



Okta Single Sign-On

Configuration Guide



Table of Contents

Introduction.....	3
Integration.....	4
Envi Configuration.....	10

Introduction

The Okta sign-on provider makes it easy to manage application logins and permissions. The SSO integration allows you to effectively manage access to Envi using a secure and scalable identity management system.

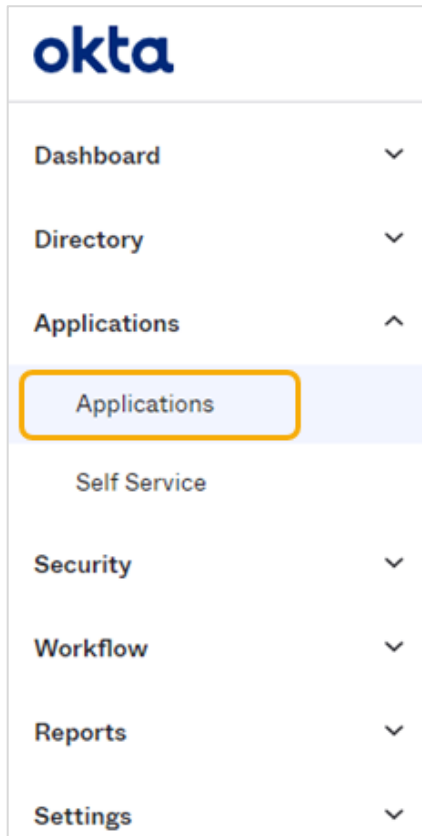
The Okta SSO provider prevents common weak points in the authentication experience, including username and password login or password reset requests. You do not need to manually renew or worry about weak login credentials that cause security issues and enforce session timeouts and require users to sign in again after these time-outs. It also provides a familiar login experience across your applications.

Note: This step-by-step guide explains how to set up single sign-on to your Envi account with the Okta SSO provider.

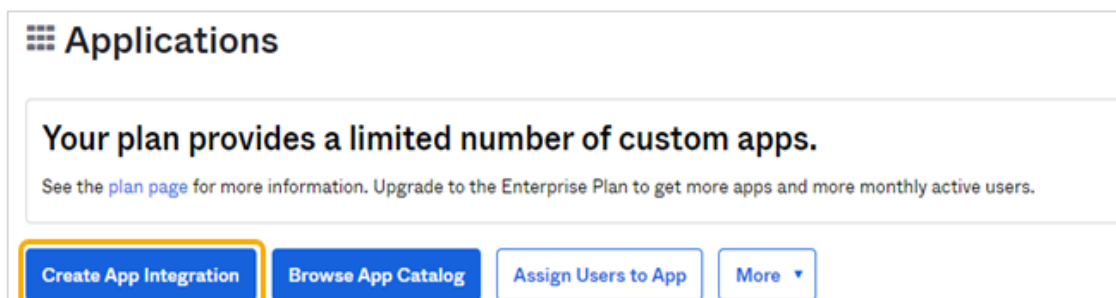
Integration

Perform the following steps to get your Okta account tied to your Envi account.

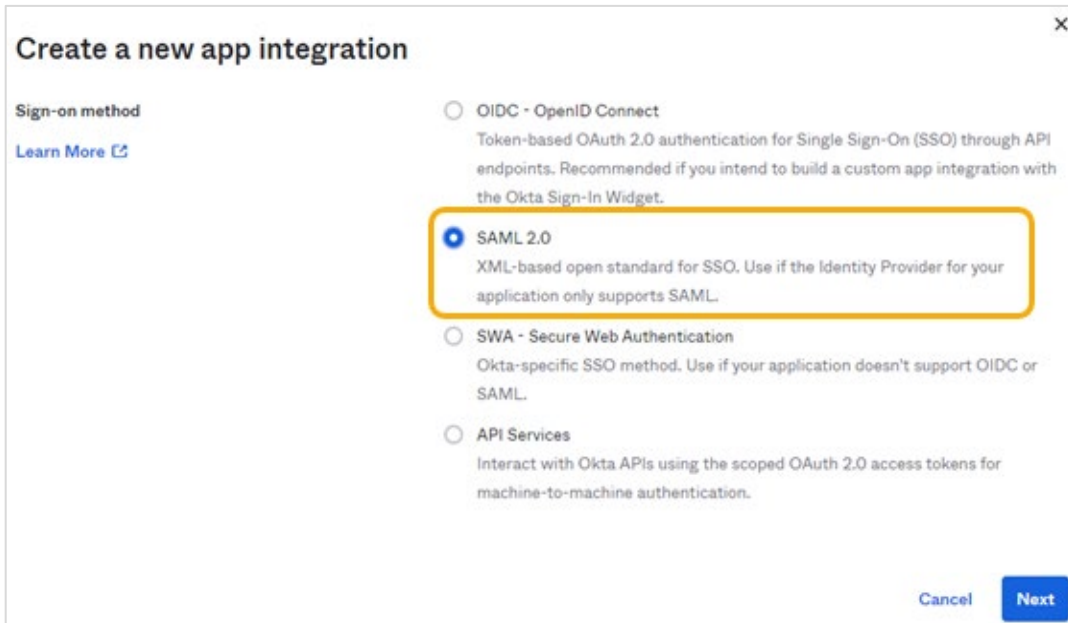
1. Sign in to the [Okta](#) site.
2. Select **Applications** > **Applications** from the site menu.



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



4. In the **Create a new app integration** pop-up select **SAML 2.0** as a desired integration type and click **Next**.



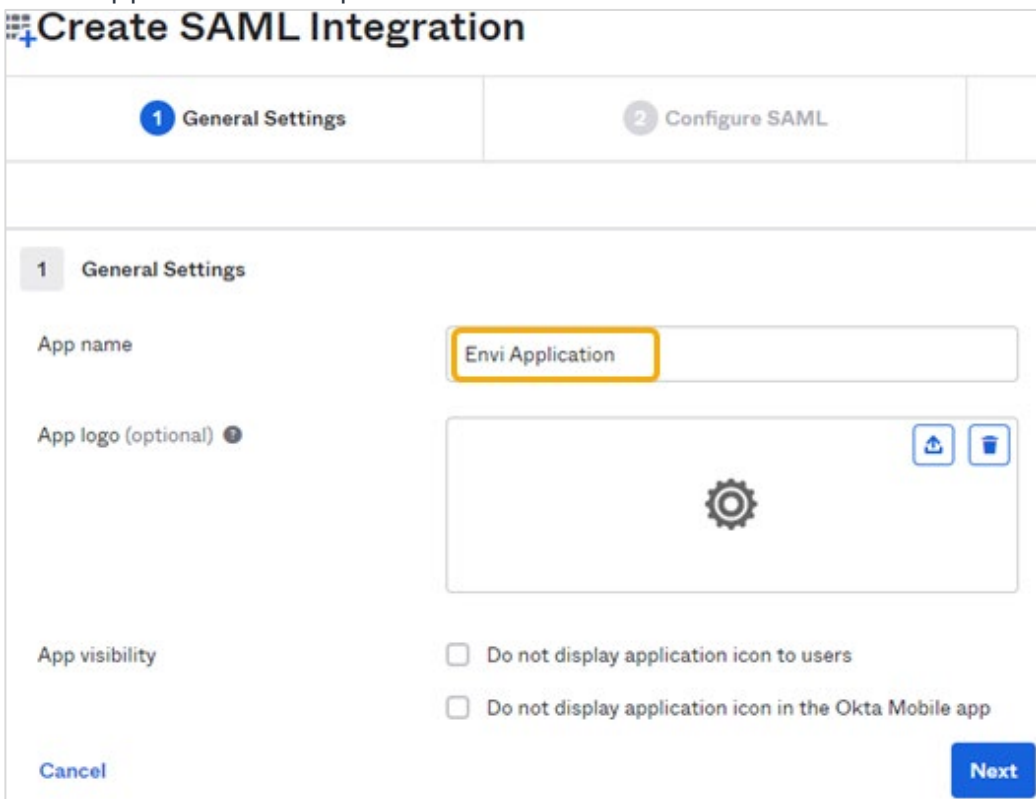
Create a new app integration

Sign-on method [Learn More](#)

- ☐ **OIDC - OpenID Connect**
Token-based OAuth 2.0 authentication for Single Sign-On (SSO) through API endpoints. Recommended if you intend to build a custom app integration with the Okta Sign-In Widget.
- ☒ **SAML 2.0**
XML-based open standard for SSO. Use if the Identity Provider for your application only supports SAML.
- ☐ **SWA - Secure Web Authentication**
Okta-specific SSO method. Use if your application doesn't support OIDC or SAML.
- ☐ **API Services**
Interact with Okta APIs using the scoped OAuth 2.0 access tokens for machine-to-machine authentication.

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

5. On the **Create SAML Integration page** (step 1 General Settings), change the name of the application and upload other icons if needed. Then, click **Next**.





Create SAML Integration

1 General Settings **2 Configure SAML**

1 General Settings

App name

App logo (optional) 

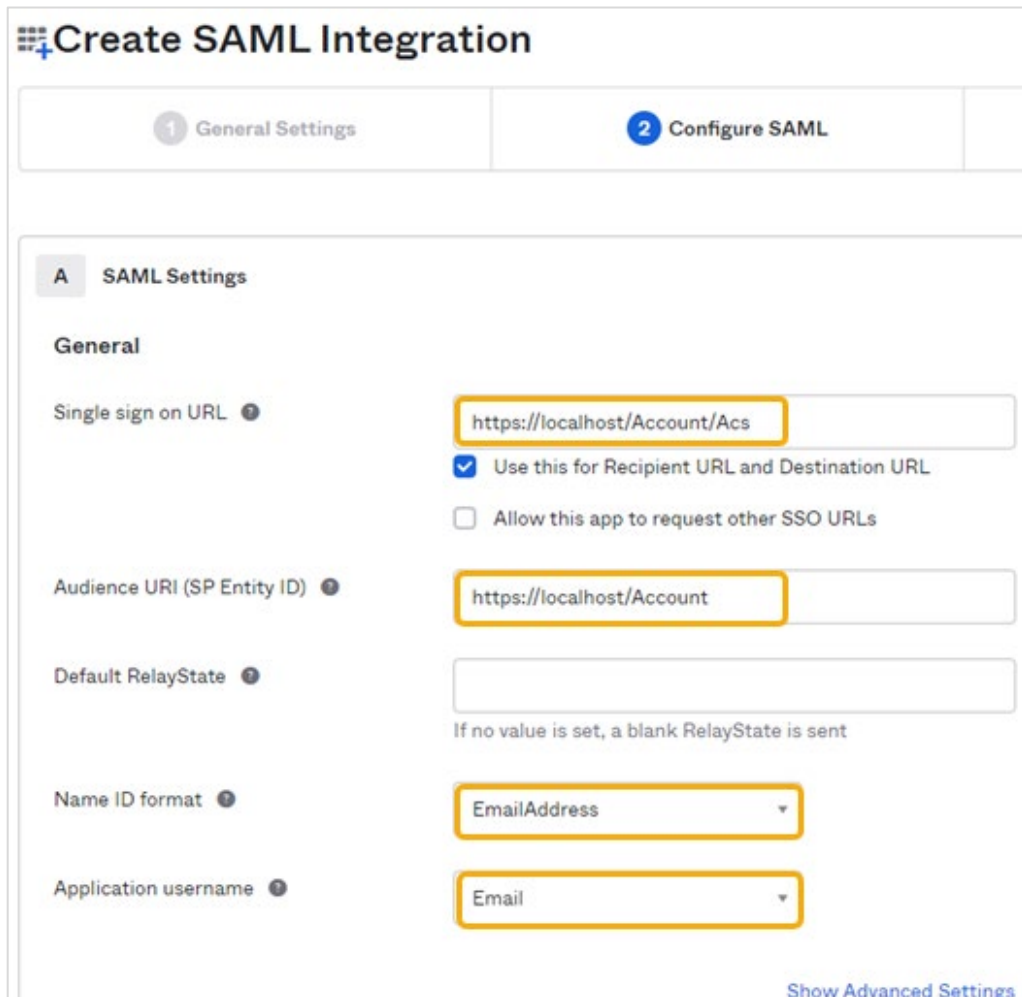


App visibility

- ☐ Do not display application icon to users
- ☐ Do not display application icon in the Okta Mobile app

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

6. On the **Create SAML Integration** page (step 2 Configure SAML), fill in the **Single sign on URL** (application base URL + /Account/Acs) and **Audience URI** (SP Entity ID), (application base URL + /Account) fields. Select **EmailAddress** for the **Name ID format** dropdown and **Email** for the **Application username** dropdown.




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. Click **Next** and **Finish**.

- After you create the application, you will be navigated to the application details page (the **Sign On** tab). At the bottom of this page copy the **URL of Identity Provider metadata** link, which you will use for 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.

- Go to the **Assignments** tab. Here, you can assign application users or user groups that should be able to sign in.

Envi Application

Active View Logs Monitor Imports

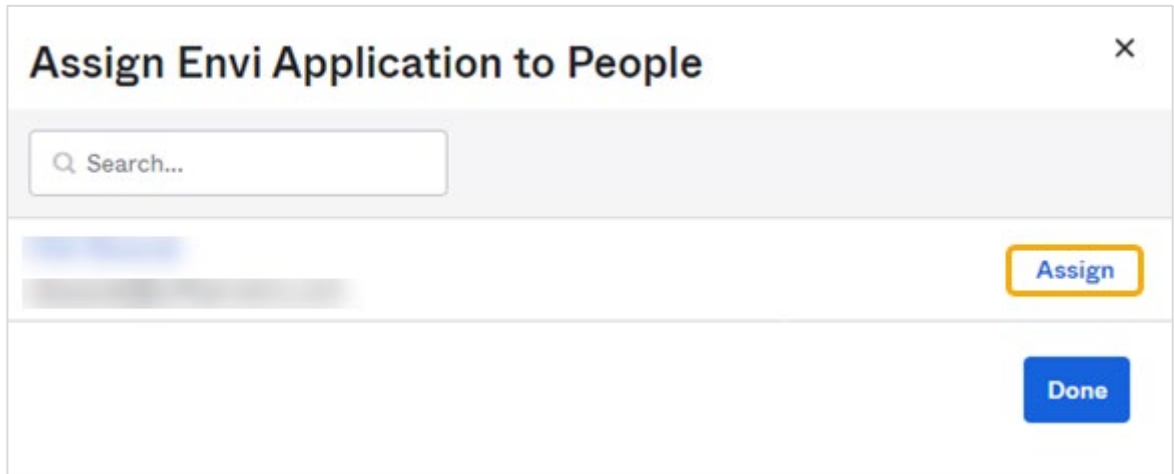
General Sign On Mobile Import **Assignments**

[Assign](#) [Convert Assignments](#) Search... [People](#)

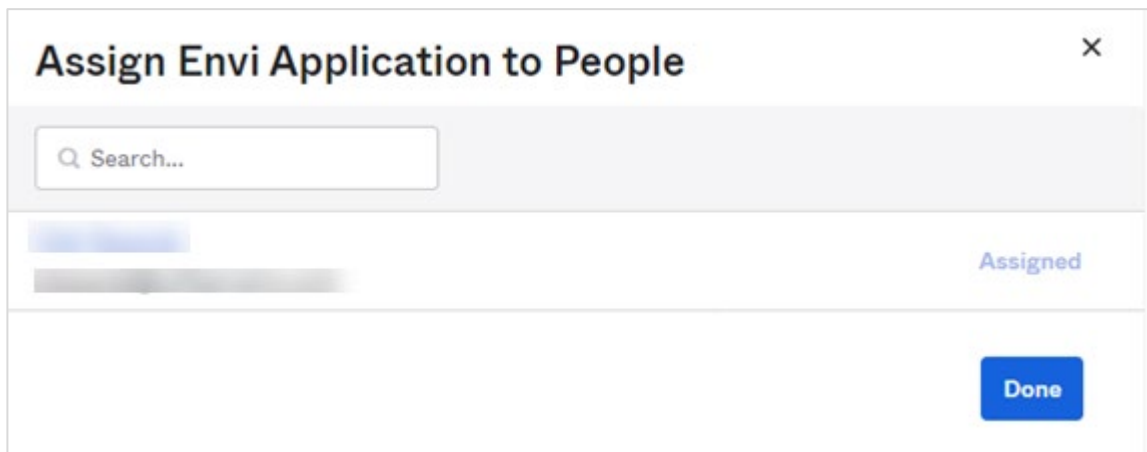
Filters	Person	Type
People		
Groups		
		01101110
		01101111
		01101100
		01101100
		01101101
		01101110
		01100111
		No users found

10. To grant access to the application for existing users, do the following:

- a. Click **Assign**, and then select the **Assign to People** item.
- b. Search the users you need, and then click the **Assign** link.

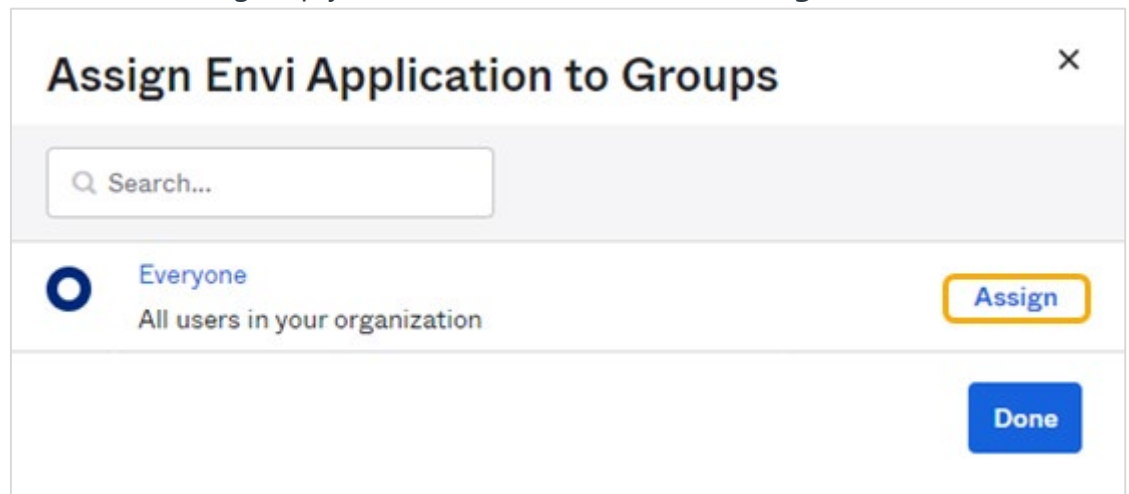


- c. Verify the person's username, then click **Save** and **Go Back**. You will be returned to the previous page, so you can proceed with assigning other users. When all needed users are assigned, click **Done**.



11. To grant access to the application for existing user groups, do the following:

- a. Click **Assign**, and then select the **Assign to Groups** item.
- b. Search the user group you need, and then click the **Assign** link.



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 is a search bar with a magnifying glass icon and the text "Search...". Under the search bar, there is a list of user groups. The first group is "Everyone" with a blue radio button icon, and the description "All users in your organization". To the right of this group is a yellow "Assign" button. At the bottom right of the dialog box is a blue "Done" button.

- c. When all needed user groups are assigned, click **Done**.

Perform these steps for all users and user groups that should log in with SSO. Now, the single sign-on configuration is ready for use.

Envi Configuration

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

1. Log in to the Envi application.
2. Go to the **Domain List**, select the needed Domain, and click **Edit**.
3. Select the **HTTP Redirect** authentication type and click **Upload Metadata**.

Domains > Domain Name Domain_Name

DETAILS ORGANIZATIONS USERS PASSWORD DICTIONARIES CERTIFICATES 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: 0

Endpoint URL:

Identifier URL:

SSO Message: Please provide your SSO credentials for further logins

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

4. Specify metadata location URL and click **OK**.

Upload Metadata X

Upload From: URL

Identifier URL: https://identifierurl

OK Cancel

Note: Use the **URL of Identity Provider** metadata link from the step 8.

5. Make sure that **Endpoint URL** and **Identifier URL** are populated with the new values.

Domains > Domain Name SSO2 Domain

DETAILS ORGANIZATIONS USERS PASSWORD DICTIONARIES UPDATE RESOURCES SECURITY

Edit

Name: SSO2 Domain

Description: For HTTP Redirect

Domain Type: Simple

Session Timeout, m: 20

Mobile Token Expiration, h:

Default UI: Default [Update Users](#)

Status: Active

Authentication: HTTP Redirect

Failed Attempts: 255

Endpoint URL:

Identifier URL:

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

6. While creating a user, select the needed domain with the **HTTP Redirect** type of authentication. 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	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, a user can sign in to the Envi application using Okta SSO.