

envi



OneLogin Single Sign-On

Integration Guide



Table of Contents

Integration	2
Envi Configuration	8

Introduction

OneLogin is a **single sign-on (SSO)** provider that simplifies the management of application sign-ins and permissions. With **OneLogin SSO** integration, you can effectively control access to your **Envi** application using a secure and scalable identity management system.

OneLogin 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 the **OneLogin** provider.

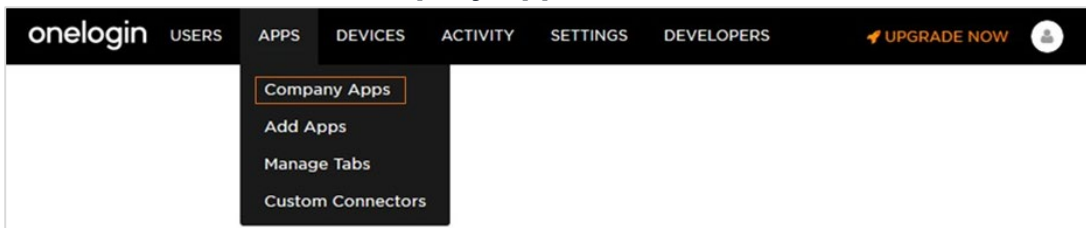
Integration

Follow the steps below to get your **OneLogin** account linked to your **Envi** account.

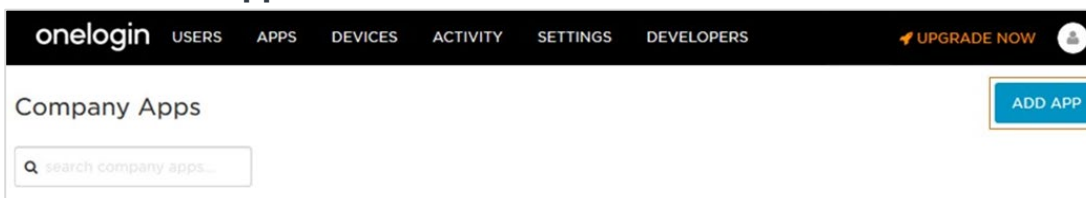
1. Sign in to the [OneLogin](#) site.
2. In the upper-right corner of the page, select **Administration**.



3. On the **APPS** tab, select **Company Apps**.

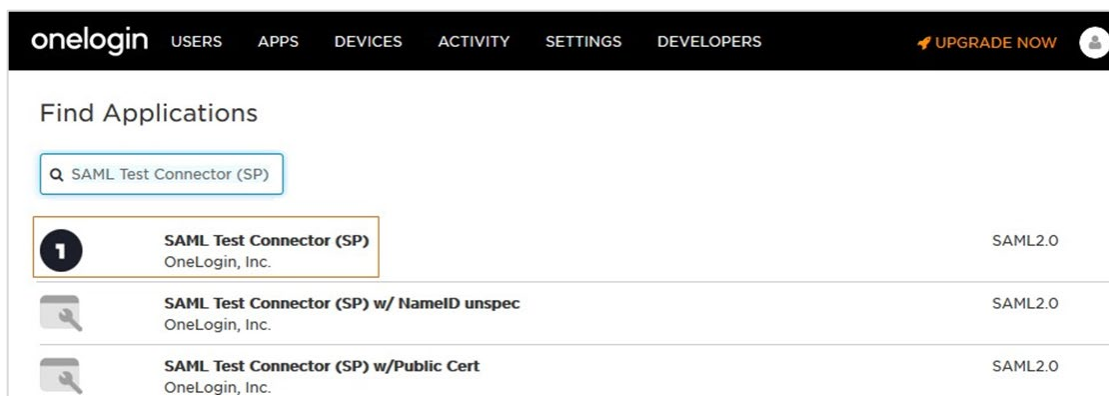


4. Select the **Add App** button.



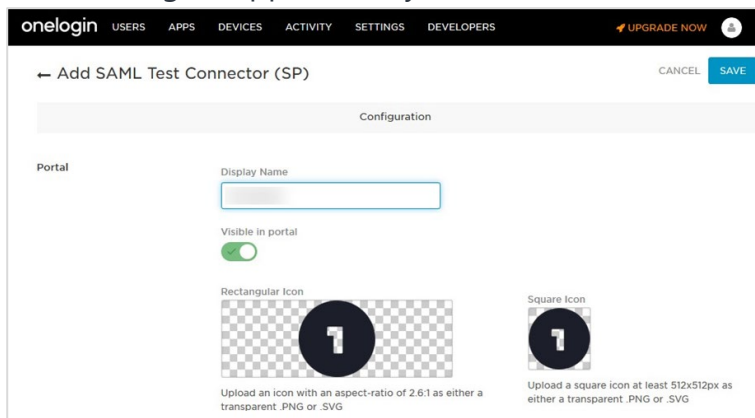
5. In the **Find Applications** search box, enter **SAML Test Connector (SP)** and select it from the list.

Note: If you need to use the browser extension, enter **SAML Test Connector (IdP)**.

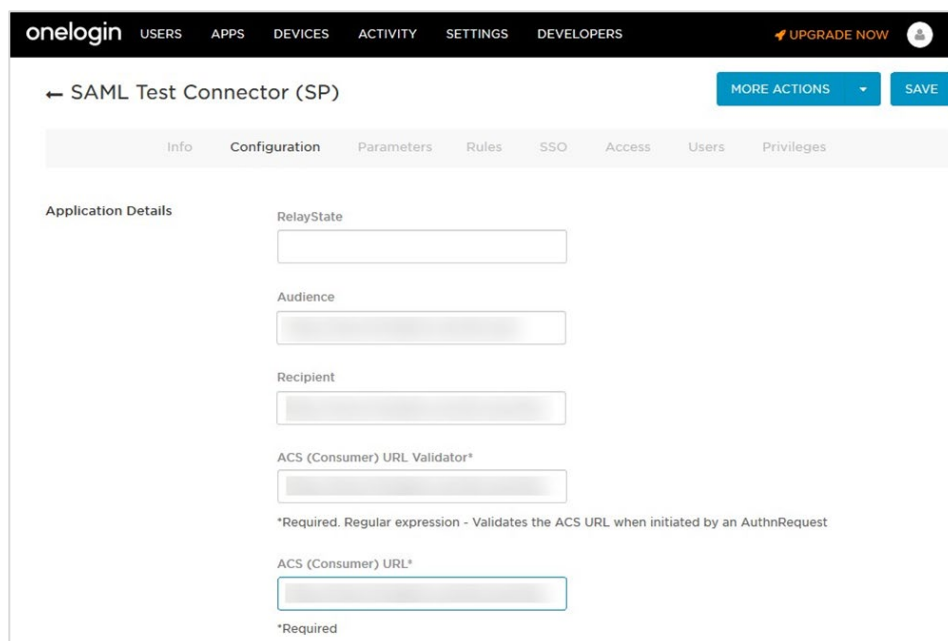


6. On the **Add SAML Test Connector (SP) Configuration** page, do the following steps:
 - a. Enter **Display Name** (for example, envi).
 - b. Upload icons if needed.
 - c. Select **Save**.

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

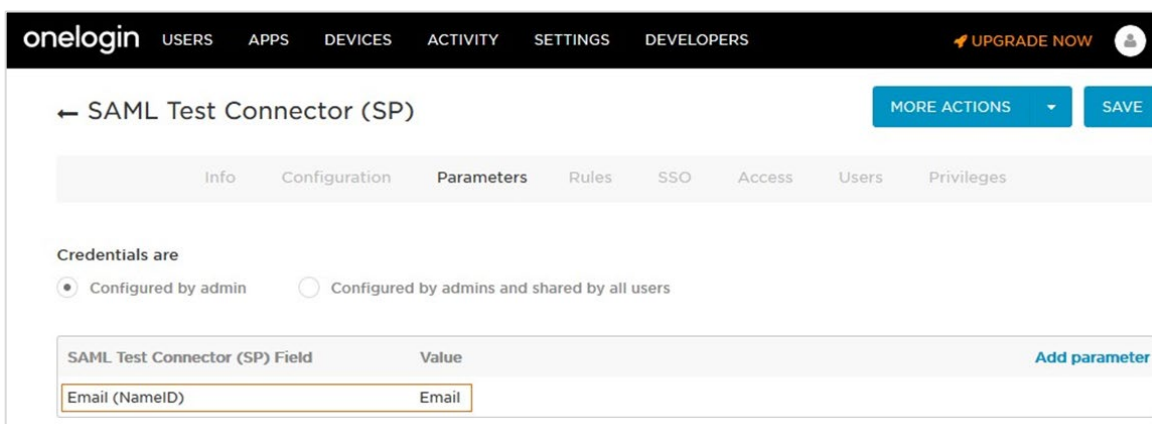


7. On the **Application Details** page, go to the **Configuration** tab and then do the following steps:
 - a. In the **Audience** box, enter an application base URL + /Account.
 - b. In the **Recipient** box, enter an application base URL + /Account/Acs.
 - c. In the **ACS (Consumer) URL Validator** box, enter an application base URL + /Account/Acs.
 - d. In the **ACS (Consumer) URL** box, enter an application base URL + /Account/Acs.
 - e. Select **Save**.



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

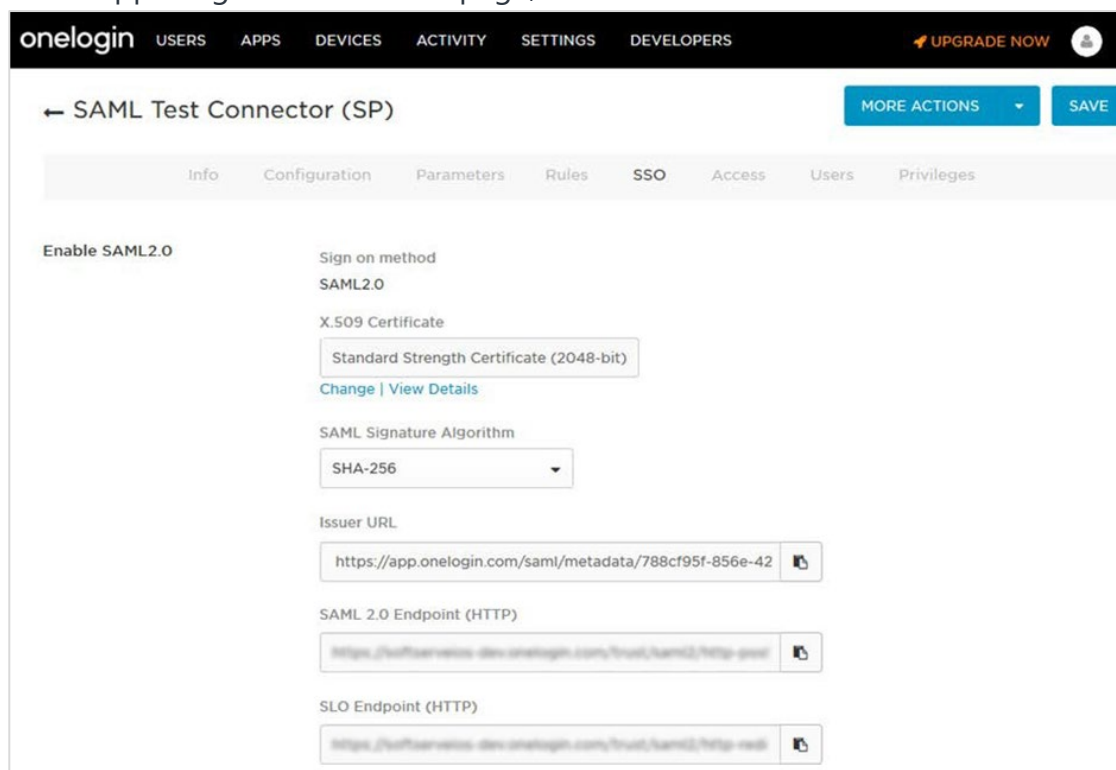
Note: If another parameter exists, remove it. To do this, select a parameter > **Delete**.



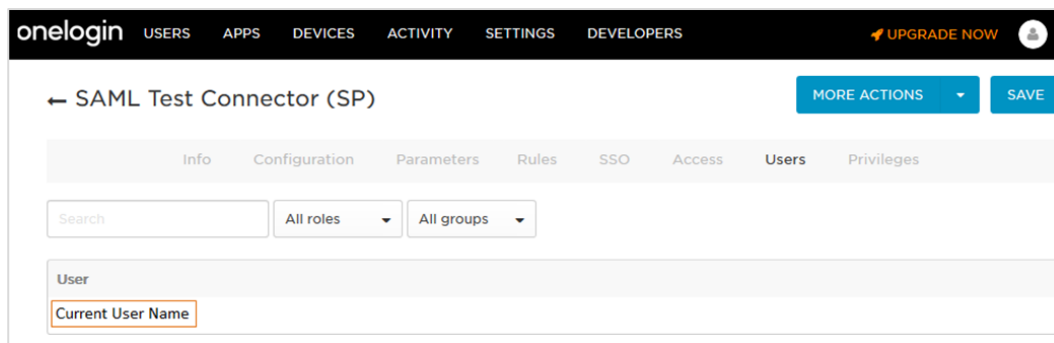
9. Go to the **SSO** tab and then do the following steps:
 - a. In the **X.509 Certificate** box, enter **Standard Strength Certificate (2048-bit)**.
 - b. In the **SAML Signature Algorithm** dropdown list, select **SHA-256**.

Note: All other boxes will be auto-populated.

- c. Copy the **Issuer URL** which you will use for the **Envi** configuration later.
- d. In the upper-right corner of the page, select **Save**.

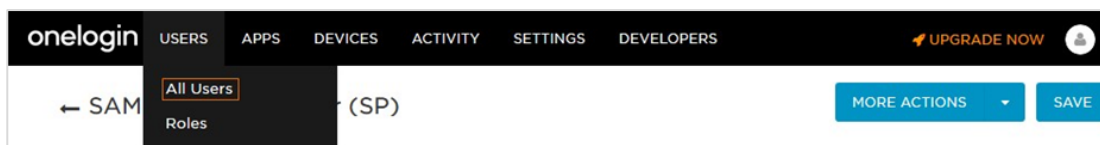


Note: Go to the **Users** tab > the **Users** list to find and view current user details.



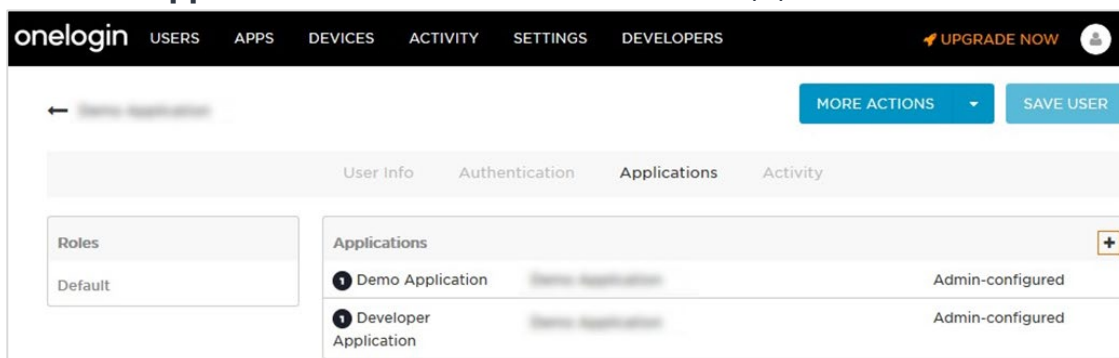
10. To grant access to the application to other existing users, do the following steps:

a. Go to **Users** > **All Users**.

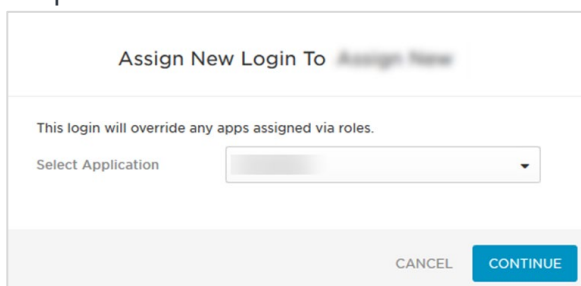


b. Select a needed user.

c. Go to the **Applications** tab and then select the **Plus (+)** icon.

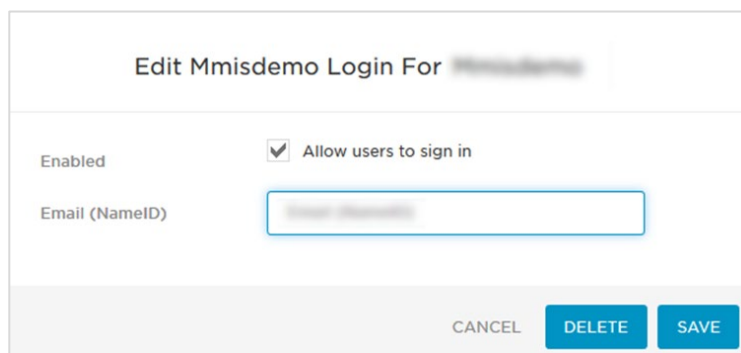


d. In the **Assign New Login To** pop-up window, select your application from the dropdown list and select **Continue**.



- e. In the **Edit Login For** pop-up window, select the **Allow users to sign in** checkbox and then select **Save**.

Note: Do not change the **Email (NameID)**, as it should show the current user's email address.



Edit Mmisdemo Login For

Enabled Allow users to sign in

Email (NameID)

CANCEL DELETE SAVE

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

Domains > Domain Name Domain_Name Default Change

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 ⓘ

Require force authentication.
 Require device registration.
 Restrict IP 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 **Issuer URL** (For more information, go to the [Integration](#) section, step 9).
 - 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

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 **OneLogin** 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	Report Format:	PDF
Phone Ext.:	Phone Ext.	Email Format:	Plain Text
Fax:	Fax	SSO User Name:	SSO User Name
Time Zone:	(UTC+13:00) Samoa		
Default UI:	Envi HTML v.2		
Status:	Active		

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