

envi



Okta Single Sign-On

Integration Guide



Table of Contents

Introduction.....	2
Integration	3
Envi Configuration	7

Introduction

Okta is a **single sign-on (SSO)** provider that simplifies the management of application sign-ins and permissions. With **Okta SSO** integration, you can effectively control access to your **Envi** application using a secure and scalable identity management system.

Okta provider prevents common vulnerabilities in the authentication experience, including username and password sign-ins or password reset requests.

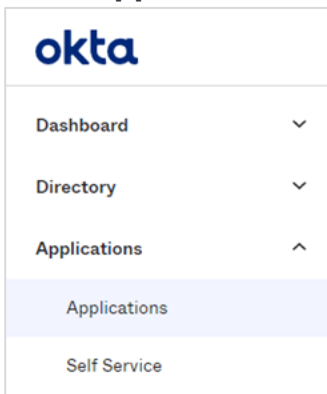
You don't need to manually renew or worry about weak sign-in credentials that cause security issues, enforce session timeouts, and require users to sign in again after these timeouts.

This step-by-step guide explains how to configure **SSO** to your **Envi** account with **Okta** provider.

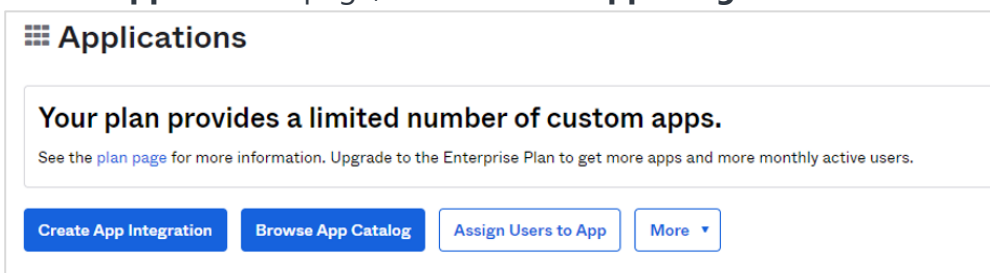
Integration

Follow the steps to get your **Okta** account linked to your **Envi** account.

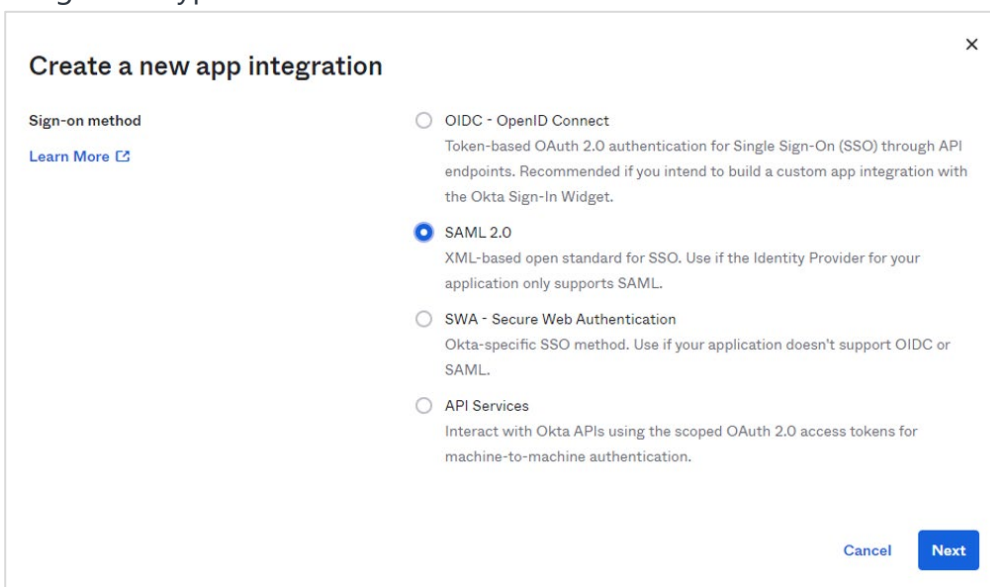
1. Sign in to the [Okta](#) site.
2. In the **Applications** dropdown list, select **Applications**.



3. On the **Applications** page, select **Create App Integration**.



4. In the **Create a new app integration** pop-up window, select the **SAML 2.0** integration type and then select **Next**.



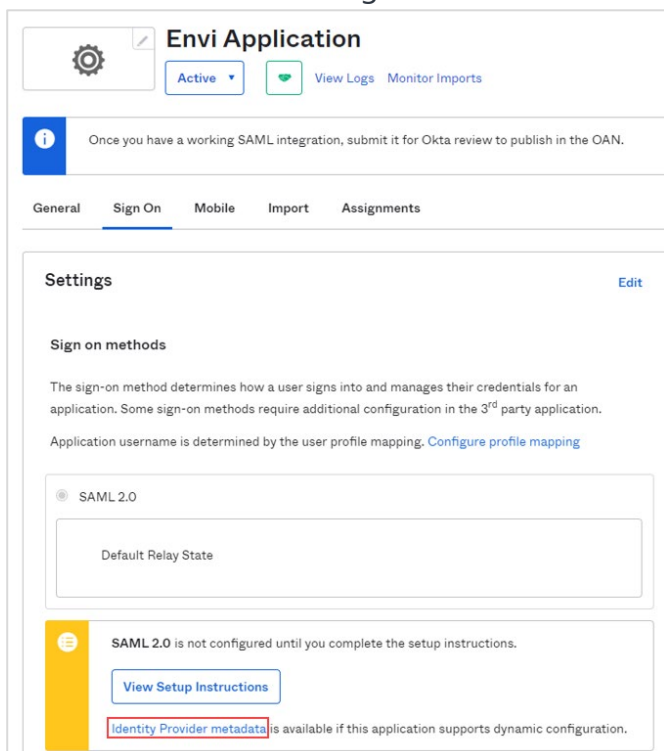
5. In the **General Settings** section, do the following steps:

- a. Enter **App name**.
- b. Upload **App logo** if needed.
- c. Select **Next**.

6. In the next **Configure SAML** section, do the following steps:

- a. In the **Single sign-on URL** box, enter an application base URL + /Account/Acs.
- b. In the **Audience URI (SP Entity ID)** box, enter an application base URL + /Account.
- c. In the **Name ID format** dropdown list, select **EmailAddress**.
- d. In the **Application username** dropdown list, select **Email**.
- e. Select **Next** and then **Finish**.

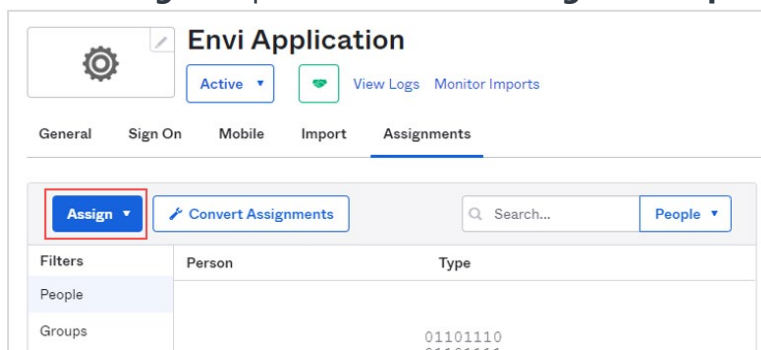
7. Then, you will be redirected to the **Sign On** tab with your application details. At the bottom of the tab, copy the **Identity Provider metadata** link URL, which you will use for the **Envi** configuration later.



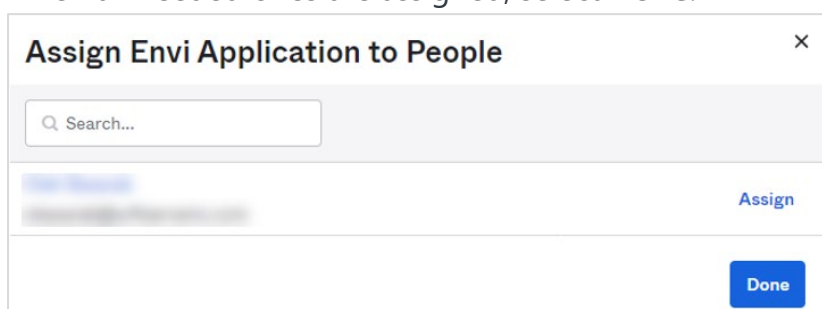
8. To assign application users or user groups that should be able to sign in with **SSO**, go to the **Assignments** tab.

- a. To grant access to the application for existing **users**, do the following steps:

- I. In the **Assign** dropdown list, select **Assign to People**.



- II. In the search box, enter the names of users you want to add.
- III. Select the **Assign** link next to a needed user.
- IV. When all needed ones are assigned, select **Done**.



- b. To grant access to the application for existing **user groups**, do the following steps:
- I. In the **Assign** dropdown list, select **Assign to Groups**.
 - II. In the search box, enter the names of user groups you want to add.
 - III. Select the **Assign** link next to a needed group.
 - IV. When all needed ones are assigned, select **Done**.

Assign Envi Application to Groups ×

Q Search...

Everyone
All users in your organization [Assign](#)

Done

Now, the **SSO** configuration is ready for use.

Envi Configuration

In the **Envi** application, set up the following domain and user configurations:

1. Sign in to the **Envi** application.
2. Go to **My Profile > Domain List**.
3. Select a needed domain and select **Edit**.
4. In the **Authentication** dropdown list, make sure that **HTTP Redirect** is selected, and then select **Upload Metadata**.

Domains > Domain Name Domain_Name Default Change

DETAILS ORGANIZATIONS USERS PASSWORD DICTIONARIES RESOURCES SECURITY

Update Cancel

Name*: Domain_Name

Description: Description

Session Timeout, m: 20

Mobile Token Expiration, h:

Default UI: Default [Update Users](#)

Status: Active

Authentication: HTTP Redirect **Upload Metadata**

Failed Attempts*: 255 ⓘ

Endpoint URL:

Identifier URL:

SSO Message*: Please provide your SSO credentials for further ⓘ

Require force authentication.
 Require device registration.
 Restrict IP Addresses.

5. In the **Upload Metadata** pop-up window, perform the following steps:
 - a. In the **Upload From** dropdown list, select **URL**.
 - b. In the **Select File** box, enter the URL of the **Identity Provider metadata** link (For more information, go to the [Integration](#) section, step 7).
 - c. Select **OK**.

Upload Metadata ✕

Upload From: URL

Identifier URL*: [http://login.microsoftonline.com/895cf5e-95fc-493c...](#)

OK Cancel

Note: Make sure that the **Endpoint URL** and **Identifier URL** are updated with new values and that the **Certificates** section contains new certificates.

Domains > Domain Name Domain_Name

DETAILS ORGANIZATIONS USERS PASSWORD DICTIONARIES RESOURCES SECURITY

Edit

Name: Domain_Name

Description: Description

Session Timeout, m: 20

Mobile Token Expiration, h:

Default UI: Default [Update Users](#)

Status: Active

Authentication: HTTP Redirect

Failed Attempts: 255

Endpoint URL: [http://login.microsoftonline.com/895cf5e-95fc-493c...](#)

Identifier URL: [http://app.onelogin.com/saml/...](#)

SSO Message: Please provide your SSO credentials for further logins

Do not require force authentication.
 Do not require device registration.
 Do not restrict IP Addresses

Note: While creating a user, perform the following steps:

- a. Select the needed domain with **HTTP Redirect** type of authentication.
- b. In the **SSO User Name** field, enter the username from the **Okta** application.

Users > User Name UserName@xx.com

DETAILS OPTIONS ORGANIZATIONS SECURITY

[Edit](#) [Validate Email](#)

User Name:	UserName@xx.com	User Type:	User
First Name:	FirstName	Domain:	Domain_Name
Last Name:	LastName	Default Organization:	UVZ
Title:	Title	Role:	None
Email Address:	Email@xx.com	Org User Type:	Interface
Phone:	Phone	Report Format:	PDF
Phone Ext.:	Phone Ext.	Email Format:	Plain Text
Fax:	Fax	SSO User Name:	SSO User Name
Time Zone:	(UTC+13:00) Samoa		
Default UI:	Envi HTML v.2		
Status:	Active		

Now, you can sign in to the **Envi** application using **Okta SSO**.