



Azure Active Directory Single Sign-On

Integration Guide

Introduction

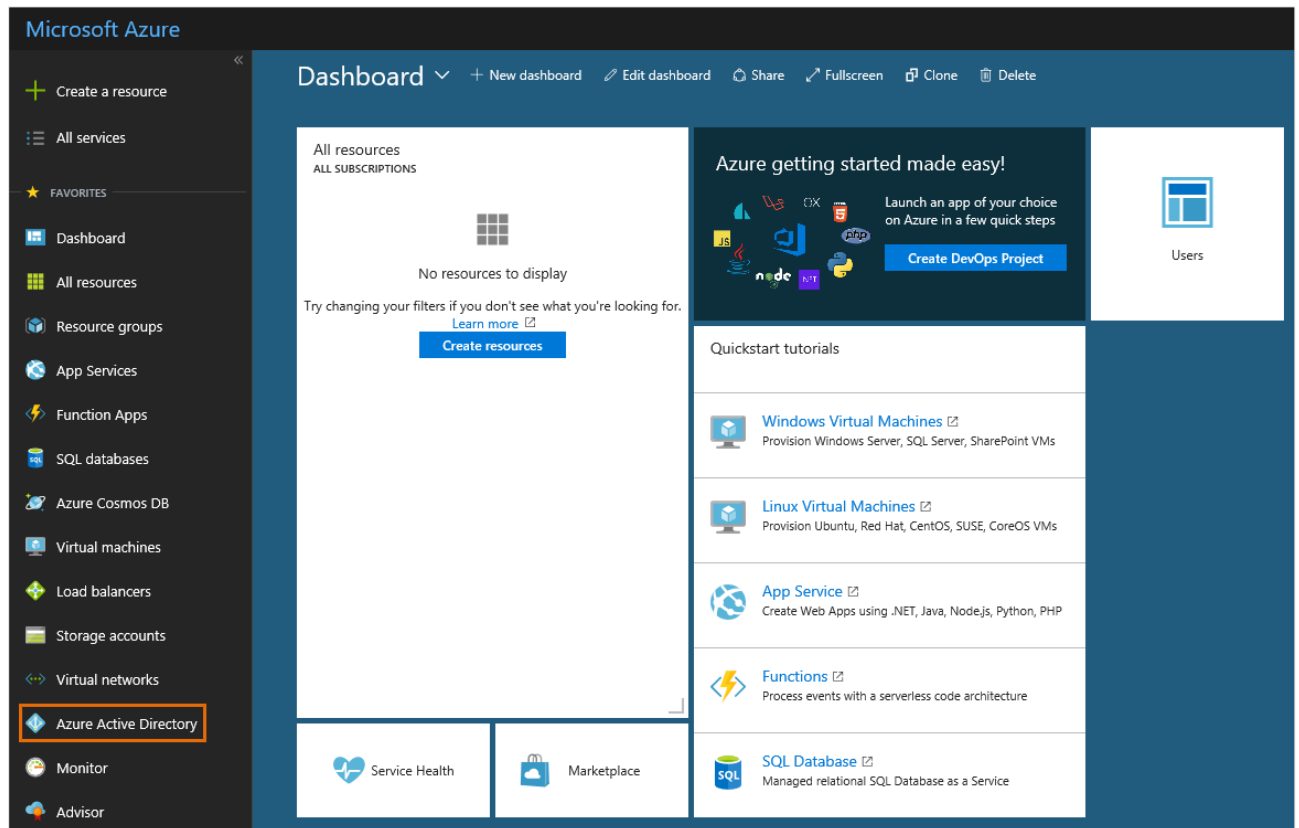
Azure Active Directory (Azure AD) is a Microsoft Azure service which provides identity and access management. It helps to protect sensitive data and applications both on-premises and in the cloud with integrated multi-factor authentication ensuring secure local and remote access. Azure AD also offers comprehensive reports, analytics, and self-service capabilities to reduce costs and enhance security. This provider gives your end users the possibility to authenticate to the Envi application using their Azure AD account.

With this SSO integration, you can simplify your entire organization's password management process and avoid problematic user password management.

Integration

This step-by-step guide explains how to set up single sign-on with the Azure AD provider.

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



3. Go to Enterprise applications.

The screenshot shows the Microsoft Azure portal interface. On the left is a navigation pane with various services. The main area displays the 'iosenvi' Azure Active Directory instance. The 'Enterprise applications' link in the 'MANAGE' section is highlighted with an orange box. On the right, there is a 'Sign-ins' chart and a 'What's new in Azure AD' section.

Navigation Pane (Left):

- Create a resource
- All services
- FAVORITES
- Dashboard
- All resources
- Resource groups
- App Services
- Function Apps
- SQL databases
- Azure Cosmos DB
- Virtual machines
- Load balancers
- Storage accounts
- Virtual networks
- Azure Active Directory
- Monitor
- Advisor

Main Content Area (Center):

Home > iosenvi

iosenvi
Azure Active Directory

MANAGE

- Overview
- Quick start
- Users
- Groups
- Enterprise applications** (highlighted)
- Devices
- App registrations
- Application proxy
- Licenses
- Azure AD Connect
- Custom domain names
- Mobility (MDM and MAM)
- Password reset
- Company branding
- User settings
- Properties

Right Panel:

Switch directory Delete directory

iosenvi.onmicrosoft.com

iosenvi
Azure AD Premium P2

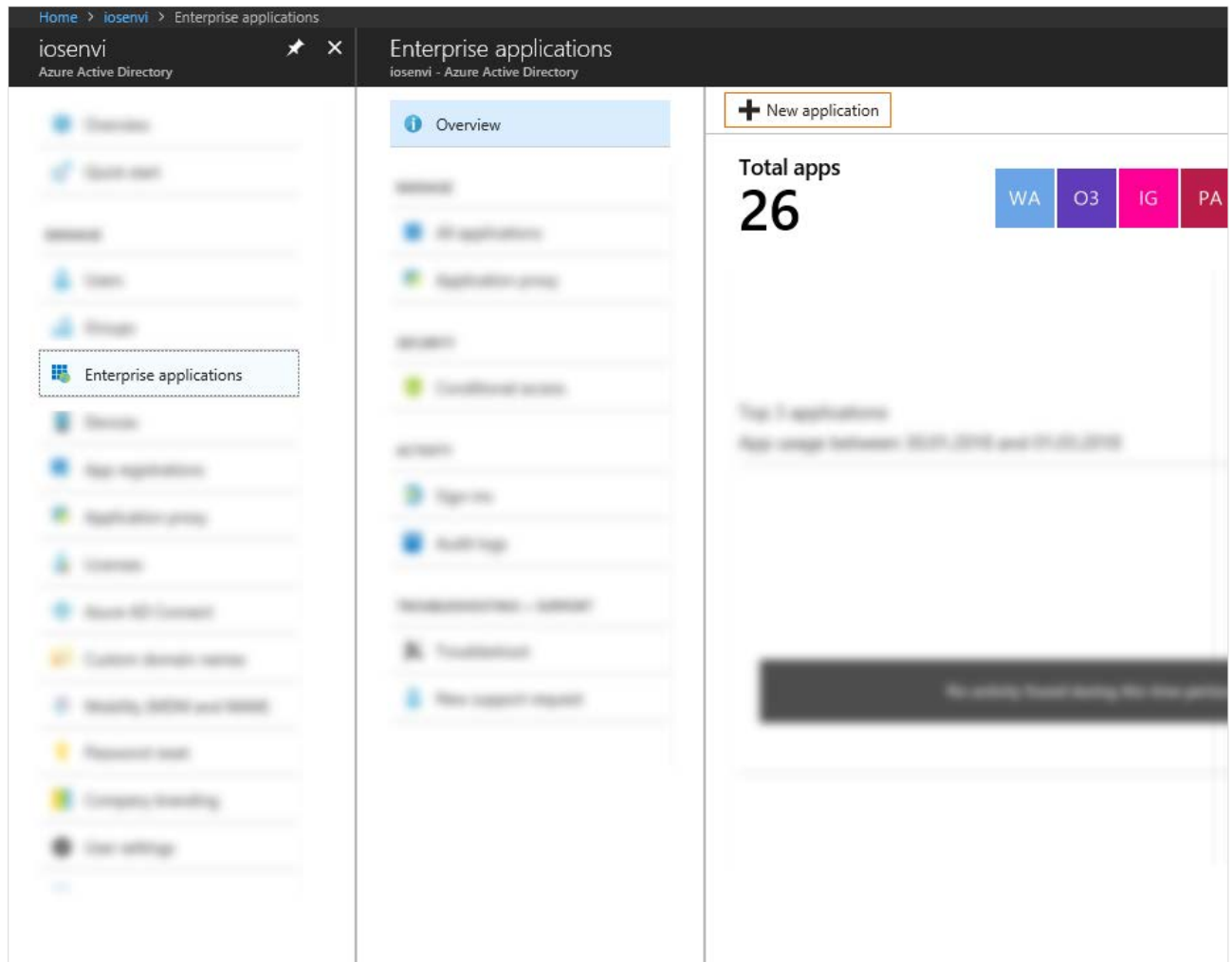
Sign-ins

Line chart showing sign-in activity from 4 Dec to 25 Dec. The y-axis ranges from 0 to 100.

What's new in Azure AD
Stay up to date with the latest release notes and blog posts.
16 entries since December 15, 2017. [View archive](#)

<input checked="" type="checkbox"/> All services	(16)	New feature
<input type="checkbox"/> 3rd Party Integration	(2)	Enterprise Apps - 3rd Party Integration
<input type="checkbox"/> Identity Security & Prote...	(1)	January 20, 2018
<input type="checkbox"/> SSO	(2)	
<input type="checkbox"/> Directory	(2)	New Federated Apps available in
<input type="checkbox"/> Identity Lifecycle Manage...	(1)	

4. Click + New application.



5. Select Non-gallery application on the top of the screen.

The screenshot shows the Microsoft Azure portal interface. On the left is a navigation pane with 'All services' and 'FAVORITES'. The main area is titled 'Add an application' and contains three cards: 'Application you're developing', 'On-premises application', and 'Non-gallery application'. The 'Non-gallery application' card is highlighted with an orange border. Below these cards is a section 'Add from the gallery' with a search bar and a grid of featured applications including Box, Concur, Docusign, Dropbox for Business, Google, Jira, and others.

Microsoft Azure

Home > Iosenvi > Enterprise applications > Categories > Add an application

Categories

- All (2927)
- Business management (284)
- Collaboration (391)
- Construction (8)
- Consumer (38)
- Content management (122)
- CRM (142)
- Data services (135)
- Developer services (104)
- E-commerce (72)
- Education (123)
- ERP (67)
- Finance (243)
- Health (57)
- Human resources (248)
- IT infrastructure (157)
- Mail (32)

Add an application

- Application you're developing**
Register an app you're working on to integrate it with Azure AD
- On-premises application**
Configure Azure AD Application Proxy to enable secure remote access
- Non-gallery application**
Integrate any other application that you don't find in the gallery

Add from the gallery

Enter a name

Featured applications

- Box
- Concur
- Docusign
- Dropbox for Business
- Google
- Jira
- Microsoft Dynamics 365
- Microsoft Teams

6. On the **Add your own application** section, enter the application name (for example, **envi.net**) and click the **Add** button.

The screenshot shows the 'Add your own application' dialog in Azure AD. The dialog has a dark header with the title 'Add your own application'. Below the header, there are three tabs: 'Application you're developing', 'On-premises application', and 'Non-gallery application'. The 'Non-gallery application' tab is selected and highlighted with a blue border. Below the tabs, there are three cards. The first card is 'Application you're developing' with a blue icon and text 'Register an app you're working on to integrate it with Azure AD'. The second card is 'On-premises application' with a green icon and text 'Configure Azure AD Application Proxy to enable secure remote access'. The third card is 'Non-gallery application' with a blue icon and text 'Integrate any other application that you don't find in the gallery'. Below the cards, there is a section titled 'Add from the gallery' with a search bar and a grid of application icons. To the right of the main content, there is a sidebar with a 'Name' field containing 'envi.net' and a green checkmark. Below the field, there is a paragraph of text: 'Once you decide on a name for your new application, click the "Add" button below and we'll walk you through some simple configuration steps to get the application working.' Below this text, there is a section titled 'Supports:' with three items: 'SAML-based single sign-on', 'Automatic User Provisioning with SCIM', and 'Password-based single sign-on'. Each item has a 'Learn more' link. At the bottom of the sidebar, there is a blue 'Add' button.

After adding the application, you will be navigated to the application configuration page.

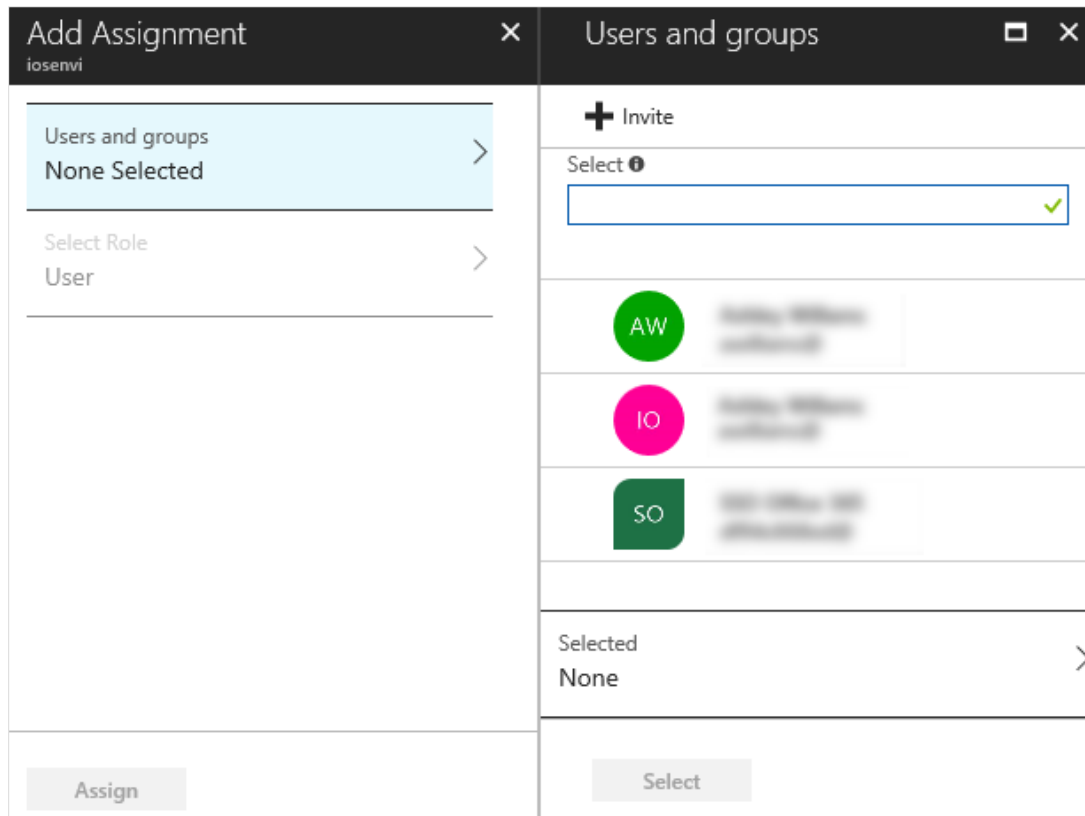
7. You should have at least one preconfigured AD user. Click the **Assign a user for testing (required)** section.

The screenshot shows the 'Quick start' page for an 'Enterprise Application' in the Azure portal. The left-hand navigation pane is expanded, showing sections for 'MANAGE' (Properties, Users and groups, Single sign-on, Provisioning, Application proxy, Self-service), 'SECURITY' (Conditional access, Permissions), 'ACTIVITY' (Sign-ins, Audit logs), and 'TROUBLESHOOTING + SUPPORT'. The main content area on the right is titled 'Quick start' and contains several sections: 'Overview (recommended)' with a lightning bolt icon; 'Assign a user for testing (required)' with a group of people icon and a blue highlight box; 'Create your test user in mmisdemo (required)' with a person icon; 'Configure single sign-on (required)' with a circular arrow icon; 'Set up conditional access (optional)' with a shield icon; and 'Configure self-service (optional)' with a key icon.

8. Click the **+ Add user** button.

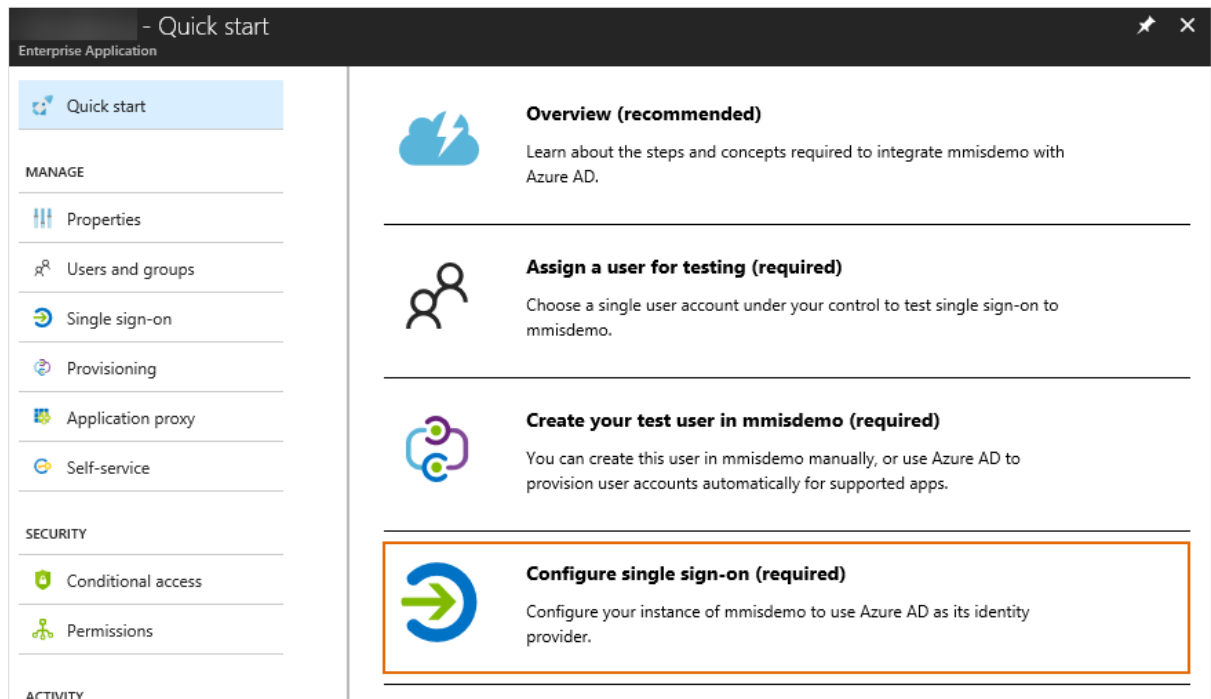
The screenshot shows the 'Users and groups' page in the Azure portal. At the top, there's a search bar and a toolbar with buttons for '+ Add user', 'Edit', 'Remove', and 'Update Credentials'. Below the toolbar is a table with columns for 'DISPLAY NAME', 'OBJECT TYPE', and 'ROLE ASSIGNED'. The table is currently empty, displaying the message 'No application assignments found'.

9. On the **Add Assignment** section, click the **Users and Groups** and select the appropriate user. Then click the **Select** button.

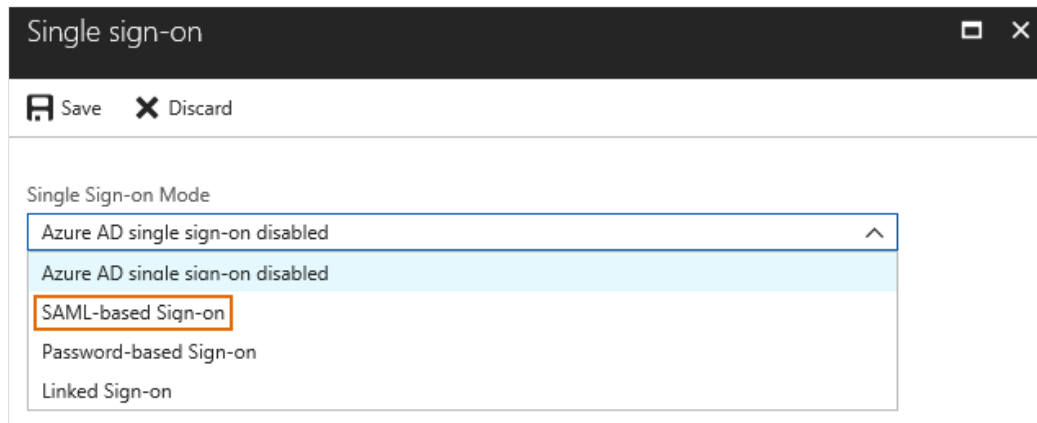


10. Click **Assign**, and then close the **Users and Groups** section.

11. Select the **Configure single sign-on (required)** section.

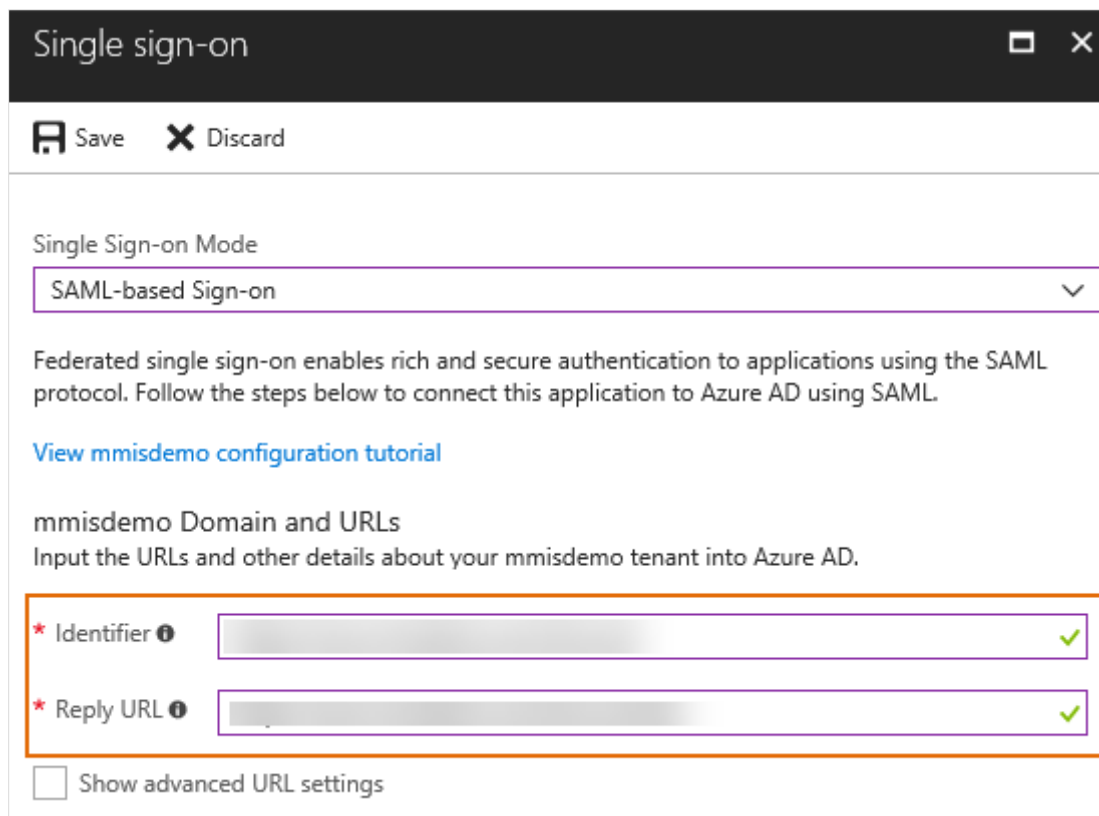


12. On the **Single sign-on** section, select the **SAML-based Sign-on** option.



The screenshot shows the 'Single sign-on' configuration window. At the top, there are 'Save' and 'Discard' buttons. Below them is the 'Single Sign-on Mode' dropdown menu. The menu is open, showing four options: 'Azure AD single sign-on disabled', 'Azure AD single sign-on disabled' (highlighted in light blue), 'SAML-based Sign-on' (highlighted with an orange border), 'Password-based Sign-on', and 'Linked Sign-on'.

13. Fill in the **Identifier** (application base URL + /Account) and **Reply URL** (application base URL + /Account/Acs) fields.



The screenshot shows the 'Single sign-on' configuration window with 'SAML-based Sign-on' selected in the dropdown. Below the dropdown, there is a description of federated single sign-on and a link to 'View mmisdemo configuration tutorial'. Under the heading 'mmisdemo Domain and URLs', there is a prompt to 'Input the URLs and other details about your mmisdemo tenant into Azure AD.' Below this, there are two input fields: 'Identifier' and 'Reply URL'. Both fields are filled with placeholder text and have a green checkmark icon to their right. The entire section containing these fields is highlighted with an orange border. At the bottom, there is a checkbox labeled 'Show advanced URL settings'.

14. Scroll the page down and make sure that **user.userprincipalname** is selected as a **User Identifier**. Select the **View and Edit all other user attributes** check box, and then delete all other attributes except for **user.userprincipalname**.

Single sign-on

Save Discard

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

* Identifier ✓

* Reply URL ✓

☐ Show advanced URL settings

[Test SAML Settings](#)
Please Save the values to test the settings.

User Attributes [Learn more](#)

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

User Identifier ▼

☒ View and edit all other user attributes



SAML Token Attributes

NAME	VALUE	NAMESPACE
givenname	user.givenname	http://schemas.xmlsoap.or...
surname	user.surname	
emailaddress	user.mail	
name	user.userprincipalname	http://schemas.xmlsoap.or...

[Pin to dashboard](#)

Delete

15. Scroll down and manage the certificate used by Azure AD to sign SAML tokens issued for your application. For this:
- There is a default certificate created automatically. But you can create the new one and specify different certificate signing options.
 - Download the **Metadata XML** file and save it for further usage in the Envi application.

 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	01.03.2021	D6B8B02410352805A55DB9928DAD621B4383...	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.

- Specify **Notification Email**, and then click **Save** on the top of the page.

At this point, the single sign-on configuration is ready.

Envi Configuration

In the Envi application, set up the following domain and user configurations:

1. Sign in 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 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.

4. Select the saved metadata file (step 15), and then click **OK**.

Upload Metadata

Upload From: File

Select File: mmisdemo.xml

OK Cancel

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 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

- While creating user, select the needed domain with **HTTP Redirect** type of authentication. In the **SSO User Name** field enter the username from the Azure ID 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	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 sign in the Envi application using Azure Active Directory single sign-on.

Troubleshooting

This guide will help you find troubleshooting information about common issues regarding SSO. If you face a problem while sign in, make sure you have followed all steps in the tutorial for configuring the application. Also, there can be the following errors.

Password page appears after entering username

After entering the username, you may be redirected to the page prompting you to enter a password. In such case, check if you entered the correct SSO username. Also, you can be within the domain configured for the remote authentication. To troubleshoot this issue, contact your administrator.

Incorrect page after entering username

After entering the username, you may be redirected to the incorrect page. In such case, verify if correct endpoint URL and identifier URL are loaded for you.

Note: You can upload metadata to Envi 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 click **Download** to receive **Federation Metadata XML**.

Not assigned role in application

After you entered the username and were redirected to the correct SSO endpoint URL, the following message appears:

The signed in user 'username' is not assigned to a role for the application.

In such case, make sure that you are added to **Users and Groups** in the Envi application of Azure RD. For this, contact your administrator.

Error after sign in SSO application

After you have entered the username, were redirected to the correct endpoint URL, and signed in the Envi application, an error appears. Navigate to **Envi User Details** and ensure that usernames in Envi and SSO match.