



Okta Single Sign-On

Integration Guide



Table of Contents

ntroduction	2
ntegration	3
	_
nvi 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.

okta	
Dashboard	~
Directory	~
Applications	^
Applications	
Self Service	

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

Applications
Your plan provides a limited number of custom apps. See the plan page for more information. Upgrade to the Enterprise Plan to get more apps and more monthly active users.
Create App Integration Browse App Catalog Assign Users to App More 🔻

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**.

Create SAML Integ	gration
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 Mabile app
Cancel	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**.

General Settings	2	Configure SAML
A SAML Settings		
General		
Single sign on URL 🔞	https://localhost/Acco	ount/Acs
	Use this for Recipie	nt URL and Destination URL quest other SSO URLs
Audience URI (SP Entity ID) 🔞	https://localhost/Acco	bunt
Default RelayState 🛛 🛛		
	lf no value is set, a blank	RelayState is sent
Name ID format 🗿	EmailAddress	•

 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.

0	Once you have a working SAML integration, submit it for Okta review to publish in the OAN.
General	Sign On Mobile Import Assignments
Settin	gs E
Sign o	n methods
The sig	n-on method determines how a user signs into and manages their credentials for an
The sig applica	n-on method determines how a user signs into and manages their credentials for an tion. Some sign-on methods require additional configuration in the 3 rd party application.
The sig applica Applica	n-on method determines how a user signs into and manages their credentials for an tion. Some sign-on methods require additional configuration in the 3 rd party application. tion username is determined by the user profile mapping. Configure profile mapping
The sig applica Applica	n-on method determines how a user signs into and manages their credentials for an iion. Some sign-on methods require additional configuration in the 3 rd party application. tion username is determined by the user profile mapping. Configure profile mapping ML 2.0
The sig applica Applica	n-on method determines how a user signs into and manages their credentials for an ition. Some sign-on methods require additional configuration in the 3 rd party application. Ition username is determined by the user profile mapping. Configure profile mapping ML 2.0 Default Relay State
The sig applica Applica	n-on method determines how a user signs into and manages their credentials for an ion. Some sign-on methods require additional configuration in the 3 rd party application. tion username is determined by the user profile mapping. Configure profile mapping ML 2.0 Default Relay State
The sig applica Applica	n-on method determines how a user signs into and manages their credentials for an i:on. Some sign-on methods require additional configuration in the 3 rd party application. tion username is determined by the user profile mapping. Configure profile mapping ML 2.0 Default Relay State SAML 2.0 is not configured until you complete the setup instructions.
The sig applica Applica	n-on method determines how a user signs into and manages their credentials for an sion. Some sign-on methods require additional configuration in the 3 rd party application. tion username is determined by the user profile mapping. Configure profile mapping ML 2.0 Default Relay State SAML 2.0 is not configured until you complete the setup instructions.
The sig applica Applica	n-on method determines how a user signs into and manages their credentials for an tion. Some sign-on methods require additional configuration in the 3 rd party application. tion username is determined by the user profile mapping. Configure profile mapping ML 2.0 Default Relay State SAML 2.0 is not configured until you complete the setup instructions. View Setup Instructions

- 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**.

Ø	Active Vi	ion ew Logs Monitor Imports	
General	Sign On Mobile Import	Assignments	
Assign 🔻	Convert Assignments	Q Search	People •
Filters	Person	Туре	
People			
Groups		01101110	

- 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 Peo	ple ×
Q 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**.

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_Nam e				Default Chan
DETAILS ORGANIZATI	ONS USERS PASSWORD DICTIO	NARIES RESOURCES	SECURITY		
Update Cancel					
Name:*	Domain_Name	Authentication	HTTP Redirect	Upload Metadata	
Description:	Description	Failed Attempt	s:* 255		(i)
Session Timeout, m:	20	Endpoint URL:			
Mobile Token Expiration, h:		Identifier URL:			
Default UI:	Default v Update Users	SSO Message.	Please provide your	r SSO credentials for further	(i)
Status:	Active	▼ Require fo	prce authentication.		
		Require de Restrict IP	evice registration. 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 <u>Integration</u> section, step 7).
 - c. Select OK.

Upload Metada	ita		×
Upload From:	URL		•
Identifier URL*			
		ОК	Cancel

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

∕ Edit				
Name:	Domain_Name		Authentication:	HTTP Redirect
Description:	Description		Failed Attempts:	255
Session Timeout, m:	20		Endpoint URL:	http://login.microsoftonline.com/f895cf5e-95fc-493c
Mobile Token Expiration,	h:		Identifier URL:	http://app.onelogin.com/saml/
Default UI:	Default	Update Users	SSO Message:	Please provide your SSO credentials for further logins
Status:	Active		Do not require fo	prce authentication.
			Do not require de	evice 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.

DETAILS OPTIC	INS ORGANIZATIONS SECURITY		
✓ Edit Vali	date Email		
User Name:	UserName@xx.com	User Type:	User
First Name:	FirstName	Domain:	Domain_Name
Last Name:	LastName	Default Organization:	UVZ
litle:	Title	Role:	None
Email Address:	Email@xx.com	Org User Type:	Interface
Phone:	Phone		
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	N	
Status:	Active		

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