Set up 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.

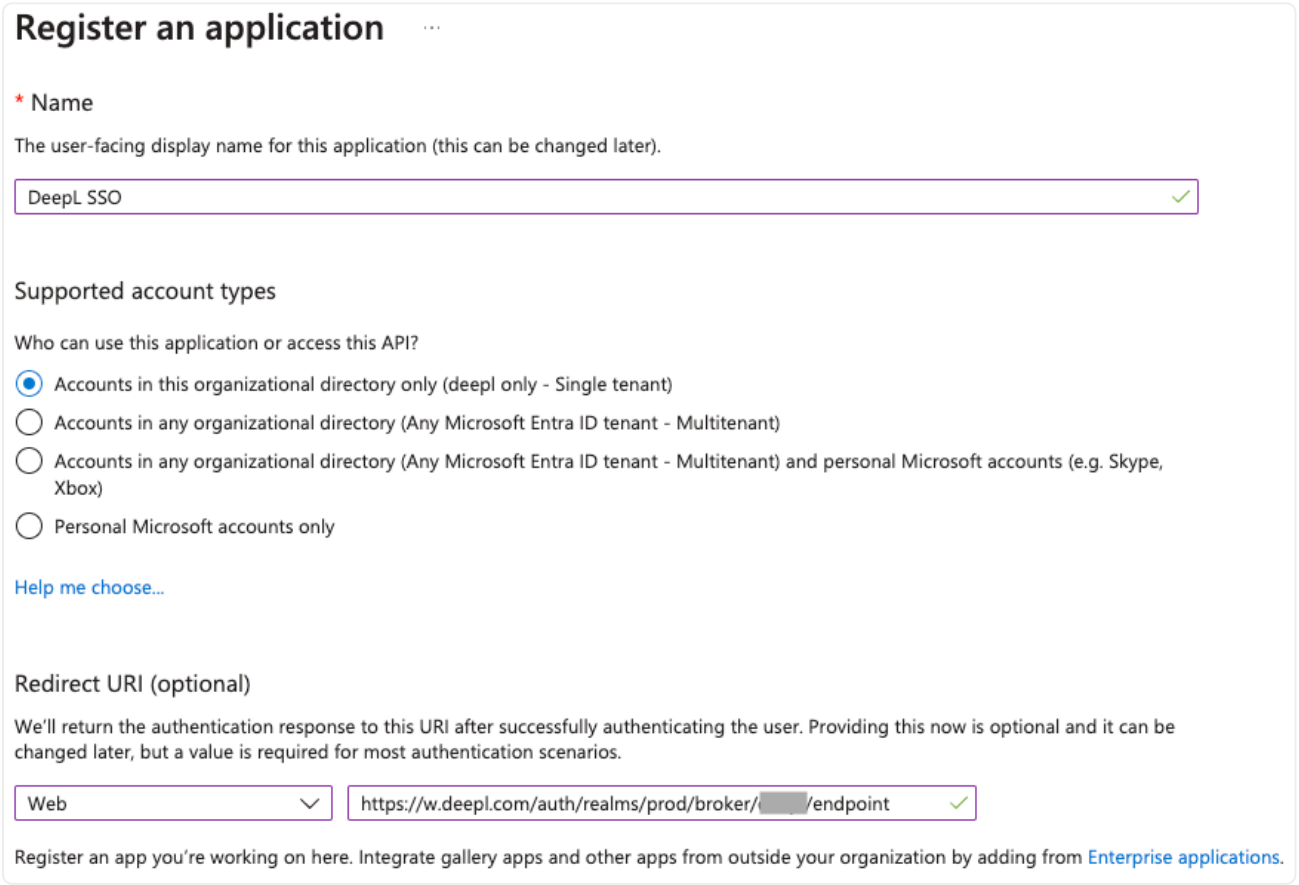
To use Just-In-Time (JIT) provisioning with group synchronization, you need to update your SSO configuration in both DeepL and your Microsoft Entra ID instance. For more

information, see the document Subscription Management by Groups.

Set the SSO configuration in Microsoft Entra ID

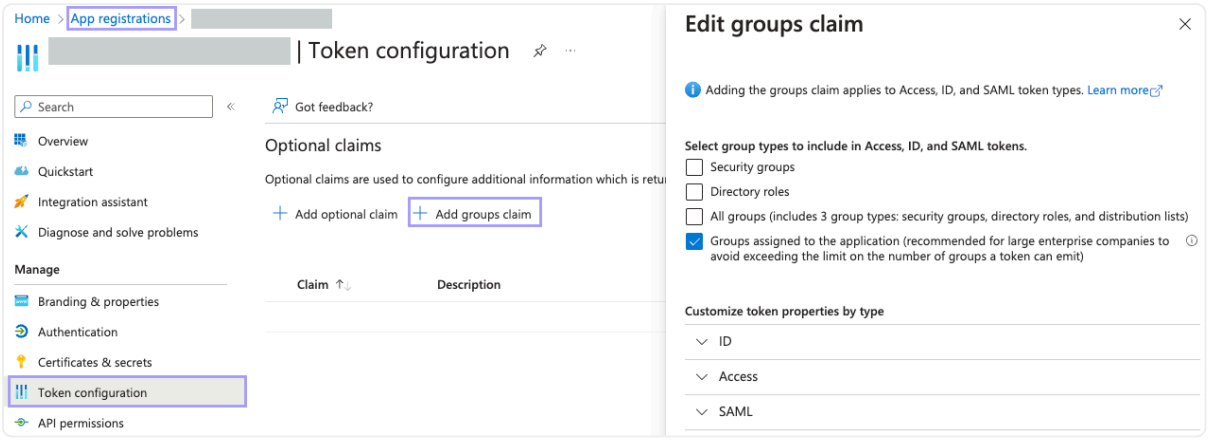
Register application

1. Go to your Microsoft Entra ID instance and select *App registrations*.
2. Click on *New registrations* in the top panel.
3. Enter *DeepL SSO* under *Name*.
4. Under *Supported account types* keep the default settings as *Accounts in this organizational directory only.*
5. Under *Redirect URI*, select *Web* and enter https://w.deepl.com/auth/realms/prod/broker/ALIAS/endpoint.
   (Replace ALIAS with your chosen company Company SSO domain. The ALIAS value can be found under Company SSO domain in the SSO configuration area in your *DeepL account*.)
6. Click *Register.*



Add groups claim

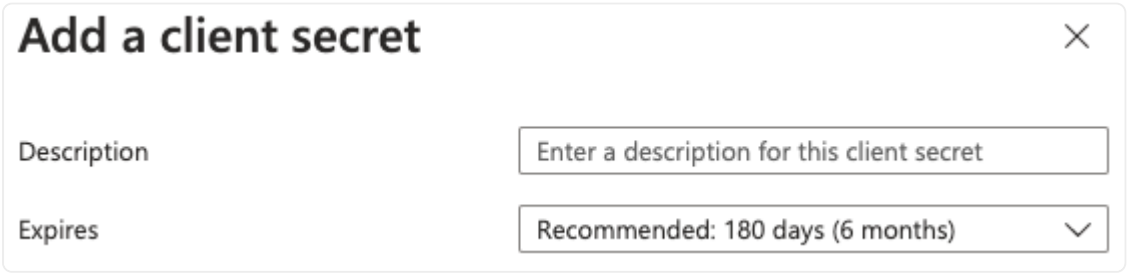
1. Select *Token configuration* under *Manage*.
   In the list you see that no group claim is configured in the token.
2. To add a group claim, click on *Add groups claim*.
3. Select *Groups assigned to application* under *Select group types to include in Access, ID, and SAML tokens*.
4. Select *Group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



> 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.

Create client secret

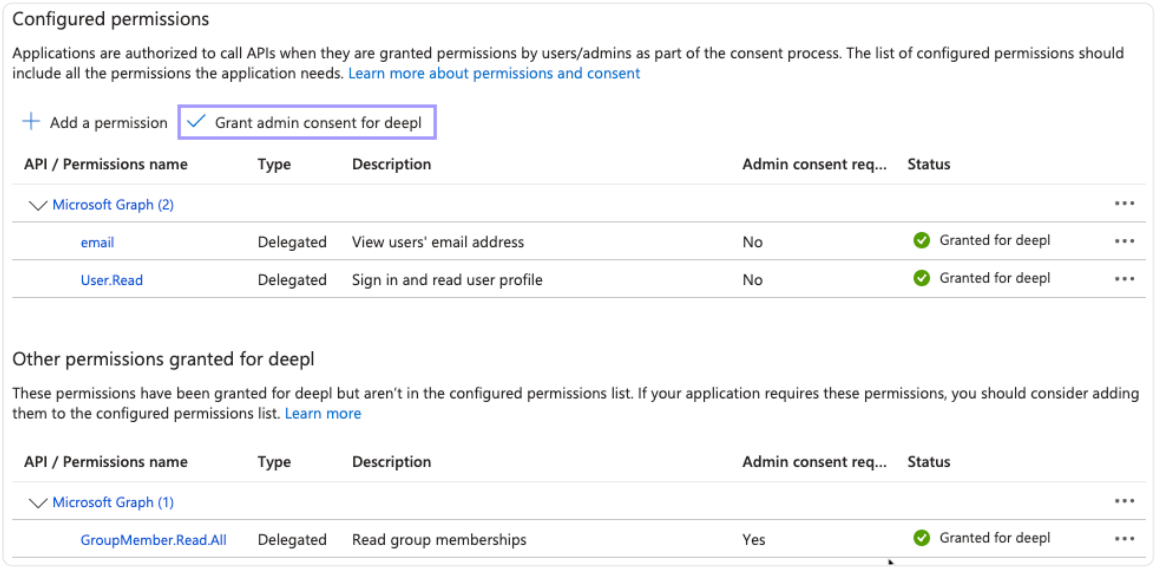
1. Select *Certificates & secrets* in the left-hand panel.
2. Under *Client secrets*, click on *New client secret*.
3. Add a description and select an expiration period.
4. Click *Add* and copy the secret value to a safe place. You will need it later in the DeepL set up.



ⓘ You will not be automatically notified when the client secret expires. You need to monitor this on your own.

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*.

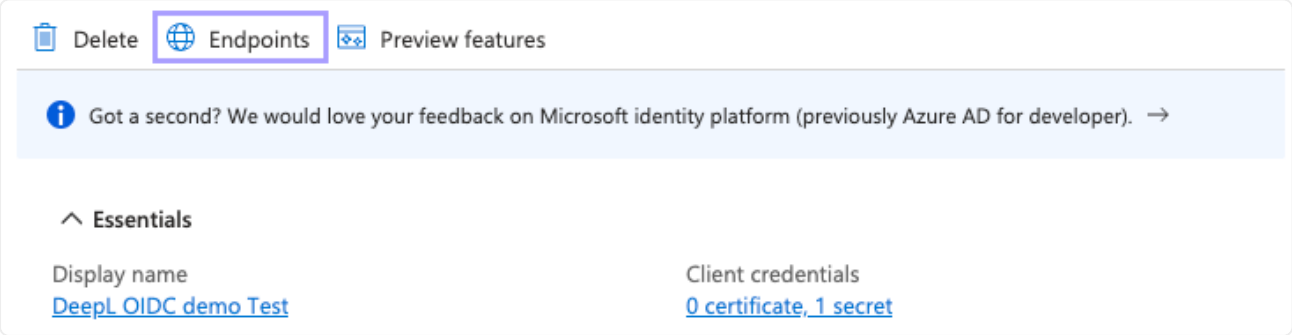


Configure assignment

1. Go to *Applications* and select *Enterprise applications* in the left-hand menu.
2. Select your registered application.
3. Under *Manage*, select *Properties* in the left-hand panel.
4. Set *Assignment required* to *Yes*.

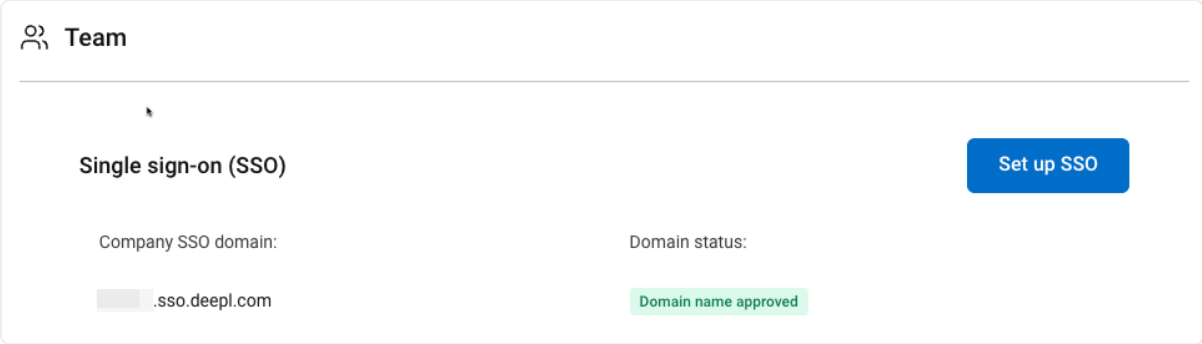
Collect endpoints

1. Go back to *App registrations* under *Applications* and select your registered application.
2. Select *Overview* in the left-hand panel.
3. Copy the *Application (client) ID*, which you need to enter in your DeepL account in the next step.
4. Select *Endpoints* from the top menu bar.
5. Copy the URL of the OpenID Connect metadata document from the list of endpoints. You will need to enter them in your DeepL account in the next step.

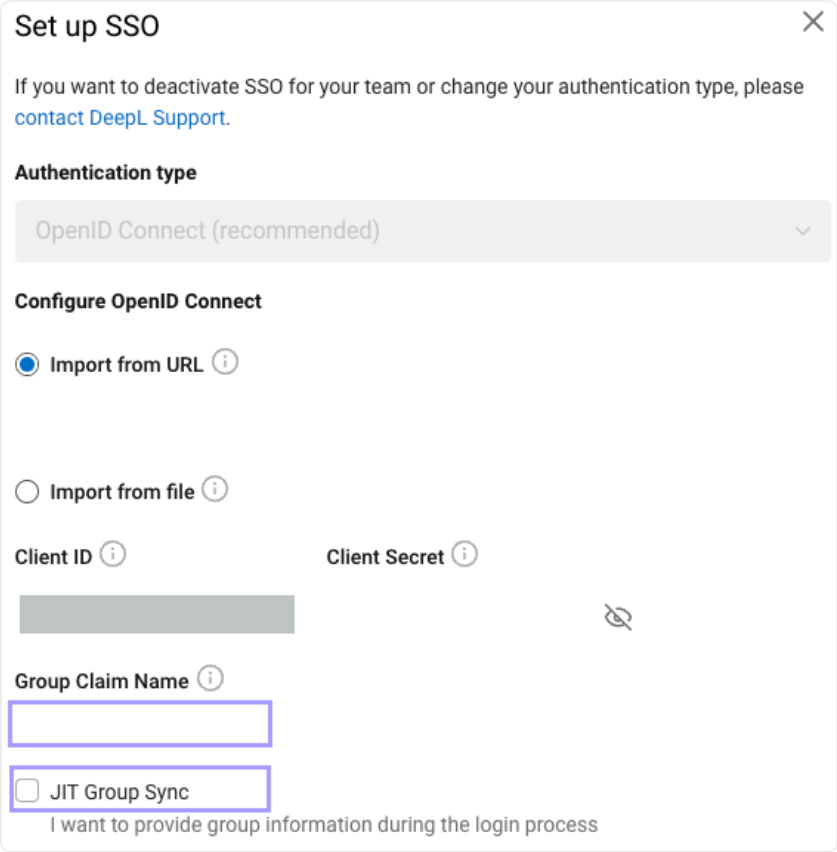


Set the SSO configuration in DeepL Accounts

1. Click on your user and select *Account* and go to the *Settings* tab.
   Under *Team* and *Single sign-on* the SSO domain has the status *Domain name approved*.

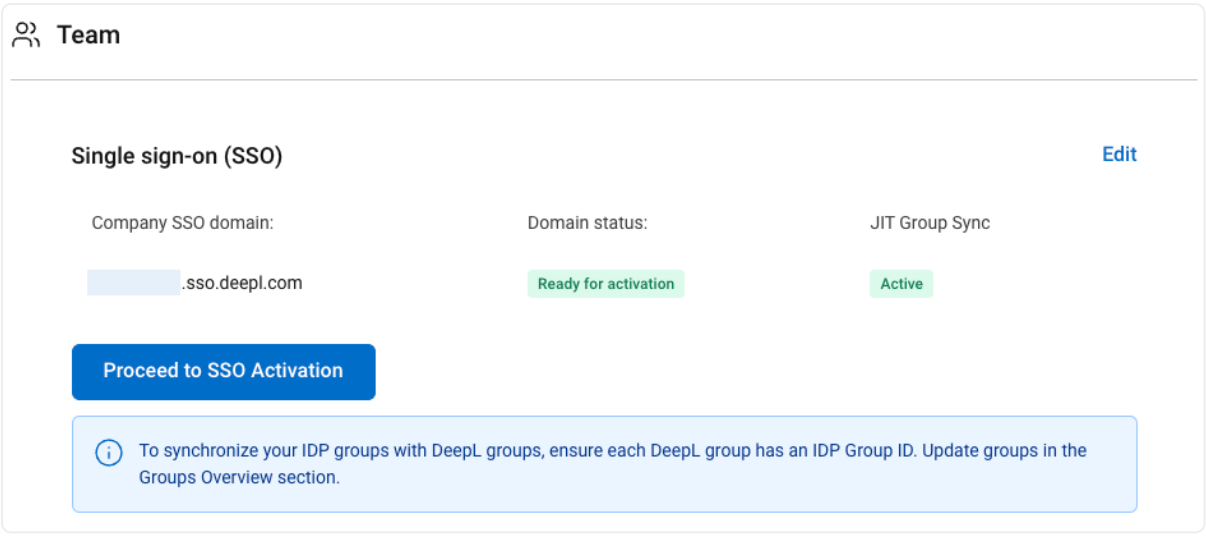


2. Click *Set up SSO* next to *Single sign-on*.



3. Enter the following information from the configured application in OneLogin.
   - OpenID Connect metadata
     Enter the URL from Microsoft Entra ID. For more information, see Collect endpoints.
   - Client ID
     You find the Client ID in Microsoft Entra ID in your registered Application when you select *Overview* in the left-side menu under *Application (client) ID*.
   - Client Secret
     For more information, see Create client secret.
   - Enter *groups* as the *Group Claim Name*.
4. Enable *JIT Group Sync*.

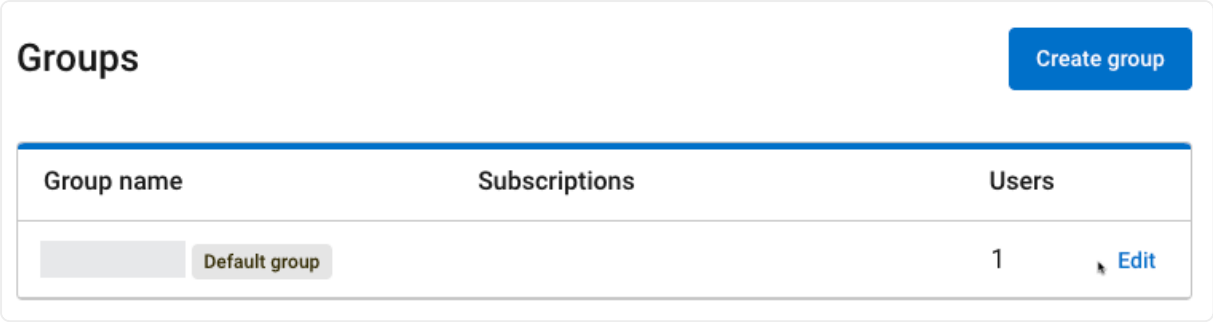
5. Confirm and Save changes.
6. Activate SSO.



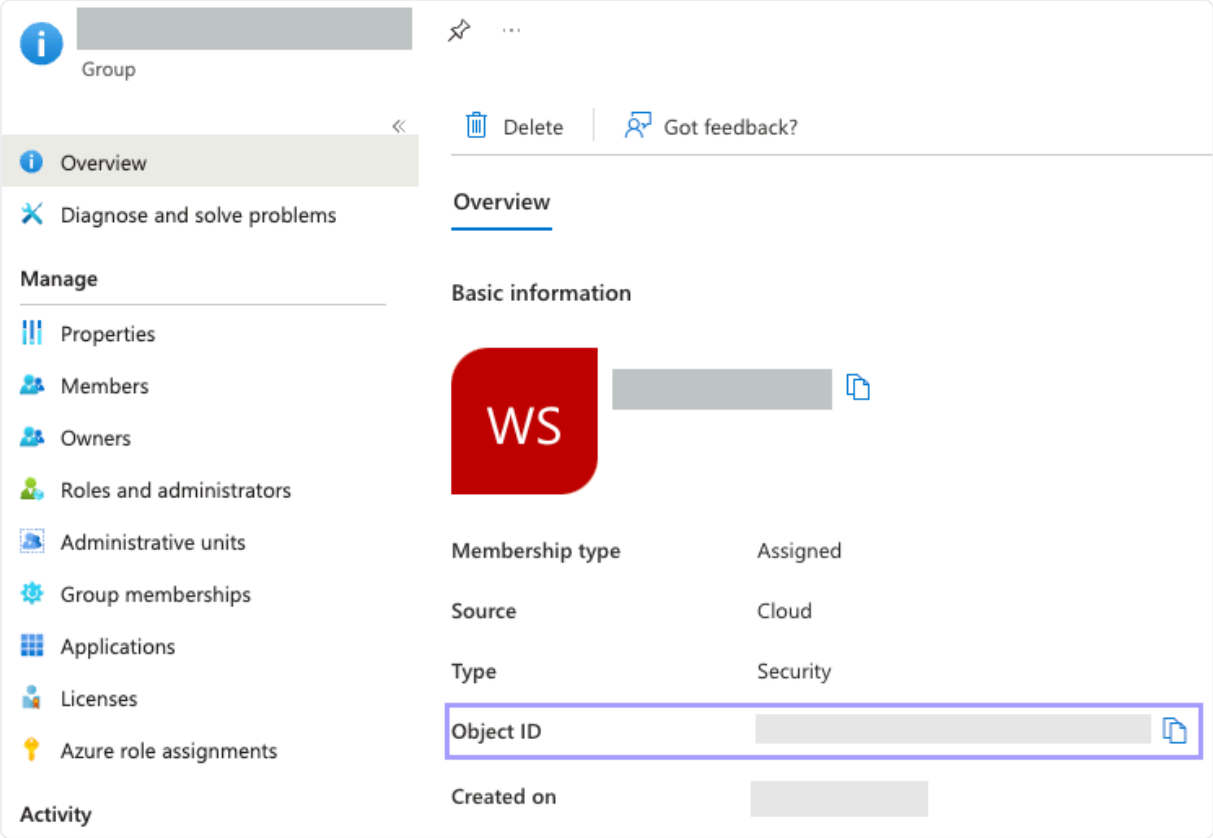
Set up groups

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*.

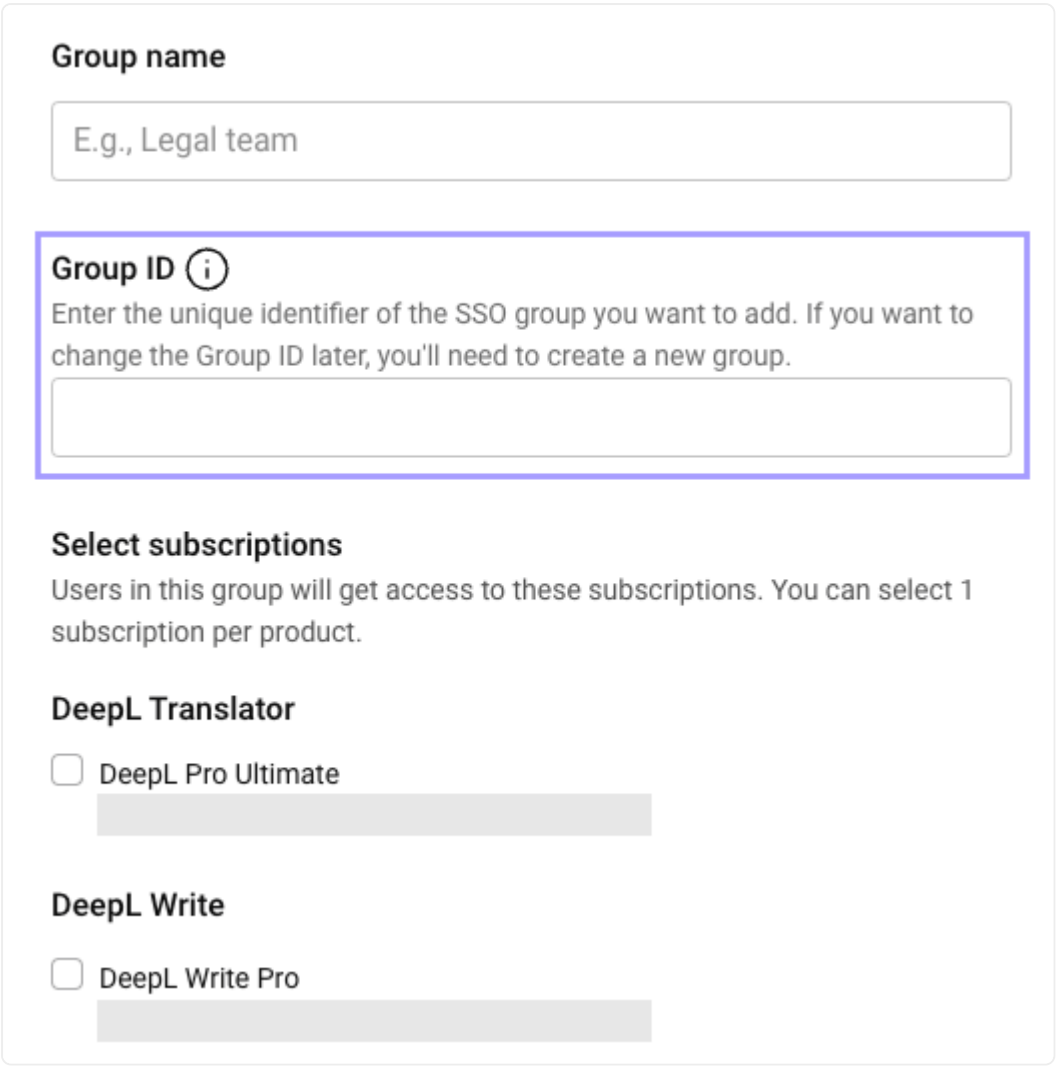
> ⚠ JIT Provisioning Group Sync does not create groups based on the OIDC token. If the token includes groups that do not exist in DeepL, that group information will be ignored, and the user is added only to the Default group. For more information about this default behavior, please consult the *Default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



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.



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



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.