



OneLogin Single Sign-On

Integration Guide



Table of Contents

Integration2	
Envi Configuration	

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 <u>OneLogin</u> site.
- 2. In the upper-right corner of the page, select **Administration**.



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

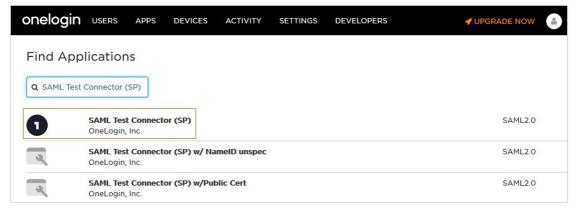
apany Apps Apps				
Anns				
Арра				
age Tabs				
om Connector	5			
	nage Tabs stom Connectors	nage Tabs stom Connectors		

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

onelogin USERS	APPS	DEVICES	ACTIVITY	SETTINGS	DEVELOPERS	VPGRADE NOW
Company Apps						ADD APP
Q search company apps						

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.

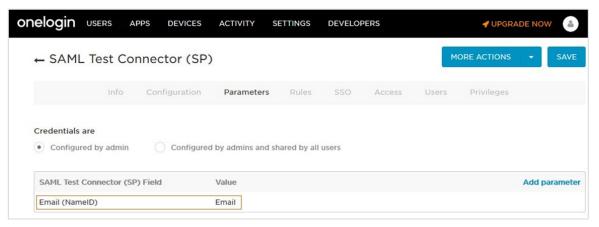
onelogin USERS	APPS DEVICES ACTIVITY	SETTINGS DEVELOPERS	VPGRADE NOW
← Add SAML Te	est Connector (SP)		CANCEL SAVE
		Configuration	
Portal	Display Name Visible in portal Constraints of the second s	spect-ratio of 2.6.1 as either a	Square Icon Upload a square icon at least 512x512px as either a transparent. PNG or .SVG

- 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**.

	APPS DEVICES	ACTIVITY S	ETTINGS	DEVELOPERS	🖌 UPG	RADE NOW	
← SAML Test Cor	nnector (SP)					IS 🔻 SAV	/E
Info	Configuration	Parameters	Rules	SSO Access	Users Privilege	S	
Application Details	RelayState						
	Audience						
	Recipient						
	ACS (Consum	ner) URL Validat	tor*				
	*Required. Re	egular expressio	n - Validates t	he ACS URL when initi	ated by an AuthnReque	st	
	ACS (Consun	ner) URL*					
	*Required						

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**.

onelogin users A	PPS DEVICES ACTIVITY	SETTINGS	DEVELOPERS		🖋 UPGRAD	ENOW	ell .
← SAML Test Con	nector (SP)				MORE ACTIONS	•	SAVE
Info	Configuration Parameter	ers Rules	SSO Access	Users	Privileges		
Enable SAML2.0	Sign on method SAML2.0 X.509 Certificate Standard Strength Ce Change View Details SAML Signature Algori SHA-256 Issuer URL https://app.onelogin SAML 2.0 Endpoint (HTTP)	thm com/saml/metada	it) ata/788cf95f-856e-42	0 IO			
	https://softworveiss.cl	les analogin avera	huid, hamil, hitp-redi	10			

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

onelogin	USERS	APPS	DEVICES	ACTIVITY	SETTINGS	DEVELOP	PERS		🗲 UPGRA	DE NOV	v 🏥
← SAMI	L Test Co	onneo	ctor (SP)					м	ORE ACTIONS	•	SAVE
	Info	Cor	figuration	Parameter	s Rules	SSO	Access	Users	Privileges		
			All roles	✓ All grou	ps 👻						
User											
Current Us	er Name										

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

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

onelogin	USERS	APPS	DEVICES	ACTIVITY	SETTINGS	DEVELOPERS	VPGRADE NOW
← SAM	All User Roles	s	(SP)				MORE ACTIONS

- b. Select a needed user.
- c. Go to the **Applications** tab and then select the **Plus** (+) icon.

onelogin u	SERS APPS	DEVICES	ACTIVITY	SETTINGS	DEVELOPERS	VPGRADE NOW
← iters iss						MORE ACTIONS + SAVE USER
		User In	nfo Auth	entication	Applications	Activity
Roles		Applicat	ions			+
Default		1 Demo	Application	Darrow Aug	and the second sec	Admin-configured
		Devel Applicat		Darris Ag		Admin-configured

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

Assign New Lo	gin To	ign New	
This login will override any apps as	signed via roles	i.	
Select Application			-
		CANCEL	CONTINU

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 Mn	nisdemo Login For
Enabled Email (NameID)	Allow users to sign in
	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		H	Default Chang
DETAILS ORGANIZATI	IONS USERS PASSWORD DICTIONARIES	RESOURCES SECURIT	ΤΥ	
Update Cancel				
Name:*	Domain Name	Authentication:	HTTP Redirect	
Description:	Description	Failed Attempts:*	255	(i)
Session Timeout, m:	20	Endpoint URL:		
Mobile Token Expiration, h:		Identifier URL:		
Default UI:	Default Update Users	SSO Message.*	Please provide your SSO credentials for further	()
Status:	Active	Require force authe	ntication.	
		Require device regis	stration.	
		Restrict IP Addresse	^{15.}	

- 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 <u>Integration</u> section, step 9).
 - c. Select **OK**.

Upload Metada	ta		×
Upload From: Identifier URL*	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.

ORGANI	ZATIONS USERS	PASSWORD DICTIONARIES	RESOURCES SEC	URITY
/ 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 force authentication.	
			Do not require device registration.	
			Do not restrict IP Ac	draggar

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.

OPTIC	ONS ORGANIZATIONS SECURITY		
✓ Edit Vali	date Email		
Jser 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		
Status:	Active		

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