

How to Sign in SanerNow through Azure AD using SAML SSO

Pre-requisites for signing in via Azure AD SSO

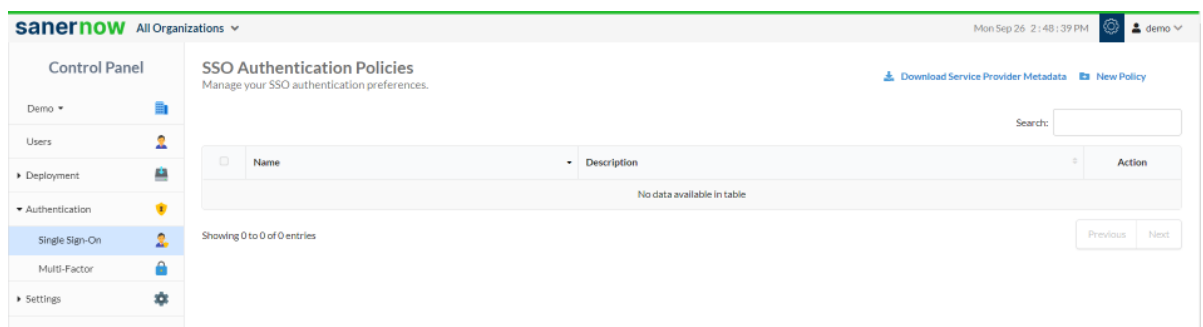
Following are the pre-requisites to configure Azure AD SSO

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

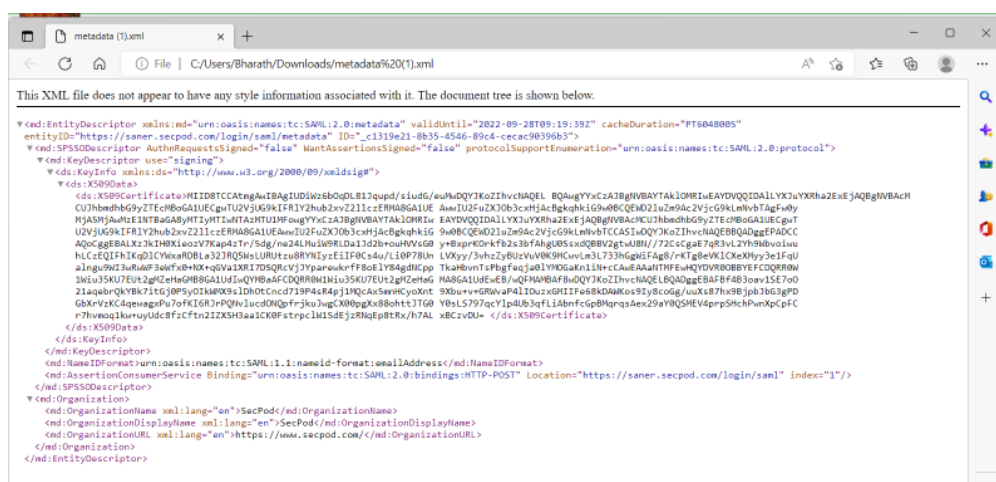
Follow the steps given below to retrieve the information mentioned above.

Steps to configure SAML-based SSO

1. Sign in to saner.secpod.com
2. Go to **Control Panel**
3. Under Authentication, select **Single Sign On**

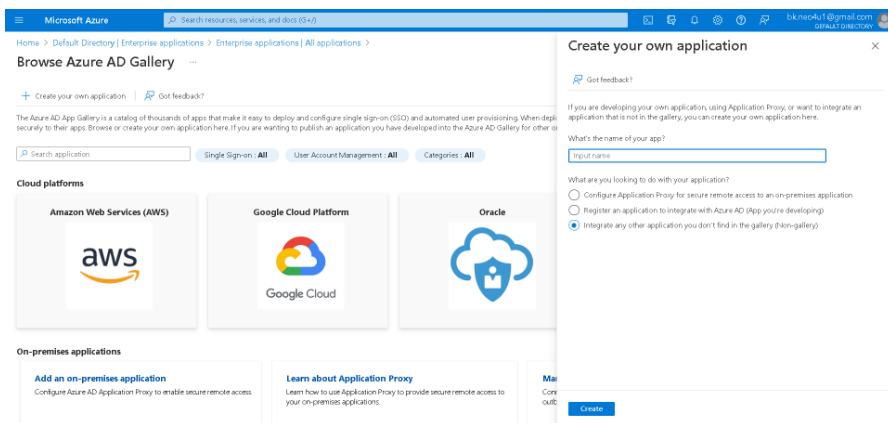


4. Click on **Download SSO metadata file**
5. Open the downloaded metadata file from your browser or a text editor.



6. Copy and save the Entity ID and ACS URL from the metadata file you downloaded.
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 and enter the name of the app (SanerNow App) and click on create.



11. Once the app is created, click on 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.email 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 SAML signing certificate section

3 SAML Certificates

Token signing certificate		Edit
Status	Active	
Thumbprint	8013E6C1D8D7F28A5F76DF568B82582F94C6FAC2	
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	

Verification certificates (optional) (Preview)		Edit
Required	No	
Active	0	
Expired	0	

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 new SSO policy.

SSO Authentication Policy

Name (*)

Description (*)

Issuer ID (*)

SSO URL (*)

Certificate (*)

Signed Authentication

- 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

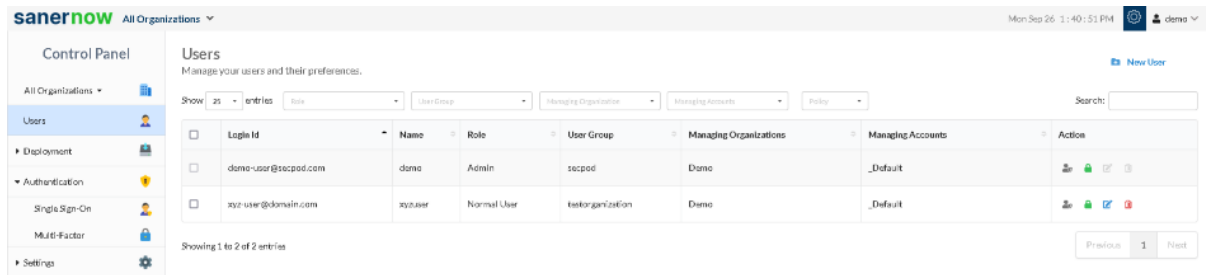
Steps to Assign users to the app in Azure AD

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

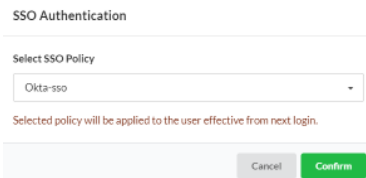
Assign SSO policy to SanerNow Users

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

- Go to Control Panel. Click on Users.



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



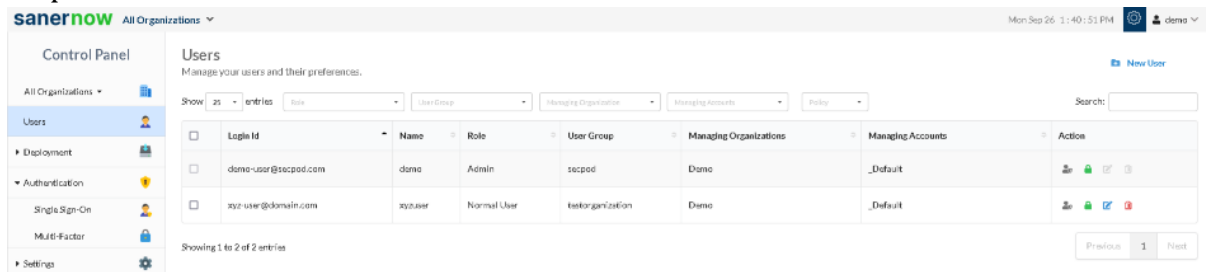
- Click on Confirm

How to apply SSO Policy to the New SanerNow user

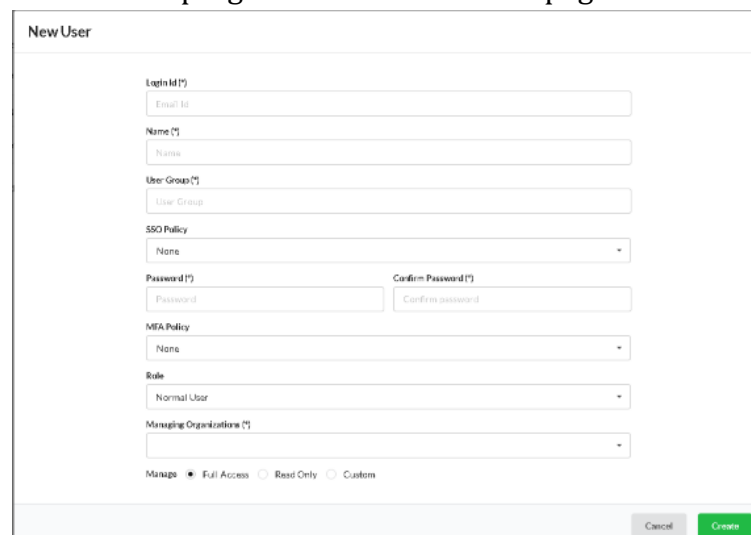
Step 1: Log in to SanerNow and then click Control Panel at the top-right to access the Control Panel page.

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 will automatically select that organization and show its accounts.

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



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



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: To assign SSO Policy to the user, select the created SSO policy from the drop-down.

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

Test the SAML configuration

Test if the configuration is working properly using the following steps

Via SP-initiated flow:

1. Go to 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 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.