
Setup guide for DeepL Single Sign-On (SSO)

SAML: Okta

Table of contents

[Requirements](#)

[1\) Create the DeepL SSO app](#)

[2\) Extract the XML information setting the connection](#)

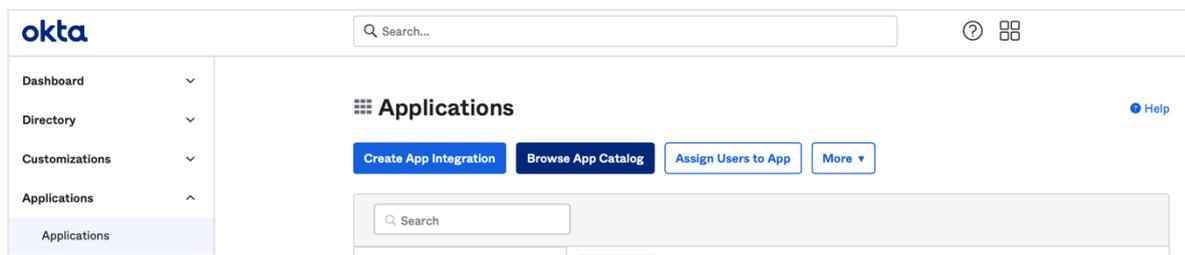
[3\) Enable DeepL Pro for your users](#)

Requirements

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

1) Create the DeepL 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 protocol: SAML 2.0
3. Name the application DeepL or DeepL SSO, check the box for *Do not display application icon to users*, and click *Next*

Create SAML Integration

1 General Settings 2 Configure SAML 3 Feedback

1 General Settings

App name: DeepL SSO

App logo (optional):

App visibility: Do not display application icon to users

[Cancel](#) [Next](#)

4. Enter the Single Sign On URL: <https://w.deepl.com/auth/realms/prod/broker/ALIAS/endpoint>
(replace ALIAS with your chosen company DOMAIN)

Enter the Audience URL: <https://w.deepl.com/auth/realms/prod>

A SAML Settings

General

Single sign on URL [?]:
 Use this for Recipient URL and Destination URL
 Allow this app to request other SSO URLs

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](#)

5. Add the Attribute Statements *firstName*, *lastName*, and *email*

Name	Name format (optional)	Value
firstName	Unspecified	user.firstName
lastName	Unspecified	user.lastName
email	Unspecified	user.email

[Add Another](#)

[LEARN MORE](#)

6. Click on *Next*, check the box to confirm that you're using the app as an internal app, and then click *Finish*

Create SAML Integration

1 General Settings 2 Configure SAML 3 Feedback

3 Help Okta Support understand how you configured this application

⚠ We found some errors. Please review the form and make corrections.

Are you a customer or partner?

I'm an Okta customer adding an internal app

I'm a software vendor. I'd like to integrate my app with Okta

i The optional questions below assist Okta Support in understanding your app integration.

App type This is an internal app that we have created

[Previous](#) [Finish](#)

Why are you asking me this?

This form provides Okta Support with useful background information about your app. Thank you for your help—we appreciate it.

2) Extract the XML information setting the connection

1. Open the app and click on the tab *Sign On*. Then click on *View Setup Instructions*.

General **Sign On** Import Assignments

Settings [Edit](#)

Sign on methods

The sign-on method determines how a user signs into and manages their credentials for an application. Some sign-on methods require additional configuration in the 3rd party application.

Application username is determined by the user profile mapping. [Configure profile mapping](#)

SAML 2.0

Default Relay State

SAML 2.0 is not configured until you complete the setup instructions.

[View Setup Instructions](#)

[Identity Provider metadata](#) is available if this application supports dynamic configuration.

Credentials Details

Application username format Okta username

Update application username on Create and update [Update Now](#)

About

SAML 2.0 streamlines the end user experience by not requiring the user to know their credentials. Users cannot edit their credentials when SAML 2.0 is configured for this application. Additional configuration in the 3rd party application may be required to complete the integration with Okta.

Application Username

Choose a format to use as the default username value when assigning the application to users.

If you select **None** you will be prompted to enter the username manually when assigning an application with password or profile push provisioning features.

2. Scroll all the way down, copy the XML text from the IDP metadata, and save it as an XML file

2 Identity Provider Issuer:

3 X.509 Certificate:

-----BEGIN CERTIFICATE-----

-----END CERTIFICATE-----

[Download certificate](#)

Optional

1 Provide the following IDP metadata to your SP provider.

3. Provide the following data under set up SSO in your [DeepL Account settings](#):

- Choose SAML as Authentication type
- Add the previously saved XML file
- Choose the NameID (which you chose in Okta, see Step 1.4)
- Add the attributes as defined in point 5 in Step 1

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

SAML ▼

Configure SAML

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 i

Import from file i

NameID policy format

Email ▼

Assertion attribute: First name i

Assertion attribute: Last name i

Assertion attribute: Email address i

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

← Back to Applications

DeepL SSO

Active ▼ View Logs Monitor Imports

General Sign On Import **Assignments**

Assign ▼
Convert assignments ▼

People ▼

Filters	Person	Type
<ul style="list-style-type: none"> People Groups 		<div style="text-align: center;"> </div> <p>01101110 01101111 01101100 01101100 01101101 01101110 01100111</p> <p style="text-align: center;">No users found</p>

REPORTS

- [Current Assignments](#)
- [Recent Unassignments](#)

SELF SERVICE

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

[Go to self service settings](#)

Requests Disabled

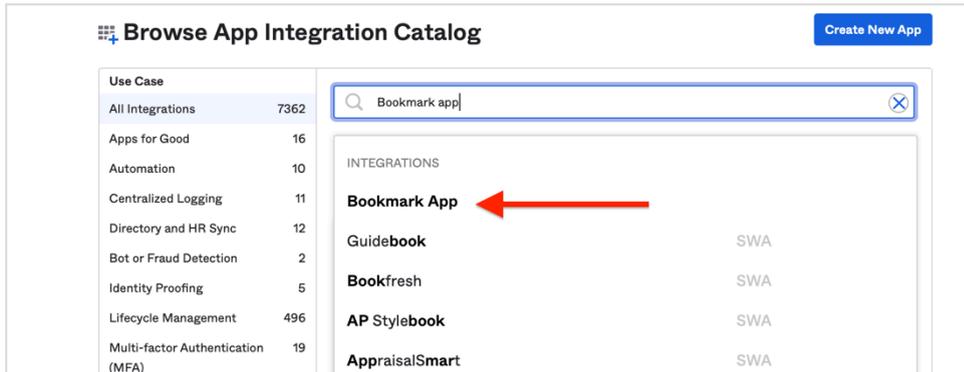
Approval -

Edit

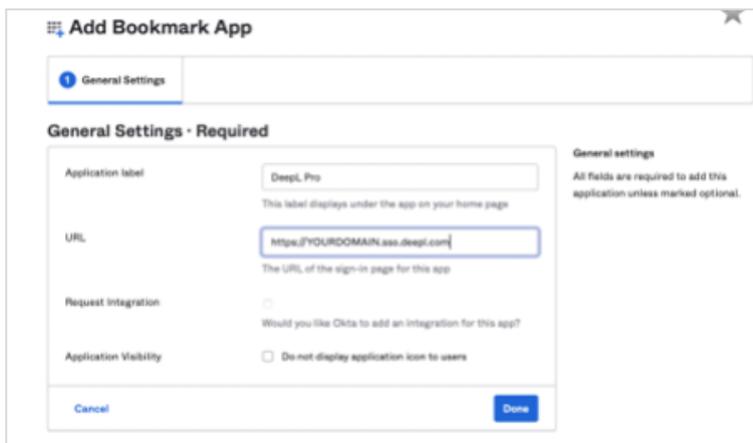
© 2022 Okta, Inc. [Privacy](#) [Version 2022.04.0 E](#) [OK!4 US Cell](#) [Status site](#) [Download Okta Plugin](#) [Feedback](#)

To not display the icon for the end users we must create a visible app link for them.

2. Open the *Applications* section and click on *Browse App Catalog*
3. Search for *Bookmark App*, and then click on the first option to add the app



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