How to Sign in Saner through AWS SSO

Pre-requisites for signing in via AWS SSO

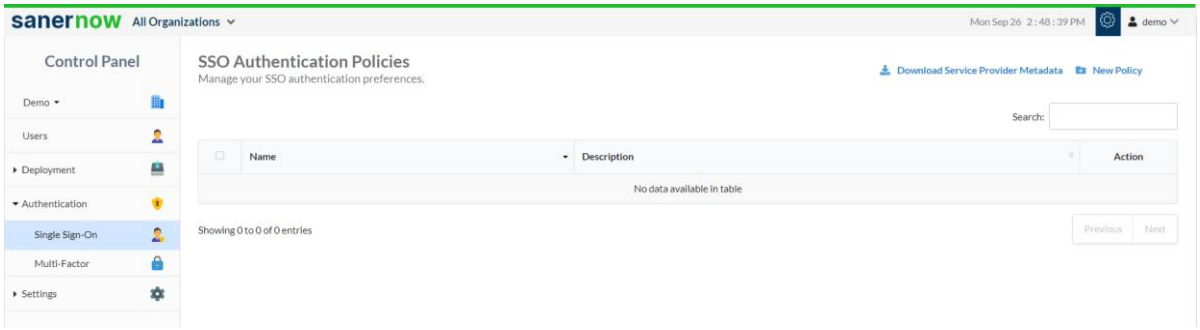
The following are the prerequisites to configure AWS SSO

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

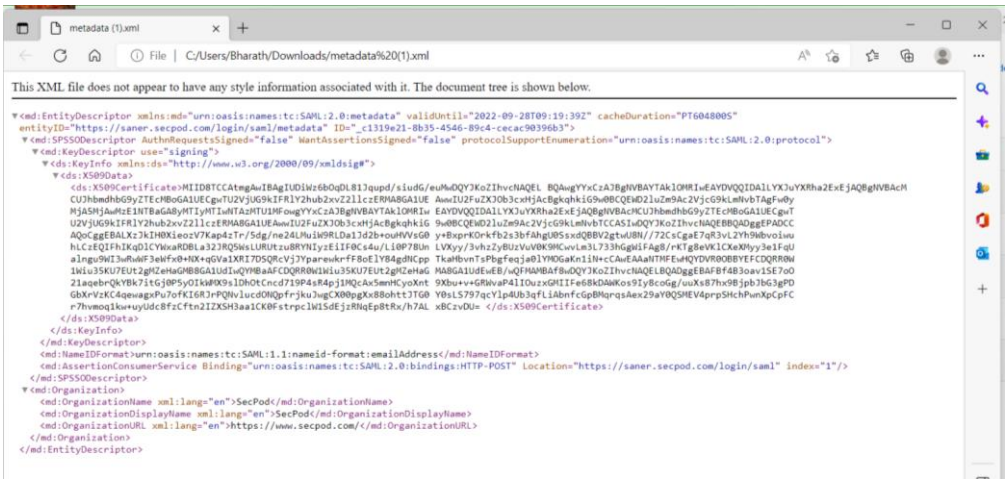
Follow the steps given below to retrieve the information mentioned above.

Steps to configure AWS SSO

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

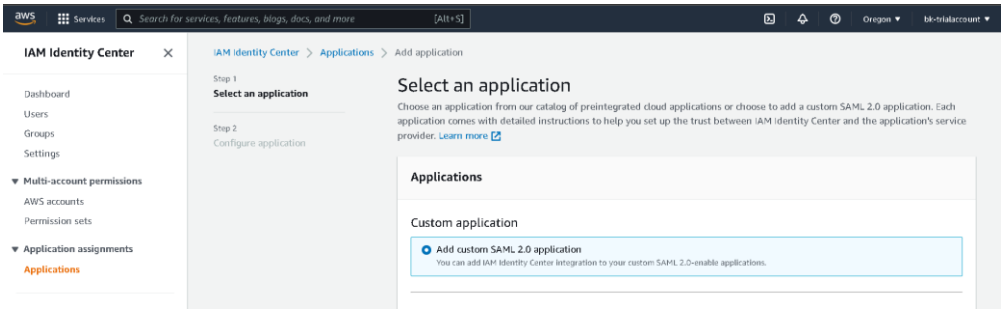


4. Click on **Download SSO metadata file**
5. Open the downloaded metadata file from your browser or a text editor.



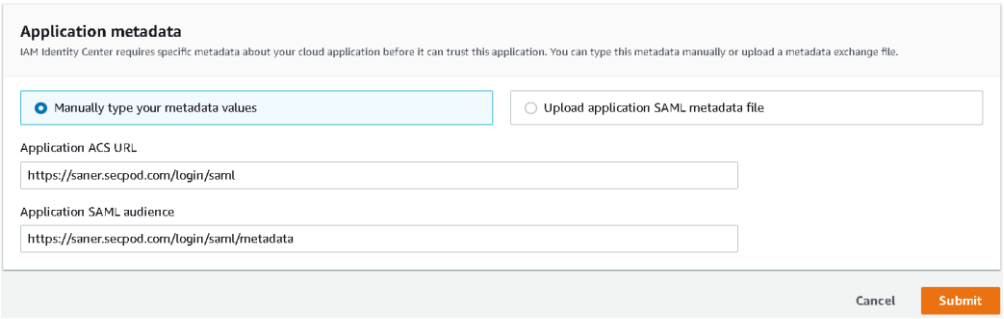
6. Copy and save the Entity ID and ACS URL from the metadata file you downloaded.
7. Sign in to your organization's AWS Admin Console.
8. Go to AWS IAM Identity Center
9. Click **Application Assignments** in the left menu, then click on **Applications**.

10. Click **Add Applications**, select **Add Custom SAML 2.0 application**, and click on **Next**.



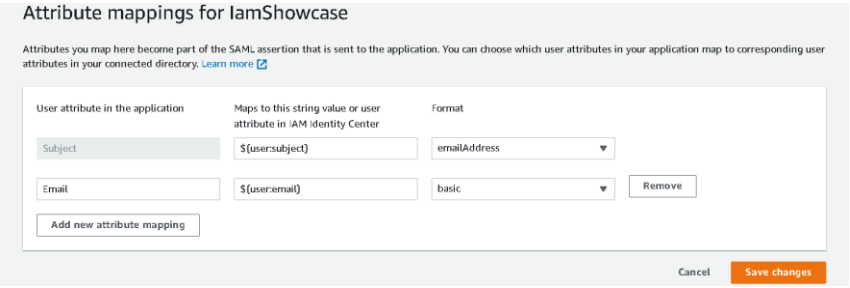
11. Under Configure Applications, enter the display name (eg: Saner App) in the Display Name field, enter description.
12. Scroll down, under IAM identity center metadata, download the metadata file and the certificate.

13. Scroll down and under Application Meta Data, enter Application ACS URL.
14. Enter Applcation SAML audience that is entity ID of Saner then click **Submit**



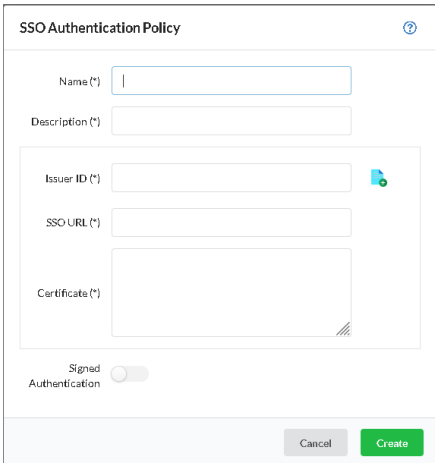
15. Once the application is created, Click on Actions drop down and select Edit Attribute mappings.
16. Now in the Attribute mapping, for subject select the format as emailAddress and enter the string value in the format “${user:subject}”
17. Click on Add new attribute mapping

18. Now enter “Email” under User Attribute. Enter the string value in the format “${user:email}”



19. Click on Save Changes.
20. Copy the Identity Provider Single Sign-On URL and identity provider issuer and X.509 Certificate from the downloaded metadata and certificate file.
21. Return to the SSO authentication page in Saner
22. Configure SSO in Saner using the downloaded certificate and copied URLs from AWS by following the steps given below:

    - Under SSO Authentication, click on new SSO policy.



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

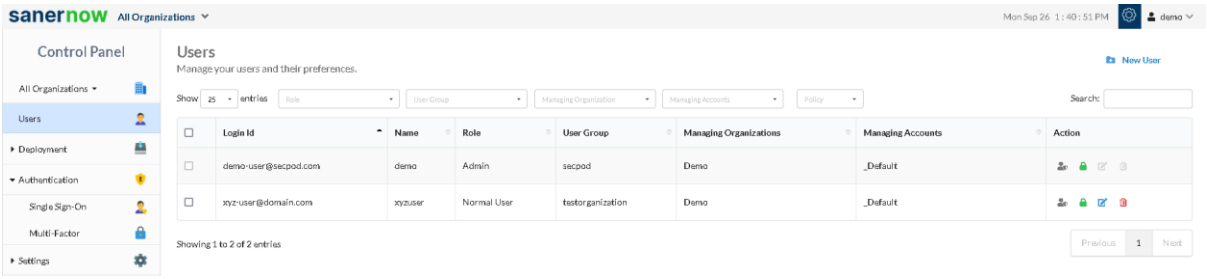
Steps to Assign users to the app in AWS

- Under Applications, select the application created (Saner App).
- Under Assigned Users, click on Assign users.
- Select the required users or group and click on Assign Users.

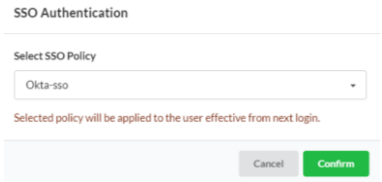
Assign SSO policy to Saner Users

Note: Before assigning the users, ensure that the User login ID in Saner matches with AWS user name

- Go to Control Panel. Click on Users.



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



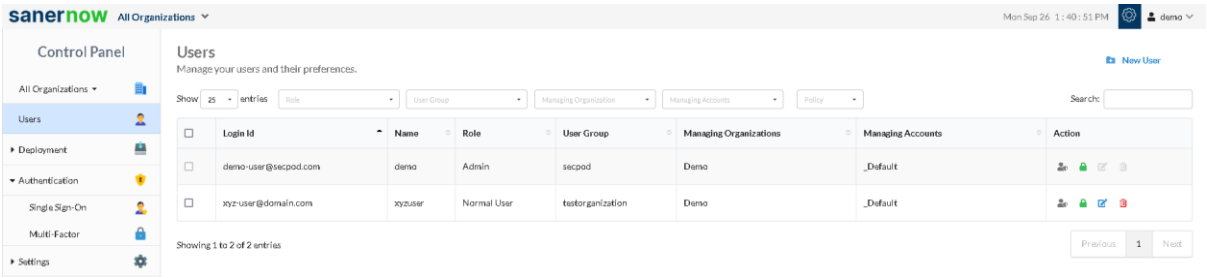
- Click on Confirm

How to apply SSO Policy to the New Saner user

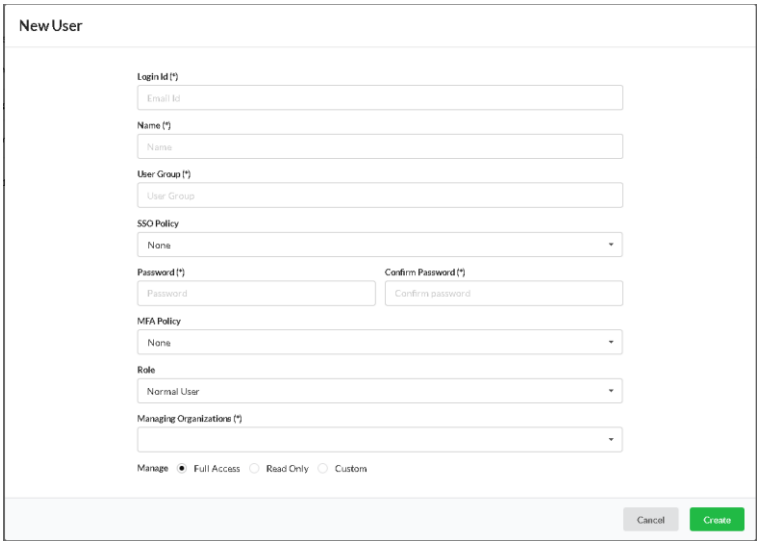
Step 1: Log in to Saner and then click Control Panel at the top-right to access the Control Panel page.

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

Via IdP-initiated flow:

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