

---

# Setup guide for DeepL Single Sign-On (SSO)

OpenID: Microsoft Entra ID (formerly Azure AD)

---

## Table of contents

### [Requirements](#)

- [1\) Open Azure AD management](#)
- [2\) Register app](#)
- [3\) Configure initial settings](#)
- [4\) Create Client Secret](#)
- [5\) Set up permissions](#)
- [6\) Configure assignment](#)
- [7\) Collect endpoints](#)
- [8\) Provide data](#)

## Requirements

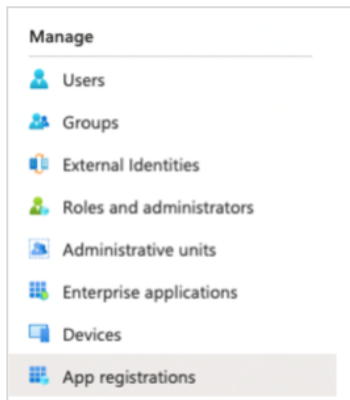
- You have an Azure AD set up
- You have administrative permissions to create an app within the Azure AD tenant
- A company domain has been defined for the DeepL environment. For further information please check our [Help Center article](#).

## 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](https://portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/Overview)

## 2) Register app

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



2. Click *New registrations* on the top panel

### 3) Configure initial settings

1. Under *Name* enter *DeepL SSO*
2. Under *Supported account types* keep the default settings as *Accounts in this organizational directory only*. Select *Other* if you require a special setting.
3. Under *Redirect URI*, select *Web* and enter *https://w.deeppl.com/auth/realms/prod/broker/ALIAS/endpoint*  
(Replace ALIAS\* with your chosen company Company SSO domain)
4. Click *Register*

A screenshot of the 'Register an application' form in the Azure AD portal. The form has a title 'Register an application' and a subtitle 'Name'. The 'Name' field is a text input containing 'DeepL SSO'. Below this is the 'Supported account types' section, which has a subtitle 'Who can use this application or access this API?'. It contains four radio button options: 'Accounts in this organizational directory only (DeepL GmbH only - Single tenant)' (selected), 'Accounts in any organizational directory (Any Azure AD directory - Multitenant)', 'Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)', and 'Personal Microsoft accounts only'. Below this is the 'Redirect URI (optional)' section, which has a subtitle 'We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.' It contains a dropdown menu set to 'Web' and a text input field containing 'https://w.deeppl.com/auth/realms/prod/broker/deepl/endpoint'.

\* ALIAS value can be found under Company SSO domain in SSO configuration area

### 4) Create Client Secret

1. Select *Certificates & Secrets* in the left-hand panel. Then, on the center panel below *Client secrets*, click on *New client secret*.

2. Name the new client secret *DeepL SSO*, and select a proper expiration date. You will not be automatically notified when this client secret expires, so you will need to monitor this on your own.
3. Click *Add*

**Add a client secret** [X]

Description:

Expires:

4. Copy the secret value to a safe place. You will need it later in the DeepL set up.

Certificates (0) **Client secrets (2)** Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

| Description | Expires   | Value                             | Secret ID                            |
|-------------|-----------|-----------------------------------|--------------------------------------|
| YourSecret  | 1/28/2024 | d897Q-WKouWQO2.uBw6rfaZ54mivNK... | 1.563342-6243-4c7e-9804-eb64446d6ff2 |

## 5) Set up permissions

1. Select *API permissions* in the left-hand panel
2. On the center panel there should already be a default permission entitled *User.Read* below *Microsoft Graph*. If not, insert it manually.
3. Click *Add a permission* in the center panel. Select *Microsoft Graph*, then select *Delegated permissions*.
4. Check the box for *email*, then click *Add permissions*

← All APIs

Delegated permissions  
Your application needs to access the API as the signed-in user.

Select permissions  
Start typing a permission to filter these results

The "Admin consent required" column shows the default value permission, user, or app. This column may not reflect the value used. [Learn more](#)

Permission

Openid permissions (1)

- email
- offline\_access
- openid
- profile

AccessReview

[Add permissions](#) [Discard](#)

## 5. Click *Grant admin consent* and confirm with *Yes*

**Grant admin consent confirmation.**

Do you want to grant consent for the requested permissions for all accounts in deepL? This will update any existing admin consent records this application already has to match what is listed below.

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This can be done in your organization, or in organizations where this app will be used. [Learn more](#)

### Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions shows all the permissions the application needs. [Learn more about permissions and consent](#)

[+ Add a permission](#)  Grant admin consent for deepL

| API / Permissions name | Type      | Description                   | Admin consent required | Status                |
|------------------------|-----------|-------------------------------|------------------------|-----------------------|
| Microsoft Graph (2)    |           |                               |                        |                       |
| email                  | Delegated | View users' email address     | No                     | Granted for all users |
| User.Read              | Delegated | Sign in and read user profile | No                     | Granted for all users |

To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try [Enterprise applications](#).

## 6) Configure assignment

1. Select *Enterprise applications* in the left-hand menu
2. Choose the application that has been created automatically
3. Select *Properties* in the left-hand panel
4. Set *Assignment required* to *Yes*

Diagnose & solve problems

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

Save Discard Delete Got feedback?

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?  Yes  No

Name \*

Homepage URL

Logo

Application ID

Object ID

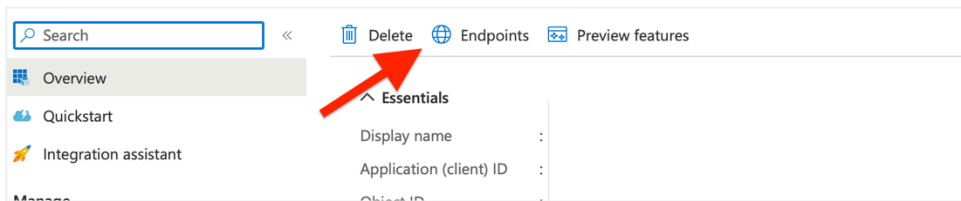
Assignment required?  Yes  No

Visible to users?  Yes  No

Notes

## 7) Collect endpoints

1. Select *Overview* in the left left-hand panel
2. Copy the *Application (client) ID* text, which you will provide to DeepL in the next step

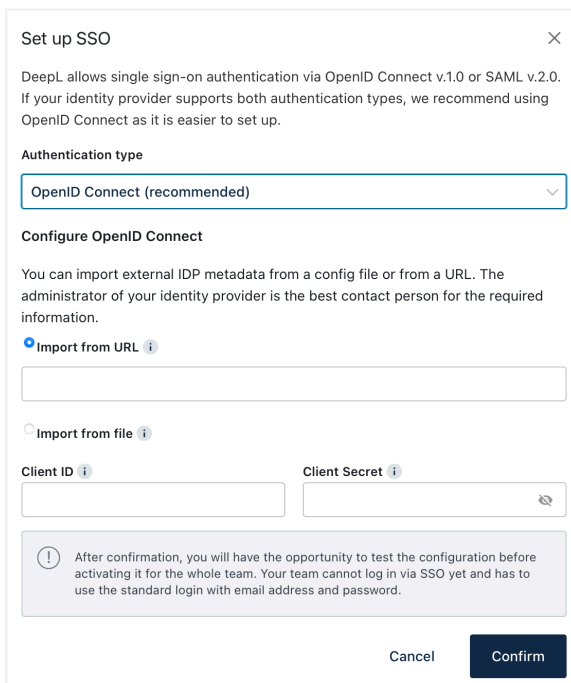


3. Select *Endpoints* from the top menu bar. Copy the URL of the *OpenID Connect metadata document* from the list of endpoints. You will also provide it to DeepL.

## 8) Provide data

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

- OpenID Connect metadata Document
- Application (Client) ID
- Client Secret

A screenshot of the 'Set up SSO' dialog box. The dialog has a title bar with a close button. Below the title, there is introductory text about SSO authentication. Under 'Authentication type', 'OpenID Connect (recommended)' is selected in a dropdown menu. The 'Configure OpenID Connect' section has two radio buttons: 'Import from URL' (selected) and 'Import from file'. Below these are input fields for 'Client ID' and 'Client Secret'. A warning message at the bottom states: '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.' At the bottom right, there are 'Cancel' and 'Confirm' buttons.