



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*.

Home > Enterprise applications | All applications > [Application Name]

SAML-based Sign-on

Enterprise Application

Overview | Upload metadata file | Change single sign-on mode

Set up Single Sign-On with SAML

An SSO implementation based on federation protocols improves security, reliability, and end user experiences and is easier to implement. Choose SAML single sign-on whenever possible for existing applications that do not use OpenID Connect or OAuth. [Learn more](#).

Read the [configuration guide](#) for help integrating DeepL SAML demo PRD 1.

1 Basic SAML Configuration

Identifier (Entity ID)

Reply URL (Assertion Consumer Service URL)

Sign on URL *Optional*

Relay State (Optional) *Optional*

Logout Url (Optional) *Optional*

Edit

2 Attributes & Claims

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname

Edit

4. Click on *Add a group claim*.

... > | SAML-based Sign-on > SAML-based Sign-on >

Attributes & Claims

+ Add new claim + Add a group claim Columns | Got feedback?

Required claim

Claim name	Type	Value
Unique User Identifier (Name ID)	SAML	user.userprincipalna... ***

Additional claims

Claim name	Type	Value
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailadd...	SAML	user.mail ***
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	SAML	user.givenname ***
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	SAML	user.userprincipalname ***
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	SAML	user.surname ***

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.

Attributes & Claims

+ Add new claim + Add a group claim Columns | Got feedback?

Required claim

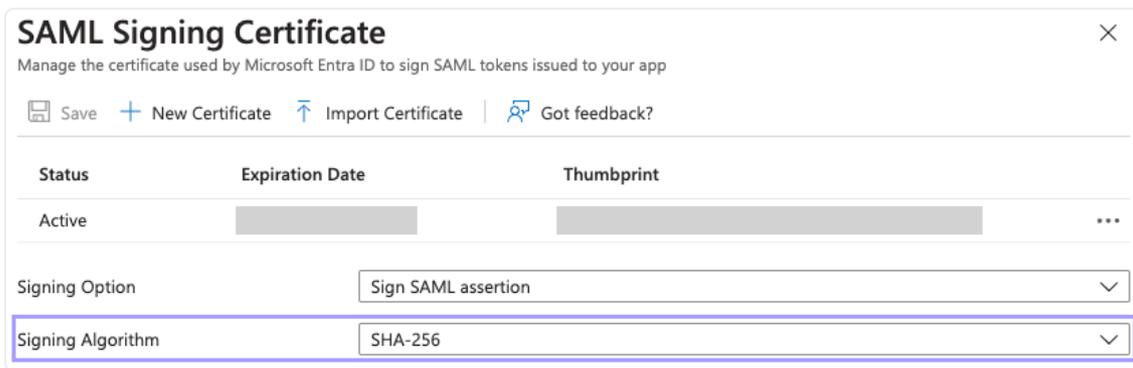
Claim name	Type	Value
Unique User Identifier (Name ID)	SAML	user.userprincipalname ... ***

Additional claims

Claim name	Type	Value
http://schemas.microsoft.com/ws/2008/06/identity/claims/groups	SAML	user.groups [All] ***
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailadd...	SAML	user.mail ***
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	SAML	user.givenname ***
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	SAML	user.userprincipalname ***
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	SAML	user.surname ***

Advanced settings

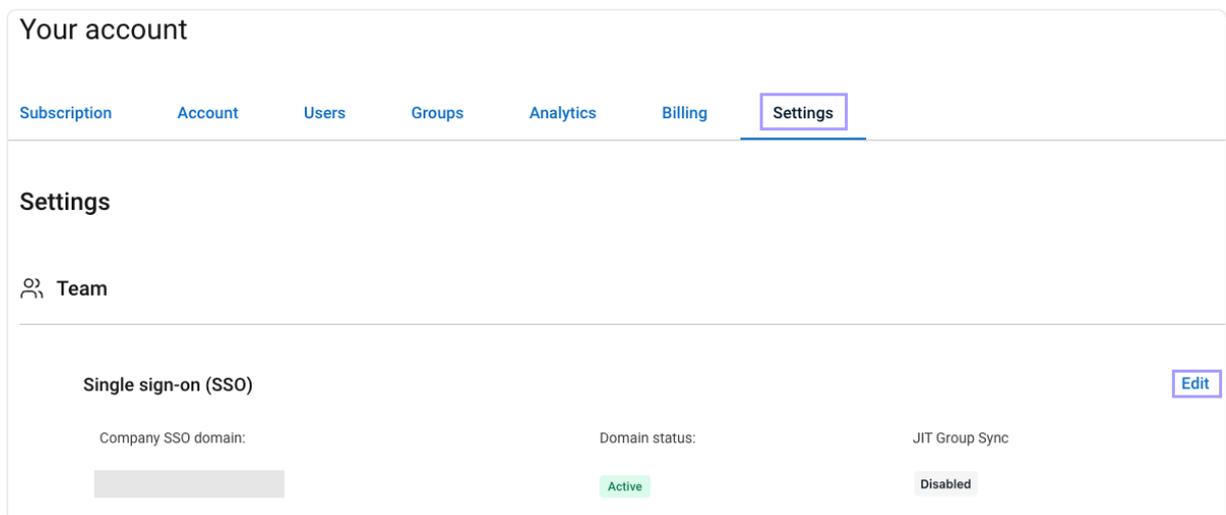
7. Click on *Edit* next to *SAML Certificates* to check if SHA-256 or SHA-512 is enabled.



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.

The screenshot shows the 'SAML Certificates' configuration page in the Azure AD portal. At the top, there are navigation links: 'Upload metadata file', 'Change single sign-on mode', 'Test this application', and 'Got feedback?'. Below these, there is a table with the following data:

name	user.userprincipalname
Unique User Identifier	user.userprincipalname
groups	user.groups

The main section is titled 'SAML Certificates' and contains two sections:

Token signing certificate (with an 'Edit' link):

Status	Active
Thumbprint	[Redacted]
Expiration	[Redacted]
Notification Email	[Redacted]
App Federation Metadata Url	<input type="text" value="https://login.microsoftonline.com/"/>
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

Verification certificates (optional) (with an 'Edit' link):

Required	No
Active	0
Expired	0

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.

Import from URL ⓘ

Import from file ⓘ

NameID policy format

Email ▾

Assertion attribute: First name ⓘ

Assertion attribute: Last name ⓘ

Assertion attribute: Email address ⓘ

Assertion Attribute: User Groups ⓘ

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

Cancel Confirm

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.

Enterprise Application

Users and groups

...

<<
+ Add user/group
✎ Edit assignment
🗑 Remove
🔑 Update credentials

ℹ The application will appear for assigned users within My Apps. Set 'visible to users?' to no...

Assign users and groups to app-roles for your application here. To create new app-roles t...

	Display Name		Object Type
<input type="checkbox"/>	TA	Translators and Writers SAML test	Group
<input type="checkbox"/>	TS	Translators SAML test	Group
<input type="checkbox"/>	WS	Writers SAML Test	Group

Overview

Deployment Plan

Diagnose and solve problems

Manage

Properties

Owners

Roles and administrators

Users and groups

Single sign-on

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.

Groups

Create group

Group name	Subscriptions	Users
<input type="text"/> Default group		1 Edit

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.

The screenshot shows the Microsoft 365 Admin Center interface for a group. On the left is a navigation pane with sections: Overview (selected), Diagnose and solve problems, Manage (Properties, Members, Owners, Roles and administrators, Administrative units, Group memberships, Applications, Licenses, Azure role assignments), and Activity. The main content area is titled 'Overview' and contains 'Basic information' for a group named 'WS'. The information includes: Membership type: Assigned; Source: Cloud; Type: Security; Object ID: [redacted] (highlighted with a blue box); and Created on: [redacted]. At the top right, there are 'Delete' and 'Got feedback?' options.

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 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.