



# OneLogin Single Sign-On

Integration Guide

## Introduction

OneLogin is a single sign-on provider, which makes it easy to manage application logins and permissions. Our OneLogin SSO integration allows you to effectively manage access to your Envi application using a secure and scalable identity management system.

OneLogin provider prevents common weak points in the authentication experience, including username and password login or password reset requests. It is very easy to access. 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.

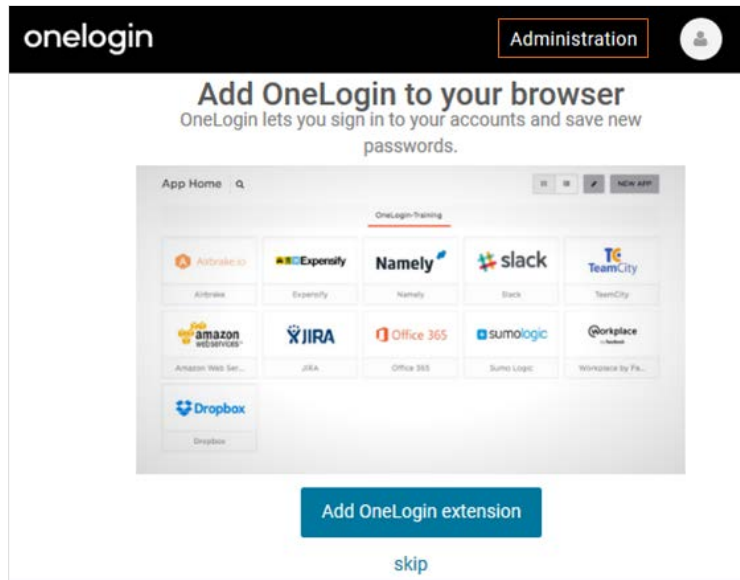
This step-by-step guide explains how to set up single sign-on to your Envi account with OneLogin provider.

**Note:** Sign up for OneLogin first to proceed with steps that this Integration Guide provides.

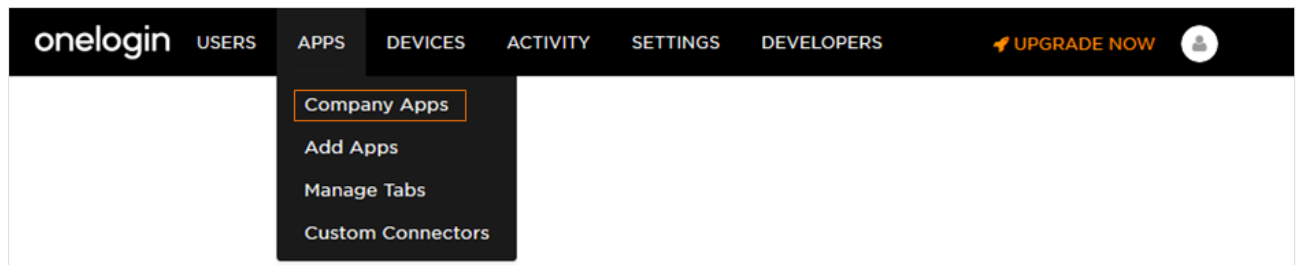
# Integration

Follow the steps below to get your OneLogin account tied to your Envi account.

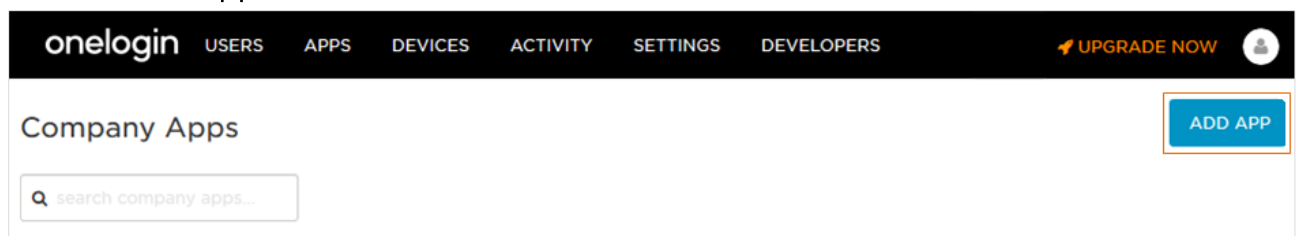
1. Log in to the [One Login](#) site.
2. Click **Administration**.



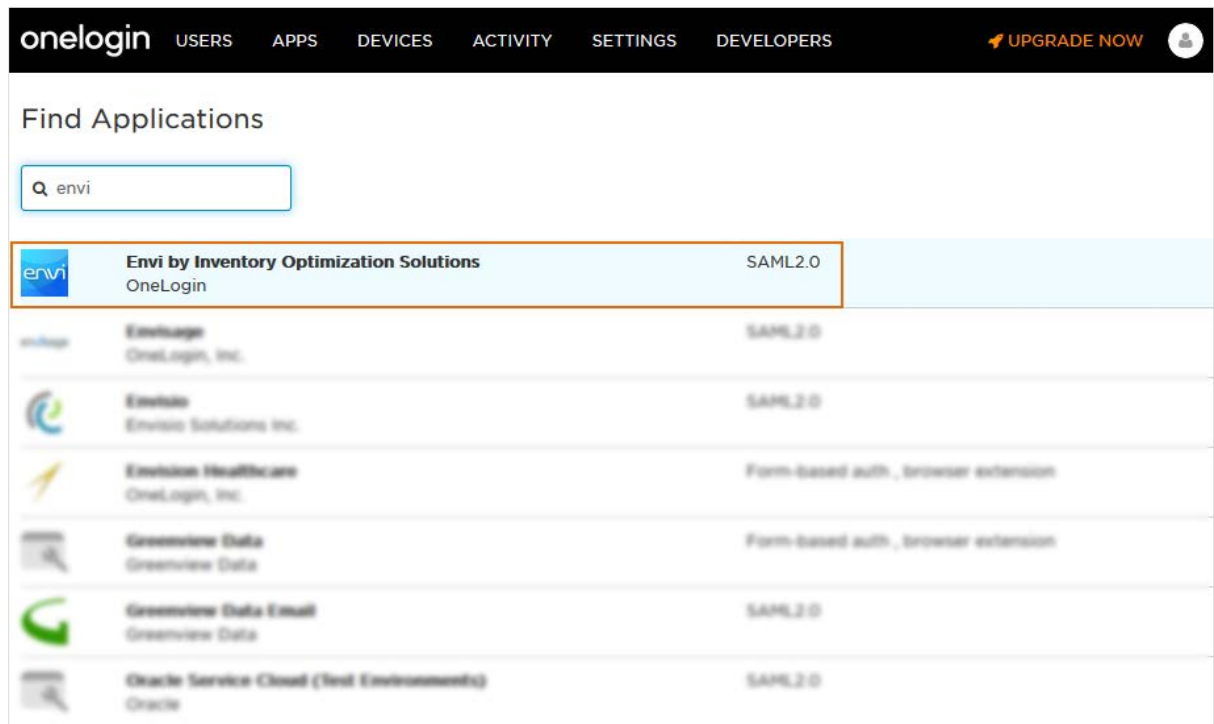
3. On the **APPS** tab, navigate to **Company Apps**.



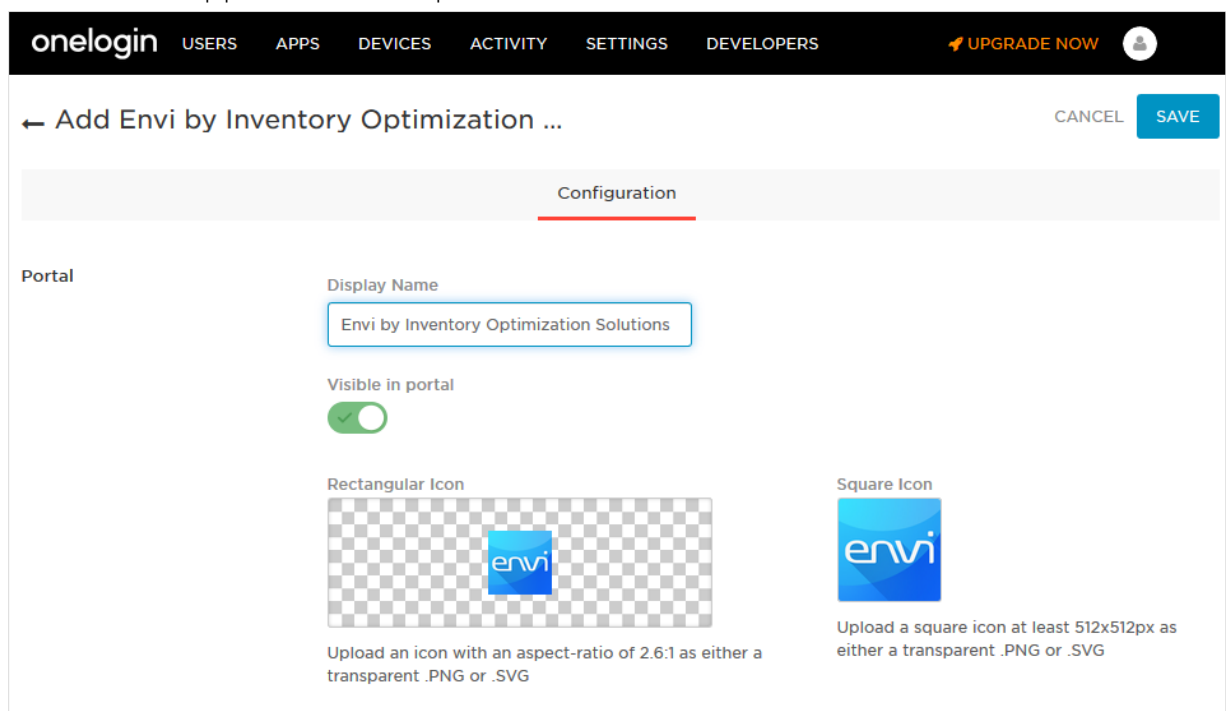
4. Click the **Add App** button.



5. In the Find Application search box type *Envi*, and then select the **Envi by Inventory Optimization Solutions** in the list of search results.

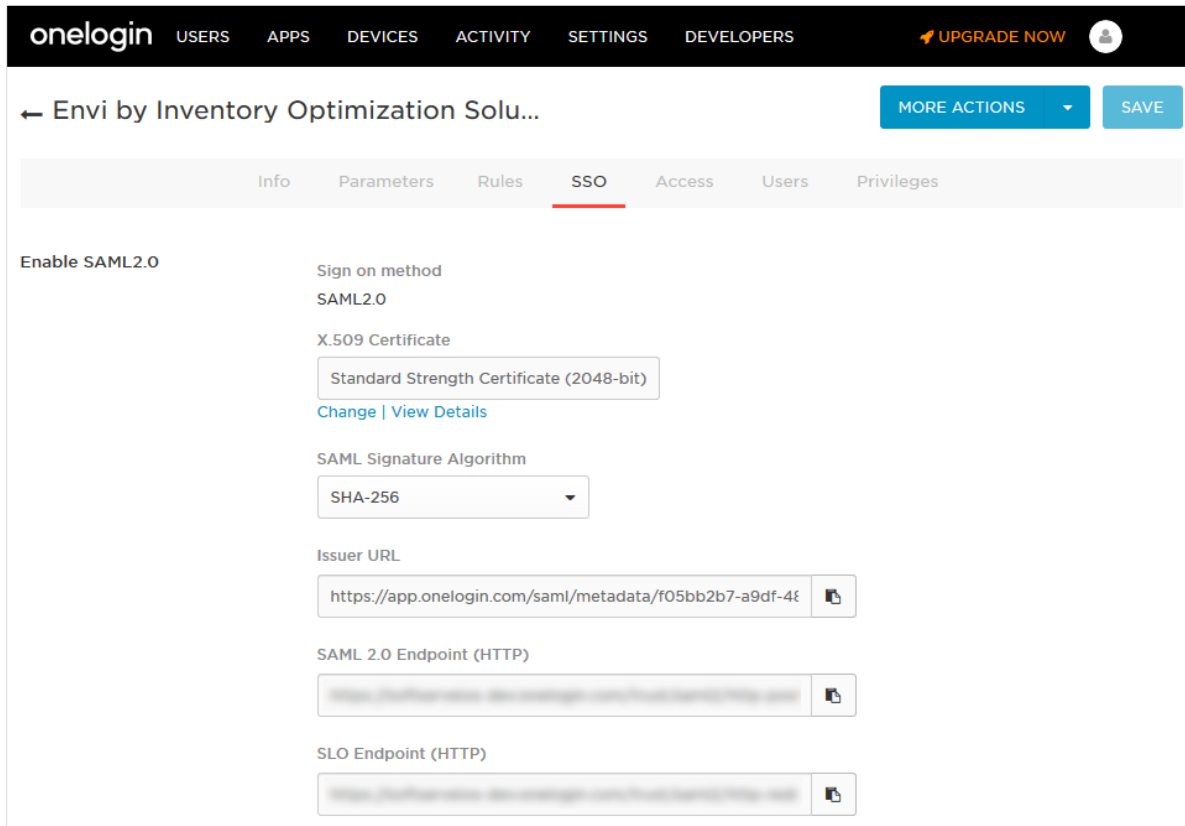


6. On the **Add Envi by Inventory Optimization Solutions Configuration** page, change name of the application and upload another icons if needed. Then, click **Save**.



After adding the application, you will be navigated to the **Application Details** page.

7. Go to the **SSO** tab. In the **SAML Signature Algorithm** drop-down menu, select **SHA-256**. All other fields will be auto-populated. Click **Save**.



onelogin USERS APPS DEVICES ACTIVITY SETTINGS DEVELOPERS [UPGRADE NOW](#)

← Envi by Inventory Optimization Solu... [MORE ACTIONS](#) [SAVE](#)

Info Parameters Rules **SSO** Access Users Privileges

**Enable SAML2.0**

Sign on method  
SAML2.0

X.509 Certificate  
Standard Strength Certificate (2048-bit)  
[Change](#) | [View Details](#)

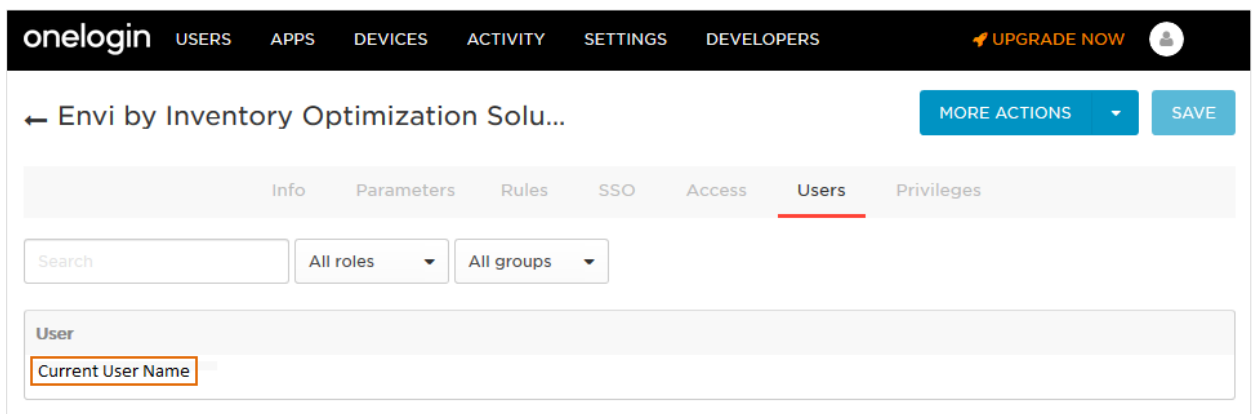
SAML Signature Algorithm  
SHA-256

Issuer URL  
https://app.onelogin.com/saml/metadata/f05bb2b7-a9df-4e...

SAML 2.0 Endpoint (HTTP)

SLO Endpoint (HTTP)

8. Copy **Issuer URL** for further steps.
9. Go to the **Users** tab. As you can see, **Current User Name** already exists in the **Users** list.



onelogin USERS APPS DEVICES ACTIVITY SETTINGS DEVELOPERS [UPGRADE NOW](#)

← Envi by Inventory Optimization Solu... [MORE ACTIONS](#) [SAVE](#)

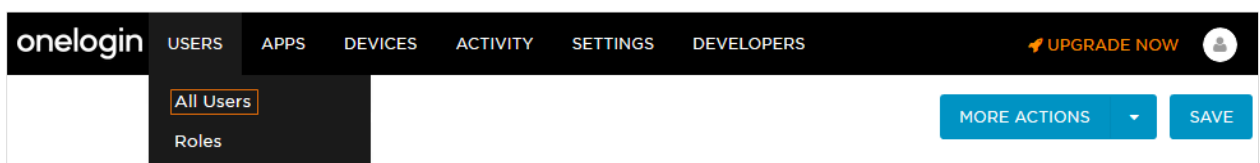
Info Parameters Rules SSO Access **Users** Privileges

Search All roles All groups

User
Current User Name

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

- a. Go to the **Users** tab and select **All Users**.

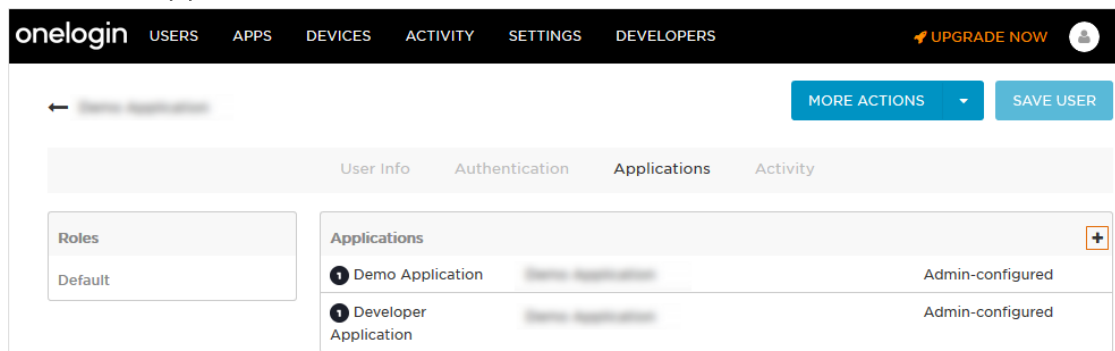


onelogin USERS APPS DEVICES ACTIVITY SETTINGS DEVELOPERS [UPGRADE NOW](#)

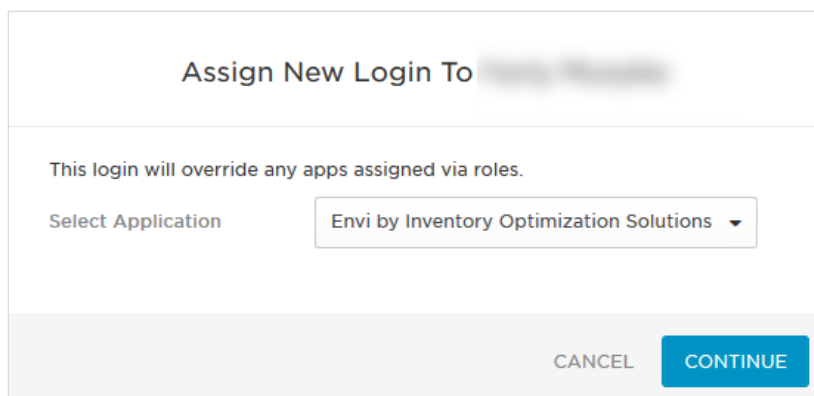
All Users Roles

[MORE ACTIONS](#) [SAVE](#)

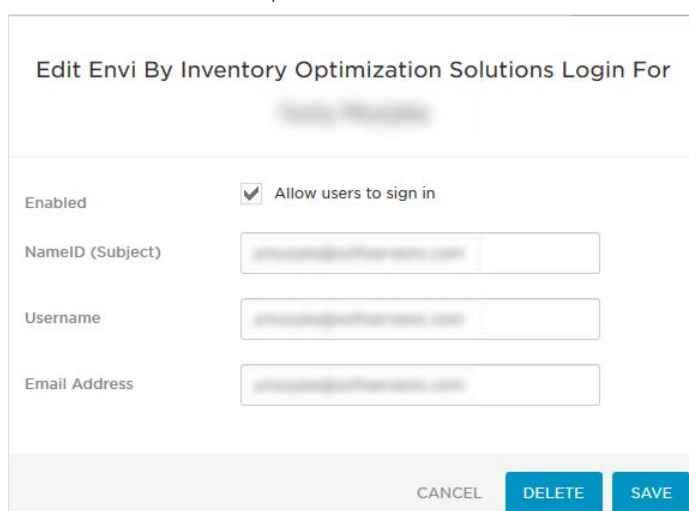
- b. Select the needed user. You will be navigated to the **User Info** tab.
- c. Go to the **Applications** tab, and then click the **Plus (+)** icon.



- d. On the **Assign New Login** dialog box, select your application from the drop-down menu, and then click **Continue**.



- e. On the **Edit Login** dialog box, select the **Allow user to sign in** check box. The **NameID (Subject)** and **Username** fields should display the email address for the current user. Then, click **Save**.



Perform these steps for all users who should log in with SSO.

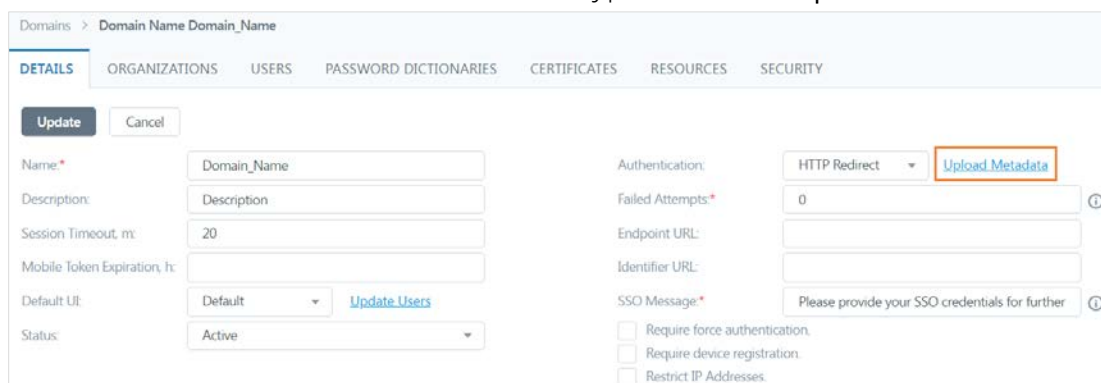
Now, the single sign-on configuration is ready for use.



## 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**, and then select the needed Domain. Click the **Edit** button.
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:

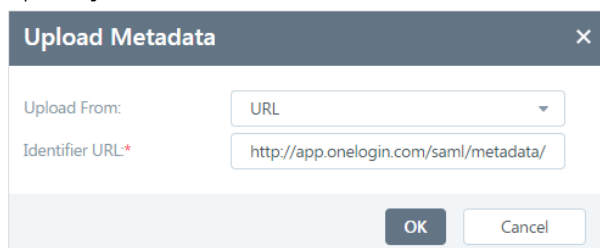
SSO Message: Please provide your SSO credentials for further logins

☐ Require force authentication.

☐ Require device registration.

☐ Restrict IP Addresses.

4. Specify metadata location URL, and then click **Ok**.



**Upload Metadata** ✕

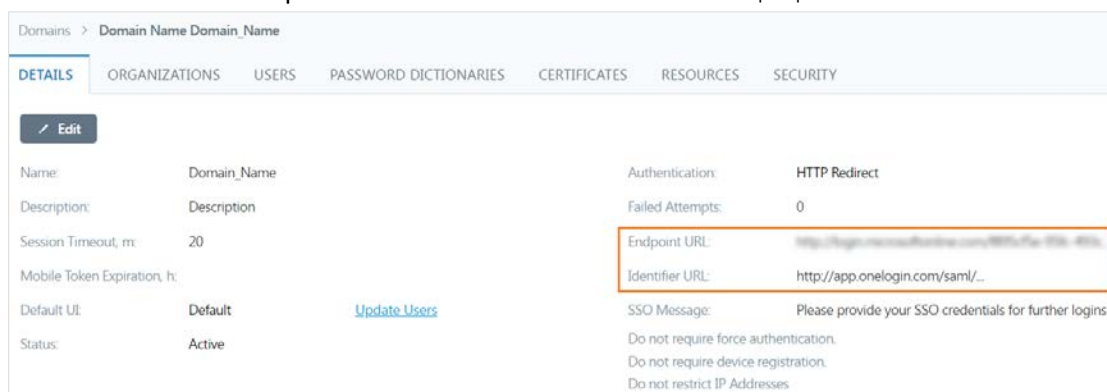
Upload From: URL

Identifier URL: http://app.onelogin.com/saml/metadata/

**OK** **Cancel**

**Note:** Use **Issuer URL** from the step 8.

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



Domains > Domain Name Domain\_Name

**DETAILS** ORGANIZATIONS USERS PASSWORD DICTIONARIES CERTIFICATES 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: 0

Endpoint URL: http://app.onelogin.com/saml/metadata/

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.

- While creating user, select the needed domain with **HTTP Redirect** type of authentication. In the **SSO User Name** field enter the username from the One Login 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:	<a href="#">Email@xx.com</a>	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, user can log in to the Envi application using One Login SSO.

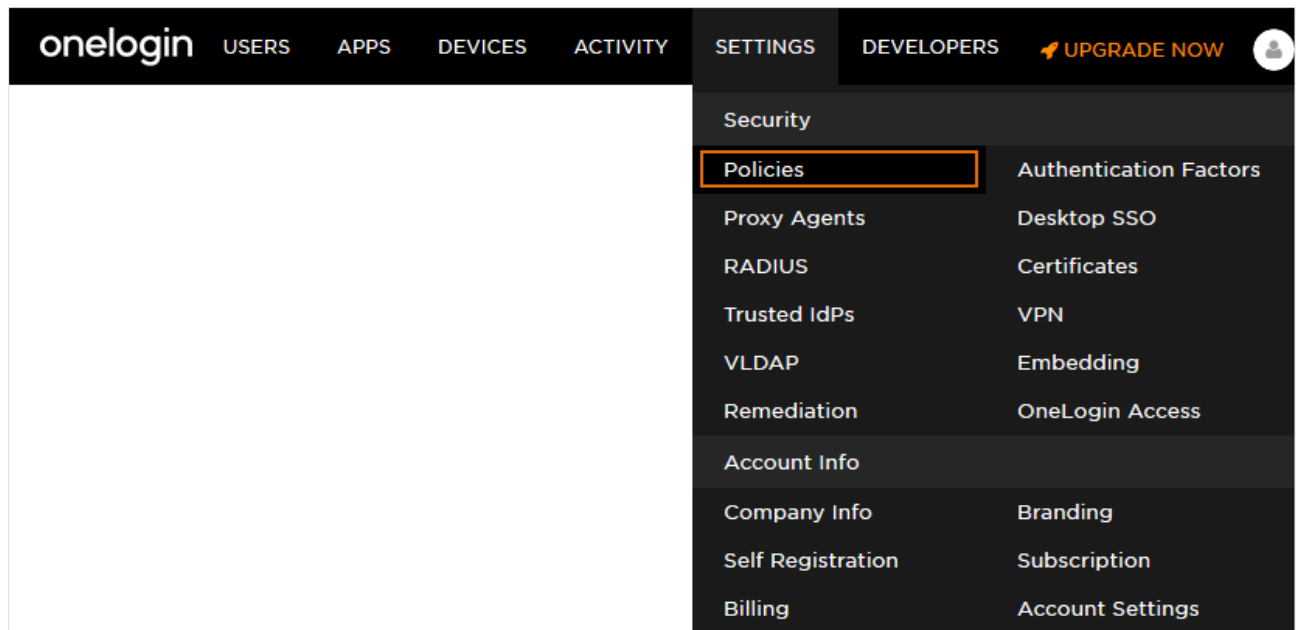


## Browser Extension

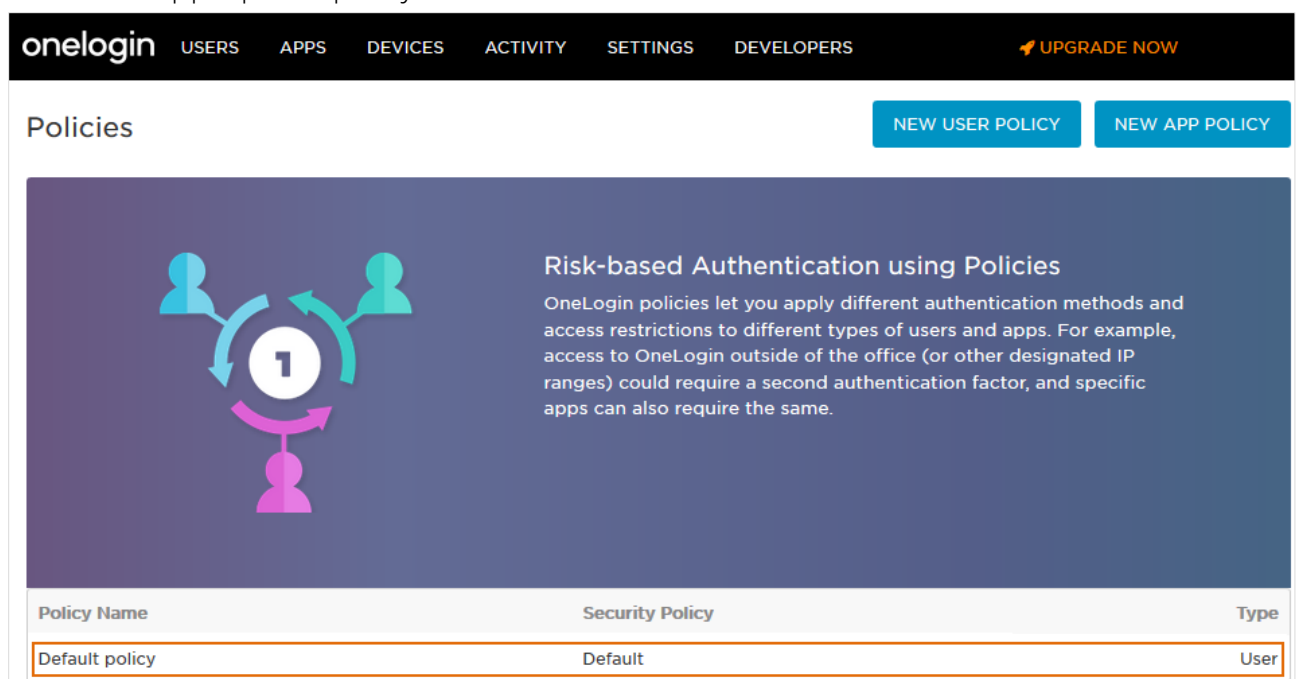
The OneLogin browser extension provides a convenient toolbar shortcut to your OneLogin dashboard.

To enable users to use browser extension, make appropriate changes in the policy assigned to this user. For this, do the following:

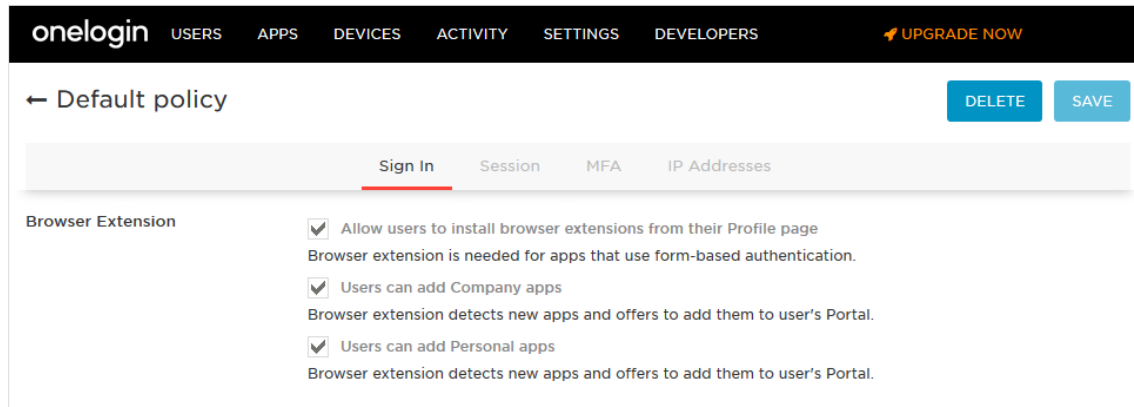
1. Go to the **Settings** tab and select **Policies**.



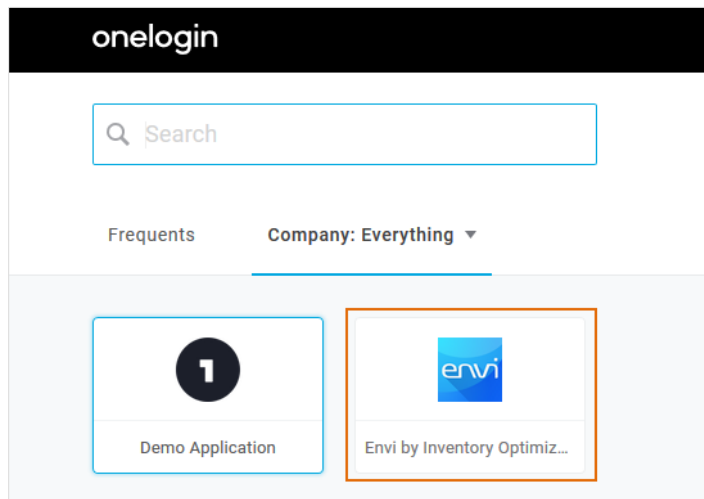
2. Select the appropriate policy.



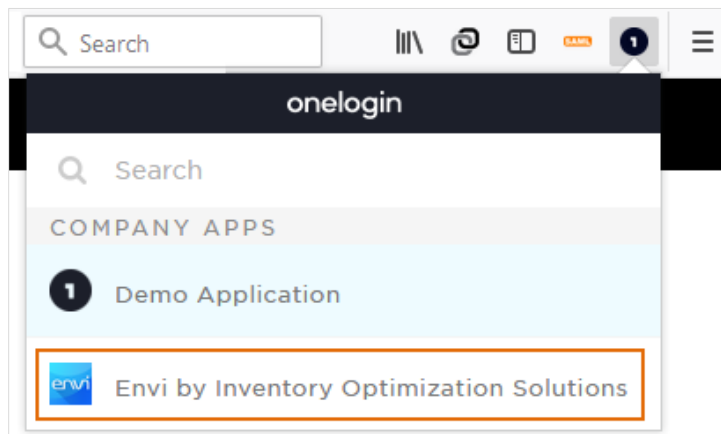
- On the **Sign In** tab, in the **Browser Extension** section, select needed check boxes, and then click **Save**.



- When all configurations are done and the extension is installed, click the appropriate application in the list on the **OneLogin** portal.



**Note:** You can select the application directly from the browser extension.



Now, the browser extension is added for the needed user.