

Configure multiple DeepL subscriptions under one instance of Microsoft Azure AD with SAML 2.0 SSO

This guide is designed to help configure multiple DeepL subscriptions under a single instance of Microsoft Azure Active Directory (AAD) using SAML 2.0 Single Sign-On (SSO). The document provides a detailed, step-by-step process to achieve this integration, leveraging AAD's multi-Assertion Consumer Service (ACS) capability.

Context

Companies with different DeepL subscriptions may need to integrate these with a Single Sign-On (SSO) system towards a single Identity Provider (IdP). This setup is useful for companies with different child companies, each requiring separate user and administrator management for privacy or administrative reasons.

Pre-requisites

- A working instance of Microsoft Azure Active Directory P1, P2, or superior.
- Approved SSO domains for the DeepL subscriptions.

Procedure Summary

1. Configure a single DeepL SAML Application in AAD: Add multiple ACS URLs, each corresponding to a separate DeepL subscription.
2. User Access via SP-Initiated Login: Users log in via DeepL's SSO domain or the "Continue with SSO" option on the DeepL login page.

Currently DeepL doesn't support IdP-Initiated SSO login. Therefore, even though this configuration requires defining a "default" ACS URL for the enterprise application -so AAD can select where to route the user when the login is initiated from there IdP- this setting will not have any practical effect since all SSO logins in DeepL need to be SP-initiated.

Step-by-Step Configuration

Step 1: Create an Enterprise Application in AAD

Step 2: Configure SAML SSO

1. **Set ACS URLs:** Enter the ACS URLs for each DeepL subscription.
 - ACS URL format: <https://w.deepl.com/auth/realms/prod/broker/{alias}/endpoint>
 - Where **{alias}** is the DeepL subscription's SSO domain without the .sso.deepl.com suffix.
2. **Entity ID:** <https://w.deepl.com/auth/realms/prod>
3. **Default ACS URL:** Select one ACS URL as the default. This setting is primarily for IdP-Initiated login, which is not used in this setup.

Basic SAML Configuration

Save | Got feedback?

Identifier (Entity ID) * ⓘ

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

Default

✓ [checkbox checked] ⓘ [trash]

[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/samldemopr2/endpoint"/> ✓	1 ✓	<input type="checkbox"/> ⓘ	[trash]
<input type="text" value="https://w.deepl.com/auth/realms/prod/broker/samldemopr1/endpoint"/> ✓	0 ✓	<input checked="" type="checkbox"/> ⓘ	[trash]

[Add reply URL](#)

4. **Other Settings:**
 - Sign-on URL: Not required.
 - Relay State: Not required.
 - Logout URL: Not required.
5. **Attributes & Claims:** Use AAD's default configuration as since our typical configuration maps the AAD attributes as:

AAD's source Attribute	DeepL's target attribute
Email, in email format	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress
User's first name	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname
User's email address	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress
User Identifier	Email

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

6. Save changes.

Step 3: Download the Federated metadata produced by AAD for the DeepL application

SAML Certificates		 Edit
Token signing certificate		
Status	Active	
Thumbprint	A0EE87522E7048D5EDE70E56480FDFB22885746E	
Expiration	18/06/2027, 15:03:18	
Notification Email	alejandro.vilchespino@gmail.com	
App Federation Metadata Url	<input type="text" value="https://login.microsoftonline.com/bc..."/>	
Certificate (Base64)	Download	
Certificate (Raw)	Download	
Federation Metadata XML	Download	
<hr/>		
Verification certificates (optional)		 Edit
Required	No	
Active	0	
Expired	0	

Step 4: Upload the metadata file obtained from AAD in each one of your DeepL subscriptions using the Import from file option. Save the changes.

Set up SSO

If you want to deactivate SSO for your team or change your authentication type, please [contact DeepL Support](#).

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 *i*

Import from file *i*

*.xml format

NameliD policy format

Email

Assertion attribute: First name *i*

Assertion attribute: Last name *i*

Assertion attribute: Email address *i*

You need to upload the same Federated metadata file in each one of the DeepL subscriptions you are setting up in your AAD, even though these subscriptions have different SSO domains.

Step 5: Grant access to users

1. Grant your users direct access to the DeepL Enterprise application you have created. You can also create a security group that represents each of the business units that will have access to the application to facilitate user management.

Step 6: Test SP-Initiated Login

1. **Login Process:**
 - Go to deepl.com > Login > Continue with SSO > Enter the company SSO domain.
 - *Result:* your DeepL user is created in the corresponding DeepL subscription for which you entered the SSO domain.
 - Use the specific DeepL SSO domain (e.g., company.sso.deepl.com).

Troubleshooting

- **Incorrect Subscription Assignment:**
 1. If a user is created in the wrong subscription, Administrators must:
 - Ask the user to log out from DeepL.
 - Get the user's DeepL account removed from the team subscription.
 - Ask the user to log in again using any of the SP-Initiated login methods making sure to log in to the right subscription.

Ensuring Users Access the Correct DeepL Subscription

When publishing the DeepL application on Azure AD's "MyApps" dashboard, two primary issues may arise:

1. **Default IdP-Initiated Login:** By default, the Enterprise application for DeepL created in AAD points to the IdP-Initiated login, which DeepL does not support.
2. **Routing to Default ACS URL:** Even if IdP-Initiated login were supported, the MyApps dashboard routes users to the default ACS URL, leading all users to be created in the subscription corresponding to the lowest index ACS URL.

Solution

To resolve these issues, create "dummy" DeepL application icons for each company and assign users accordingly. This ensures users see only the DeepL icon that points to their specific subscription.

Procedure

1. **Configure the Main DeepL Application:** Set it up as a normal enterprise application with SSO and multiple ACS URLs.
2. **Create Dummy DeepL Applications:** Create a dummy application for each subscription with a fixed SSO link.
3. **Assign Visibility:** Make each dummy application visible only to the users of the corresponding subscription.
4. **Hide the Main Application:** Hide the main DeepL application from all users to avoid displaying duplicate icons on the Azure MyApps dashboard.

Step-by-Step Guide

Prerequisite: All DeepL subscriptions have been configured with SSO against the same AAD instance as previously explained.

Steps

1. **Create a Dummy DeepL Enterprise Application:**
 - **Type:** Non-gallery application
 - **Name:** Use a descriptive name (e.g., "DeepL - Company B") to simplify IT administration.

- **Single-Sign-On Method:** Select LINKED and enter the fixed URL to access the app, which will be the SSO domain URL for the specific subscription (e.g., company.sso.deepl.com).

Home > Enterprise applications | All applications > Browse Microsoft Entra Gallery > DeepL Subscription B

DeepL Subscription B | Single sign-on

Enterprise Application

- Overview
- Deployment Plan
- Diagnose and solve problems

Manage

- Properties
- Owners
- Roles and administrators
- Users and groups
- Single sign-on**
- Provisioning
- Application proxy
- Self-service
- Custom security attributes

Security

- Conditional Access
- Permissions
- Token encryption

Single sign-on (SSO) adds security and convenience when users sign on to applications in Microsoft Entra ID by enabling a user in your organization to sign in to every application they use with only one account. Once the user logs into an application that credential is used for all the other applications they need access to. [Learn more](#).

Select a single sign-on method [Help me decide](#)

Disabled

Single sign-on is not enabled. The user won't be able to launch the app from My Apps.

SAML

Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.

Password-based

Password storage and replay using a web browser extension or mobile app.

Linked

Link to an application in My Apps and/or Office 365 application launcher.

Home > Enterprise applications | All applications > Browse Microsoft Entra Gallery > DeepL Subscription B

DeepL Subscription B | Linked Sign-on

Enterprise Application

- Overview
- Deployment Plan
- Diagnose and solve problems

Manage

- Properties
- Owners
- Roles and administrators
- Users and groups
- Single sign-on**
- Provisioning

Change single sign-on modes

Linked sign-on lets you configure the target location when a user selects the app in your organization's My Apps or Office 365 portal. This option does not add single sign-on to the application. Choose linked sign-on when the application is configured for single sign-on in another identity provider service. [Learn more](#)

Configure Sign-on URL

Provide the URL your users will use to navigate to DeepL Subscription B

Sign on URL

2. Grant Access to Users:

- Assign users to both the main and dummy applications corresponding to their company. Use security groups for easier management.
- Is it critical that the user should be granted access to both the “main” application and the dummy application corresponding to her company

3. Hide the Main Application:

- Go to Properties > Visible to users? > NO.
- Save the changes to make the main app invisible to end-users, who will only see the dummy application for their company.

Home > Enterprise applications | All applications > Browse Microsoft Entra Gallery > Enterprise applications | All applications > DeepL SAML demo PRD 1

DeepL SAML demo PRD 1 | Properties

Enterprise Application

Save Discard Delete Got feedback?

- Overview
- Deployment Plan
- Diagnose and solve problems

Manage

- Properties**
- Owners
- Roles and administrators
- Users and groups
- Single sign-on
- Provisioning
- Application proxy
- Self-service
- Custom security attributes

Security

- Conditional Access
- Permissions
- Token encryption

Activity

- Sign-in logs
- Usage & insights
- Audit logs
- Provisioning logs

View and manage application settings for your organization. Editing properties like display information, user sign-in settings, and user visibility settings requires Global Administrator, Cloud Application Administrator, Application Administrator roles. [Learn more.](#)

If this application resides in your tenant, you can manage additional properties on the [application registration](#).

Enabled for users to sign-in?	<input checked="" type="radio"/> Yes <input type="radio"/> No
Name *	DeepL SAML demo PRD 1
Homepage URL	https://account.activedirectory.windowsazure.com:444/applications/de...
Logo	 <input type="text" value="Select a file"/>
User access URL	https://launcher.myapps.microsoft.com/api/signin/b2bd1155-1df2-49...
Application ID	b2bd1155-1df2-4930-837c-2dc358c1cbb3
Object ID	1f3ddf9f-f715-4422-934e-695ab95d28b8
Terms of Service Url	Publisher did not provide this information
Privacy Statement Url	Publisher did not provide this information
Reply URL	https://w.deepl.com/auth/realms/prod/broker/samldemopr2/endpoint
Assignment required?	<input checked="" type="radio"/> Yes <input type="radio"/> No
Visible to users?	<input type="radio"/> Yes <input checked="" type="radio"/> No
Notes	

myapps.microsoft.com

My Apps

Apps

Add apps Create collection Customise view

Apps Settings



Add-Ins



DeepL Subscription B

The “real” SSO application is not visible for this user.

Dummy icon pointing to subscriptionb.sso.deepl.com

4. **User Creation in the Correct Subscription:**

- Users will be created in the appropriate DeepL subscription after accessing the dummy application icon.
- It doesn't matter which ACS URL is the default one in the SAML configuration, because we are forcing SP-Initiated login with the dummy icons on the Azure *My Apps* dashboard.