Set up SSO for subscription management by groups: OpenID Connect and OneLogin

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: OneLogin
- 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.

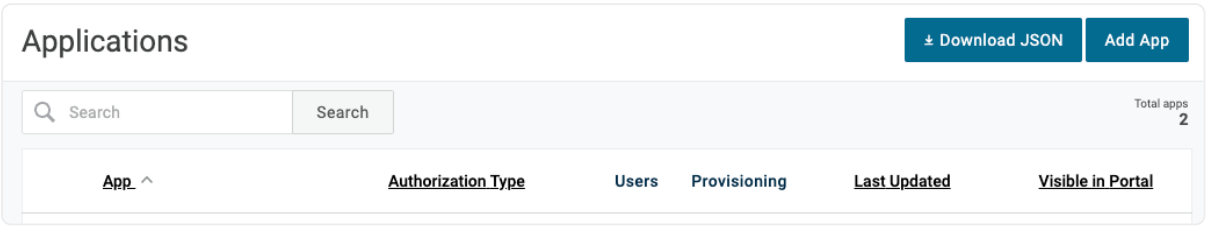
To use Just-In-Time (JIT) provisioning with group synchronization, you need to update your SSO configuration in both DeepL and your OneLogin instance. For more information, see

the document Subscription Management by Groups.

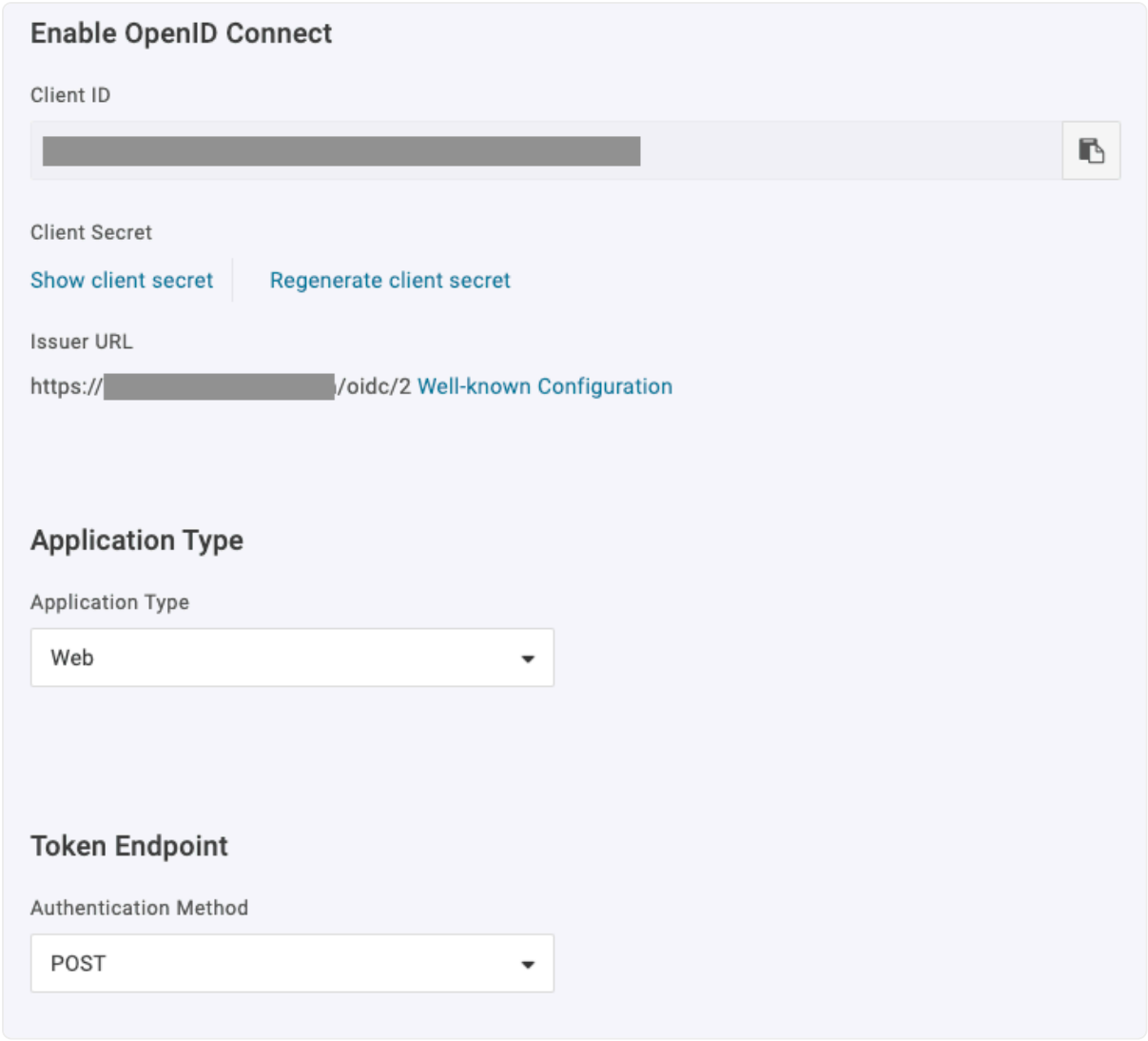
Set the SSO configuration in OneLogin

Add application

1. Go to your OneLogin instance and select *Applications*.
2. Click on *Add Apps*.



3. Search for the OIDC connector *OpenId Connect (OIDC)*.
4. Enter *DeepL SSO* under *Display Name* and keep *Visible in portal* enabled.
5. Upload the DeepL icon and *Save*.
6. Select *Configuration* from the left-side menu.
   - Enter the *Login Url:* *https://ALIAS.sso.deepl.com*
     (Replace ALIAS with your chosen company SSO domain. The ALIAS value can be found under *Company SSO domain* in the SSO configuration area in your *DeepL account*.
   - Enter under *Redirect URI:*
     https://w.deepl.com/auth/realms/prod/broker/ALIAS/endpoint
     (Replace ALIAS with your chosen company SSO domain. The ALIAS value can be found under *Company SSO domain* in the SSO configuration area in your *DeepL account*.
7. Select *SSO* from the left side menu.
   - Set *Authentication Method* in section *Token Endpoint* to *POST*.
   - Enable *Login Hint*.
8. Save the changes.



Edit groups parameter

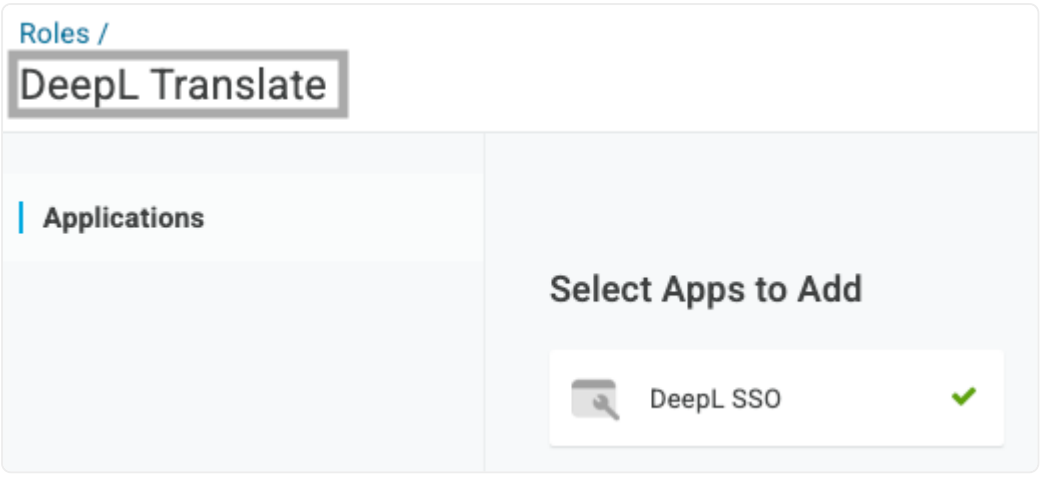
1. Select *Parameters* from the left-side menu.
   There is a default parameter called *Groups*.
2. Click on the parameter *Groups* and select the following in section *Default if no value is selected*.
   - *User Roles*
   - *Semicolon Delimited input (Multi-value output)*
3. Save the changes.

> ⓘ The configuration also works if you source the OneLogin directory from Microsoft Entra ID.

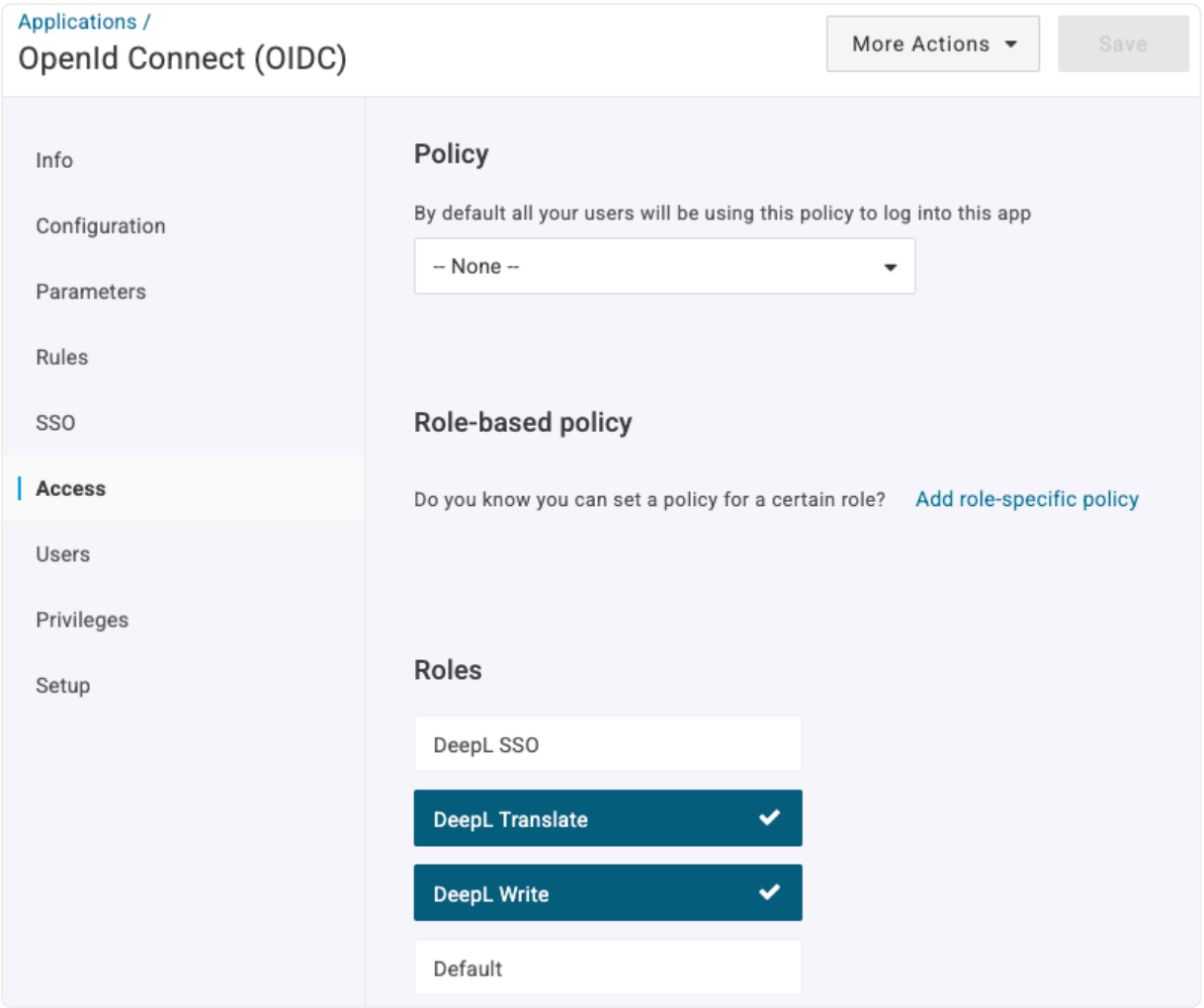
Set up roles and grant access

1. Go to *Users* and select *Roles*.
2. Click on *New Role*, enter a role name and select the DeepL application.

3. Save the changes.



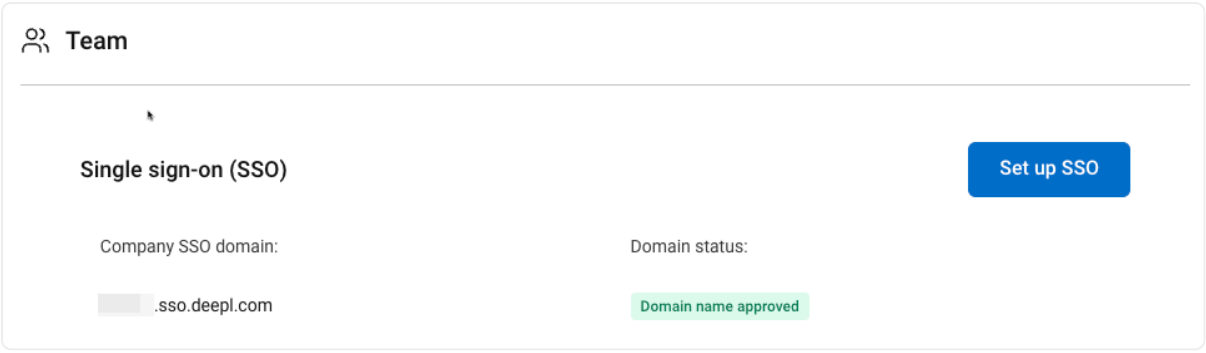
4. Add all roles necessary for DeepL user access.
5. Go to *Applications* and select the DeepL application.
6. Select *Access* from the left-side menu.
7. Select the roles you've created for DeepL access.



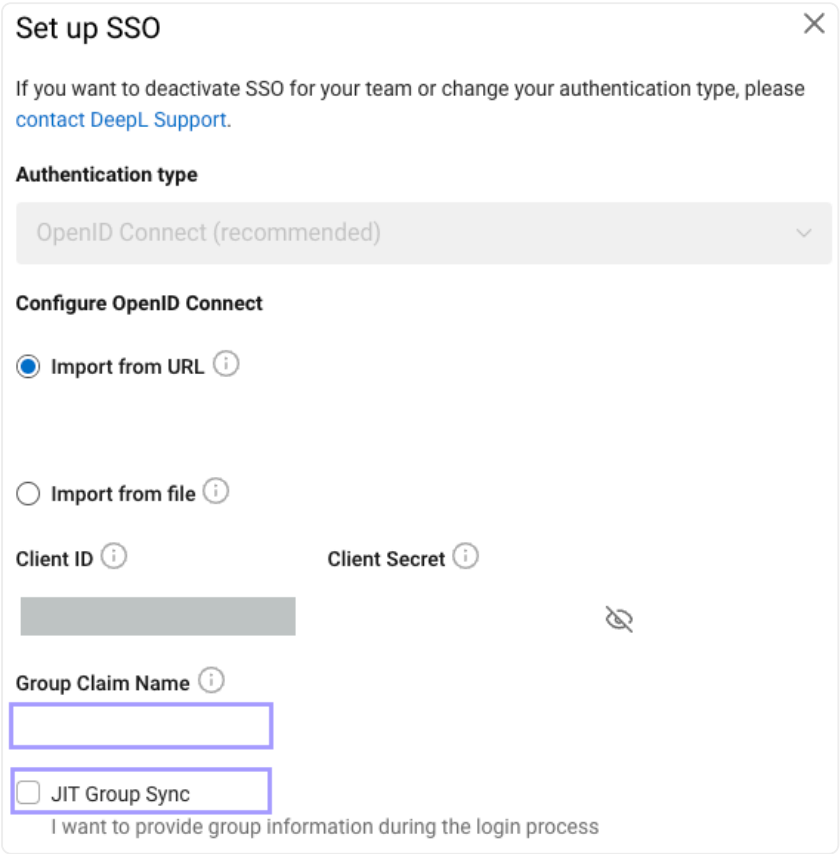
8. Add users to the created roles.

Set the SSO configuration in DeepL account

1. Login as an admin in your DeepL account.
2. 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*.

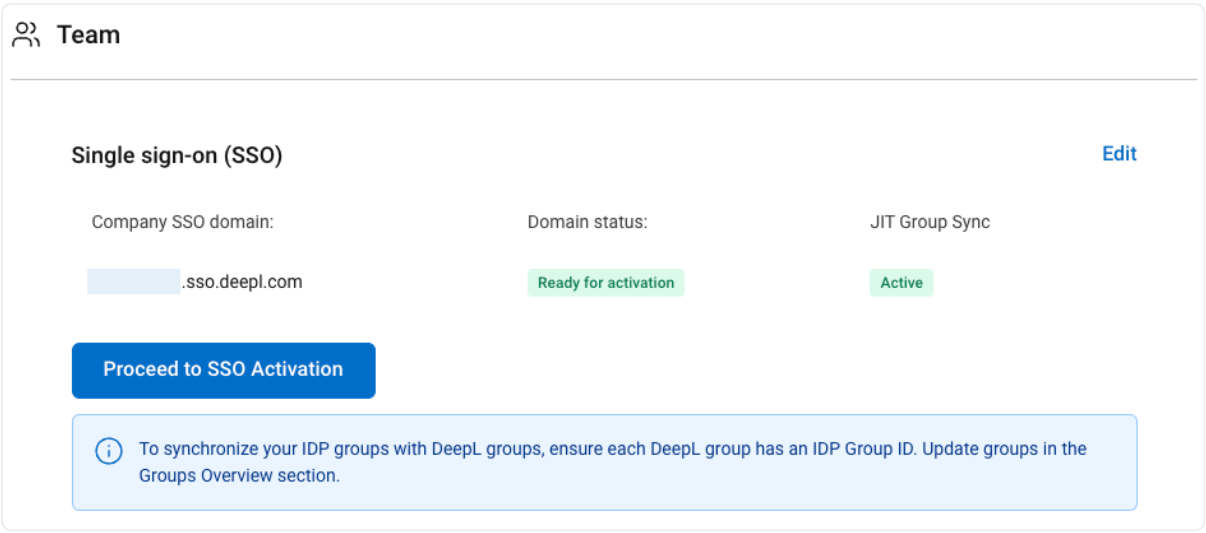


3. Click *Set up SSO* next to *Single sign-on*.



4. Enter the following information from the configured application in OneLogin.
   - OpenID Connect metadata
     You find the Well-known configuration URL in OneLogin under *SSO* and *Issuer URL*. Right-click on the URL and select *Copy link address*.
   - Client ID
   - Client Secret
   - Enter *groups* as the *Group Claim Name*.
5. Enable *JIT Group Sync*.
6. Confirm and Save changes.

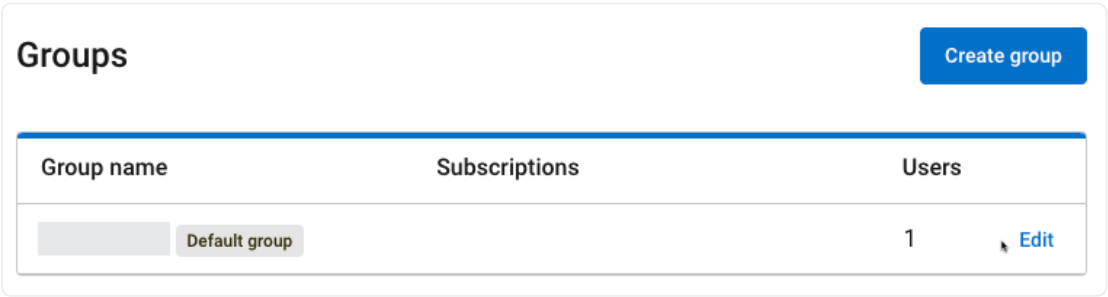
7. Activate SSO.



Set up groups in DeepL account

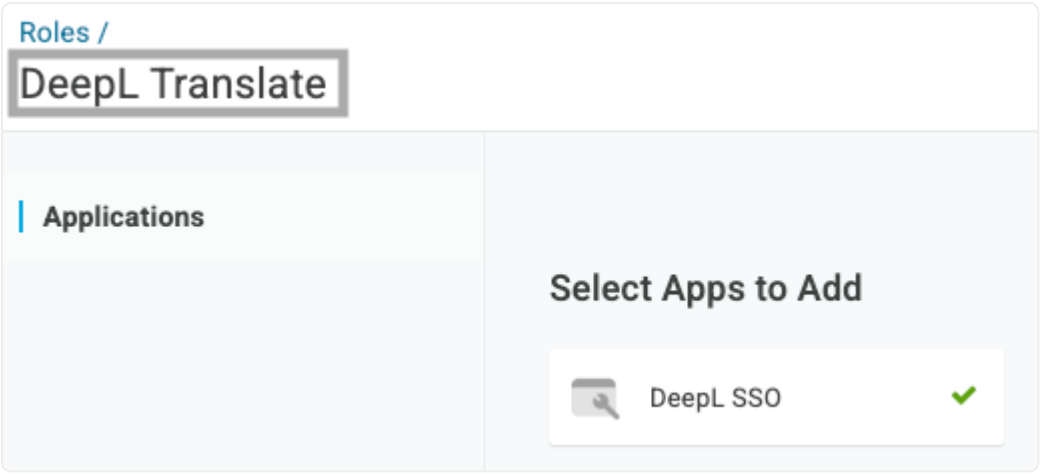
1. Go to your *DeepL account*.
2. Go to tab *Groups* and click on *Create Group*.

> ⓘ 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.

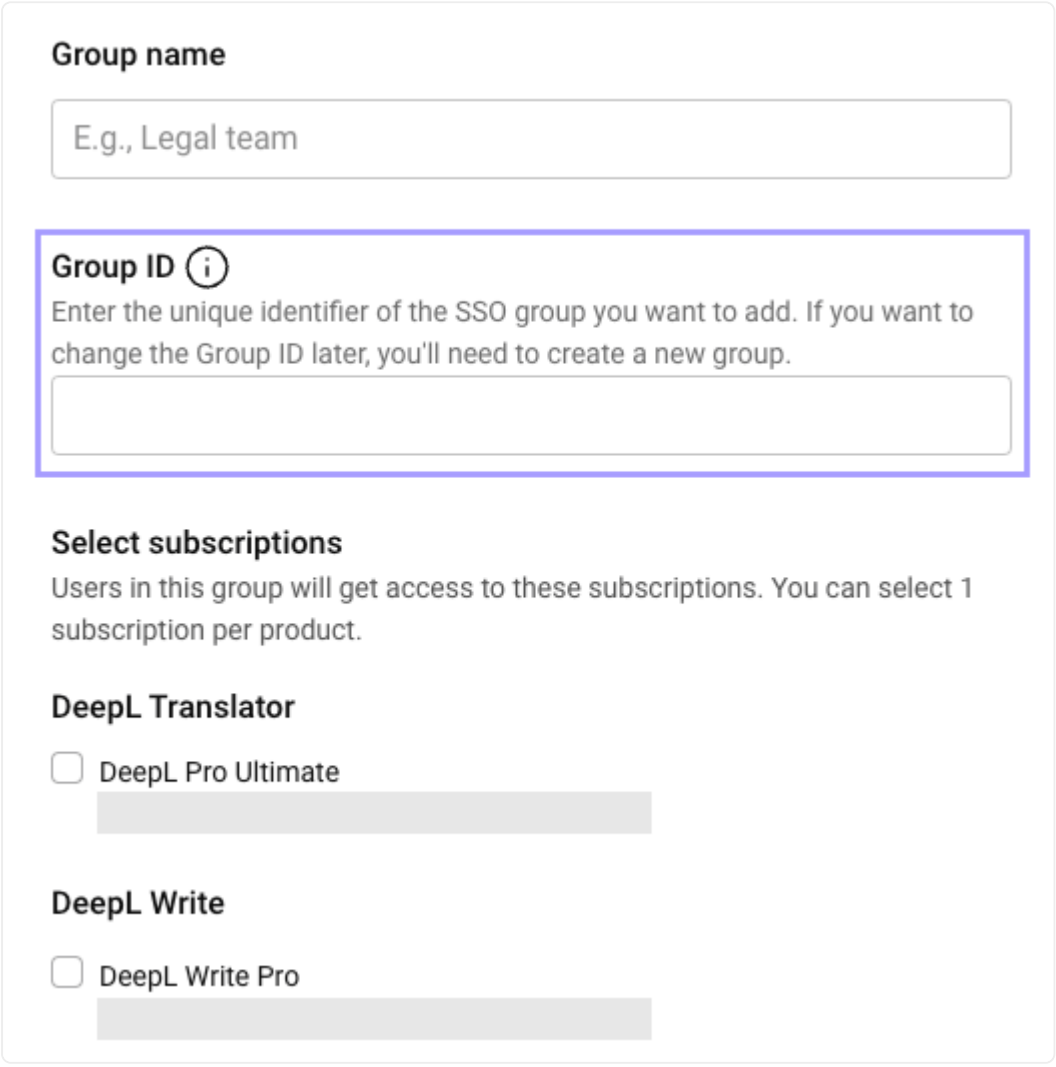


3. Enter a *Group name*.
   We recommend using the same name that you used for your roles in OneLogin. However, you may choose a different name, e.g., if your organization uses concealed role names in the identity provider.
4. Enter the *Role name* string from OneLogin under *Group ID* in your DeepL account.

ⓘ The group ID is handled as case-sensitive. Check that you entered the correct lower and upper case writing of the role name from OneLogin.



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



6. Click on *Create group* to save the changes.
7. Repeat this process for each role from your OneLogin instance. As a result, the roles you have granted access to the DeepL application will be reflected in your DeepL

Account.
8. Before testing, contact us by creating a request.
   Wait for the confirmation from our side.
9. 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 OneLogin 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.