



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.

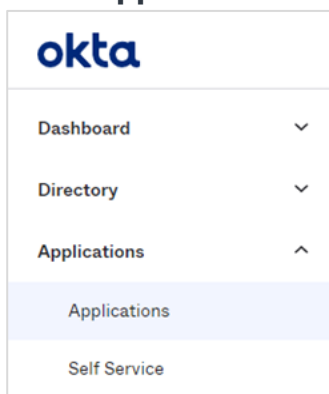
You don't need to manually renew or worry about weak sign-in credentials that cause security issues, enforce session timeouts, and require users to sign in again after these timeouts.

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

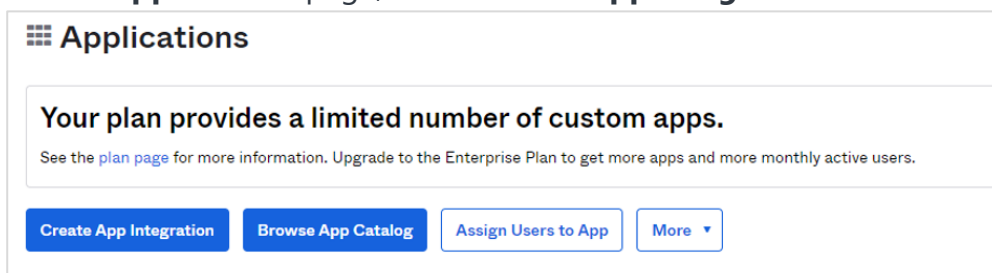
Integration

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

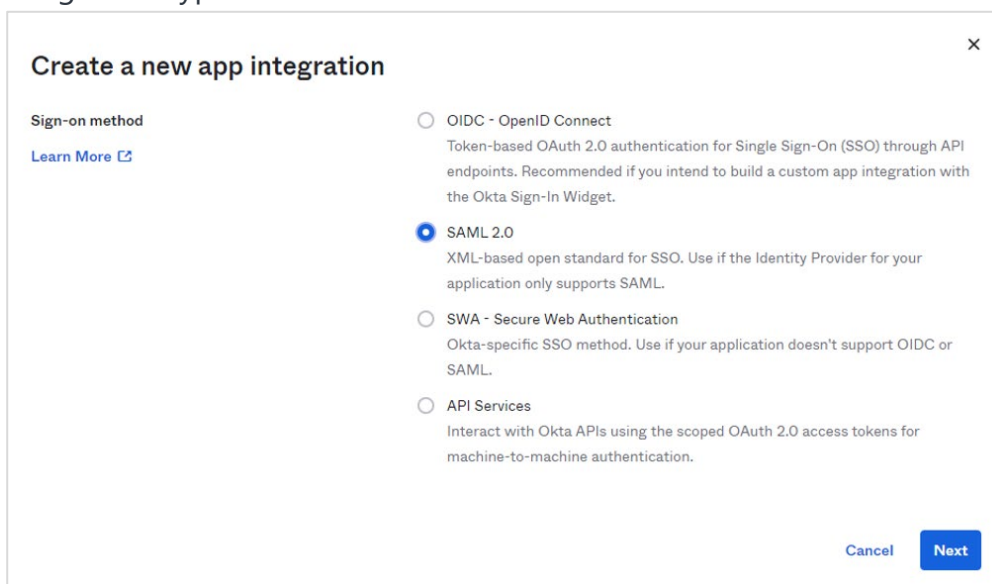
1. Sign in to the [Okta](#) site.
2. In the **Applications** dropdown list, select **Applications**.



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:

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

Create SAML Integration

1 General Settings 2 Configure SAML

1 General Settings

App name: Envi Application

App logo (optional):

App visibility: ☐ Do not display application icon to users
☐ Do not display application icon in the Okta Mobile app

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

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

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

Create SAML Integration

1 General Settings 2 Configure SAML

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:

[Show Advanced Settings](#)

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.

Envi Application

Active View Logs Monitor Imports

Once you have a working SAML integration, submit it for Okta review to publish in the OAN.

General Sign On Mobile 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.

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**.

Envi Application

Active View Logs Monitor Imports

General Sign On Mobile Import Assignments

Assign Convert Assignments Search... People

Filters	Person	Type
People		
Groups		01101110 01101111

- 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**.

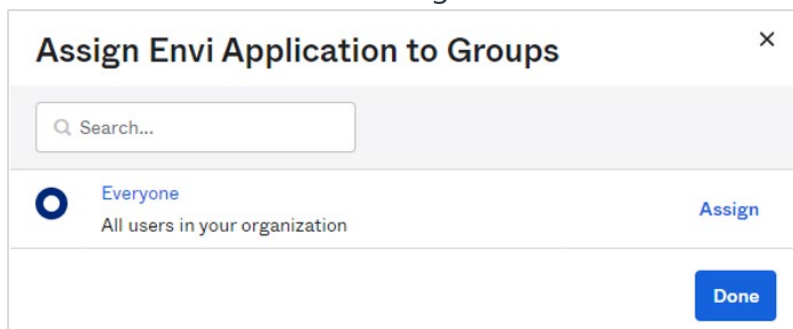
Assign Envi Application to People X

Search...

Assign

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**.



The screenshot shows a dialog box titled "Assign Envi Application to Groups" with a close button (X) in the top right corner. Below the title bar is a search bar with a magnifying glass icon and the placeholder text "Search...". Below the search bar is a list of user groups. The first group is "Everyone" with a blue radio button icon to its left. Below the group name is the description "All users in your organization". To the right of the group name is a blue "Assign" link. At the bottom right of the dialog box is a blue "Done" button.

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**, then select a needed domain and select **Edit**.
3. In the **Authentication** dropdown list, make sure that **HTTP Redirect** is selected, and then select **Upload Metadata**.

Domains > Domain Name Domain_Name

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 logins

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

4. 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:

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/f895cf5e-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

5. To create a new user, do the following steps:
 - a. In the **Authentication** dropdown list, select **HTTP Redirect**.
 - b. In the **SSO User Name** box, 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	Session Timeout:	201
Phone Ext.:	Phone Ext.	Report Format:	PDF
Fax:	Fax	Email Format:	Plain Text
Time Zone:	(UTC+13:00) Samoa	SSO User Name:	SSO User Name
Default UI:	Envi HTML v.2		
Status:	Active		

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