



# Set up SSO for subscription management by group: SAML 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 group. 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 group.

 Subscription management by group 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: 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 group 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 [About subscription management by group](#).

## Set the SSO configuration in Okta

1. Go to your Okta instance and open the *Applications* section.
2. Click on *Create App* integration in the top panel
3. Select *SAML 2.0* and click *Next*.
4. Enter *DeepL SSO* under *Application label*.
5. Upload the DeepL icon.
6. Select *Do not display application icon to users* and *Save*.
7. Under *Sign-in redirect URIs* enter

```
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*.)

8. Under *Audience URI* enter

```
https://w.deepl.com/auth/realms/prod
```

## 9. Select a Name ID format

**A SAML Settings**

**General**

Single sign-on URL ⓘ   
 Use this for Recipient URL and Destination URL

Audience URI (SP Entity ID) ⓘ

Default RelayState ⓘ   
If no value is set, a blank RelayState is sent

Name ID format ⓘ

Application username ⓘ

Update application username on

[Show Advanced Settings](#)

## 10. Under *Attribute Statements* enter the following

**Attribute Statements (optional)** [LEARN MORE](#)

Name	Name format (optional)	Value
<input type="text" value="firstName"/>	<input type="text" value="Unspecified"/>	<input type="text" value="user.firstName"/>
<input type="text" value="lastName"/>	<input type="text" value="Unspecified"/>	<input type="text" value="user.lastName"/>
<input type="text" value="email"/>	<input type="text" value="Unspecified"/>	<input type="text" value="user.email"/>

[Add Another](#)

11. Under *Group Attribute Statements* enter the following

**Group Attribute Statements (optional)**

Name	Name format (optional)	Filter
groups	Unspecified ▼	Matches regex ▼ .*

[Add Another](#)

12. Click *Next*.

13. Confirm that you're using the as an internal app in the next step and click *Finish*.

Get the XML information for the connection

1. In your Okta instance and the application for DeepL access, go to the Sign On tab
2. Click on *View SAML setup instructions*.
3. Scroll down to the bottom and copy the XML text under *Optional* and save it as an xml file.

# How to Configure SAML 2.0 for DeepL SAML Application



Note: These setup instructions include certificate information for this app's **most recently created** SAML signing certificate. For users to get access to the app using these instructions, that certificate must be active.

## The following is needed to configure DeepL SAML

1. Identity Provider Single Sign-On URL:

```
https://dev-95939241.okta.com/app/dev-95939241_deepl_saml_1/exkornoth6VrHDiZA5d7/sso/saml
```

2. Identity Provider Issuer:

```
http://www.okta.com/exkornoth6VrHDiZA5d7
```

3. X.509 Certificate:

```
-----BEGIN CERTIFICATE-----
MIIDQCCApCgAwIBAgI1GAZbX+4tyNA0GCSqGSIb3DQEBCwUAMIGUMQswCQYDVQQGEwJVUzETMBEG
A1UECAwKQ2FsaWZvcnRpTTEwMBQGA1UEBwwNU2FueiEZYW5jaXNjbzENMAsGA1UECgwET2t0YTEU
MBIGA1UEDwLU1NPUHJvdmlkZXIxFATBgNVBAMPDGR1d105NTkzOTI0MTEcMB0GCSqGSIb3DQEJ
ARYNAw5mb0Bva3RnLnNvbTAeFw0yNTA1MTYwNzI0MDhaFw0zNTA1MTYwNzI1MDhaMIGUMQswCQYD
VQQGEwJVUzETMBEGA1UECAwKQ2FsaWZvcnRpTTEwMBQGA1UEBwwNU2FueiEZYW5jaXNjbzENMAsG
A1UECgwET2t0YTEUMBIGA1UECwLU1NPUHJvdmlkZXIxFATBgNVBAMPDGR1d105NTkzOTI0MTEc
MB0GCSqGSIb3DQEJARYNAw5mb0Bva3RnLnNvbTCCAS1wDQYJKoZIhvcNAQEBBQADggEPADCCAQoC
ggEBAJorEP861M4d13gbZ1p8KnXY16YM4D/FwtZ1wbWpLK+9dbgpT1TQM5BjwY7ynRUEBjrdH56T
59STerpl.azThpm5Uoo525We231QRcJMY5wL.v+QCCfRn9uLWvPLHG8BXfKFe+uSt0f+TiafHPYit
AQX9GgJgI0dt.rfq76Y2/CuP0sZD1yv1M8CZfcbk1VoqRP2/R173504GX+OV5ksk1v2.jEBs2Xfa10
k2cFmW4/r/8S0prju7KfX50/TzodJpnDhtLWkxodtGPy/jVhfnePMS006szw5511HxFqBX+7Bh
J478NRrGEB4Ca5DMr13az286DU+rWnaX9wsM1hXnK9msCawEAATANBgkqhkiG9w0BAQsFAAOCQAQEA
HUTdZTOD2zCU0hg1JD7NKSZtbbfswfghqz9EvdNnThurQ0kc1ZkAtsHex08r2B17c3e7fW1pFDn
wQLTY0jXHQ/4norUP70rCx0MBqB2Ls5kuaZBHTIk5nawKHufobG1GuWSz.J1s/rATZPdZ33C05z/
+9hYk/GLjht2rU8LX1vkebf9J4hkW9QdtadEgW9a7aHRNLLHg12w1EBVjTfcYRS06AQ0hHhPx1N
bfy73C3Yw3YMJgPt.2s21n1y0sSSn2tzf6f6tJV4uLf8EVnQ07Qb9y1gUc4T11g+xsUdXH01JnEwJ
0pc01H21QrQzGJcrNspfn/wyJcy01BCGFhNL+Q==
-----END CERTIFICATE-----
```

[Download certificate](#)

## Optional

1. Provide the following IDP metadata to your SP provider.

```
<?xml version="1.0" encoding="UTF-8"?><.md:EntityDescriptor entityID="http://www.okta.com/exkornoth6VrHDiZA5d7"
```

## Set the SSO configuration in DeepL accounts

1. Go to the [Settings tab](#) in your DeepL admin account.

Under *Team* and *Single sign-on* the SSO domain has the status *Domain name approved*.

The screenshot shows the 'Team' settings page in the DeepL admin interface. Under the 'Single sign-on (SSO)' section, there is a 'Set up SSO' button. Below this, the 'Company SSO domain' is listed as '.sso.deepl.com' and the 'Domain status' is 'Domain name approved'.

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

In the *Set up SSO* form select *SAML* as the *Authentication type*

3. Select *Import from file* and upload the xml file you've saved from your Okta SAML configuration

4. Enter the following

- *NameID policy format*: Select the policy format you've chosen in your Okta configuration of step 8 of [Set the SSO configuration in Okta](#).
- *Assertion attribute: First name* = *user.firstName*
- *Assertion attribute: Last name* = *user.lastName*
- *Assertion attribute: Email address* = *user.email*
- *Assertion attribute: User Groups* = *groups*

NameID policy format

Unspecified

Assertion attribute: First name ⓘ

user.firstName

Assertion attribute: Last name ⓘ

user.lastName

Assertion attribute: Email address ⓘ

user.email

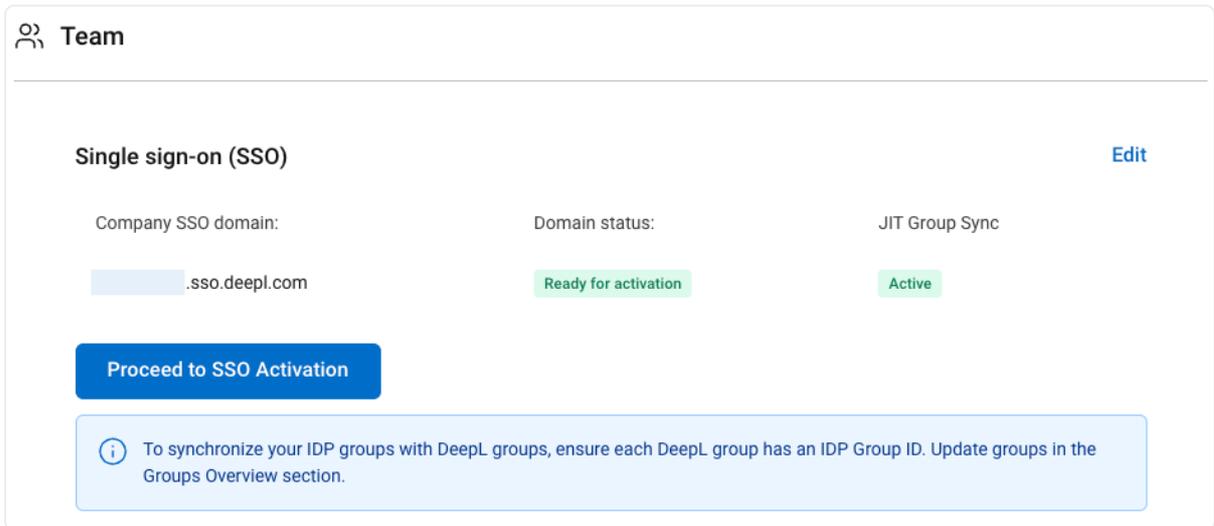
Assertion Attribute: User Groups ⓘ

groups

JIT Group Sync  
I want to provide group information during the login process

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

## 6. Activate SSO.



The screenshot shows the 'Team' settings page. At the top left is a 'Team' header with a group icon. Below it, the 'Single sign-on (SSO)' section is visible, with an 'Edit' link on the right. The configuration includes: 'Company SSO domain' set to a redacted domain followed by '.sso.deepl.com'; 'Domain status' shown as 'Ready for activation' in a green box; and 'JIT Group Sync' shown as 'Active' in a green box. A blue button labeled 'Proceed to SSO Activation' is positioned below the domain field. At the bottom, a light blue information box contains a warning icon and text: 'To synchronize your IDP groups with DeepL groups, ensure each DeepL group has an IDP Group ID. Update groups in the Groups Overview section.'

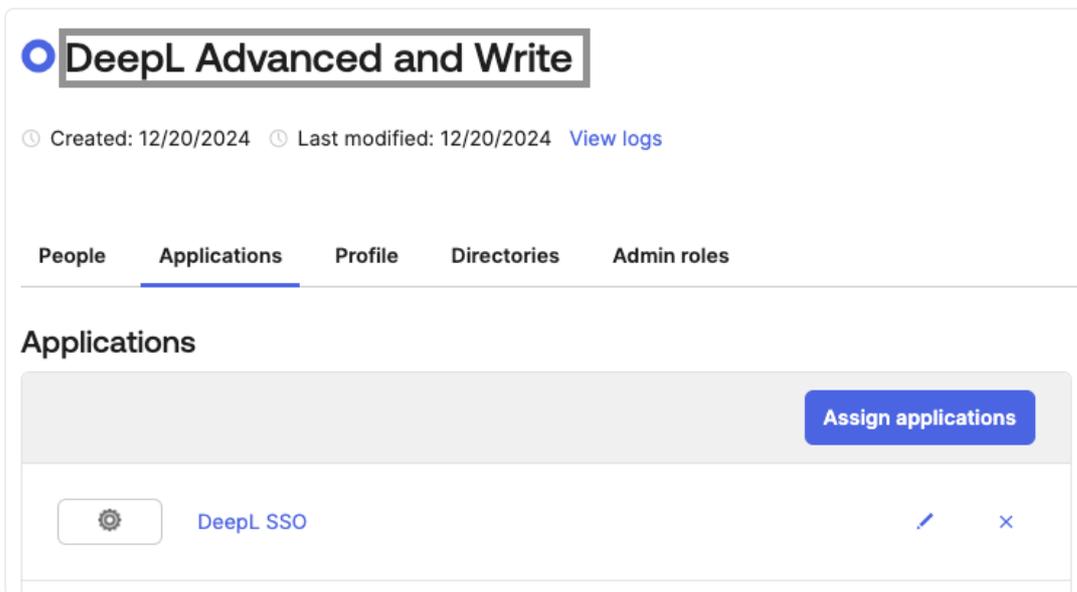
## Setup groups

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.

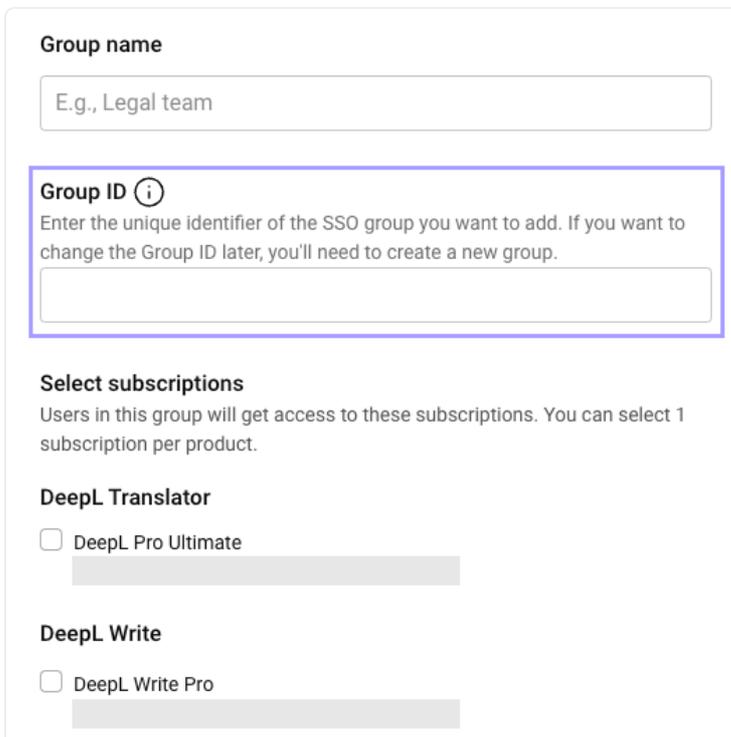
 JIT Provisioning Group Sync does not create groups based on the SAML assertion. If the assertion includes groups that do not exist in DeepL, that group information will be ignored, and the user is added only to the Default group. For more information about this default behavior, please see the *Default group* section in [this article](#).

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.

The image shows a screenshot of the 'Create group' form in the Okta Admin Console. The form is divided into several sections. The first section is 'Group name' with a text input field containing the placeholder 'E.g., Legal team'. The second section is 'Group ID', which is highlighted with a blue border. It includes an information icon (i) and a text input field. Below this is the 'Select subscriptions' section, which contains the text: 'Users in this group will get access to these subscriptions. You can select 1 subscription per product.' Underneath, there are two sections: 'DeepL Translator' with a checkbox for 'DeepL Pro Ultimate' and a greyed-out input field; and 'DeepL Write' with a checkbox for 'DeepL Write Pro' and a greyed-out input field.

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. 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.