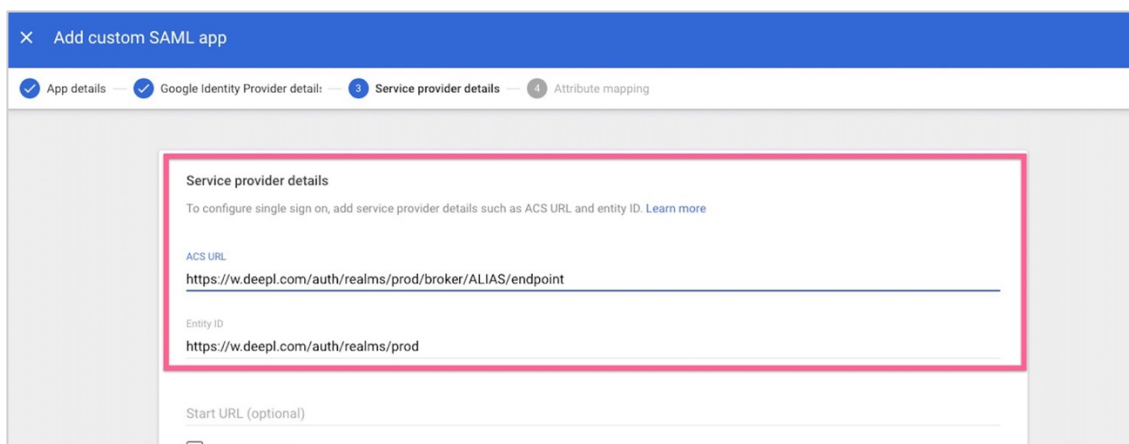
- A heading: 'Option 1: Download IdP metadata'. Below it is a blue button labeled 'DOWNLOAD METADATA', which is highlighted with a red rectangular box.
- A separator: 'OR'.
- A heading: 'Option 2: Copy the SSO URL, entity ID, and certificate'. Below this are three input fields:

- SSO URL:** A text input field containing a blurred URL, with a copy icon on the right.
- Entity ID:** A text input field containing a blurred ID, with a copy icon on the right.
- Certificate:** A text input field that is currently empty.

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`

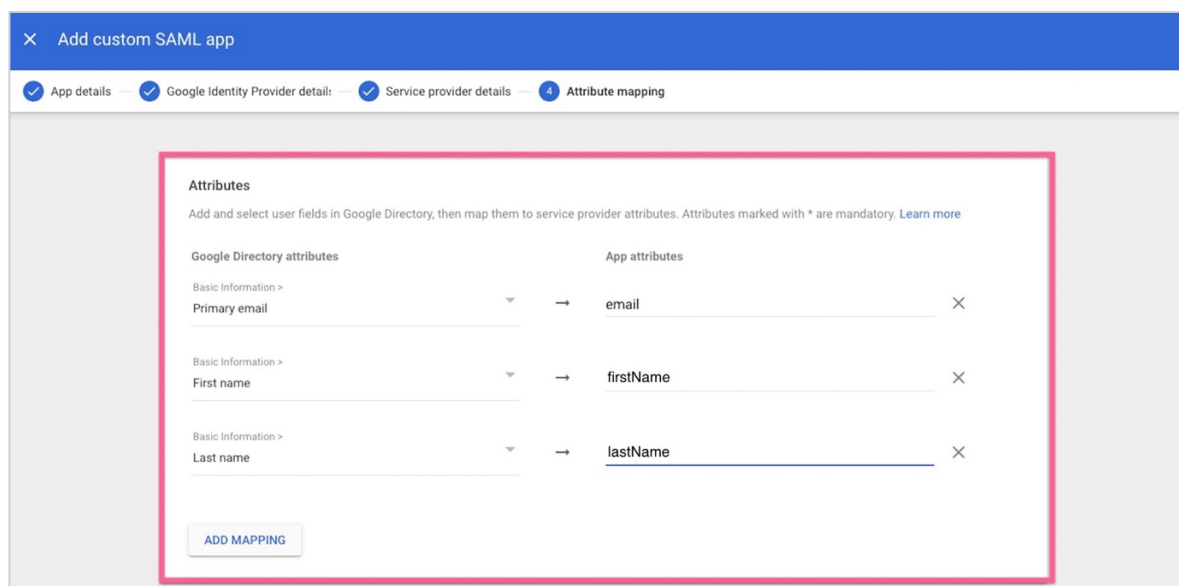


2. Click *Continue*

4) Claims and Attributes

1. Set the attribute mapping: Primary email, First name and Last name

2. Click *Finish*



5) Provide data

1. Provide the following data in your DeepL Account settings:

- 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.

Cancel Confirm

6) Turn on your SAML app on Google Workspace

Please refer to the [article in Google's Help Center](#) if necessary.