Switch to SSO for subscription management by groups: OpenID Connect and Microsoft Entra ID

DeepL has introduced subscription management by groups. With this feature users can be managed in groups to which subscriptions are assigned. As an admin, this gives you the flexibility to grant your users access to one or more DeepL products, like Translate, Write, or Voice. This guide describes how you can set up SSO for subscription management by groups.

ⓘ Subscription management by groups is available for businesses via our Sales team. To learn more about the plan details and pricing, contact our Sales team.

Prerequisites

- Admin access to DeepL
- Protocol: OIDC (Open ID Connect)
- Identity provider: Microsoft Entra ID (formerly AzureAD)
- A company domain has been defined for the DeepL environment. For further information please check Setting up SSO for teams.

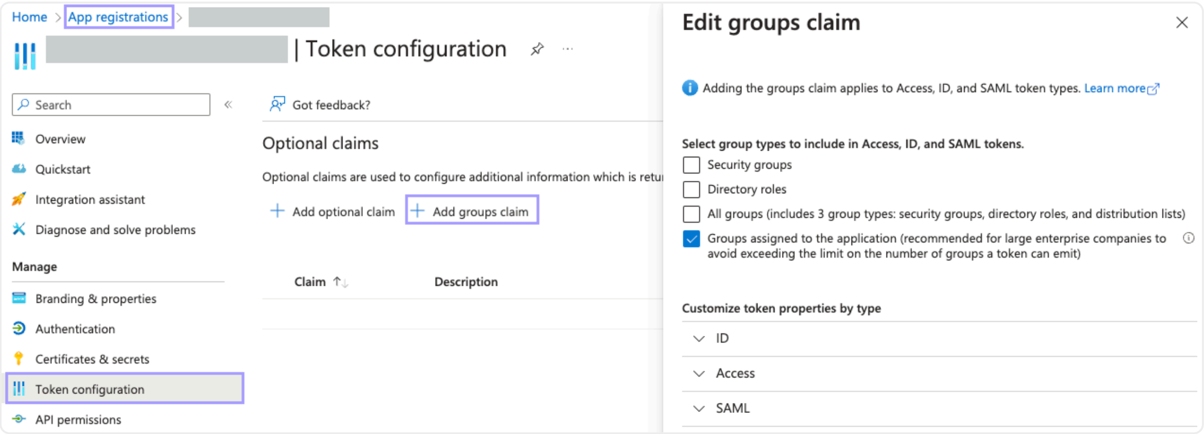
Once DeepL has enabled subscription management by groups for your organization, a new *Groups* tab will appear in the administration area in your *DeepL account*. A default group is automatically created, and all existing users are placed in this default group. All users will retain access to their current subscription, and nothing will change for them immediately.

To use Just-In-Time (JIT) provisioning with group synchronization, you need to update your SSO configuration in both DeepL and your Microsoft Entra ID instance. For more information, see the document Subscription Management by Groups.

Edit the SSO configuration in Microsoft Entra ID

Add groups claim

1. Select *Token configuration* under *Manage.*
   In the list you see that no group claim is configured in the token.
2. To add a group claim, click on *Add groups claim.*
3. Select *Groups assigned to application* under *Select group types to include in Access, ID, and SAML tokens.*
4. Select *Group ID* under *Customize token properties by type* and click *Add*.
   The groups' claim is included in the OIDC token.



Home > App registrations > [redacted]

[redacted] | Token configuration

Search

Overview
Quickstart
Integration assistant
Diagnose and solve problems

Manage
Branding & properties
Authentication
Certificates & secrets
Token configuration
API permissions

Got feedback?

Optional claims

Optional claims are used to configure additional information which is retu

+ Add optional claim + Add groups claim

Claim ↑↓	Description

Edit groups claim

Adding the groups claim applies to Access, ID, and SAML token types. Learn more

Select group types to include in Access, ID, and SAML tokens.

□ Security groups
□ Directory roles
□ All groups (includes 3 group types: security groups, directory roles, and distribution lists)
☑ Groups assigned to the application (recommended for large enterprise companies to avoid exceeding the limit on the number of groups a token can emit)

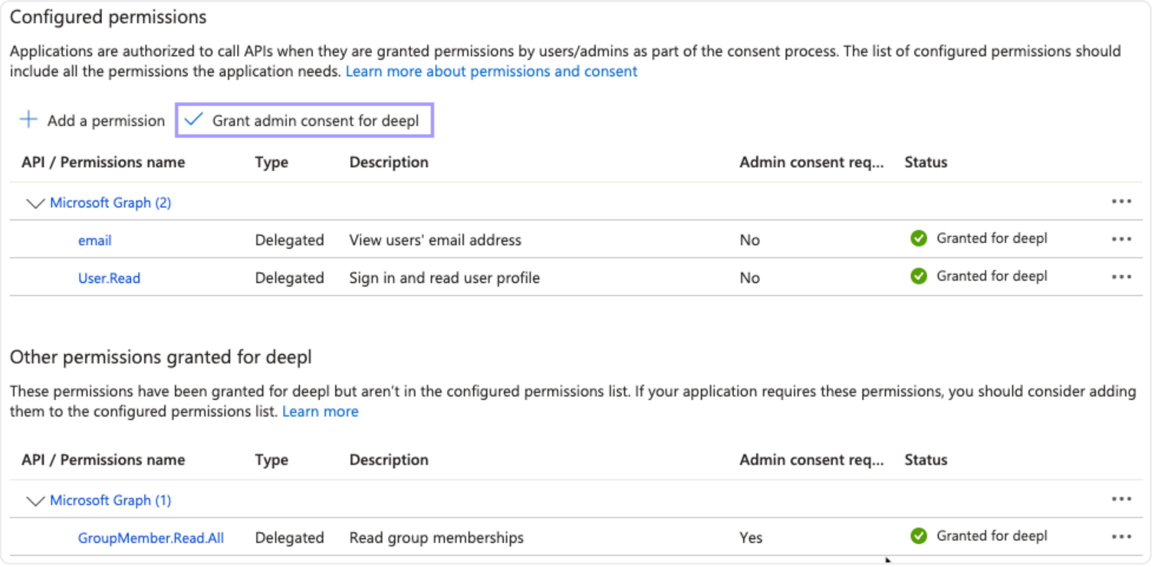
Customize token properties by type

ID
Access
SAML

> It isn't necessary to add *Group read* permissions to the MS Graph API as DeepL only needs to read group membership data in the token exchanged during login.

Set permissions

1. Select *API permissions* in the left-hand panel.
2. By default the permission *User.Read* should be listed below *Microsoft Graph*. If not, insert it manually.
3. Click *Add a permission* in the center panel.
4. Select *Microsoft Graph*, then select *Delegated permissions.*
5. Check the box for *email* and *GroupMember.Read.All* and click *Add permissions.*
6. Click *Grant admin consent* and confirm with *Yes.*



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 should include all the permissions the application needs. Learn more about permissions and consent

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

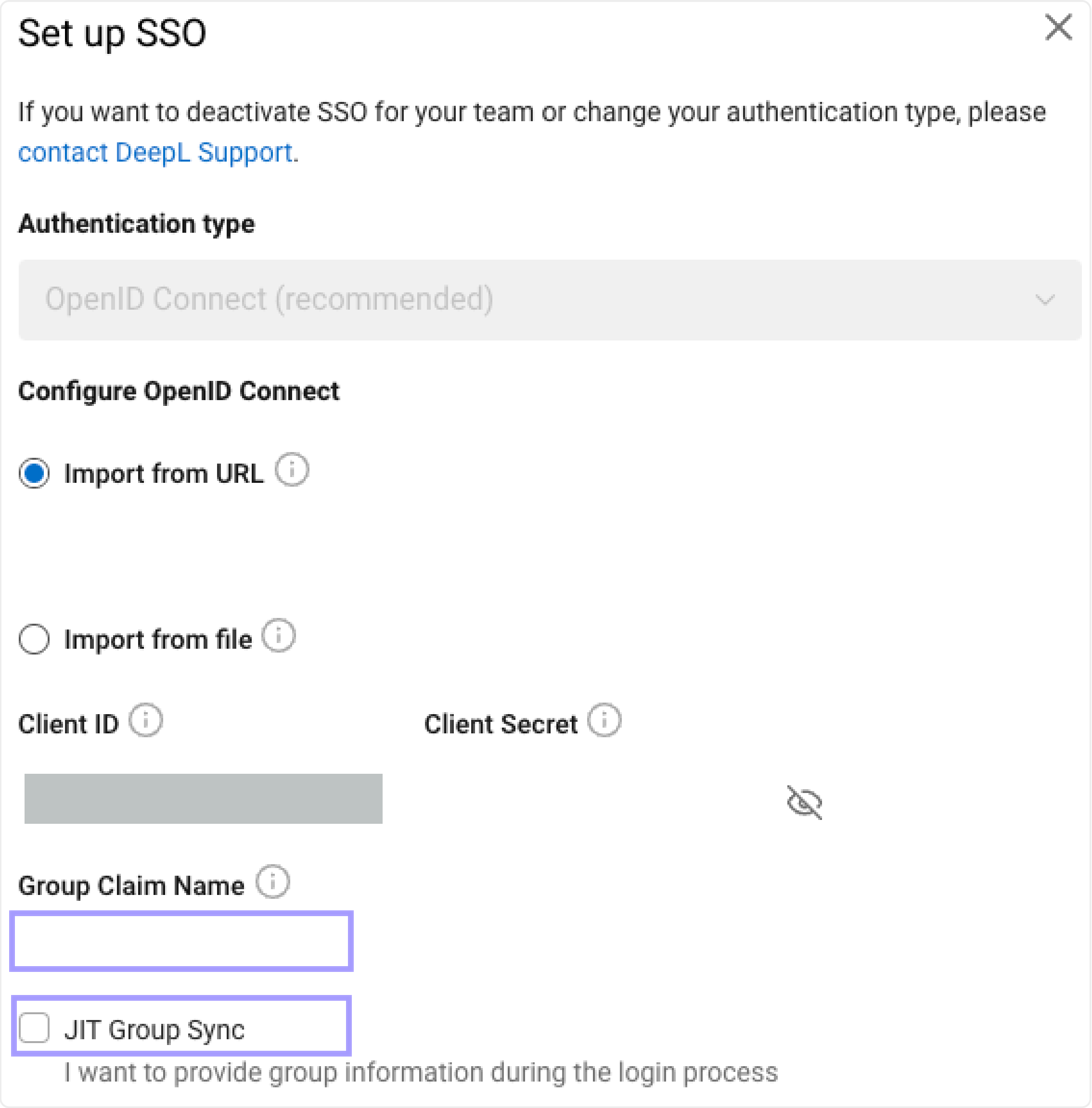
Other permissions granted for deepl

These permissions have been granted for deepl but aren't in the configured permissions list. If your application requires these permissions, you should consider adding them to the configured permissions list. Learn more

API / Permissions name	Type	Description	Admin consent req...	Status
Microsoft Graph (1)				
GroupMember.Read.All	Delegated	Read group memberships	Yes	✓ Granted for deepl

Edit the SSO configuration in DeepL account

1. Login as an admin.
2. Click on your user and select *Account* and go to the *Settings* tab.
3. Go to *Team* and *Single sign-on* and click *Edit*.
4. Enter the following information from the configured application in OneLogin.
   - OpenID Connect metadata
     Open your registered application in Microsoft Entra ID and click on *Endpoints* on the *Overview* page.
   - Client Secret
     Enter your saved Client Secret of the registered application from Microsoft Entra ID.
   - Enter *groups* as the *Group Claim Name*.
5. Enable *JIT Group Sync*.
6. Confirm and Save changes.



Set up SSO

If you want to deactivate SSO for your team or change your authentication type, please contact DeepL Support.

Authentication type

OpenID Connect (recommended)

Configure OpenID Connect

● Import from URL

○ Import from file

Client ID **Client Secret**

[redacted]

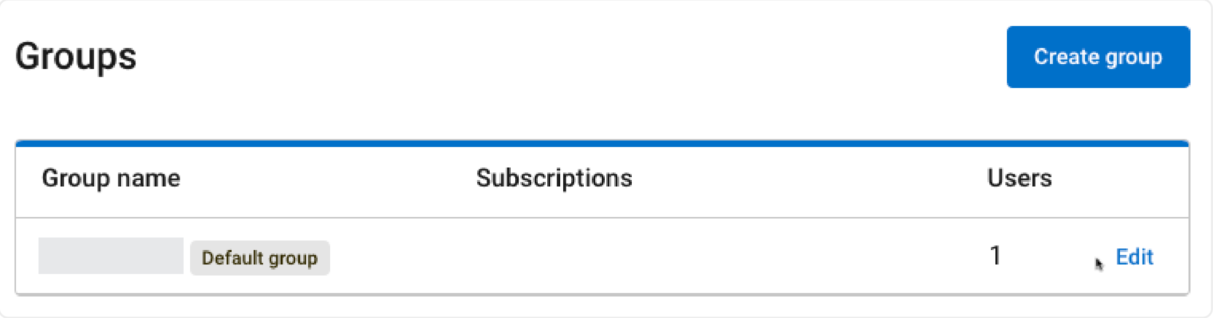
Group Claim Name

□ JIT Group Sync
I want to provide group information during the login process

Set up groups

1. Go to Microsoft Entra ID.
2. Create groups for the DeepL access and add users to the groups.
3. Go to *Enterprise applications* and select the registered application to add the groups to the application.
4. Go to your DeepL account.
5. Create the same groups that you created in your Microsoft Entra ID instance to manage your users
6. Go to tab *Groups* and click on *Create Group*.

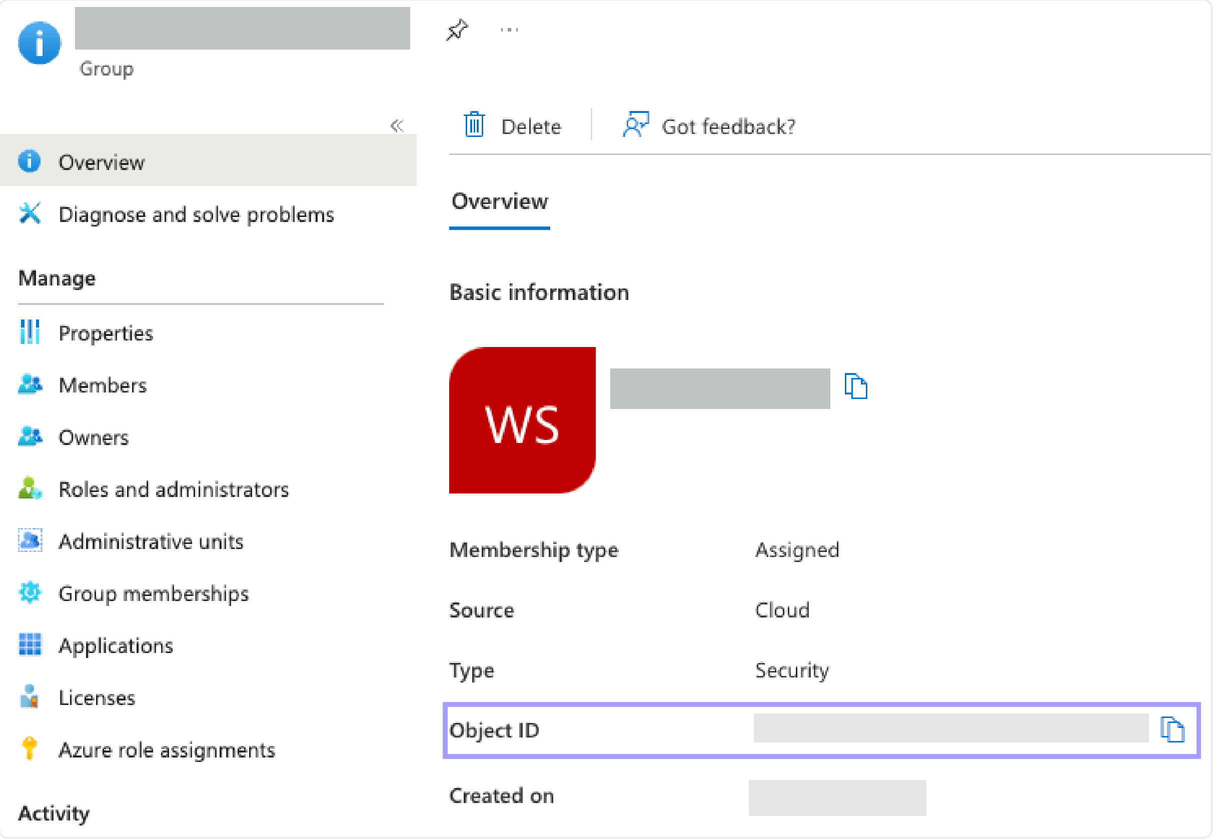
⚠ JIT Provisioning Group Sync does not create groups based on the OIDC token. If the token includes groups that do not exist in DeepL, that group information will be ignored, and the user is added only to the Default group. For more information about this default behavior, please consult the *Default Behavior* section in the document *Subscription Management by Groups*.



Groups

Group name	Subscriptions	Users	
[redacted] Default group		1	Edit

7. Enter a *Group name*.
   We recommend using the same name that you used for your groups in Microsoft Entra ID. However, you may choose a different name, e.g., if your organization uses concealed group names in the identity provider.
8. Enter the group's *Object ID* from Microsoft Entra ID under *Group ID*.
   You find the ID on the *Group* properties page.

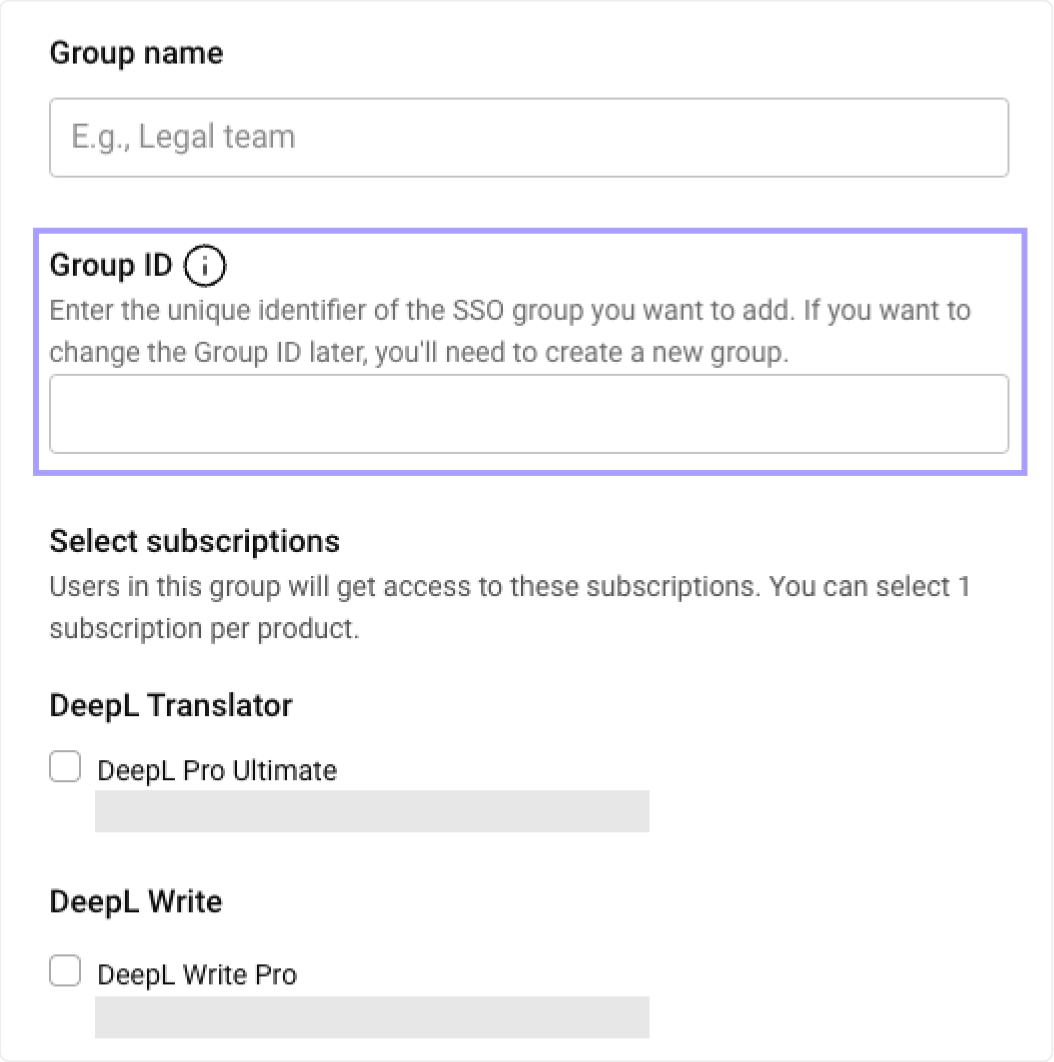


Basic information

[redacted]

Membership type	Assigned
Source	Cloud
Type	Security
Object ID	[redacted]
Created on	[redacted]

9. Select one or several subscriptions the user group should have access to



Group name

E.g., Legal team

Group ID ⓘ

Enter the unique identifier of the SSO group you want to add. If you want to change the Group ID later, you'll need to create a new group.

Select subscriptions

Users in this group will get access to these subscriptions. You can select 1 subscription per product.

DeepL Translator

□ DeepL Pro Ultimate

DeepL Write

□ DeepL Write Pro

10. Click on *Create group* to save the changes.
11. Repeat this process for each group from your Micrsoft Entra ID instance.
    As a result, the groups you have granted access to the DeepL application will be reflected in your DeepL account.
12. Test the SSO login with a user. Once the user logs in, they will be automatically assigned to the DeepL group or groups that match the Microsoft Entra ID group based on the configured Group ID.

Without JIT group synchronization

When JIT group synchronization is disabled, the group information that is passed is ignored. Users are only added to the default group in DeepL during SSO login. If you want to assign the user to an additional group, do the following.

1. Log in to DeepL as an admin and click on the account menu.
2. Select *Account* and go to the tab *Groups*.

3. To add the users to a group, click on *Edit* or *Add users* next to the group to which you want to add the users.
4. Enter the email addresses under *Add users* and save the changes.