

# How to Sign in to SanerNow through Azure AD using SAML SSO

## Pre-requisites for signing in via Azure AD SSO

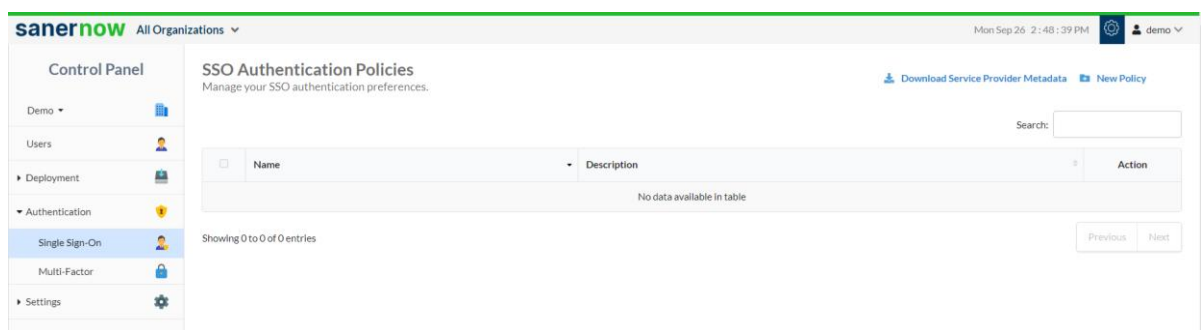
Following are the pre-requisites to configure Azure AD SSO

- Identity Provider Single Sign-On URL
- X.509 Certificate
- Issuer ID

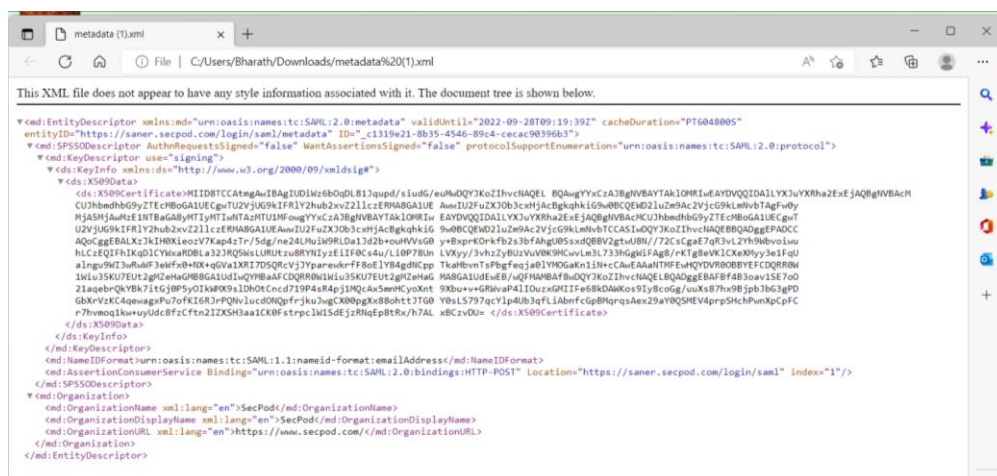
Follow the steps given below to retrieve the information mentioned above.

## Steps to configure SAML-based SSO

1. Sign in to saner.secpod.com
2. Go to the **Control Panel**
3. Under Settings, select **SSO Authentication**

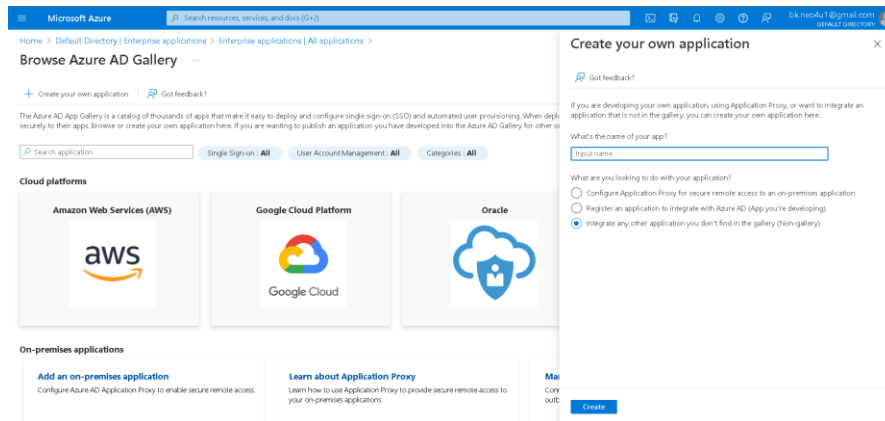


4. Click on **Download SSO metadata file**.
5. Open the downloaded metadata file from your browser or a text editor.



6. Copy and save the Entity ID and ACS URL from your downloaded metadata file.
7. Sign in to your organization's Azure AD Admin Console.

8. Click **Enterprise Applications** in the left menu.
9. Click **New Applications**, and click on **Create your Own Applications**.
10. Select Integrate any other applications, enter the app's name (SanerNow App), and click Create.



11. Once the app is created, click Setup Single Sign-on under Getting Started.
12. Under **Select a single sign-on method**, select **SAML**
13. Edit the Basic SAML configuration
14. Enter the ACS URL and the Entity ID, then click on Save.

1

### Basic SAML Configuration

✎ Edit

Identifier (Entity ID)	https://saner.secpod.com/login/saml/metadata
Reply URL (Assertion Consumer Service URL)	https://saner.secpod.com/login/saml
Sign on URL	Optional
Relay State (Optional)	Optional
Logout Url (Optional)	Optional

15. Edit Attributes & Claims
16. Click on Add New Claim, enter Email as Claim name
17. Under **Choose Name format**, select attribute as Source and user.mail as source attribute.

2

### Attributes & Claims

✎ Edit

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
bk.neo4u1@gmail.com	user.mail
Email	user.mail
Unique User Identifier	user.userprincipalname

18. Click on **Save**
19. Download the metadata XML file and base64 certificate from the SAML signing certificate section.

3

SAML Certificates

Token signing certificate

Status

Active

Thumbprint

8013E6C1DBD7F28A5F76DF568B82582F94C6FAC2

Expiration

9/1/2025, 1:13:41 PM

Notification Email

bk.neo4u1@gmail.com

App Federation Metadata Url

https://login.microsoftonline.com/1d30b3e3-dc93-...

Certificate (Base64)

[Download](#)

Certificate (Raw)

[Download](#)

Federation Metadata XML

[Download](#)

Edit

Verification certificates (optional) (Preview)

Required

No

Active

0

Expired

0

Edit

20. Copy the Identity Provider Single Sign-On URL and identity provider issuer and download or copy the X.509 Certificate from the downloaded metadata and base64 certificate file.
21. Return to the SSO authentication page in SanerNow.
22. Configure SSO in SanerNow using the downloaded certificate and copied URLs from Azure AD by following the steps given below:

- Under SSO Authentication, click on the new SSO policy.

SSO Authentication Policy

Name (\*)

Description (\*)

Issuer ID (\*)

SSO URL (\*)

Certificate (\*)

Signed Authentication

☐

Cancel

Create

- Enter Issuer ID, SSO Url, and Certificate from Azure AD.
- Specify the required name and description for the SSO policy
- Enable signed authentication if you have configured it in Azure AD
- Click on Create

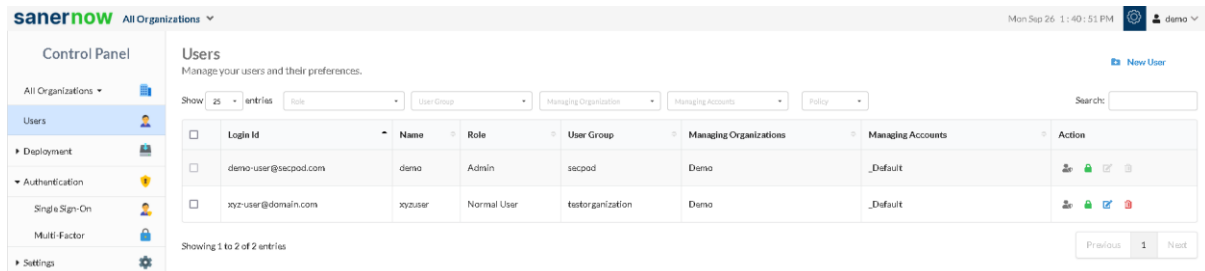
### Steps to Assign users to the app in Azure AD

- Select the created enterprise application, and click on Users & Groups from the left side menu.
- Click on Add user or group. Select the users to be assigned and click on the Select button.
- Click on Assign.

## Assign SSO policy to SanerNow Users

**Note:** Before assigning the users, ensure that the User login ID in SanerNow matches the Azure AD User name

- Go to Control Panel. Click on Users.











Control Panel

Users

Manage your users and their preferences.

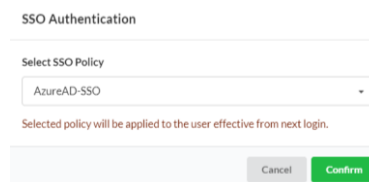
Show 25 entries Role User Group Managing Organization Managing Accounts Policy Search

	Login Id	Name	Role	User Group	Managing Organizations	Managing Accounts	Action
<input type="checkbox"/>	demo-user@secpod.com	demo	Admin	secpod	Demo	_Default	   
<input type="checkbox"/>	xyz-user@domain.com	xyzuser	Normal User	testorganization	Demo	_Default	   

Showing 1 to 2 of 2 entries

Previous 1 Next

- Select the users to whom Azure AD policy should be applied
- Under Actions, select the "Enforce SSO authentication" button
- Select the Azure AD policy from the drop-down



SSO Authentication

Select SSO Policy

AzureAD-SSO

Selected policy will be applied to the user effective from next login.

Cancel Confirm

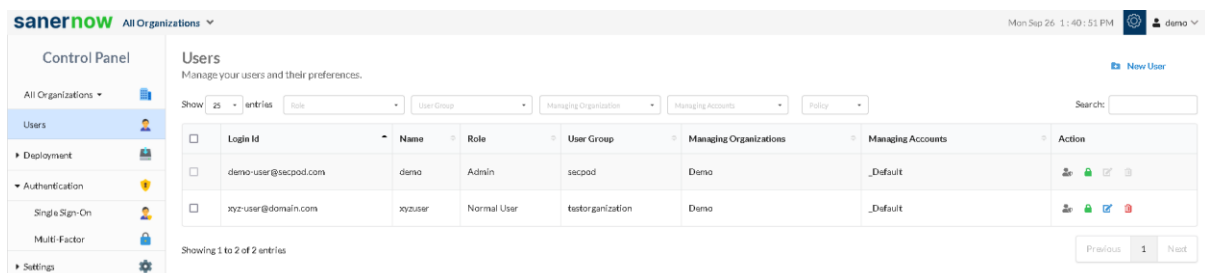
- Click on Confirm

## How to apply SSO Policy to the New SanerNow user

Step 1: Log in to SanerNow and then click Control Panel at the top-right to access the Control Panel page.

Step 2: **All Organizations** are selected from the drop-down by default on the control panel page. If the admin has created only one organization, the page automatically selects that organization and shows its accounts.

Step 3: Click the Users section in the Control Panel.











Control Panel

Users

Manage your users and their preferences.

Show 25 entries Role User Group Managing Organization Managing Accounts Policy Search

	Login Id	Name	Role	User Group	Managing Organizations	Managing Accounts	Action
<input type="checkbox"/>	demo-user@secpod.com	demo	Admin	secpod	Demo	_Default	   
<input type="checkbox"/>	xyz-user@domain.com	xyzuser	Normal User	testorganization	Demo	_Default	   

Showing 1 to 2 of 2 entries

Previous 1 Next

Step 4: Click New User on the top right corner of the Users page.

**New User**

Login Id (\*)

Name (\*)

User Group (\*)

SSO Policy

Password (\*)

Confirm Password (\*)

MFA Policy

Role

Managing Organizations (\*)

Manage ☒ Full Access ☐ Read Only ☐ Custom

Step 5: Specify the Login ID, Name, Organization, and Password.

Step 6: Select the role of the user from the drop-down menu.

Step 7: Select the managing organizations from the drop-down menu

Step 8: Select the created SSO policy from the drop-down to assign an SSO Policy to the user.

Step 9: Click the Create button to apply the SSO policy to the new user

### Test the SAML configuration

Test if the configuration is working correctly using the following steps

Via SP-initiated flow:

1. Go to the SanerNow sign-in page.
2. Enter your email address, and click Next. You will be redirected to Azure AD for authentication.
3. If you have not already signed in to Azure AD, enter your Azure AD credentials to sign in. You will be automatically redirected back to SanerNow and will be signed in.

Via IdP-initiated flow:

1. Sign in to the Azure AD end-user dashboard.
2. Click on the SAML app (SanerNow app) you have configured for SanerNow. You will be redirected to SanerNow and will be signed in.