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

- Prerequisites
- Edit the SSO configuration in Microsoft Entra ID
- Edit the SSO configuration in DeepL accounts
- Set up groups
- Without JIT group synchronization

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: SAML 2.0
- 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.

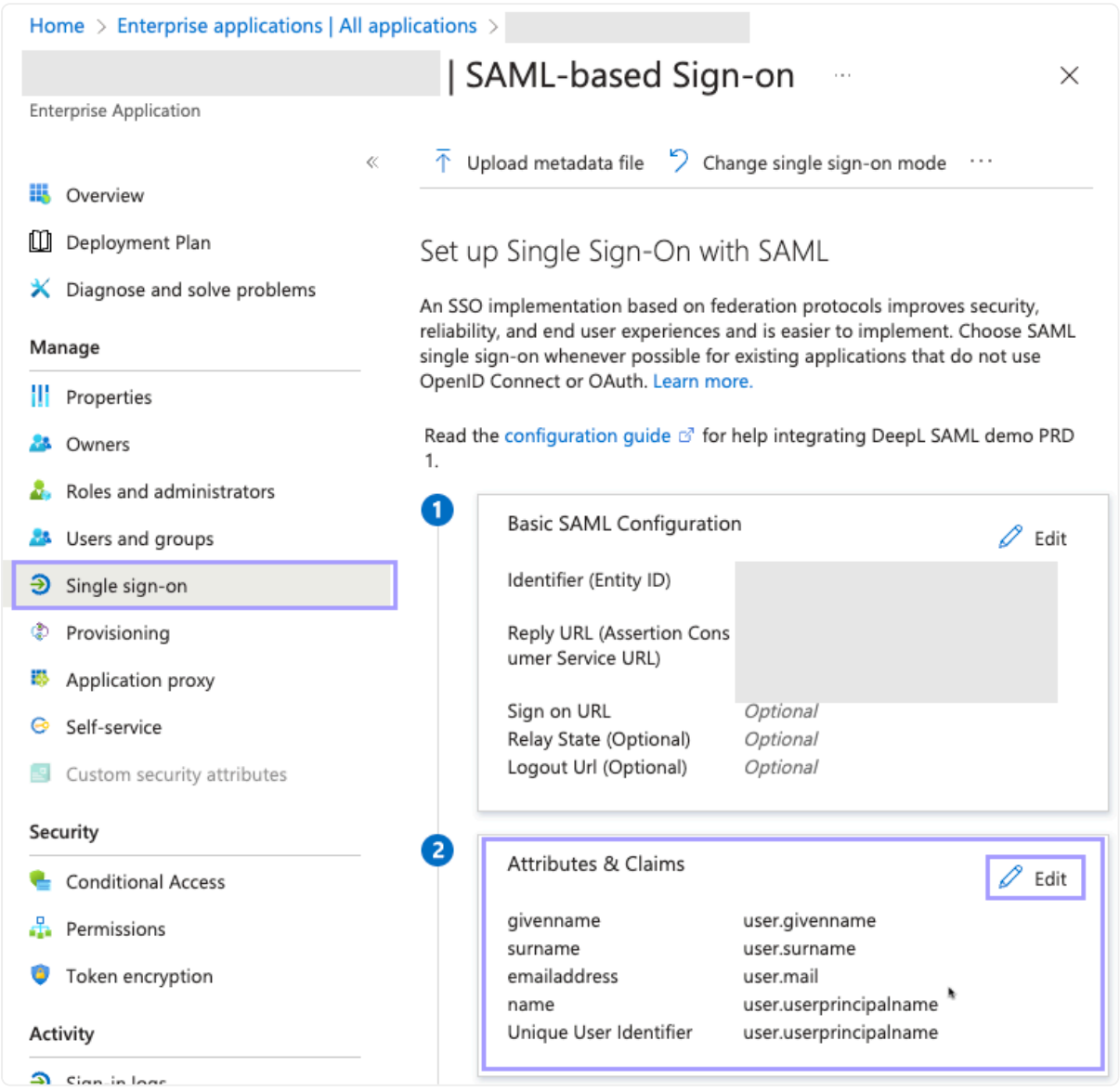
Once DeepL has enabled subscription management by groups for your organization, a new *Groups* tab will appear in the admin area in your *DeepL account*. A default group is automatically created, and all existing users are placed in this default group. All users will retain access to their current subscription, 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

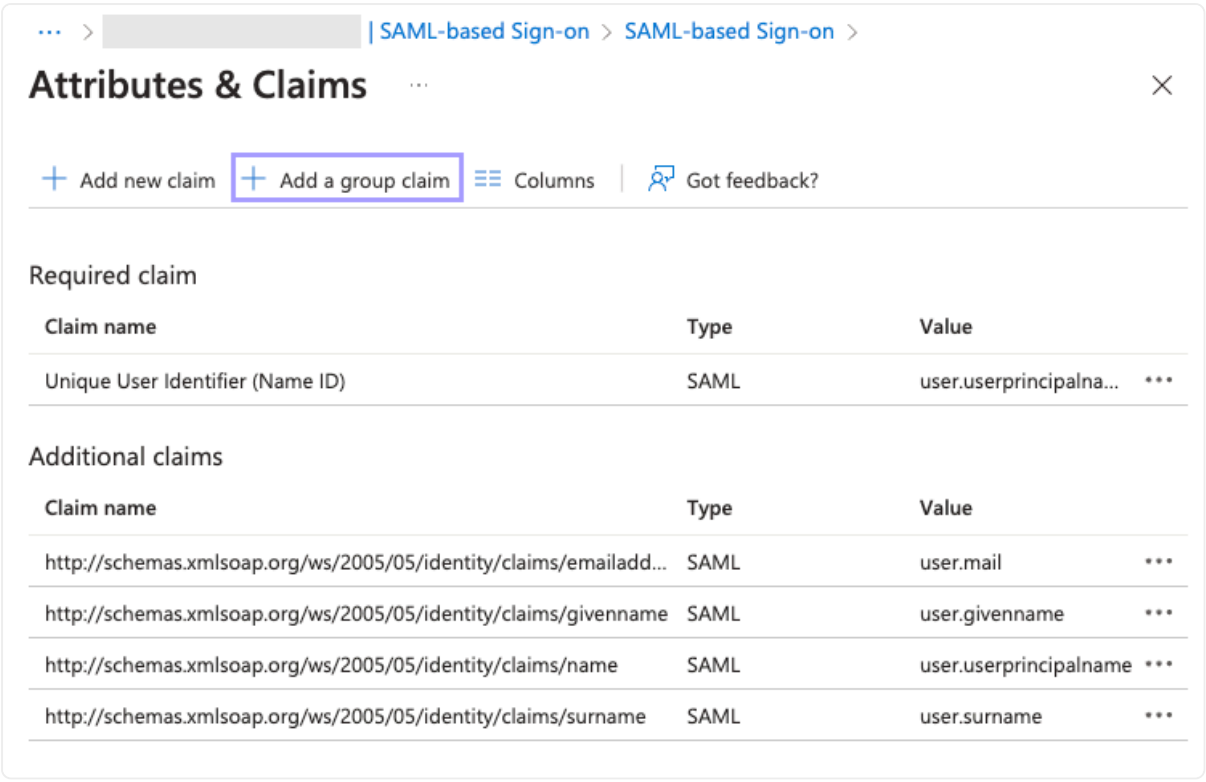
information, see the document Subscription Management by Groups.

Edit the SSO configuration in Microsoft Entra ID

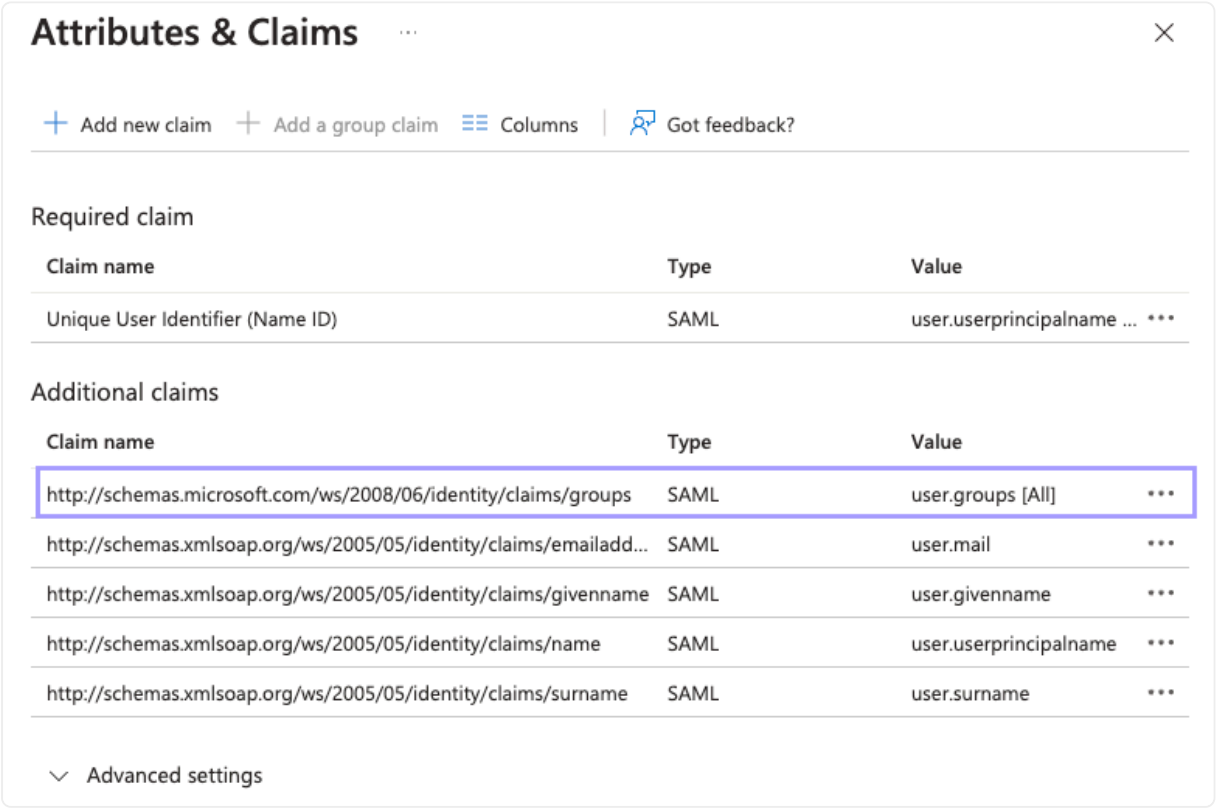
1. Go to your Microsoft Entra ID instance and the DeepL application under *Enterprise applications*.
2. Select *Single sign-on* under *Manage*.
   Under *Attributes & Claims* you see the current list of attributes that are being passed in the SAML token for SSO login.
3. To add the groups attribute, click on *Edit*.



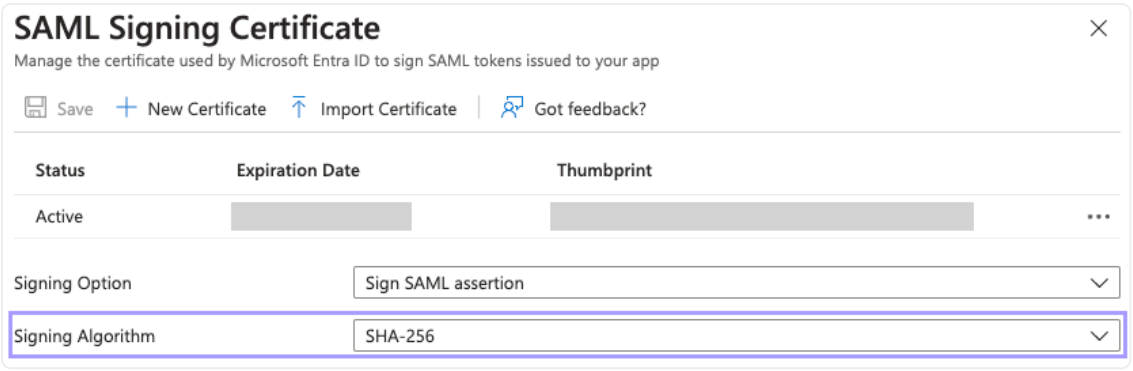
4. Click on *Add a group claim*.



5. In the *Group Claims* dialog, select *Groups assigned to the application* and *Group ID* under *Source attribute*.
   After saving the changes, the *user.groups* attribute is displayed in the list.
6. Save the changes.
   The group attribute is now included in the SSO reference.

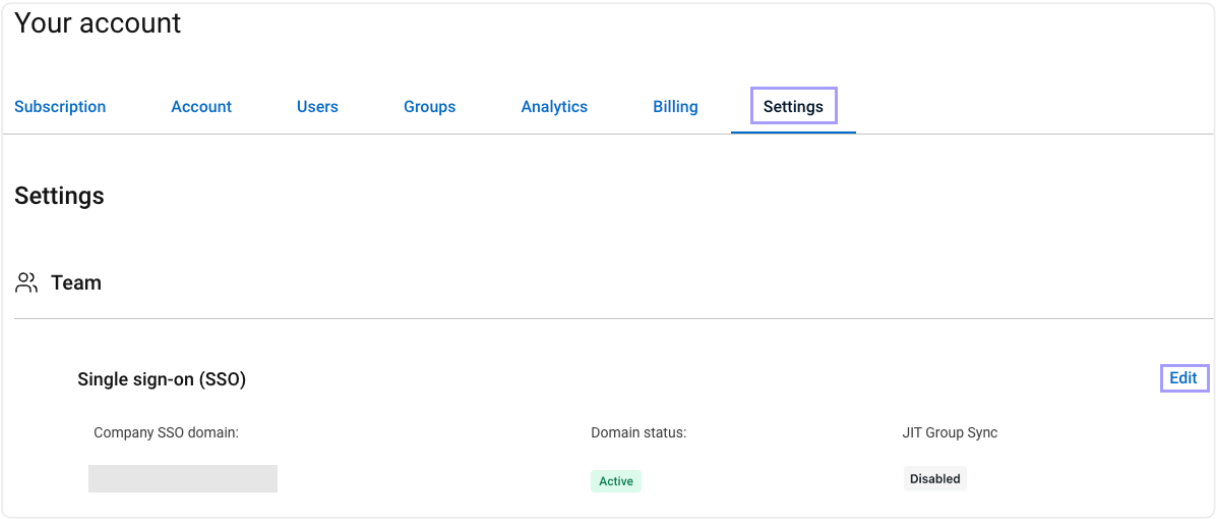


7. Click on *Edit* next to *SAML Certificates* to check if SHA-256 or SHA-512 is enabled.



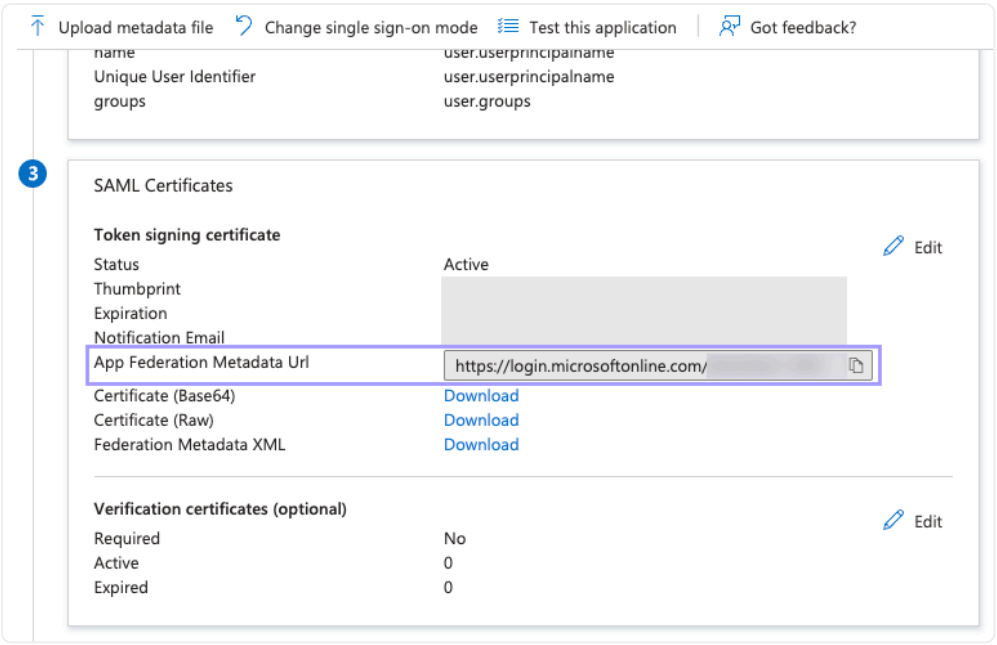
Edit the SSO configuration in DeepL accounts

1. Login as an admin.
2. Click on your user and select *Account* and go to the *Settings* tab.
   Under *Team* and *Single sign-on* SSO is already configured and activated. *JIT Group Sync* is still Deactivated.



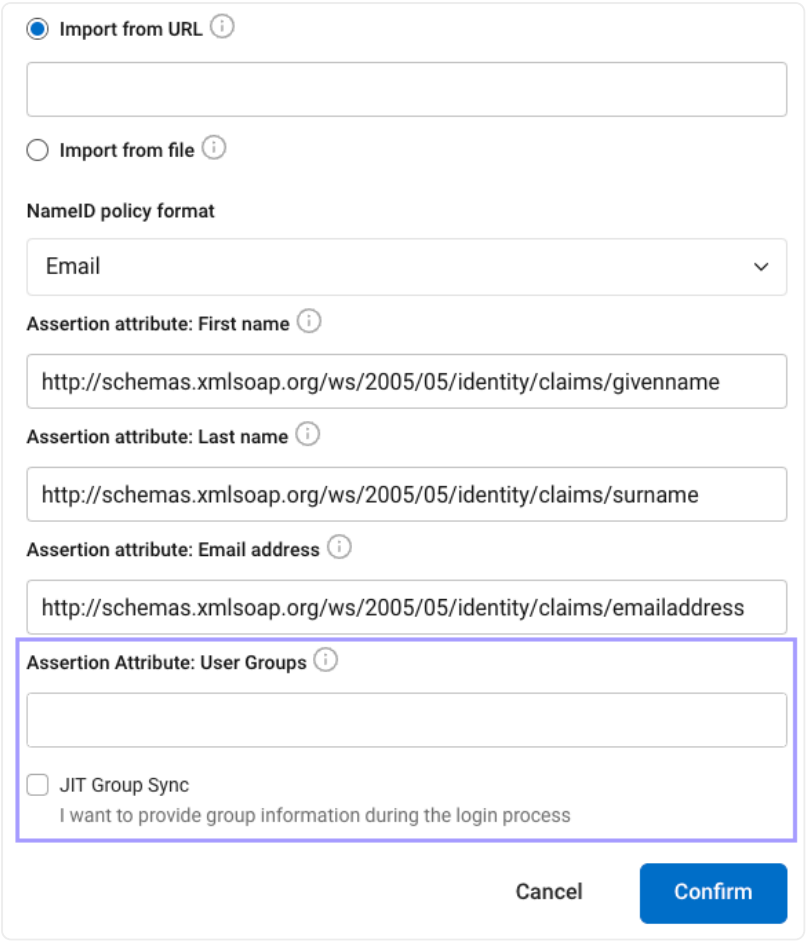
3. Click *Edit* next to *Single sign-on (SSO)*.
   In the *Set up SSO* form you see two new fields: *Assertion Attribute: User Groups* and *JIT Group Sync*.
4. Select *Import from URL* and enter the *Federation Metadata XML URL* from the Microsoft Entra ID instance which you find under *Single sign-on* and *SAML*

Certificates.



5. Enter http://schemas.microsoft.com/ws/2008/06/identity/claims/groups under *Assertion Attribute: User Groups* and enable *JIT Group Sync*.
   The user's group memberships will be read by DeepL during the login.

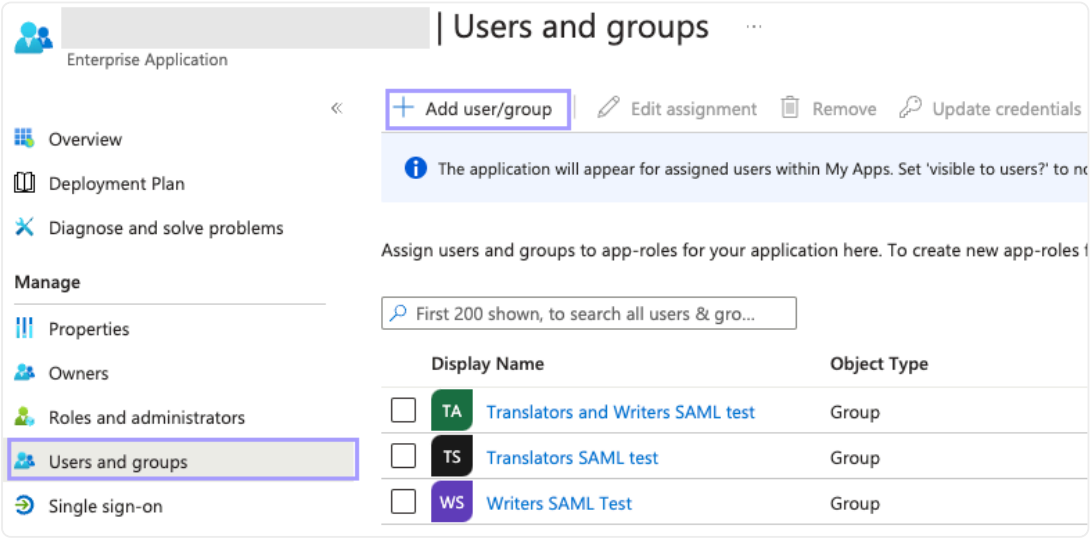
> ⓘ Leave the values of the other assertion attributes unchanged. They don't need to be changed to enable JIT group synchronization.



6. Confirm and Save changes.

Set up groups

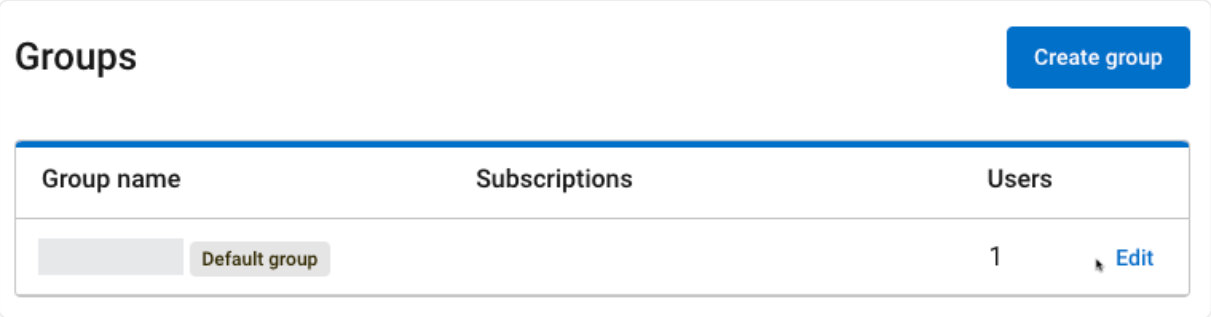
1. Go to Microsoft Entra ID.
2. Create groups for DeepL access.
3. Add users to the groups.
4. Assign the groups to the Enterprise application.



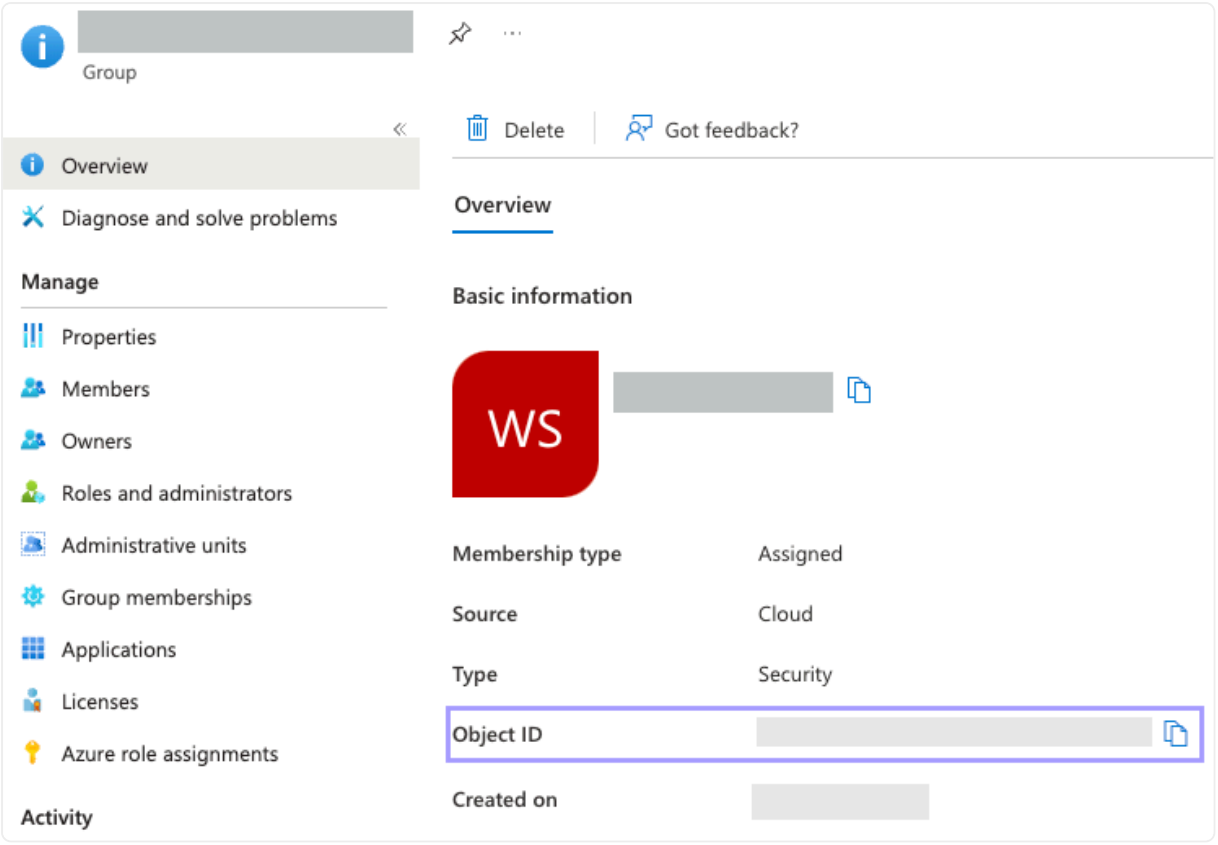
5. Go to your DeepL account.

6. Create the same groups that you created in your Microsoft Entra ID instance to manage your users.
7. Go to tab *Groups* and click on *Create Group*.

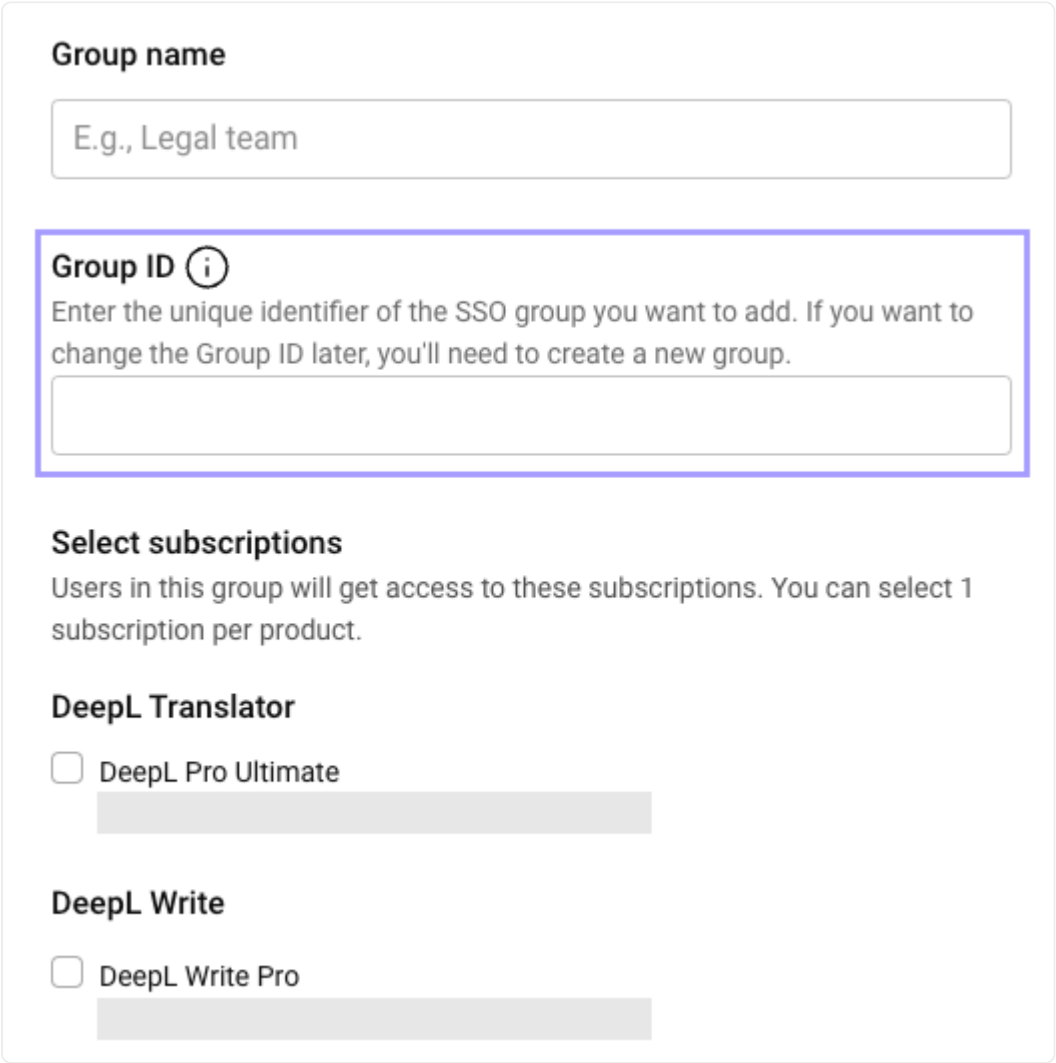
> ⓘ JIT Provisioning Group Sync doesn't create groups based on the user's SAML assertion. If a user's SAML assertion includes groups that don't exist in DeepL, that group information will be ignored and the user will be added to the default group. For more information, see the Subscription Management by Groups document.



8. 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.
9. Enter the group's Object ID from Microsoft Entra ID under *Group ID*.
   You find the ID on the Group properties page.



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



11. Click on *Create group* to save the changes.
12. Repeat this process for each group from your Microsoft Entra ID instance.
    As a result, the groups you have granted access to the DeepL application will be reflected in your DeepL account.
13. 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.