



# 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.

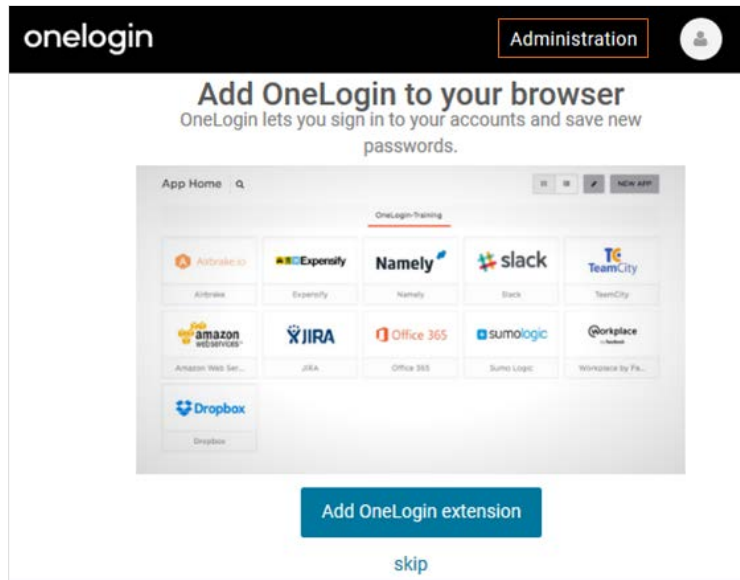
This step-by-step guide explains how to set up single sign-on to your Envi account with OneLogin provider.

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

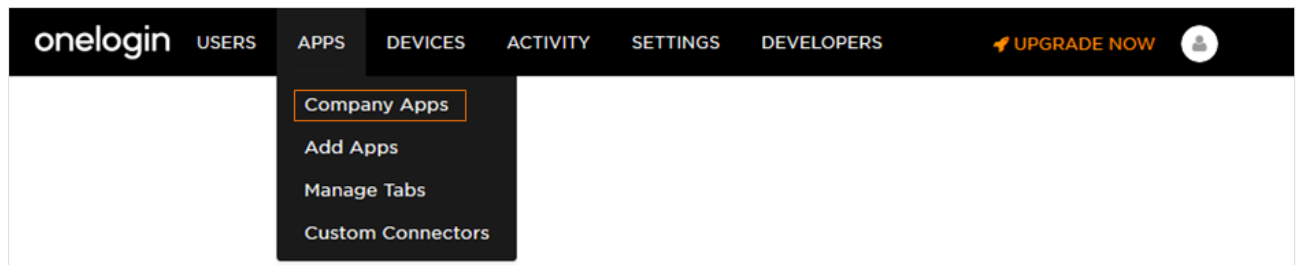
# Integration

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

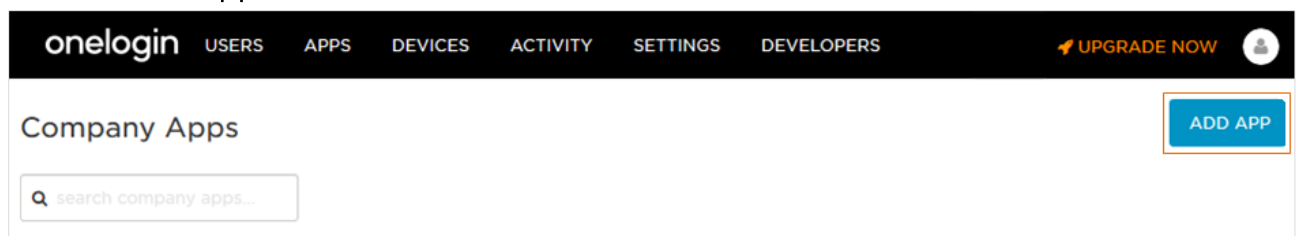
1. Log in to the [One Login](#) site.
2. Click **Administration**.



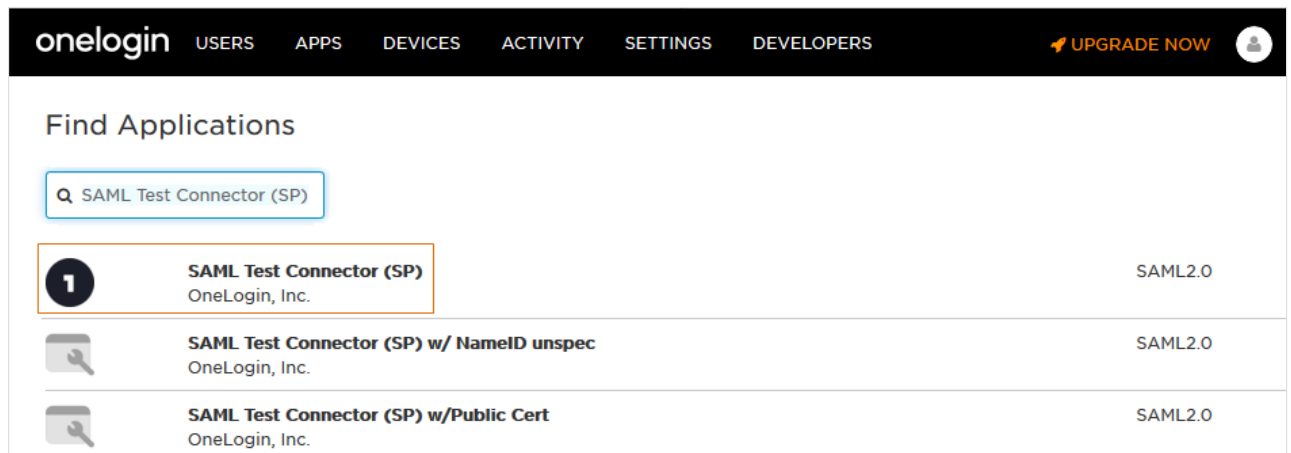
3. On the **APPS** tab, navigate to **Company Apps**.



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

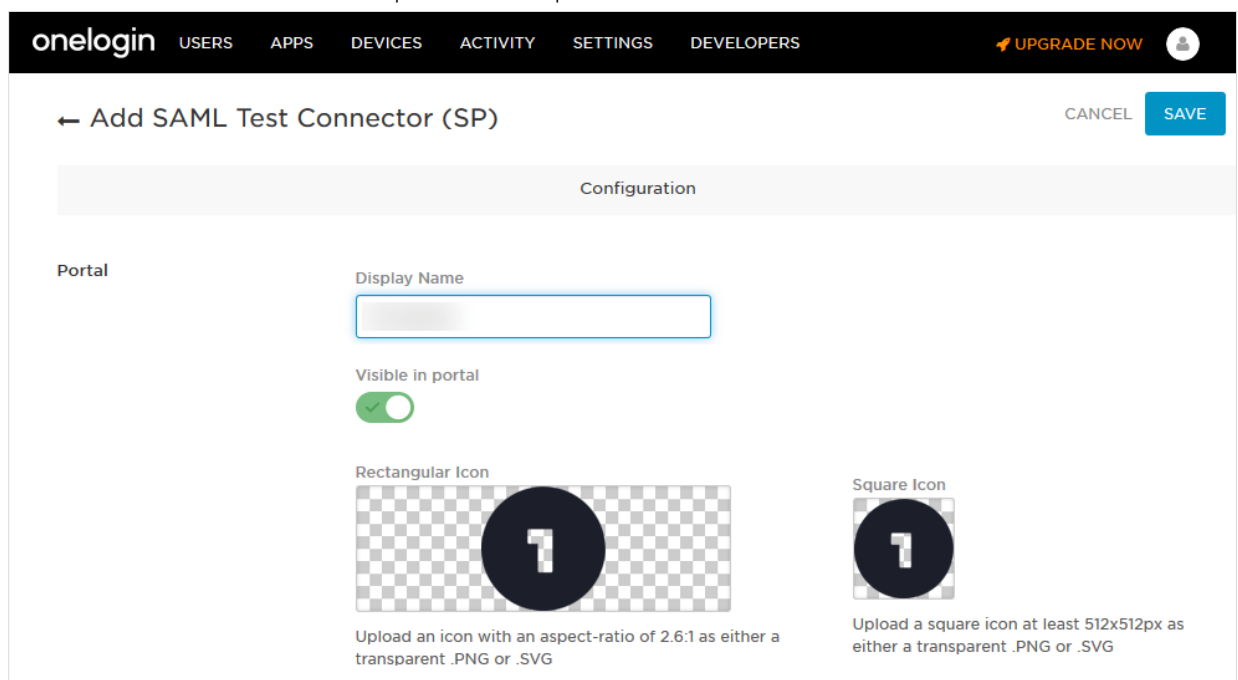


5. In the **Find Application** search box, type *SAML Test Connector (SP)*, and then select the **SAML Test Connector** in the list of search results.



**Note:** In case you want to use the browser extension, type *SAML Test Connector (IdP)*.

6. On the **Add SAML Test Connector (SP) Configuration** page, type the application name in the **Portal** field (for example, *envi*), upload icons if needed, and then click **Save**.



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

7. On the **Application Details** page, go to the **Configuration** tab, and then fill in the following fields.
  - a. Audience (application base URL + /Account)
  - b. Recipient (application base URL + /Account/Acs)
  - c. ACS (Consumer) URL Validator (application base URL + /Account/Acs)
  - d. ACS (Consumer) URL (application base URL + /Account/Acs)

The screenshot shows the OneLogin management interface. The top navigation bar includes 'onelogin', 'USERS', 'APPS', 'DEVICES', 'ACTIVITY', 'SETTINGS', and 'DEVELOPERS'. On the right, there is an 'UPGRADE NOW' button and a user profile icon. The main content area is titled '← SAML Test Connector (SP)' and has a 'MORE ACTIONS' dropdown and a 'SAVE' button. Below the title is a tabbed interface with 'Info', 'Configuration', 'Parameters', 'Rules', 'SSO', 'Access', 'Users', and 'Privileges'. The 'Configuration' tab is active. Under 'Application Details', there are five input fields: 'RelayState', 'Audience', 'Recipient', 'ACS (Consumer) URL Validator\*', and 'ACS (Consumer) URL\*'. The 'ACS (Consumer) URL\*' field is highlighted with a blue border. Below the 'ACS (Consumer) URL Validator\*' field is a note: '\*Required. Regular expression - Validates the ACS URL when initiated by an AuthnRequest'. Below the 'ACS (Consumer) URL\*' field is a note: '\*Required'.

After all required information is added, click **Save**.

8. Go to the **Parameters** tab and make sure that **Email (NameID)** is specified as a single parameter.

The screenshot shows the 'SAML Test Connector (SP)' configuration page in the OneLogin console, specifically the 'Parameters' tab. The top navigation bar includes 'onelogin', 'USERS', 'APPS', 'DEVICES', 'ACTIVITY', 'SETTINGS', and 'DEVELOPERS', along with an 'UPGRADE NOW' button and a user profile icon. The page title is 'SAML Test Connector (SP)' with a back arrow and 'MORE ACTIONS' and 'SAVE' buttons. Below the title is a tabbed interface with 'Info', 'Configuration', 'Parameters' (selected), 'Rules', 'SSO', 'Access', 'Users', and 'Privileges'. Under 'Parameters', there are two radio buttons for 'Credentials are': 'Configured by admin' (selected) and 'Configured by admins and shared by all users'. Below this is a table with two columns: 'SAML Test Connector (SP) Field' and 'Value'. The table contains one row: 'Email (NameID)' with the value 'Email'. An 'Add parameter' link is visible on the right side of the table.

SAML Test Connector (SP) Field	Value
Email (NameID)	Email

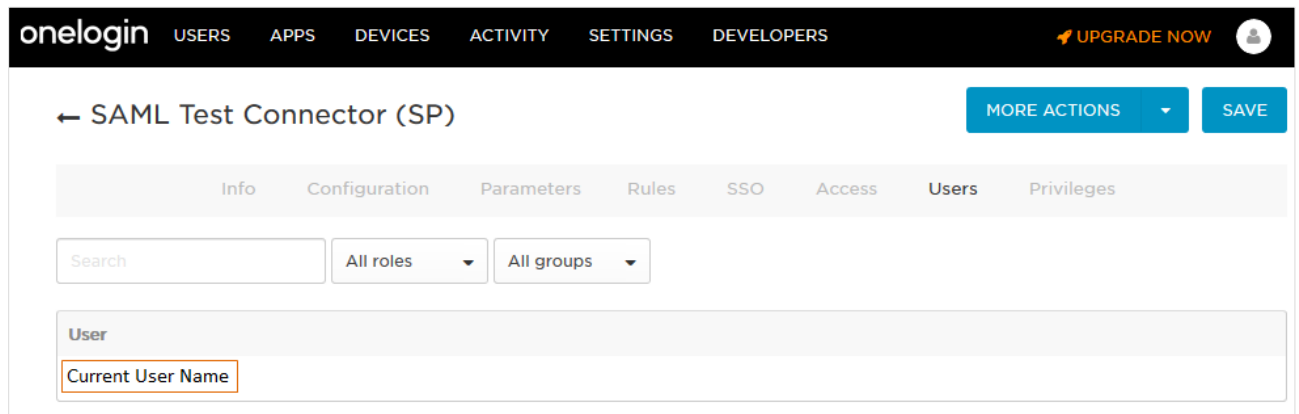
If another parameter exists, remove it. For this, select the parameter and click **Delete** button.

- Go to the **SSO** tab. In the **X.509 Certificate** field enter *Standard Strength Certificate (2048-bit)*, and then, in the **SAML Signature Algorithm** drop-down menu, select **SHA-256**. All other fields will be auto-populated. Click **Save**.

The screenshot shows the 'SAML Test Connector (SP)' configuration page in the OneLogin console, specifically the 'SSO' tab. The top navigation bar is the same as the previous screenshot. The page title is 'SAML Test Connector (SP)' with a back arrow and 'MORE ACTIONS' and 'SAVE' buttons. Below the title is a tabbed interface with 'Info', 'Configuration', 'Parameters', 'Rules', 'SSO' (selected), 'Access', 'Users', and 'Privileges'. Under 'SSO', there is a section 'Enable SAML2.0' with a checkbox that is checked. Below this are several fields: 'Sign on method' (SAML2.0), 'X.509 Certificate' (Standard Strength Certificate (2048-bit) with a 'Change | View Details' link), 'SAML Signature Algorithm' (SHA-256), 'Issuer URL' (https://app.onelogin.com/saml/metadata/788cf95f-856e-42), 'SAML 2.0 Endpoint (HTTP)' (https://officevms-dev.onelogin.com/trust/saml2/http-post), and 'SLO Endpoint (HTTP)' (https://officevms-dev.onelogin.com/trust/saml2/http-redirect). Each URL field has a copy icon on the right.

- Copy **Issuer URL** for further steps.

- Go to the **Users** tab. As you can see, **Current User Name** already exists in the **Users** list.



← SAML Test Connector (SP) MORE ACTIONS SAVE

Info Configuration Parameters Rules SSO Access **Users** Privileges

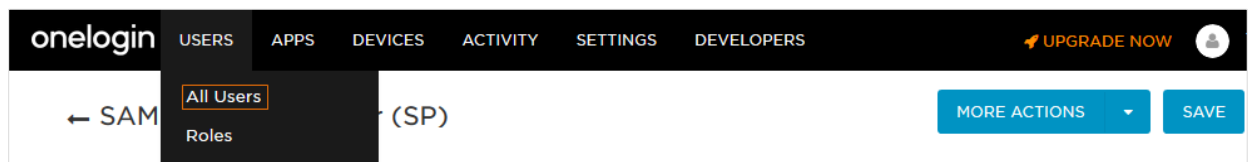
Search All roles All groups

User

User
Current User Name

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

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



← SAML Test Connector (SP) MORE ACTIONS SAVE

Info Configuration Parameters Rules SSO Access **Users** Privileges

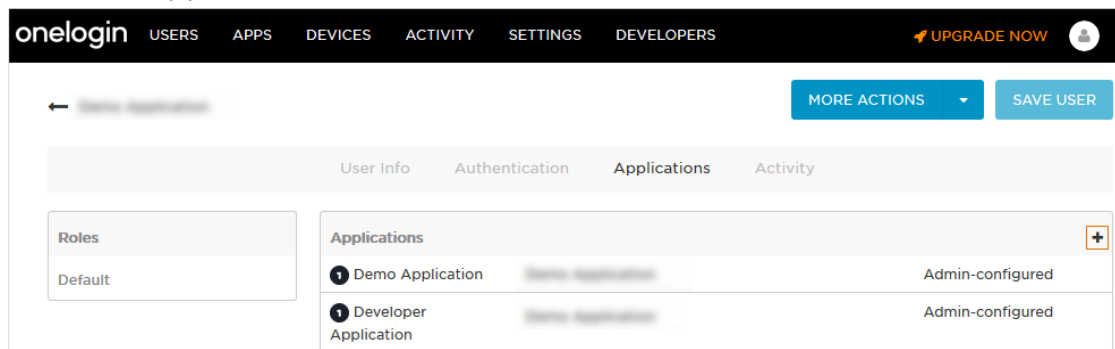
Search All roles All groups

User

User
Current User Name

- Select the needed user. You will be navigated to the **User Info** tab.

- Go to the **Applications** tab, and then click the **Plus (+)** icon.



← Current User Name MORE ACTIONS SAVE USER

User Info Authentication **Applications** Activity

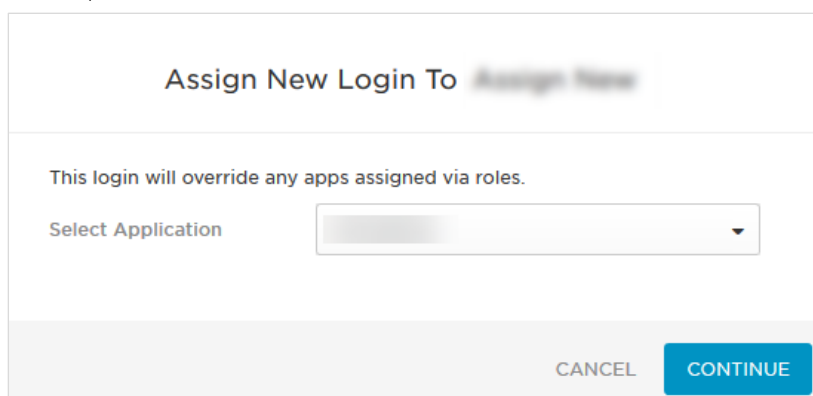
Roles

Roles
Default

Applications

Applications	Configuration
1 Demo Application	Admin-configured
1 Developer Application	Admin-configured

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



Assign New Login To **Assign New**

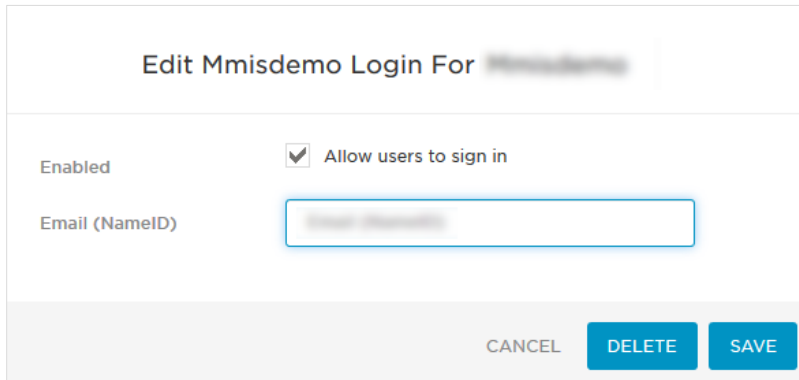
This login will override any apps assigned via roles.

Select Application

CANCEL CONTINUE



- e. On the **Edit Login** dialog box, select the **Allow user to sign in** check box. Do not change the **Email (NameID)** field. It should display the email address for the current user. Then click **Save**.



Dialog box titled "Edit Mmisdemo Login For Mmisdemo".

Enabled ☒ Allow users to sign in

Email (NameID)

CANCEL DELETE 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 ⓘ

☐ 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 9.

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.

6. 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		

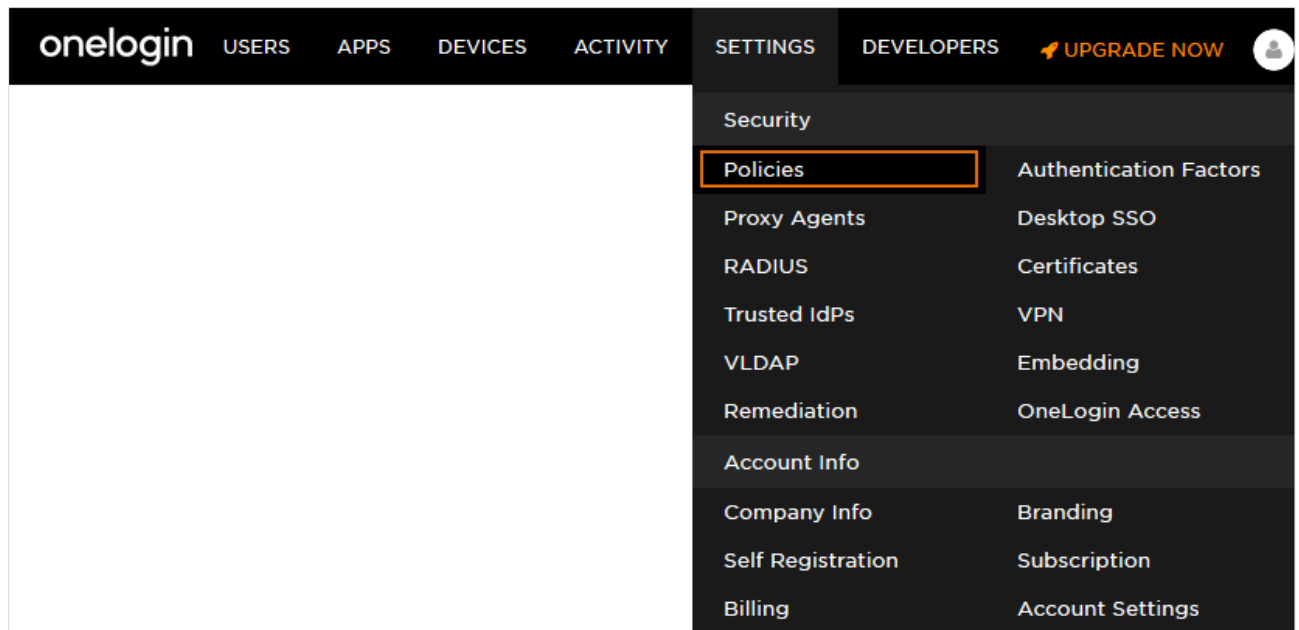
Now, user can log in to the Envi application using One Login SSO.

## Browser Extension

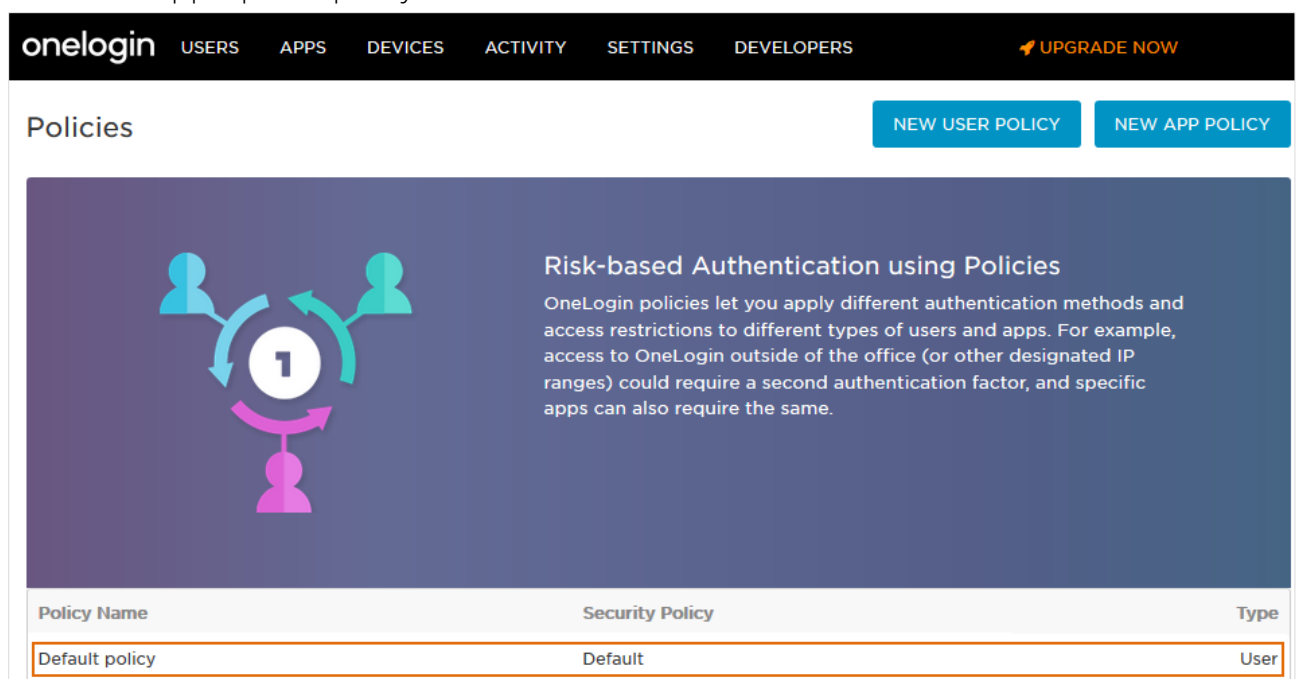
The OneLogin browser extension provides a convenient toolbar shortcut to your OneLogin dashboard.

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

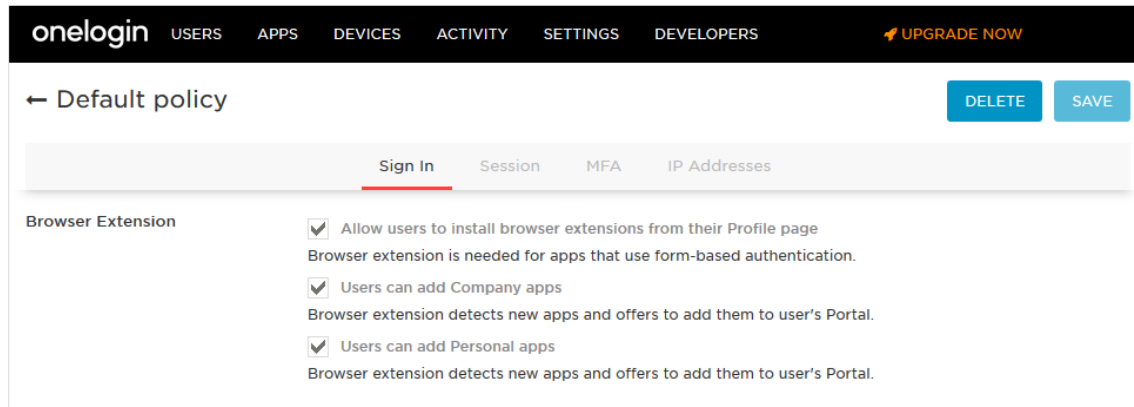
1. Go to the **Settings** tab and select **Policies**.



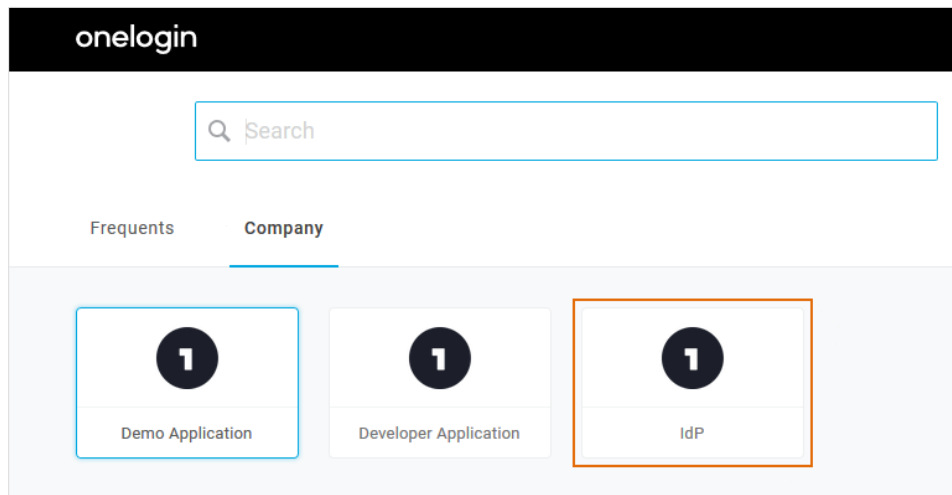
2. Select the appropriate policy.



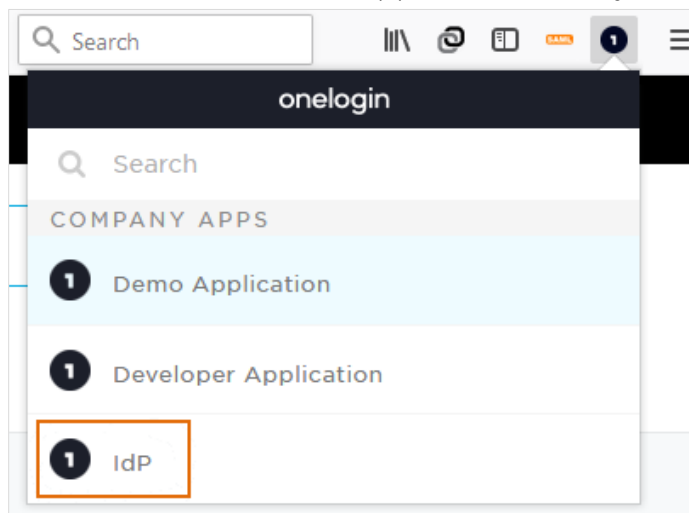
3. On the **Sign In** tab, in the **Browser Extension** section, select needed check boxes, and then click **Save**.



4. 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.