

envi



Azure Active Directory Single Sign-On

Integration Guide



Table of Contents

Introduction.....	2
Integration	3
Envi Configuration	8
Troubleshooting.....	10

Introduction

Azure Active Directory (Azure AD) is a Microsoft Azure service designed for efficient identity and access management. It helps to protect sensitive data and applications on-premises and in the cloud with integrated multi-factor authentication, ensuring secure local and remote access.

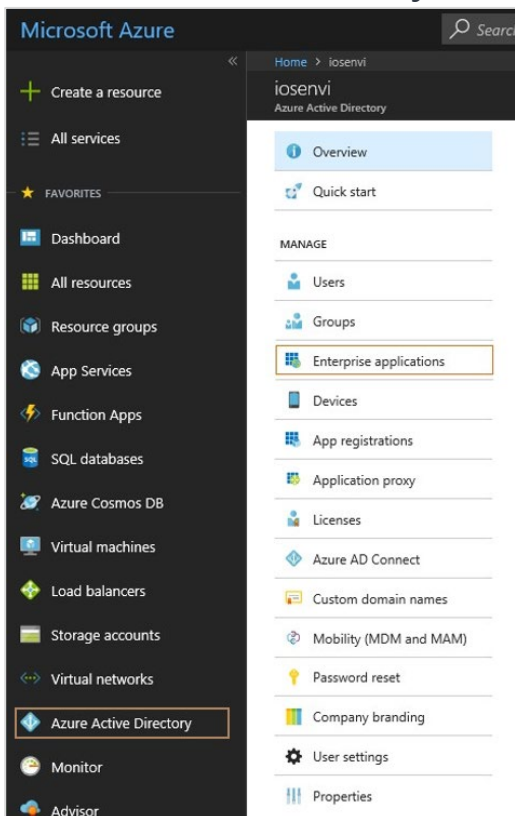
Azure AD also offers a suite of powerful tools, including comprehensive reporting, analytics, and self-service capabilities to reduce costs and enhance security. The provider allows your end-users to authenticate to the **Envi** application using their **Azure AD** account.

By integrating a **single sign-on (SSO)** with **Azure AD**, you can simplify your entire organization's password management process and avoid problematic user password management.

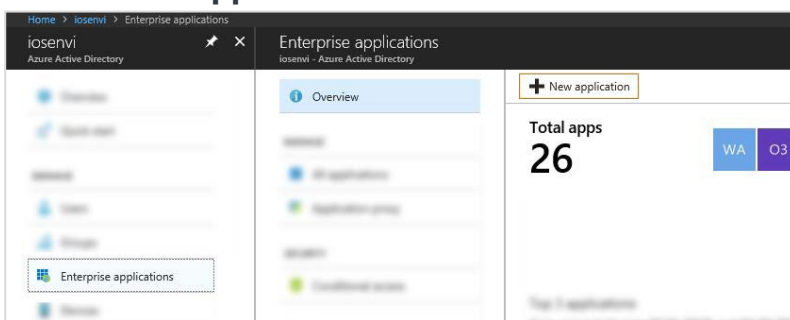
Integration

Perform the following steps to set up **SSO** with the **Azure AD** provider.

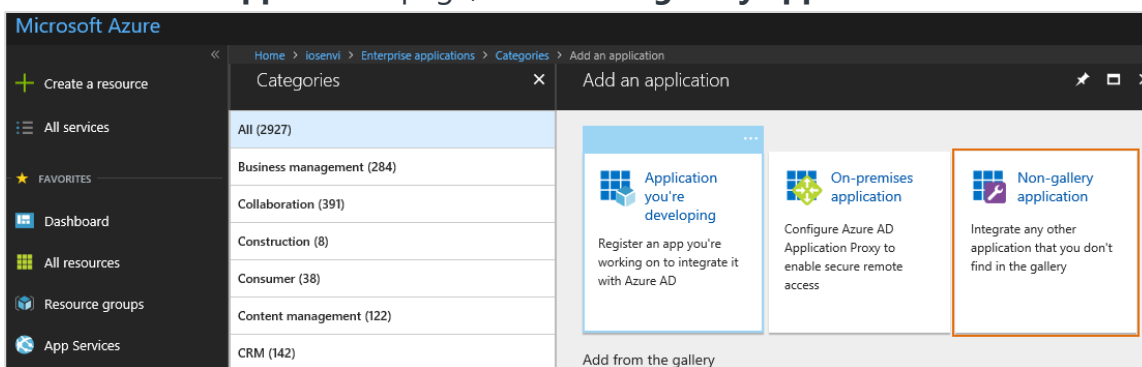
1. Sign in to the [Azure](#) portal.
2. Go to **Azure Active Directory** > **Enterprise applications**.



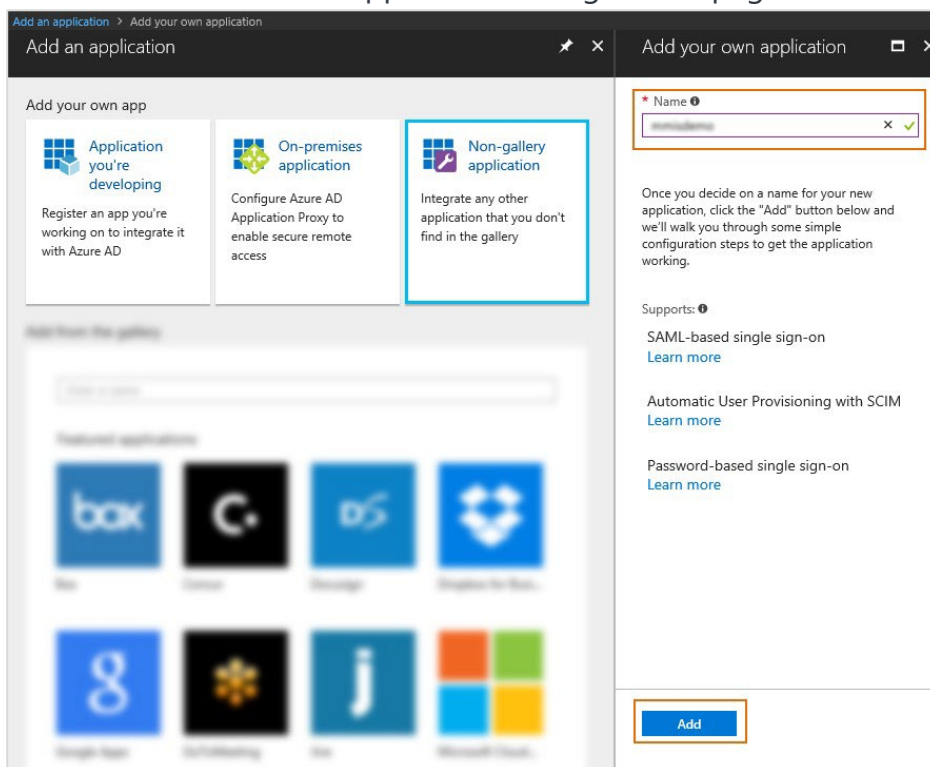
3. Select **+New application**.



4. On the **Add an application** page, select **Non-gallery application**.

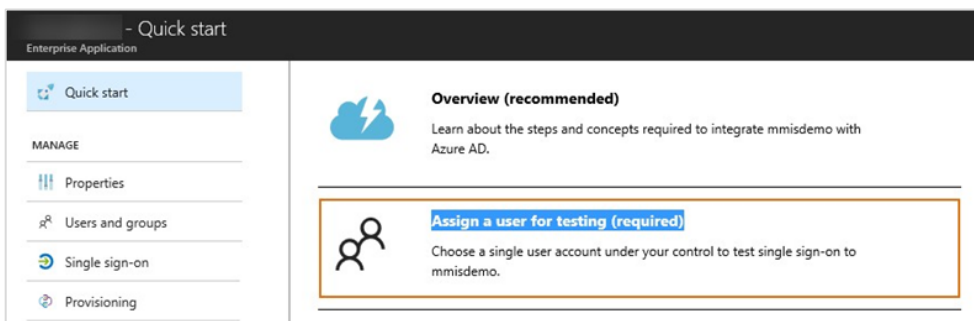


- In **Add your own application**, enter a name for a new application (for example, envi.net), and then select the **Add** button. After you have added an application, you will be redirected to the application configuration page.

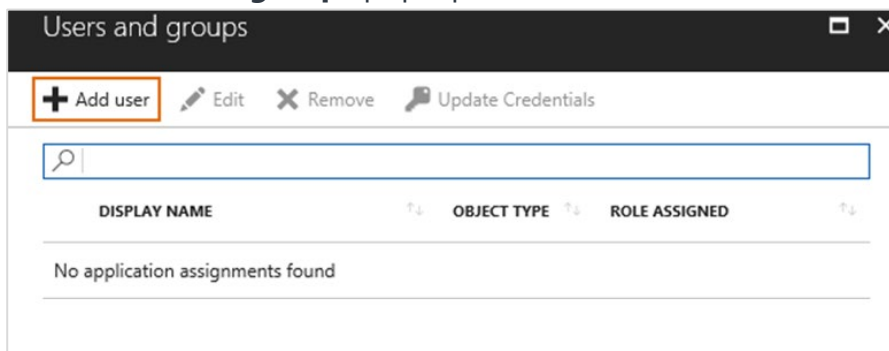


- On the **Quick start** page, select **Assign a user for testing (required)**.

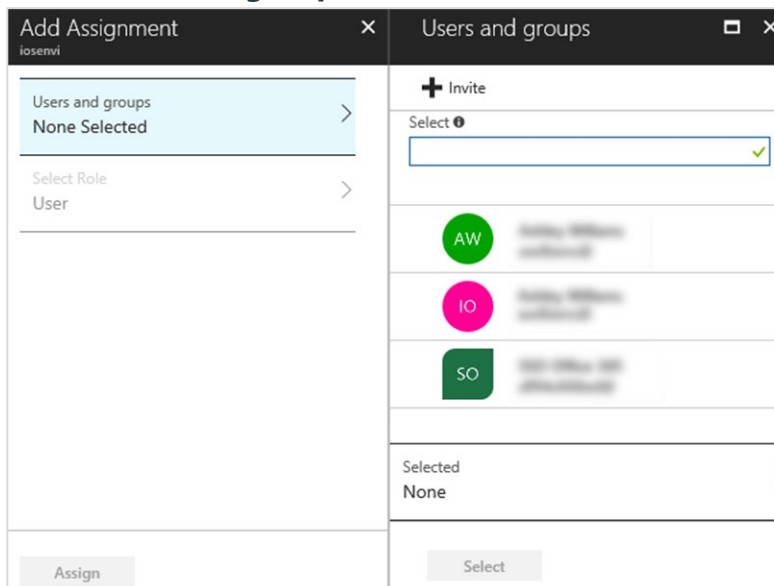
Note: You should have at least one preconfigured AD user to proceed.



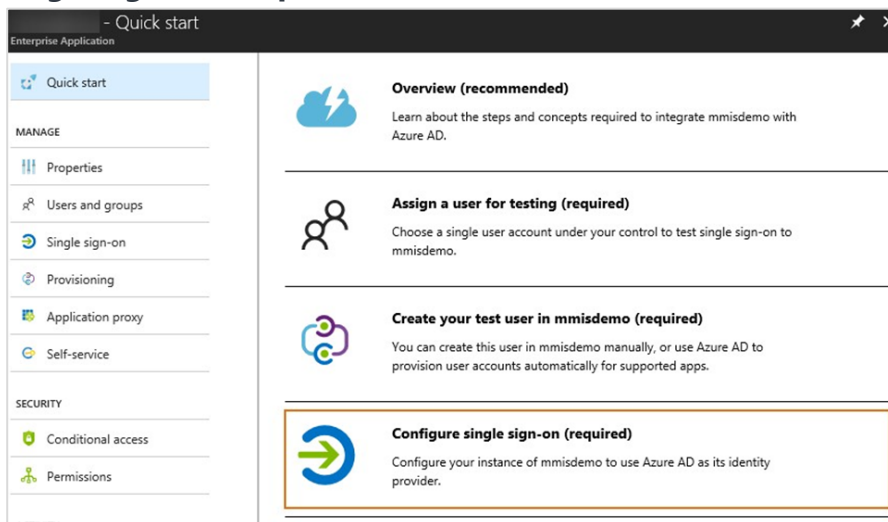
- In the **Users and groups** pop-up window, select the **+Add user** button.



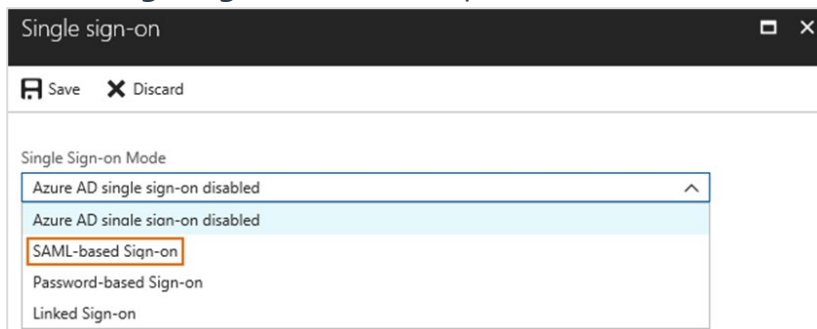
8. On the **Add Assignment** page, perform the following steps:
 - a. Select **Users and groups**.
 - b. Use the search box to select all needed users.
 - c. When all needed ones are added, select the **Select** button.
 - d. Select the **Assign** button.
 - e. Close **Users and groups**.



9. Then, you will be redirected to the **Quick start** page again. Here, select **Configure single sign-on (required)**.



10. In the **Single sign-on Mode** dropdown list, select **SAML-based Sign-on**.



11. On the **Single sign-on** page, do the following steps:

- a. In the **Identifier** box, enter an application base URL + /Account.
- b. In the **Reply URL** box, enter an application base URL + /Account/Acs.

Single sign-on

Save Discard

Single Sign-on Mode

SAML-based Sign-on

Federated single sign-on enables rich and secure authentication to applications using the SAML protocol. Follow the steps below to connect this application to Azure AD using SAML.

[View mmsidemo configuration tutorial](#)

mmsidemo Domain and URLs

Input the URLs and other details about your mmsidemo tenant into Azure AD.

* Identifier ✓

* Reply URL ✓

Show advanced URL settings

12. Move through the page to the **User Attributes** section and then perform the following steps:

- a. In the **User Identifier** dropdown list, make sure that the **user.userprincipalname** value is selected.
- b. Select the **View and Edit all other user attributes** checkbox.
- c. Delete all other attributes except for the **user.userprincipalname** (to do that, select the ellipsis (...) button next to a needed namespace > **Delete**.)

Single sign-on

Save Discard

User Attributes [Learn more](#)

Edit the user information sent in the SAML token when user sign in to mmsidemo.

User Identifier ✓

View and edit all other user attributes

SAML Token Attributes

NAME	VALUE	NAMESPACE
givenname	user.givenname	http://schemas.xmlsoap.or... <input type="button" value="..."/>
surname	user.surname	Pin to dashboard <input type="button" value="Delete"/>
emailaddress	user.mail	
name	user.userprincipalname	http://schemas.xmlsoap.or... <input type="button" value="..."/>

13. In the **SAML Signing Certificate** section, manage the certificate used by **Azure AD** to sign **SAML** tokens issued for your application. You'll find a default certificate created automatically. If needed, you can create a new one and specify different certificate signing options. Here, you also need to perform the following steps:
- Download the **Metadata XML** file and save it for further usage in the **Envi** application.
 - Enter **Notification Email**.
 - Select **Save** at the top of the page.

Save
 Discard

NAME	VALUE	NAMESPACE
name	user.userprincipalname	http://schemas.xmlsoap.or... ..

[Add attribute](#)

SAML Signing Certificate [Learn more](#)

Manage the certificate used by Azure AD to sign SAML tokens issued to mmisdemo.

STATUS	EXPIRATION	THUMBPRINT	DOWNLOAD
Active			Certificate (Base64) Certificate (Raw) Metadata XML

[Create new certificate](#)

Show advanced certificate signing settings

[Learn more](#)

* Notification Email

mmisdemo Configuration
mmisdemo must be configured to use Azure AD as a SAML identity provider. Click below to view instructions on how to do this.

Now, the **SSO** configuration is ready.

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 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 Authentication: HTTP Redirect **Upload Metadata**

Description: Description Failed Attempts*: 255 ⓘ

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 logins ⓘ

Status: Active 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 **File**.
 - b. In the **Select File** box, enter the path to the saved metadata file location (For more information, go to the [Integration](#) section, step 13).
 - c. Select **OK**.

Upload Metadata ✕

Upload From: File

Select File*:

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 Authentication: HTTP Redirect

Description: Description Failed Attempts: 255

Session Timeout, m: 20 **Endpoint URL: http://login.microsoftonline.com/f895cf5e-95fc-493c...**

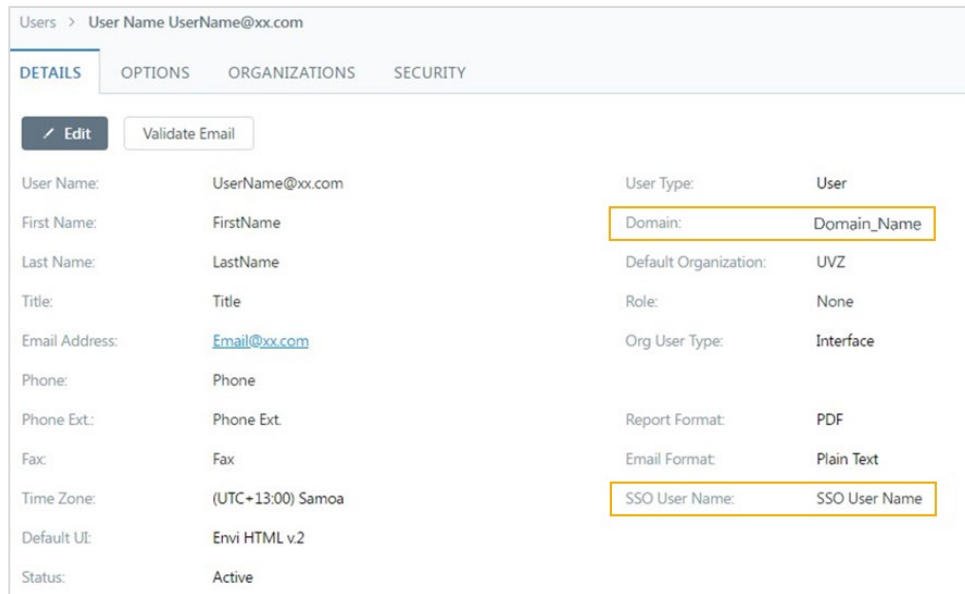
Mobile Token Expiration, h: **Identifier URL: http://app.onelogin.com/saml/...**

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 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 **Azure AD** 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 **Azure AD SSO**.

Troubleshooting

In the **Troubleshooting** section, you will discover troubleshooting solutions for common **SSO** issues. If you encounter a problem during the sign-in, make sure you have followed all steps outlined in the tutorial for the configuration. Also, there can be the following errors.

Password page is shown after entering a username

After entering your username, you may be redirected to the page prompting you to enter a password. In this case, please double-check that you've entered the correct **SSO** username and that you are within the domain configured for remote authentication. If the issue persists, please contact your administrator for troubleshooting assistance.

Incorrect page after entering a username

If you are redirected to an incorrect page after entering your username, please make sure that the correct endpoint URL and identifier URL are loaded.

Note: You can upload metadata with correct values by downloading it from the **Set-up Single Sign-On with SAML** page. For this, go to the **SAML Signing Certificate** section, and then select **Download** to receive the **Federation Metadata XML**.

Not assigned role in the application

After entering the username, you are redirected to the correct **SSO** endpoint URL. Then, the following message is shown: *The signed-in user 'username' is not assigned to a role for the application.* In this case, please make sure that you are added to **Users and Groups** in the **Envi** application of **Azure RD**. If needed, contact your administrator for assistance.

Error after signing in to the SSO application

After entering the username, you are redirected the correct endpoint URL and signed in to the **Envi** application, and then you may encounter an error. To resolve this, go to **Envi User Details** and ensure that your usernames in **Envi** and **SSO** match.