Setup guide for DeepL Single Sign-On (SSO)

OpenID: Okta

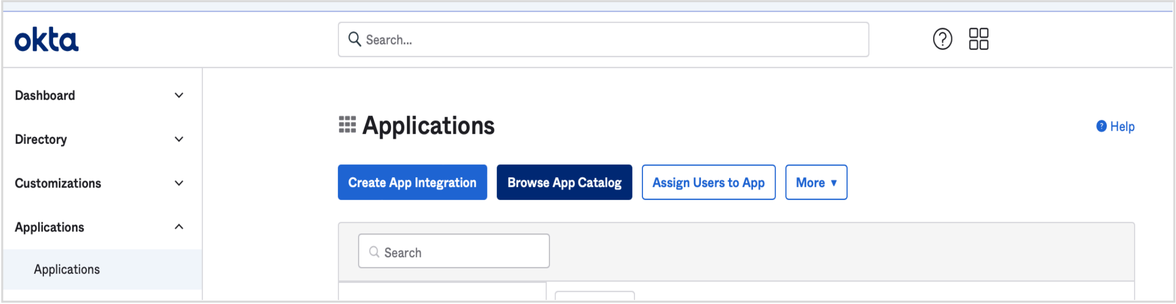
Table of contents (*if needed*)

Requirements

- A company domain has been defined for the DeepL environment. For further information please check our Help Center article.

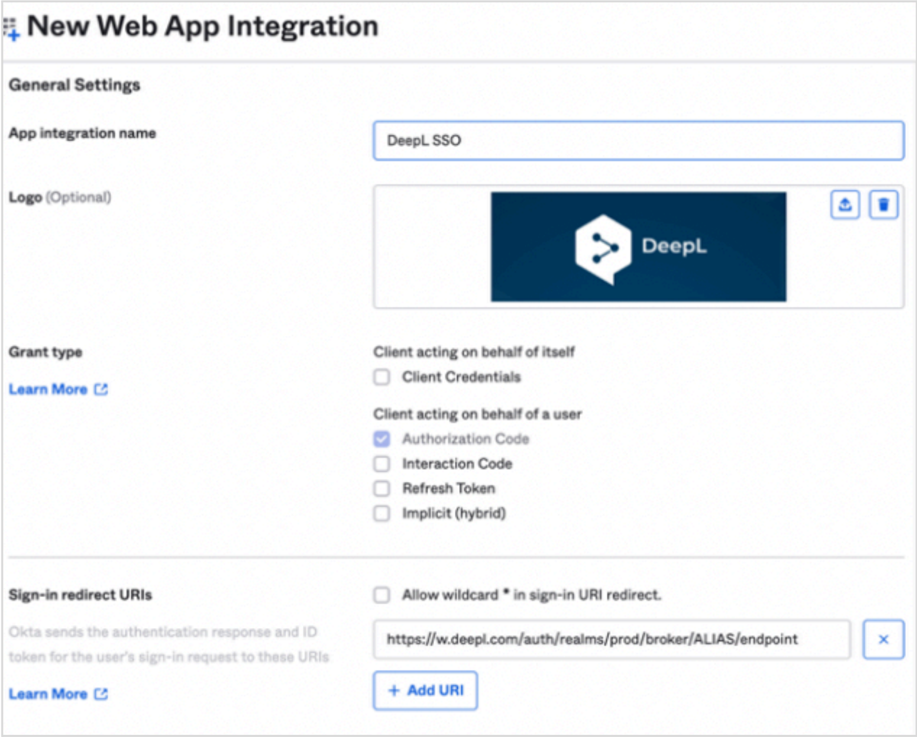
1) Create the SSO app

1. Open your Okta administration page and open the *Applications* section on the left-hand side
2. Click on *Create App Integration* and choose the sign-in method *OpenID Connect*



3. Choose *Web Application* as the application type.

4. Name the application DeepL or DeepL SSO and set the *sign-in redirect URL* to: https://w.deepl.com/auth/realms/prod/broker/ALIAS/endpoint. *(Replace ALIAS with your chosen company DOMAIN)*



New Web App Integration

General Settings

App integration name: DeepL SSO

Logo (Optional)

Grant type

Learn More

Client acting on behalf of itself

□ Client Credentials

Client acting on behalf of a user

☑ Authorization Code

□ Interaction Code

□ Refresh Token

□ Implicit (hybrid)

Sign-in redirect URIs

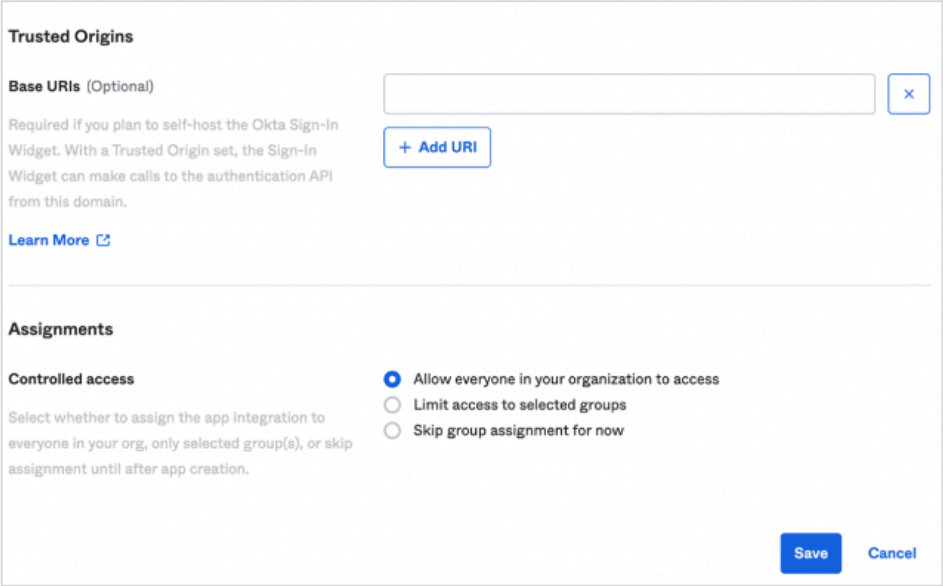
Okta sends the authentication response and ID token for the user's sign-in request to these URIs

Learn More

□ Allow wildcard * in sign-in URI redirect.

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

5. Set up controlled access here. If you want to create access groups later, choose *Skip assignment for now*, then click *Save*. The app has been created.



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.

Learn More

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.

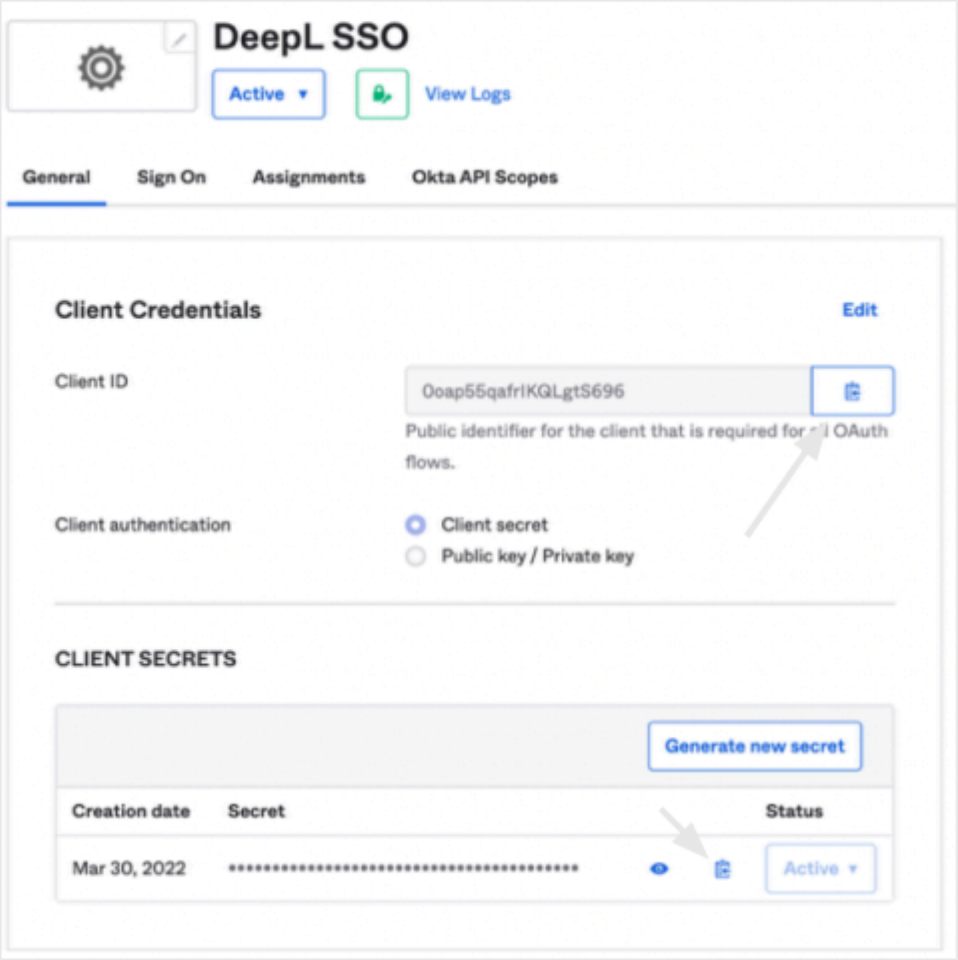
● Allow everyone in your organization to access

○ Limit access to selected groups

○ Skip group assignment for now

2) Get the client ID and secret value

1. You can copy the client ID and client secret within the app



DeepL SSO

Client Credentials Edit

Client ID: 0oap55qafrlKQLgtS696

Public identifier for the client that is required for all OAuth flows.

Client authentication: ● Client secret ○ Public key / Private key

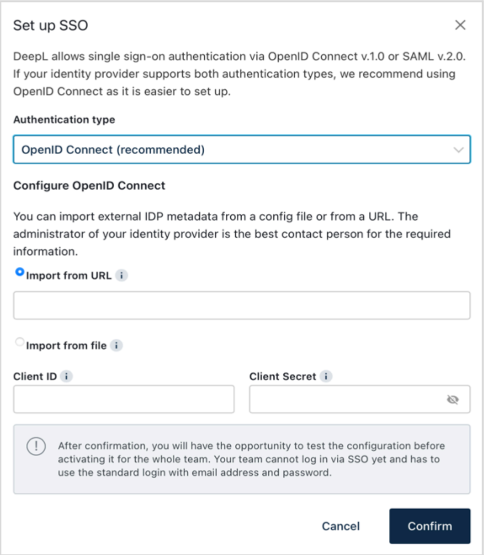
CLIENT SECRETS

Creation date	Secret	Status
Mar 30, 2022	••	Active ▾

2. You'll find the endpoint URLs for the Open ID connection here: https://YOUR_OKTA_DOMAIN.okta.com/.well-known/openid-configuration

3. Provide the following data in your DeepL Account settings:

- OpenID Connect metadata endpoints
- Application (Client) ID
- Client Secret



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

You can import external IDP metadata from a config file or from a URL. The administrator of your identity provider is the best contact person for the required information.

● Import from URL

○ Import from file

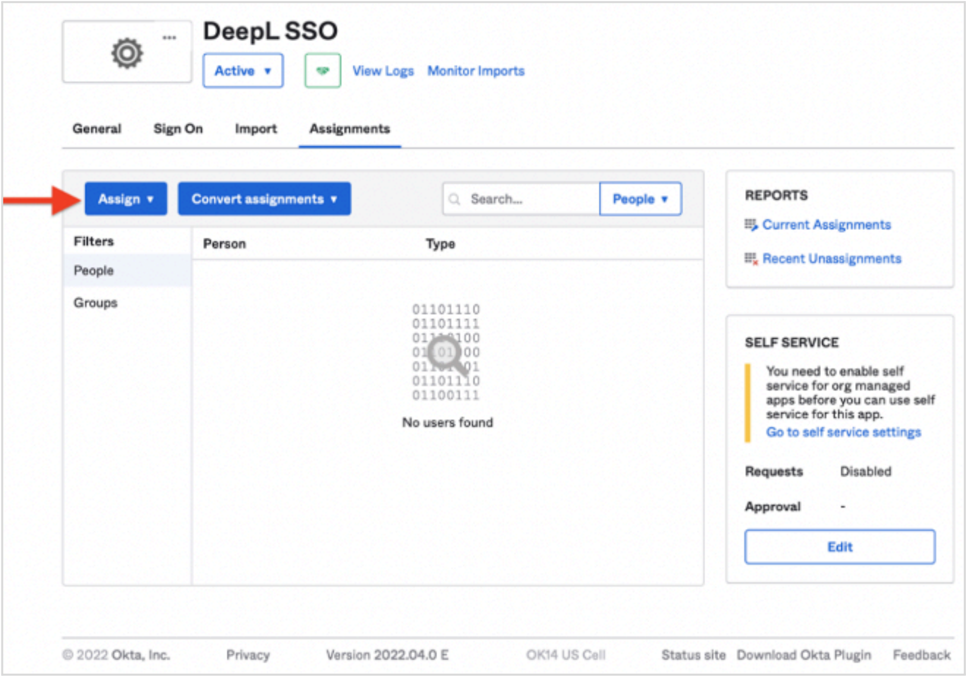
Client ID

Client Secret

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.

3) Enable DeepL Pro for your users

1. Once the SSO connection has been established, you should be able to assign users or user groups to your DeepL SSO group

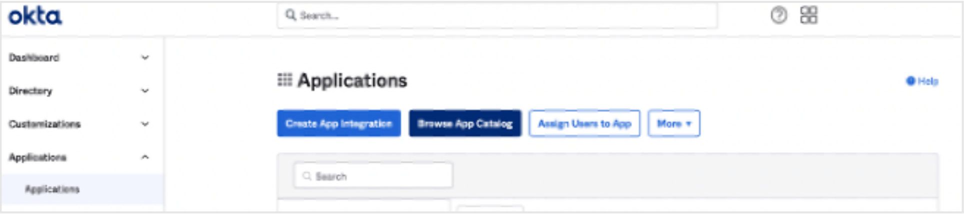


You need to enable self service for org managed apps before you can use self service for this app.

Requests Disabled

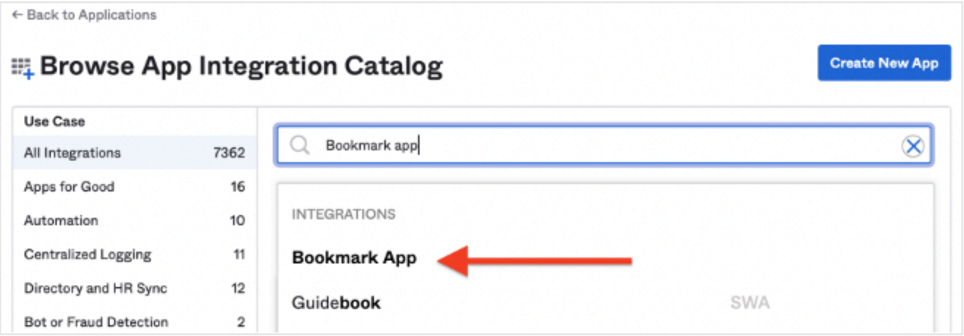
Approval -

2. Remember, we don't want to display the icon for the end users. Now we have to create a visible app link for them.



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

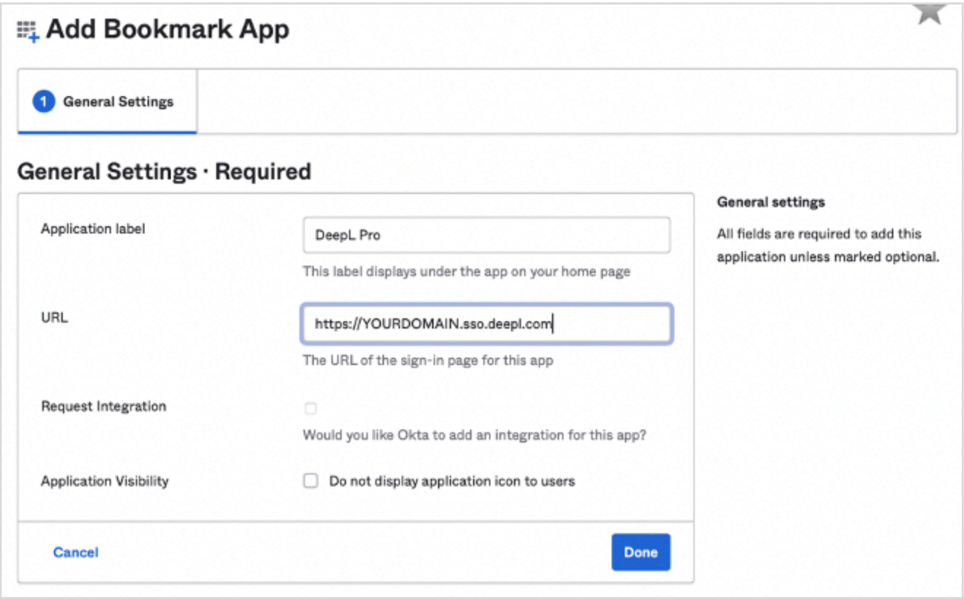
4. Search for *Bookmark App*, click on the first option, and add the app



Use Case	
All Integrations	7362
Apps for Good	16
Automation	10
Centralized Logging	11
Directory and HR Sync	12
Bot or Fraud Detection	2

Bookmark app

5. Name the bookmark app DeepL Pro, and enter the URL: https://YOURDOMAIN.sso.deepl.com. This will connect you to DeepL SSO.



Add Bookmark App

1 General Settings

General Settings · Required

Application label: DeepL Pro

This label displays under the app on your home page

URL: https://YOURDOMAIN.sso.deepl.com

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

General settings

All fields are required to add this application unless marked optional.

6. Click *Done*

You can now add the DeepL icon to the bookmark app. Don't forget to assign the same users or user groups to the bookmark app as you have to the DeepL SSO app.