DeepL Help

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

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: Okta
- A company domain has been defined for the DeepL environment. For further information please check Setting up SSO for teams.

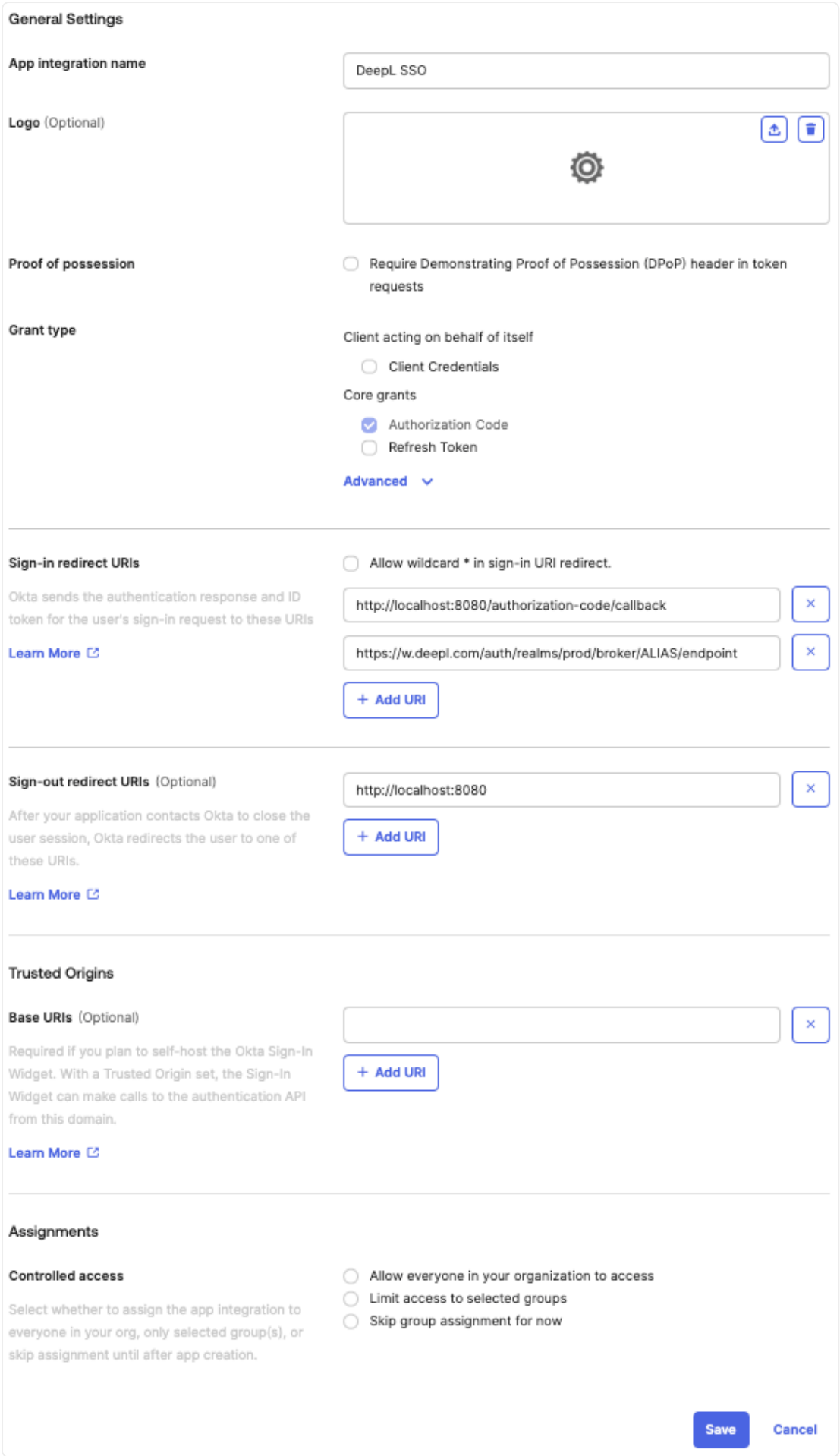
Once DeepL has enabled subscription management by groups for your organization, a new Groups tab will appear in the admin area in your DeepL Account. A default group is automatically created, and all existing users are placed in this default group. All users will retain access to their current subscription, 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 Okta instance. For more information, see the document Subscription Management by Groups.

Set the SSO configuration in Okta

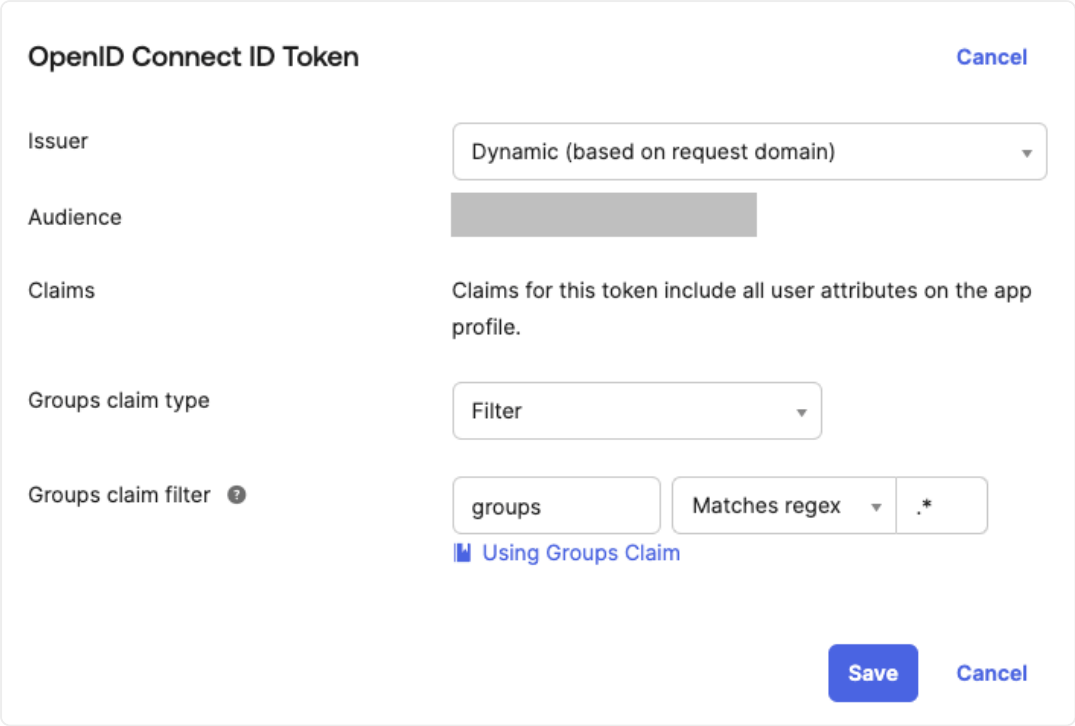
Create App integration

1. Go to your Okta instance and open the *Applications* section.
2. Click on *Create App* integration in the top panel
3. Select *OIDC - OpenID Connect* and *Web Application* and click *Next*.
4. Enter *DeepL SSO* under *App integration name*.
5. Upload the DeepL icon and *Save.*
6. Under *Sign-in redirect URIs* 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*.)
7. Under *Assignments* and *Controlled access* select one of the following
   - *Limited access to selected groups:* If you already have groups set up you can assign them to the application
   - *Skip group assignment for now:* If groups haven't been set up yet you can select this option to do the assignment later.
8. Click *Save*.



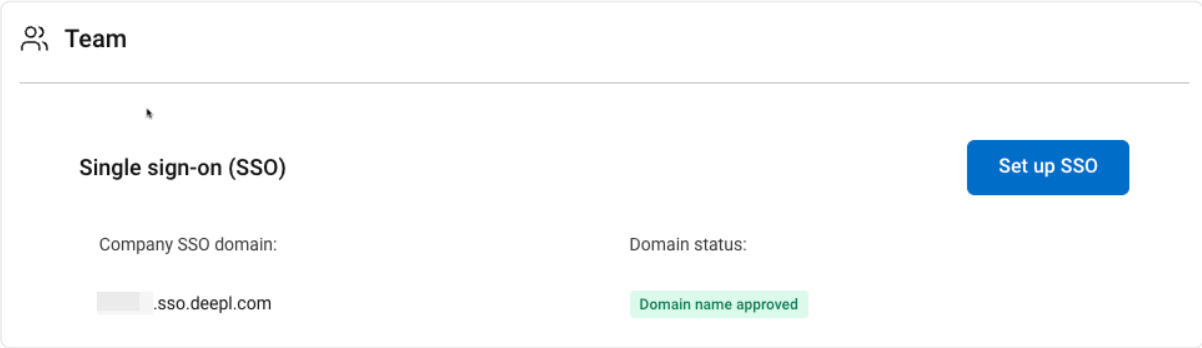
Set groups claim

1. In your Okta instance and the application for DeepL access, go to the *Sign On* tab.
2. Click *Edit* next to *OpenID Connect ID Token*.
3. Select *Filter* for *Groups claim type*.
4. For *Groups claim filter* enter *groups*, select *Matches regex*, and enter .*.



Set the SSO configuration in DeepL accounts

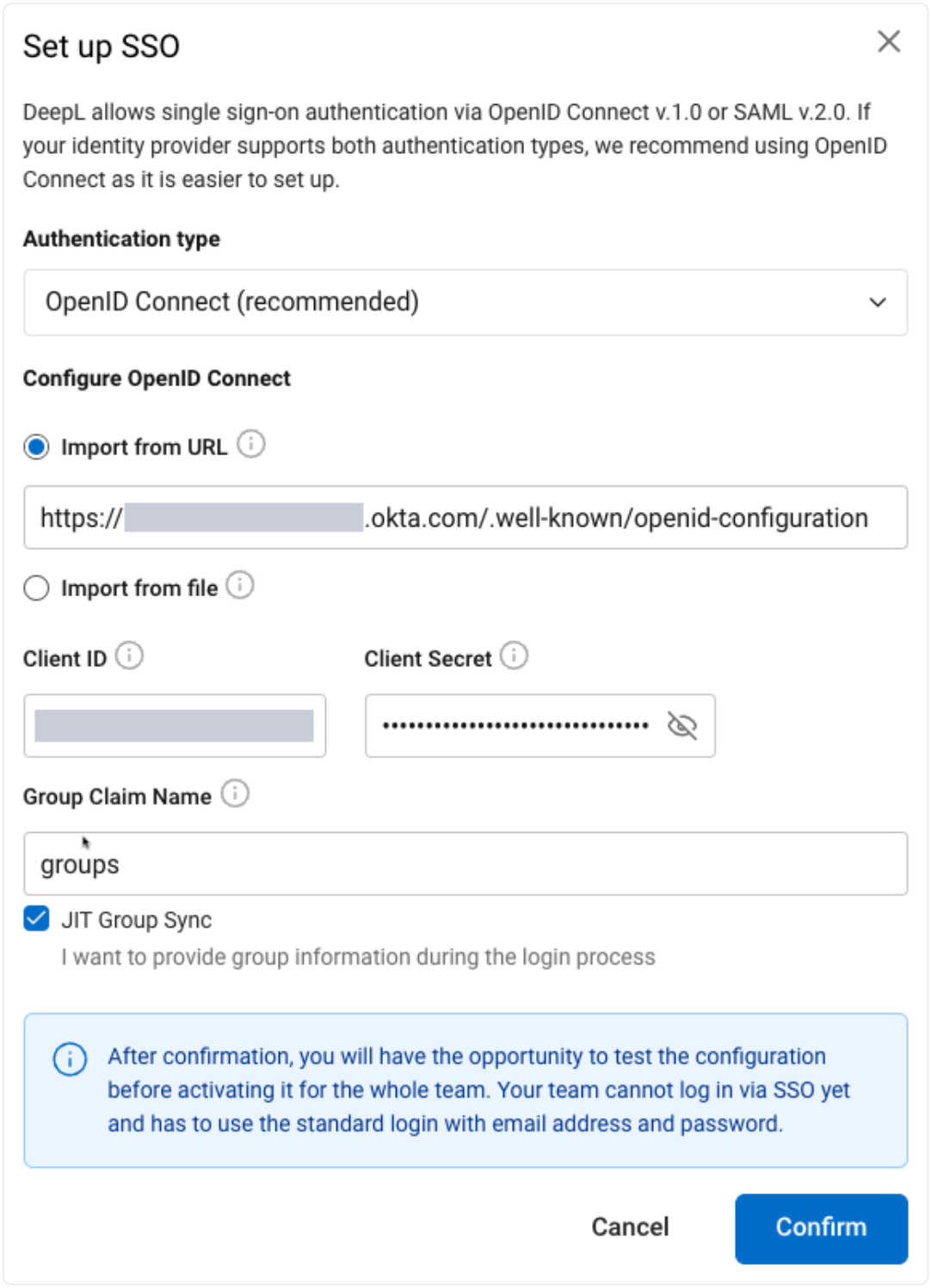
1. Login as an admin.
2. Click on your user and select *Account* and go to the *Settings* tab.
   Under *Team* and *Single sign-on* the SSO domain has the status *Domain name approved*.



3. Click *Set up SSO* next to *Single sign-on*.
   In the *Set up SSO* form select *OpenID Connect* as the *Authentication type* and enter the

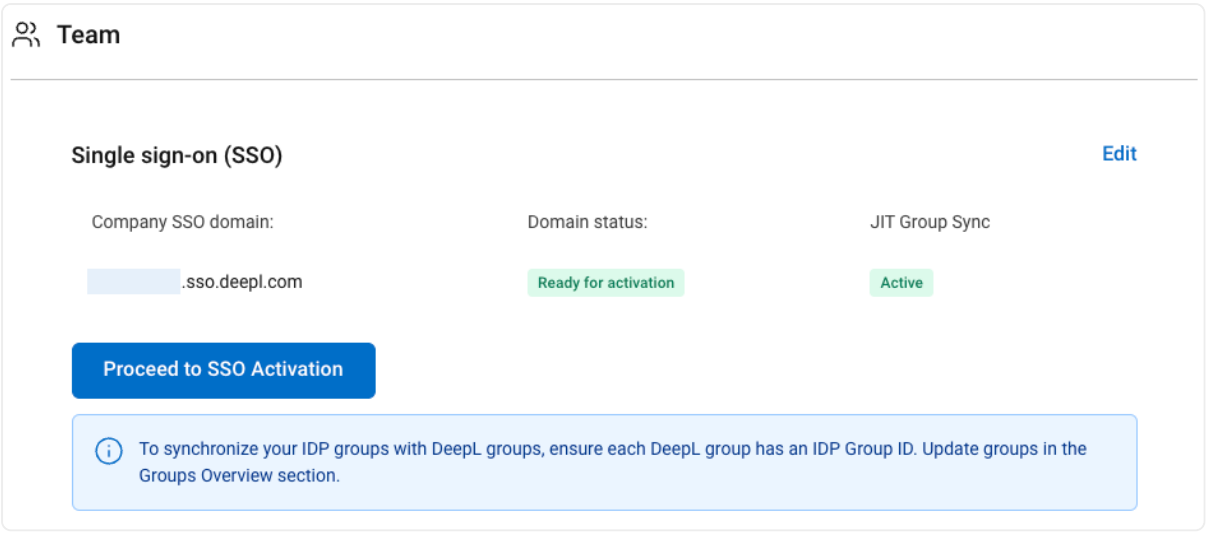
following information from Okta.

- OpenID Connect metadata endpoint: https://YOUR_OKTA_DOMAIN.okta.com/.well-known/openid-configuration (Replace YOUR_OKTA_DOMAIN with your Okta instance.)
- Client ID
- Client Secret
- Groups claim name: *groups*



4. Enable *JIT Group Sync*. The user's group memberships will be read by DeepL during the login.

5. Activate SSO.



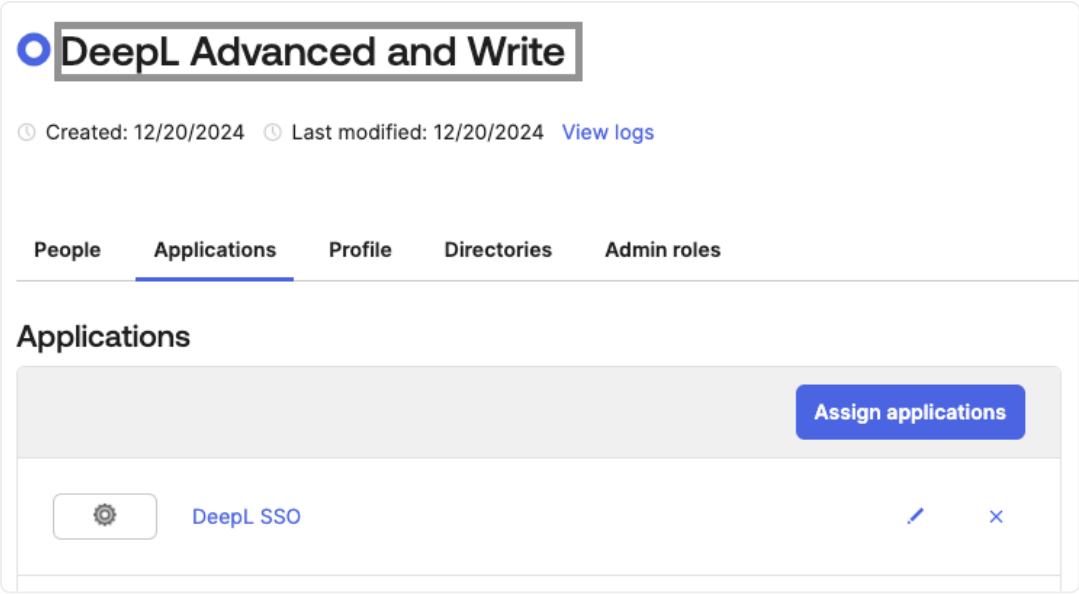
Setup groups

1. Go to Okta.
2. Create groups for the DeepL access and add users to the groups.
3. Open the DeepL SSO application and select the *Assignments* tab.
4. Click on *Assign* and select *Assign to Groups*.
5. Go to your *DeepL account*.
6. Create the same groups that you created in your Okta instance to manage your users.

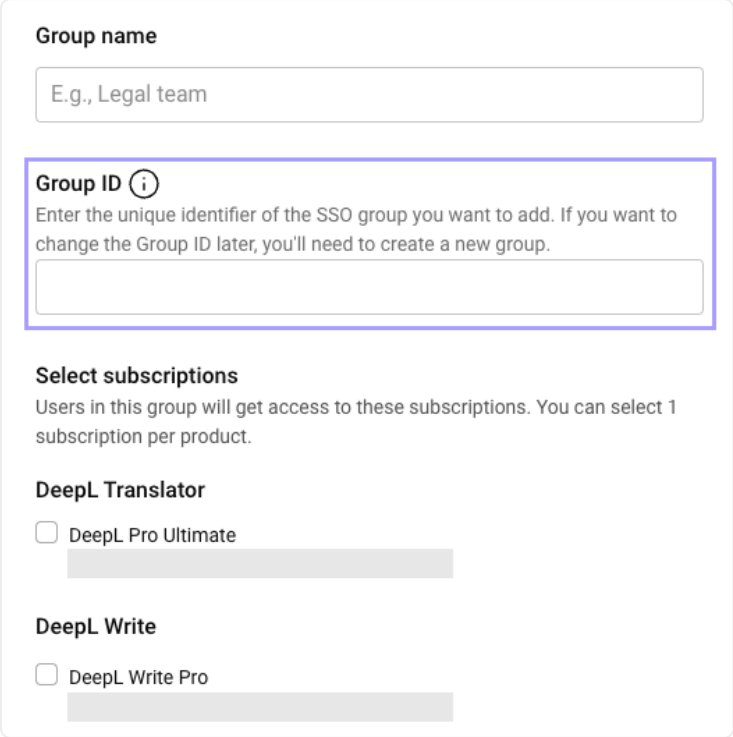
> ⚠ JIT Provisioning Group Sync does not create groups based on the OIDC token. If the token includes groups that do not exist in DeepL, that group information will be ignored, and the user is added only to the Default group. For more information about this default behavior, please consult the *Default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

7. Go to the *Groups* tab and click on *Create group*.
8. Enter a *Group name*.
   We recommend using the same name that you used for your groups in Okta. However, you may choose a different name, e.g., if your organization uses concealed group names in the identity provider.

9. Enter the group name string from Okta under *Group ID*.



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

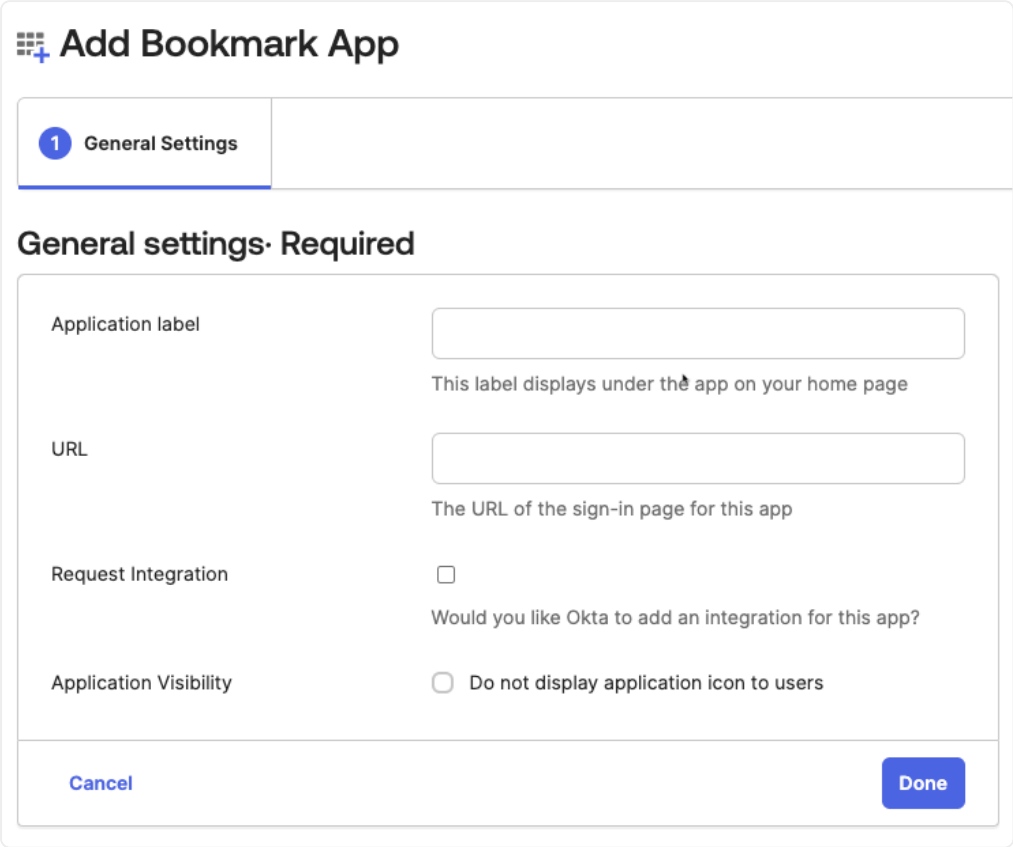


11. Click on *Create group* to save the changes.
12. Repeat this process for each group from your Okta instance. As a result, the groups you have granted access to the DeepL application will be reflected in your *DeepL account*.

Create a bookmark for your app

1. Open the *Applications* section and click on *Browse App Catalog*.

2. Search for *Bookmark App* and add the app.
3. Click on *Add Integration*.
4. Add the following information.
   - *Application label*: DeepL SSO
   - *URL*: https://ALIAS.sso.deepl.com
     (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*.)



5. Assign the same user and groups to the bookmark app as you have to the DeepL SSO app.
6. Before testing, contact us by creating a request.
   Wait for the confirmation from our side.
7. 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 Okta 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.