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

- Prerequisites
- Set the SSO configuration in Okta
- Set the SSO configuration in DeepL Accounts
- Setup groups
- Create a bookmark for your app

DeepL has introduced subscription management by groups. With this feature users can be managed in groups to which subscriptions are assigned. As an administrator, 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

- Administrator 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.

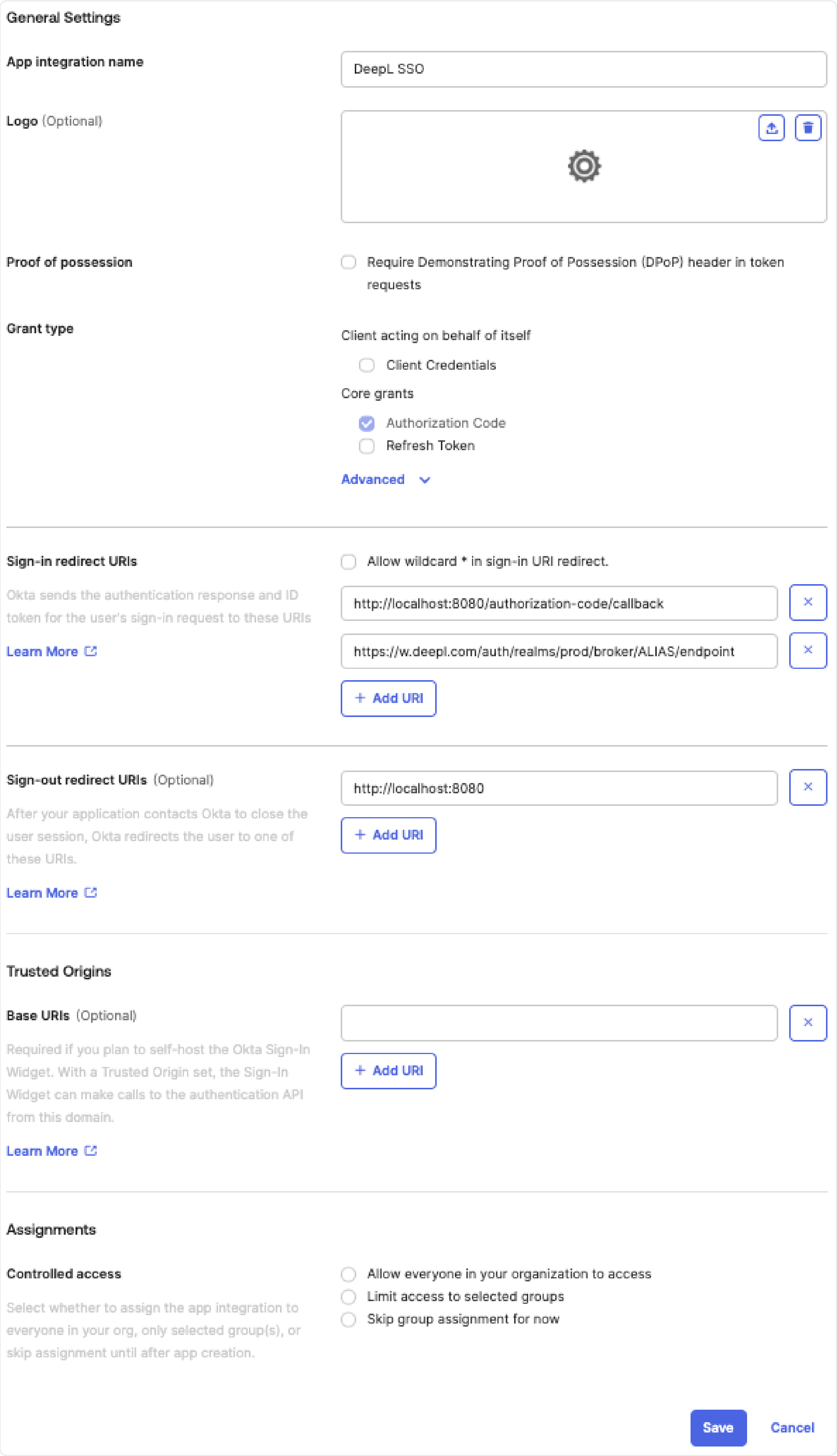
Once DeepL has enabled subscription management by groups for your organization, a new Groups tab will appear in the administration area in your DeepL Account. A default group is automatically created, and all existing users are placed in this default group. All users will retain access to their current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



General Settings

App integration name: DeepL SSO

Logo (Optional)

Proof of possession

☐ Require Demonstrating Proof of Possession (DPoP) header in token requests

Grant type

Client acting on behalf of itself

☐ Client Credentials

Core grants

☑ Authorization Code

☐ Refresh Token

Sign-in redirect URIs

Okta sends the authentication response and ID token for the user's sign-in request to these URIs

☐ Allow wildcard * in sign-in URI redirect.

http://localhost:8080/authorization-code/callback

https://w.deepl.com/auth/realms/prod/broker/ALIAS/endpoint

Sign-out redirect URIs (Optional)

After your application contacts Okta to close the user session, Okta redirects the user to one of these URIs.

http://localhost:8080

Trusted Origins

Base URIs (Optional)

Required if you plan to self-host the Okta Sign-In Widget. With a Trusted Origin set, the Sign-In Widget can make calls to the authentication API from this domain.

Assignments

Controlled access

Select whether to assign the app integration to everyone in your org, only selected group(s), or skip assignment until after app creation.

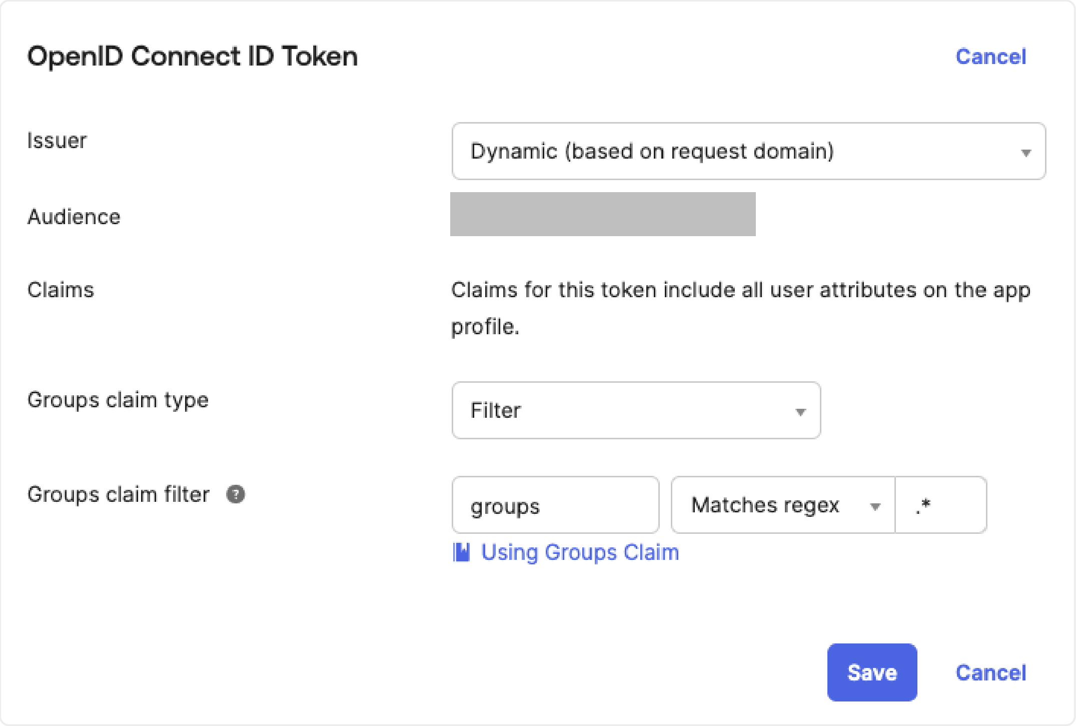
○ Allow everyone in your organization to access

○ Limit access to selected groups

○ Skip group assignment for now

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 *.**.



OpenID Connect ID Token

Issuer: Dynamic (based on request domain)

Audience: [redacted]

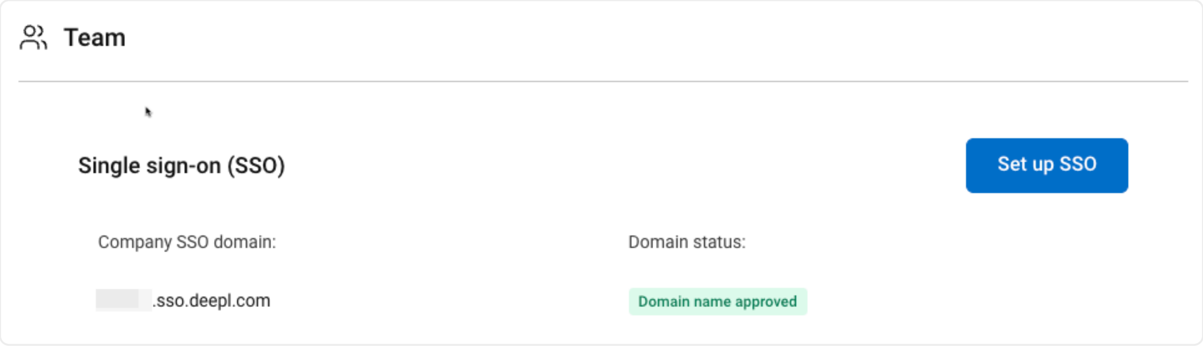
Claims: Claims for this token include all user attributes on the app profile.

Groups claim type: Filter

Groups claim filter: groups | Matches regex | .*

Set the SSO configuration in DeepL accounts

1. Login as an administrator.
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*.



Single sign-on (SSO)

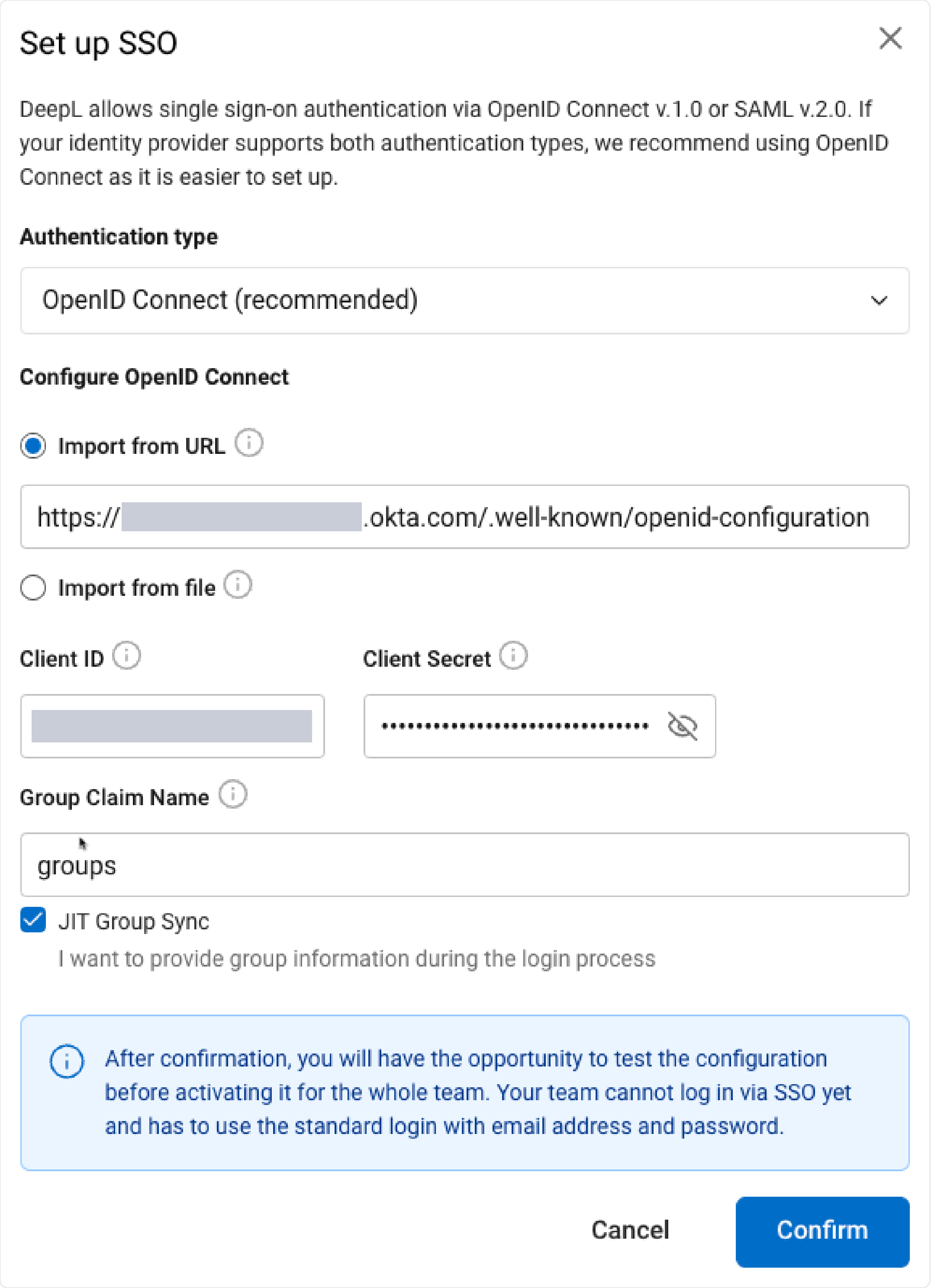
Company SSO domain: [redacted].sso.deepl.com

Domain 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*



Set up SSO

DeepL allows single sign-on authentication via OpenID Connect v.1.0 or SAML v.2.0. If your identity provider supports both authentication types, we recommend using OpenID Connect as it is easier to set up.

Authentication type

OpenID Connect (recommended)

Configure OpenID Connect

● **Import from URL**

https://[redacted].okta.com/.well-known/openid-configuration

○ **Import from file**

Client ID: [redacted]

Client Secret: ••••••••••••••••••••••••••••••••••

Group Claim Name: groups

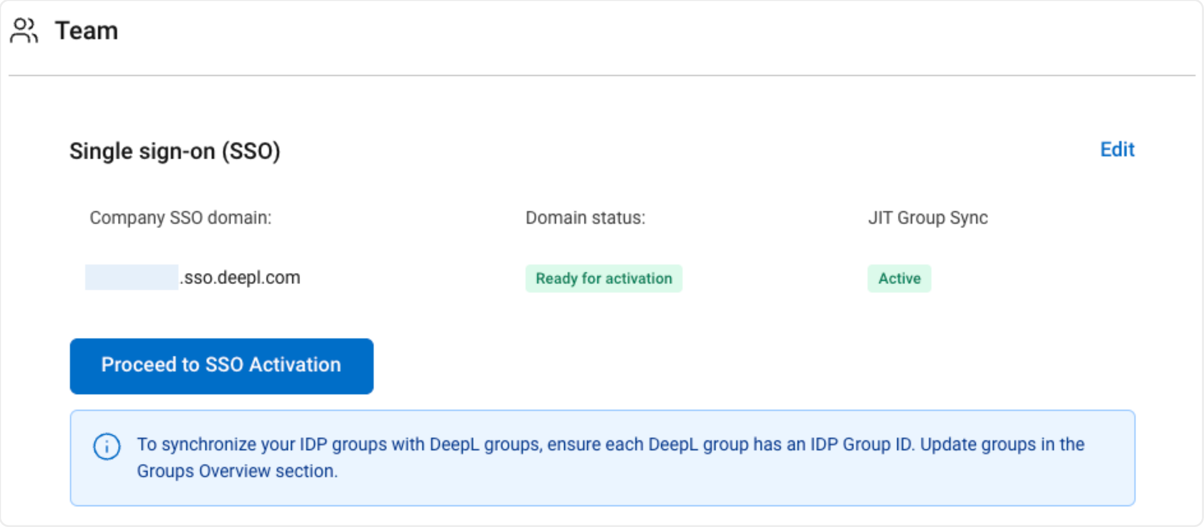
☑ JIT Group Sync

I want to provide group information during the login process

After confirmation, you will have the opportunity to test the configuration before activating it for the whole team. Your team cannot log in via SSO yet and has to use the standard login with email address and password.

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

5. Activate SSO.



Team

Single sign-on (SSO)

Company SSO domain: [redacted].sso.deepl.com

Domain status: Ready for activation

JIT Group Sync: Active

To synchronize your IDP groups with DeepL groups, ensure each DeepL group has an IDP Group ID. Update groups in the Groups Overview section.

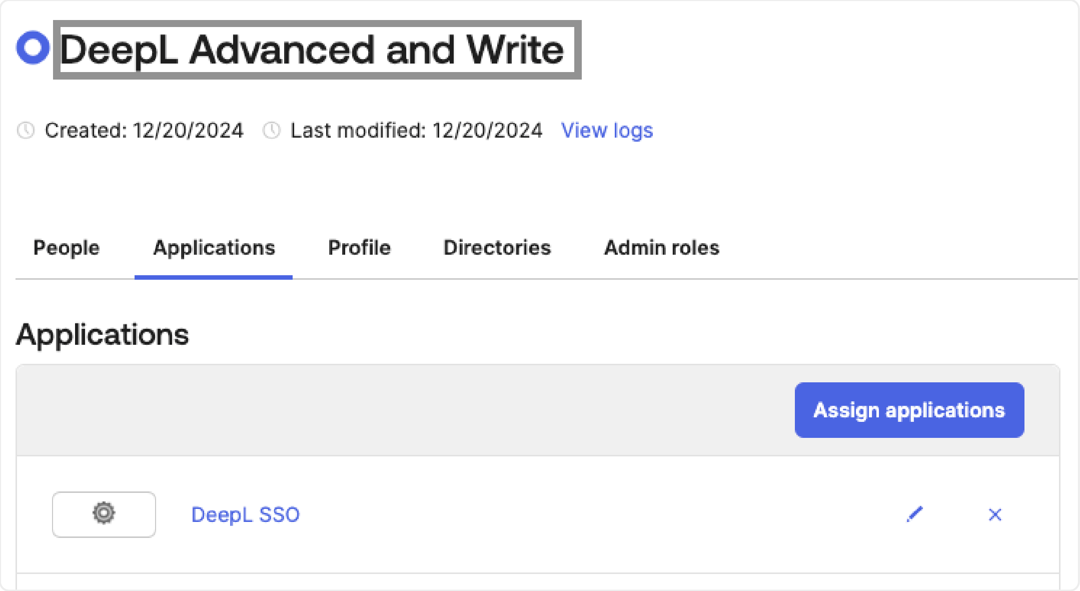
Setup groups

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.

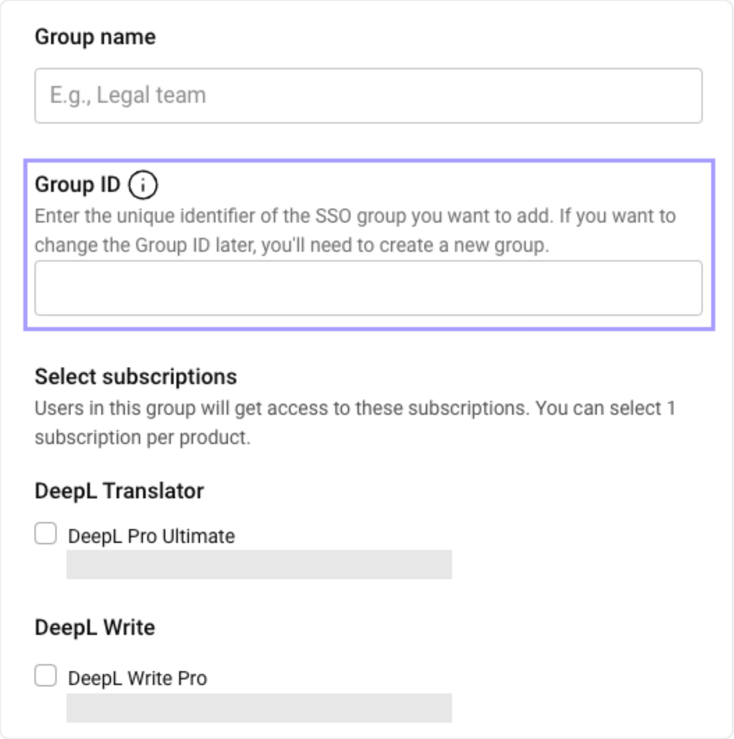
> ⚠ JIT Provisioning Group Sync does not create groups based on the OIDC token. If the token includes groups that do not exist in DeepL, that group information will be ignored, and the user is added only to the Default group. For more information about this default behavior, please consult the *Default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


DeepL Advanced and Write
Created: 12/20/2024
Last modified: 12/20/2024
View logs
People
Applications
Profile
Directories
Admin roles
Applications
Assign applications
DeepL SSO

10. 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

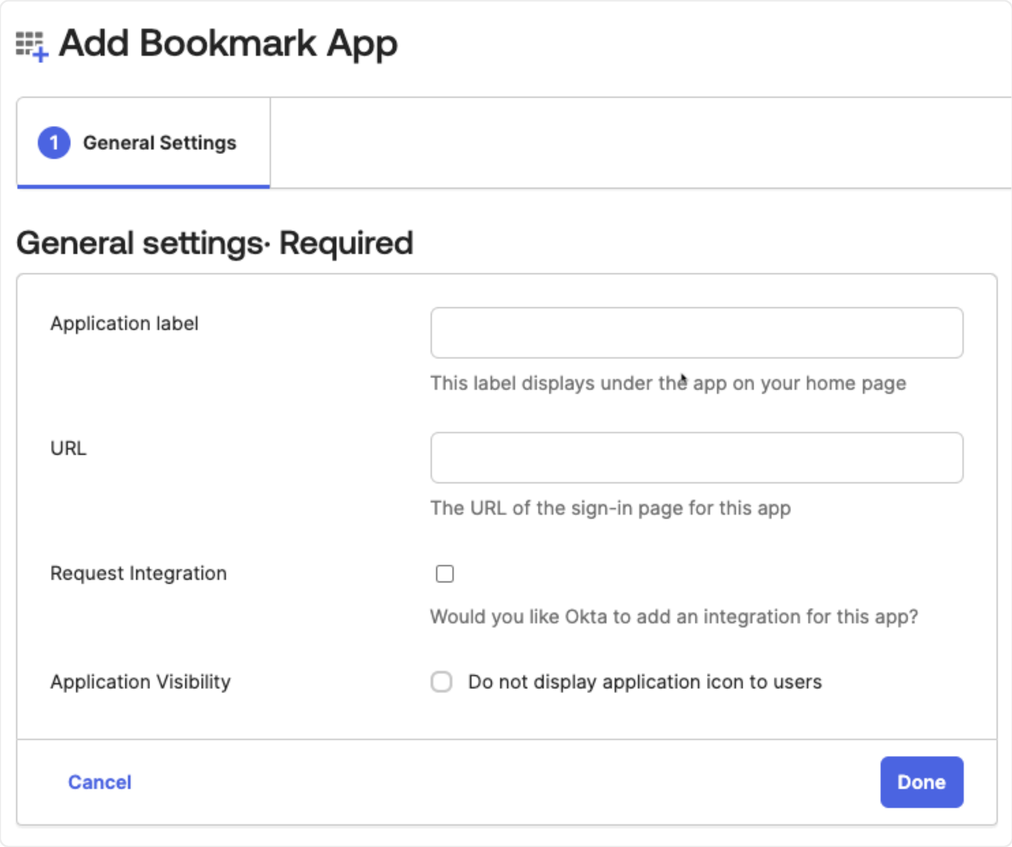
☐ DeepL Write Pro

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*.)



Add Bookmark App
1 General Settings
General settings· Required
Application label
This label displays under the app on your home page
URL
The URL of the sign-in page for this app
Request Integration
☐
Would you like Okta to add an integration for this app?
Application Visibility
○ Do not display application icon to users
Cancel
Done

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 administrator 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.

Help Center: https://support.deepl.com Web: https://www.deepl.com