



Setup guide for DeepL Single Sign-on (SSO)

Azure AD (Microsoft Entra ID) SAML

Requirements

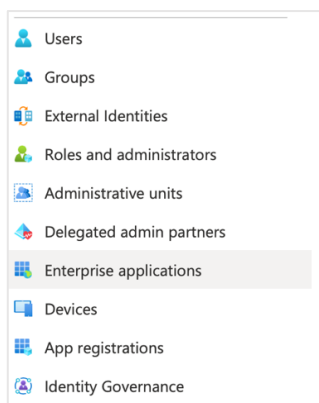
- You have an Azure AD set up
- You have administrative permissions to create an app within the Azure AD tenant
- A company domain has been defined for the DeepL environment. For further information please check our [Help Center article](#).

1) Open Azure AD management

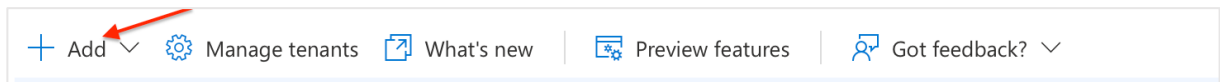
- Open <https://portal.azure.com> and select *Azure AD*. The direct link is https://portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/Overview

2) Register enterprise app

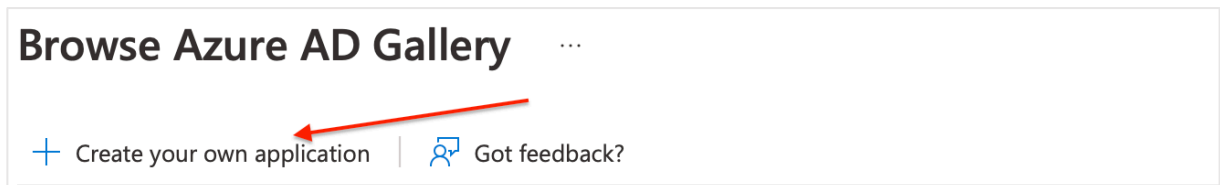
1. Select *App registrations* in the left-hand menu



2. Click *Add* on the top panel



3. Click *Create your own application*




4. Create a Non-gallery app

A screenshot of the 'Create your own application' dialog box. The title is 'Create your own application' with a close button (X) in the top right corner. Below the title is a 'Got feedback?' link. The main text reads: 'If you are developing your own application, using Application Proxy, or want to integrate an application that is not in the gallery, you can create your own application here.' Below this is a question: 'What's the name of your app?' followed by a text input field containing 'DeepL Pro' and a green checkmark. Another question follows: 'What are you looking to do with your application?' with three radio button options: 'Configure Application Proxy for secure remote access to an on-premises application', 'Register an application to integrate with Azure AD (App you're developing)', and 'Integrate any other application you don't find in the gallery (Non-gallery)'. The third option is selected. At the bottom left is a blue 'Create' button.

3) Configure initial settings


1. Click on *Set up Single Sign On*

Getting Started

**1. Assign users and groups**


Provide specific users and groups access to the applications

[Assign users and groups](#)

**2. Set up single sign on**


Enable users to sign into their application using their Azure AD credentials

[Get started](#)

**3. Provision User Accounts**

Automatically create and delete user accounts in the application

[Get started](#)

**4. Conditional Access**

Secure access to this application with a customizable access policy.


[Create a policy](#)

2. Edit basic SAML configuration

Set up Single Sign-On with SAML

An SSO implementation based on federation protocols improves security, reliability, and end user experiences and is easier to implement. Choose SAML single sign-on whenever possible for existing applications that do not use OpenID Connect or OAuth. [Learn more.](#)

Read the [configuration guide](#) for help integrating DeepL Pro .

- Basic SAML Configuration** Edit
Identifier (Entity ID) **Required**
Reply URL (Assertion Consumer Service URL) **Required**
Sign on URL *Optional*
Relay State (Optional) *Optional*
Logout Url (Optional) *Optional*
- Attributes & Claims**
 Fill out required fields in Step 1
givenname user.givenname
surname user.surname
emailaddress user.mail
name user.userprincipalname
Unique User Identifier user.userprincipalname

- Set the Entity ID to <https://w.deepl.com/auth/realms/prod>
- Set the Reply URL to <https://w.deepl.com/auth/realms/prod/broker/ALIAS/endpoint>

Replace ALIAS with your chosen company DOMAIN and save the set values.

Basic SAML Configuration

Save | Got feedback?

Identifier (Entity ID) * ⓘ

The unique ID that identifies your application to Azure Active Directory. This value must be unique across all applications in your Azure Active Directory tenant. The default identifier will be the audience of the SAML response for IDP-initiated SSO.

Default

✓ [Check] ⓘ [Delete]

[Add identifier](#)

Reply URL (Assertion Consumer Service URL) * ⓘ

The reply URL is where the application expects to receive the authentication token. This is also referred to as the "Assertion Consumer Service" (ACS) in SAML.

	Index	Default
<input type="text" value="https://w.deepl.com/auth/realms/prod/broker/ALIAS/endpoint"/> ✓	<input type="text"/>	<input checked="" type="checkbox"/> ⓘ [Delete]

[Add reply URL](#)

4) Claims and Attributes

- Set the claims and attributes:
 - email address
 - givenname
 - surname

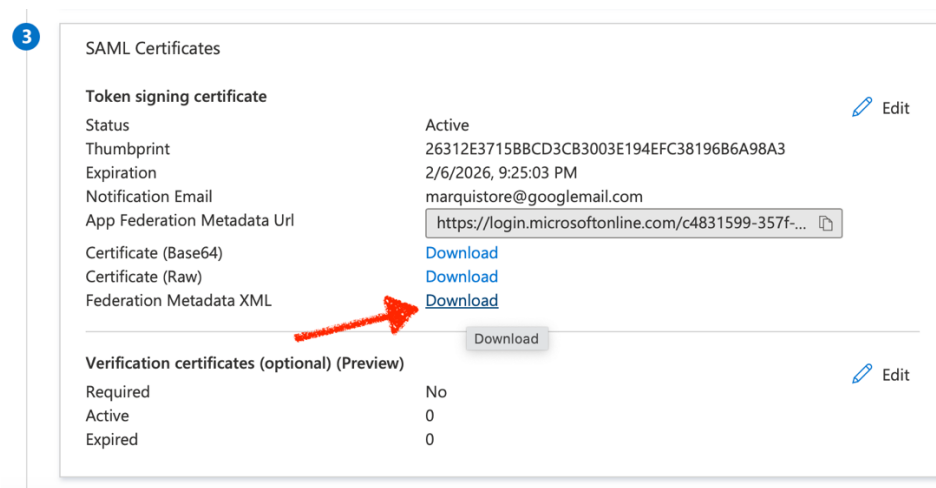
Please use following Microsoft default claim for each attribute for the set up in the DeepL interface.

2

Attributes & Claims		Edit
givenname	user.givenname	
surname	user.surname	
emailaddress	user.mail	
name	user.userprincipalname	
Unique User Identifier	user.userprincipalname	

5) Download the Metadata XML

- Click on *Download* for Federation Metadata XML

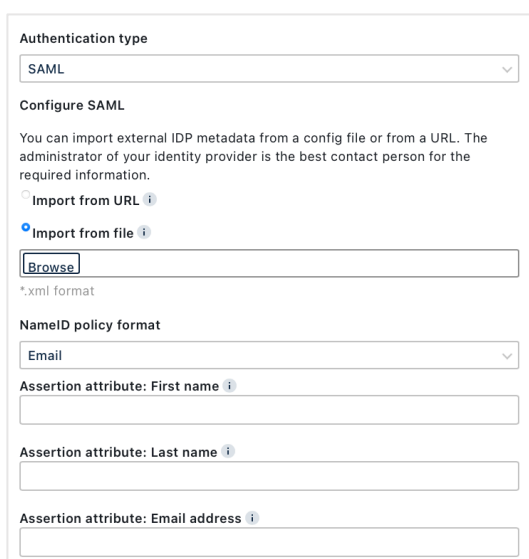


The screenshot shows a configuration page for SAML Certificates. A blue circle with the number '3' is in the top left corner. The page is titled 'SAML Certificates' and has an 'Edit' button in the top right. Under the heading 'Token signing certificate', there is a table of properties: Status (Active), Thumbprint (26312E3715BBCD3CB3003E194EFC38196B6A98A3), Expiration (2/6/2026, 9:25:03 PM), Notification Email (marquistore@googlemail.com), and App Federation Metadata Url (https://login.microsoftonline.com/c4831599-357f-...). Below these are three 'Download' links: 'Certificate (Base64)', 'Certificate (Raw)', and 'Federation Metadata XML'. A red arrow points to the 'Federation Metadata XML' link. Below this section is a 'Download' button. Under the heading 'Verification certificates (optional) (Preview)', there is another table: Required (No), Active (0), and Expired (0). An 'Edit' button is in the top right of this section.

6) Provide data

Provide the following data in your [DeepL Account settings](#):

- Federation Metadata XML
- NameID policy format: **Email**
- Set the attributes:
 - email: <http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress>
 - firstName: <http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname>
 - lastName: <http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname>



The screenshot shows a form for configuring SAML authentication. The 'Authentication type' is set to 'SAML'. Under 'Configure SAML', there is a text box explaining that external IDP metadata can be imported from a config file or a URL. The 'Import from file' option is selected, and a 'Browse' button is visible. Below this, the 'NameID policy format' is set to 'Email'. There are three text input fields for 'Assertion attribute: First name', 'Assertion attribute: Last name', and 'Assertion attribute: Email address'.

