



Setup guide for DeepL Single Sign-on (SSO)

Azure AD (Microsoft Entra ID) - OpenID

Requirements

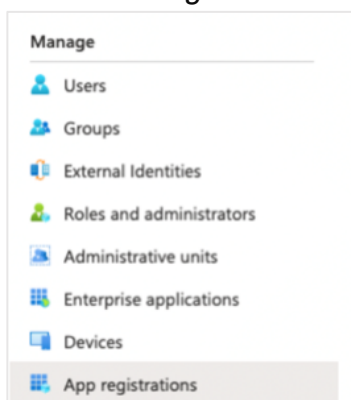
- You have an Azure AD set up
- You have administrative permissions to create an app within the Azure AD tenant
- A company domain has been defined for the DeepL environment. For further information please check our [Help Center article](#).

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

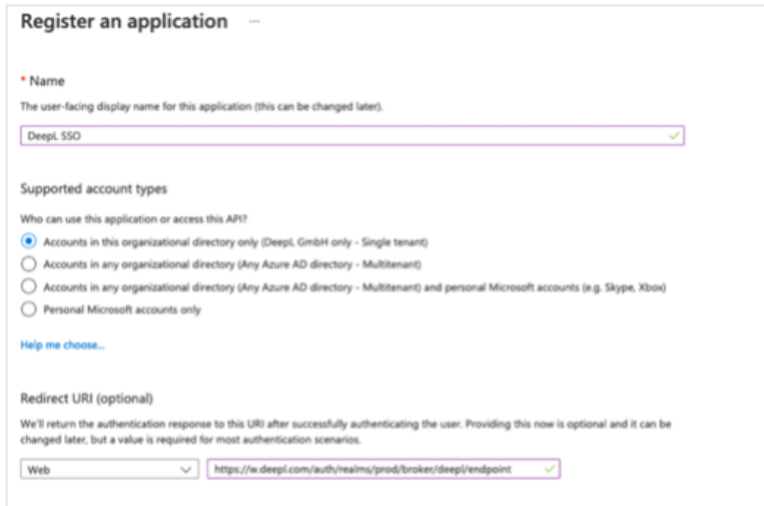
2) Register app

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 special setting.
3. Under *Redirect URI*, select *Web* and enter `https://w.deepl.com/auth/realms/prod/broker/ALIAS/endpoint` (Replace ALIAS with your chosen company DOMAIN)
4. Click *Register*



Register an application

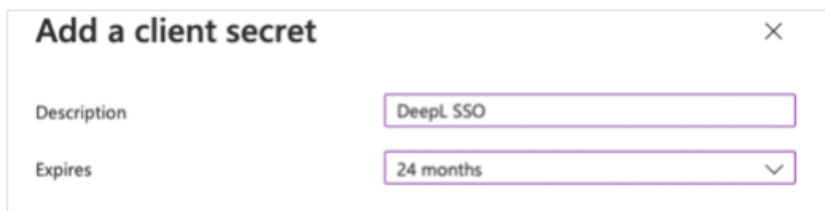
Name
The user-facing display name for this application (this can be changed later).
DeepL SSO

Supported account types
Who can use this application or access this API?
 Accounts in this organizational directory only (DeepL GmbH only - Single tenant)
 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)
 Personal Microsoft accounts only
[Help me choose...](#)

Redirect URI (optional)
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.
Web `https://w.deepl.com/auth/realms/prod/broker/deepl/endpoint`

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

Description: DeepL SSO

Expires: 24 months

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)

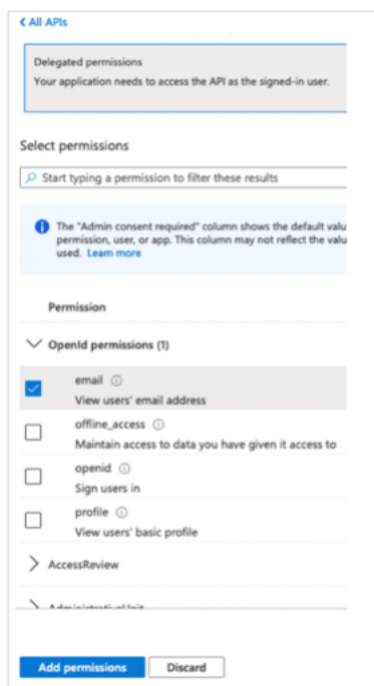
A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value	Secret ID
YourSecret	3/28/2024	d897Q-WKouWKOZ_u8wfvfaZE4mivNK...	1d5f9342-d243-4c7e-90b4-ebd4446d0ff2

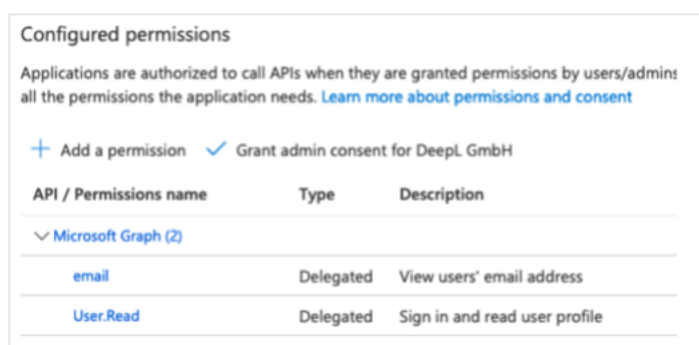
5) Set up permissions

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*

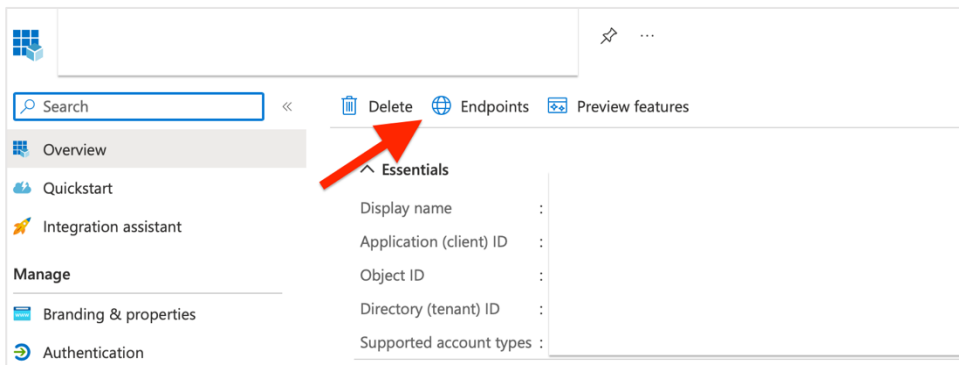


6) Collect endpoints

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.



7) Provide data

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

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

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

OpenID Connect (recommended)

Configure OpenID Connect

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*

Client ID *i* **Client Secret** *i*

! 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**

