How to Sign in Saner through Okta using SAML SSO

Pre-requisites for signing in via Okta SSO

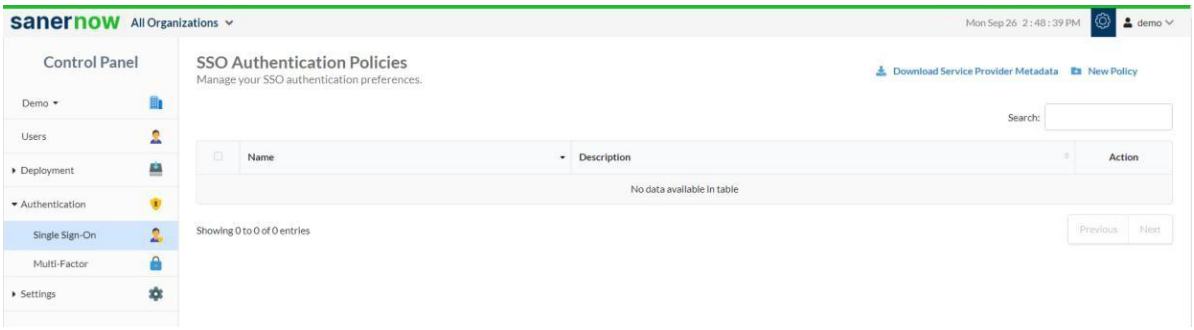
Following are the pre-requisites to configure Okta SSO

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

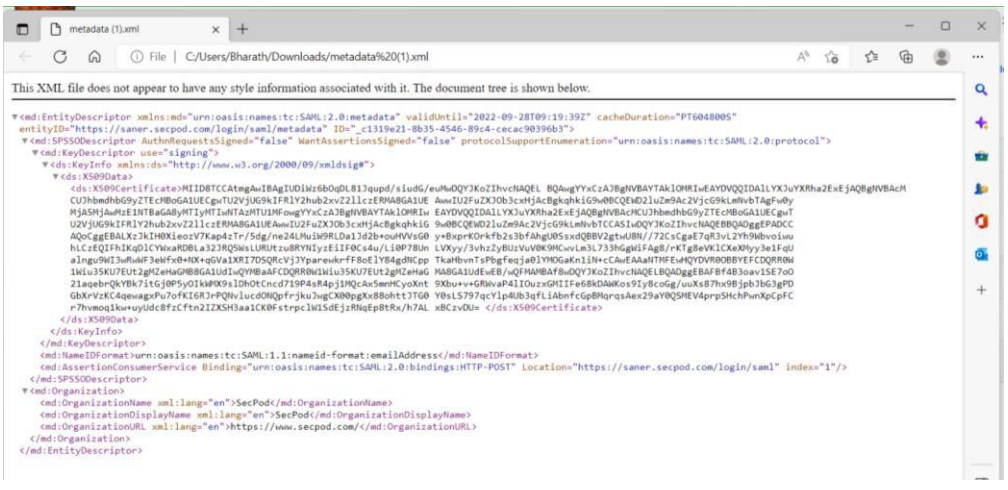
Follow the steps given below to retrieve the information mentioned above.

Steps to configure SAML-based SSO

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

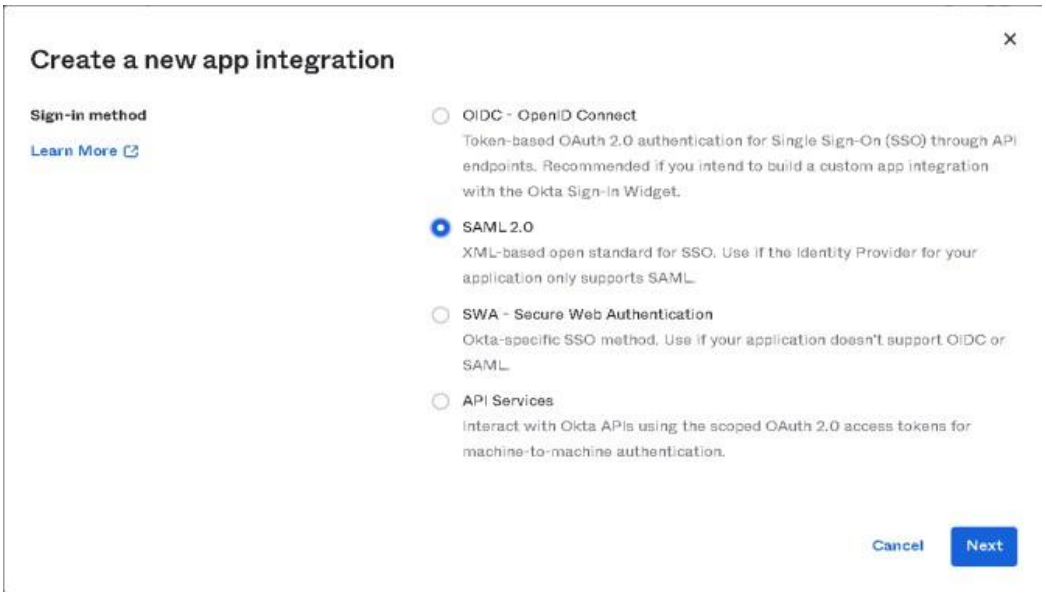


4. Click on **Download SSO metadata file**
5. Open the downloaded metadata file from your browser or a text editor.

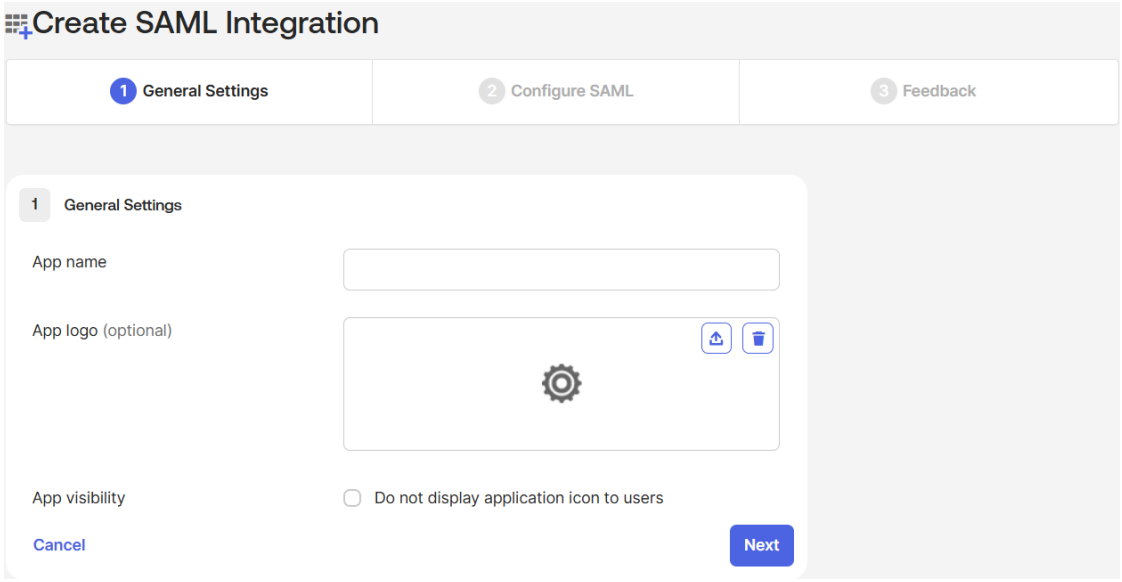


6. Copy and save the Entity ID and ACS URL from the metadata file you downloaded.
7. Sign in to your organization's Okta Admin Console.

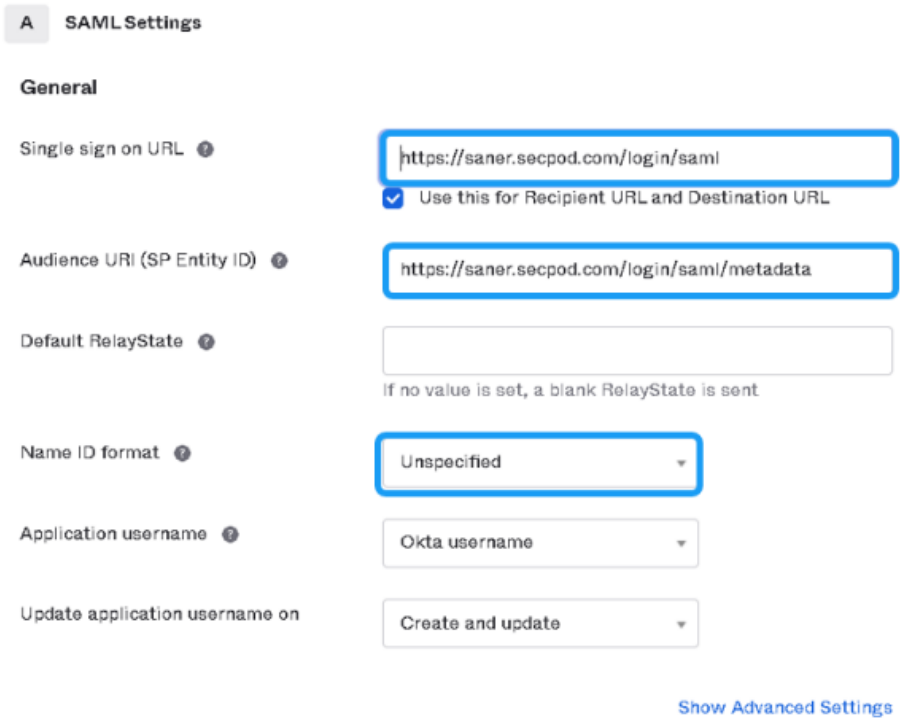
8. Click **Applications** in the left menu and click on **Applications**.
9. Click **Create App Integration**, select **SAML 2.0** and click **Next**.



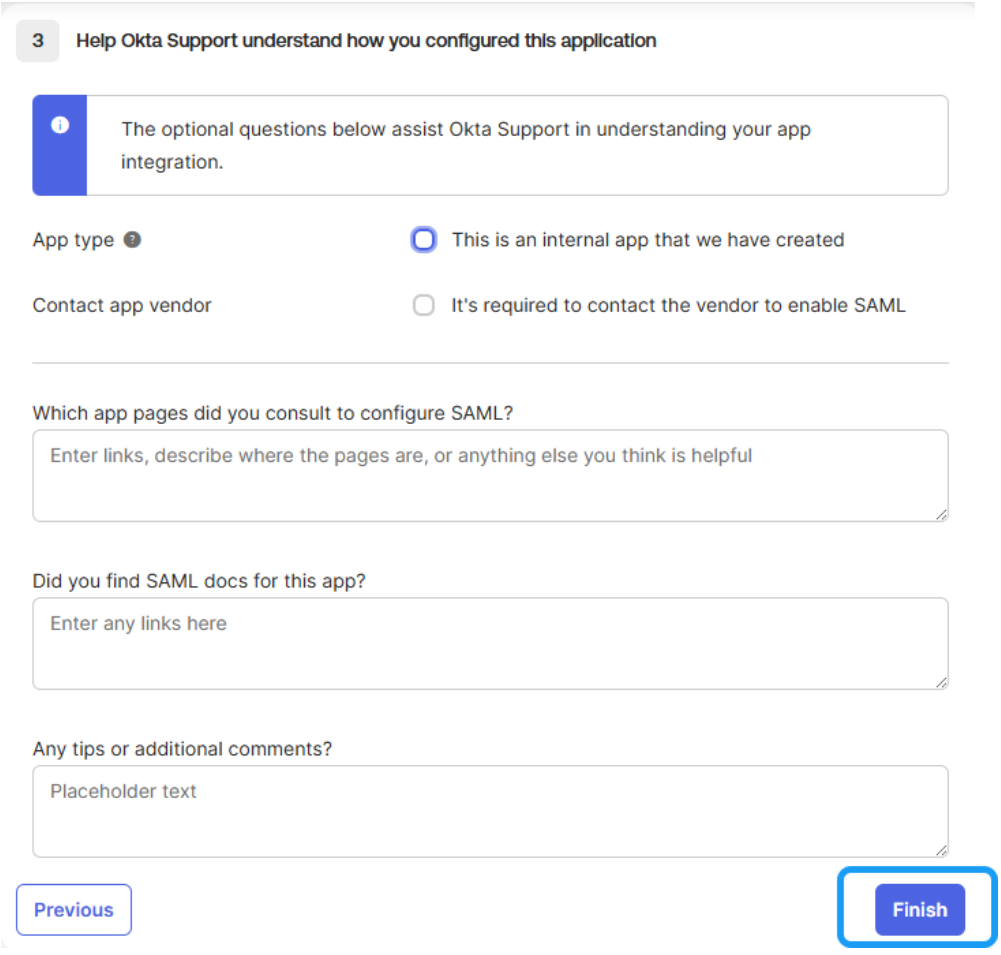
10. Under **General** settings, provide the application name in the **App Name** field and click **Next**.



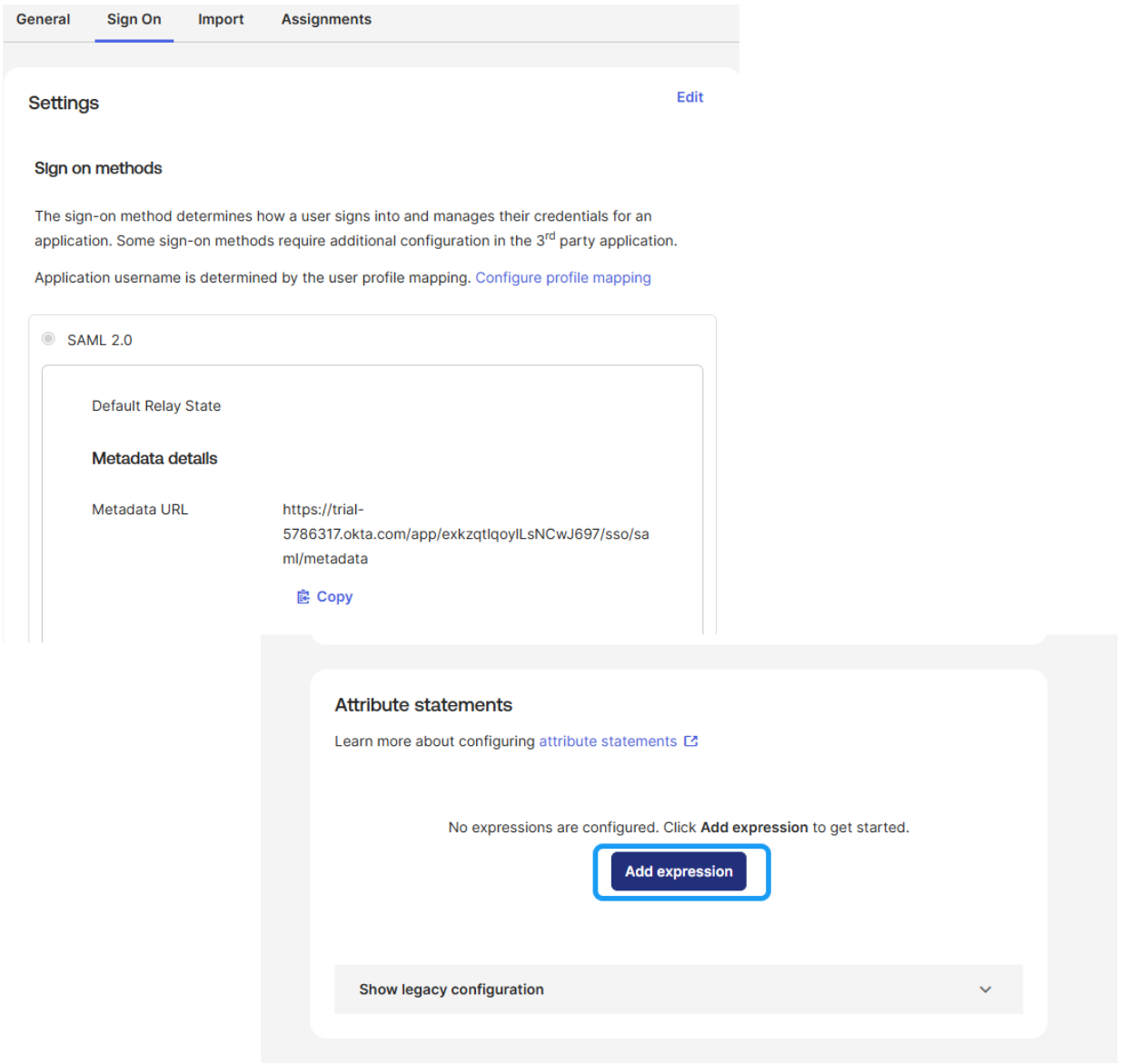
11. Enter the ACS URL in the **Single sign-on URL** field, Entity ID in the **Audience URI (SP Entity ID)** field. Next, select EmailAddress from the **Name ID format** drop-down list and Click **Next**.



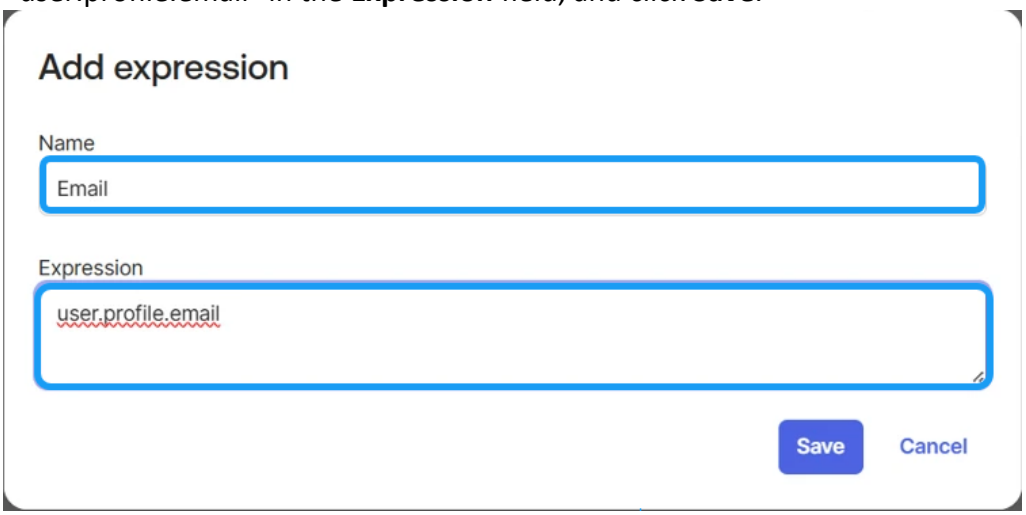
12. Providing feedback details is optional and then click **Finish**



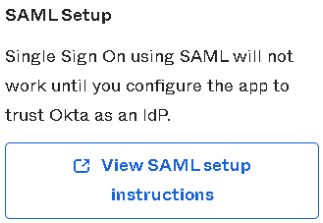
13. From the **Sign On** settings page, access **Attribute statements** to configure the expressions by clicking the **Add expression** button.



14. From the Add Expression window, enter "Email" in the **Name** field. Next, key in "user.profile.email" in the **Expression** field, and click **Save**.

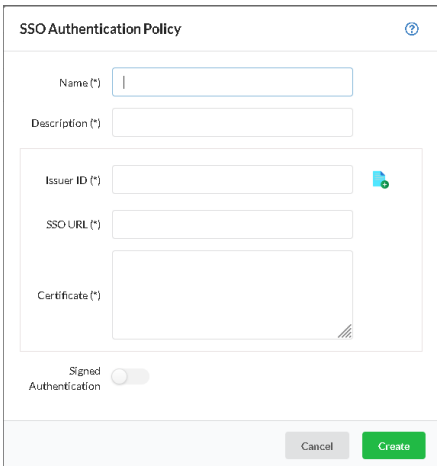


15. Scroll down and click **View SAML setup instructions**. A new page with IdP information will open.



16. Copy the Identity Provider Single Sign-On URL and identity provider issuer and download or copy the X.509 Certificate.
17. Return to the SSO authentication page in Saner.
18. Configure SSO in Saner using the downloaded certificate and copied URLs from Okta by following the steps given below:

    - Under SSO Authentication, click on new SSO policy.



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

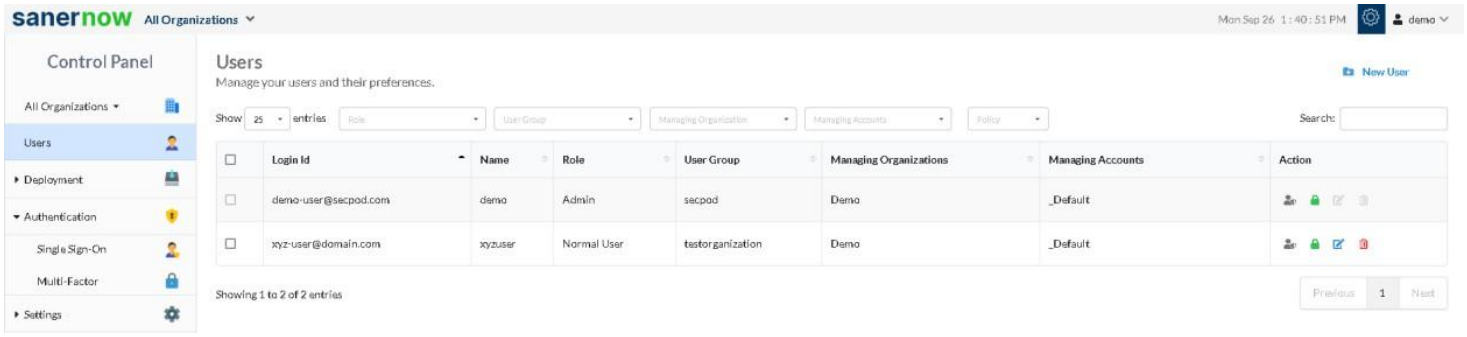
Steps to Assign users to the app in Okta

Your users in Okta can use this newly configured Saner app to sign in to Saner. Before that, ensure that you assign your users to this app. Follow the instructions in the following Okta article to assign your users to the app.
https://help.okta.com/en/prod/Content/Topics/Provisioning/lcm/lcm-assign-app-user.htm

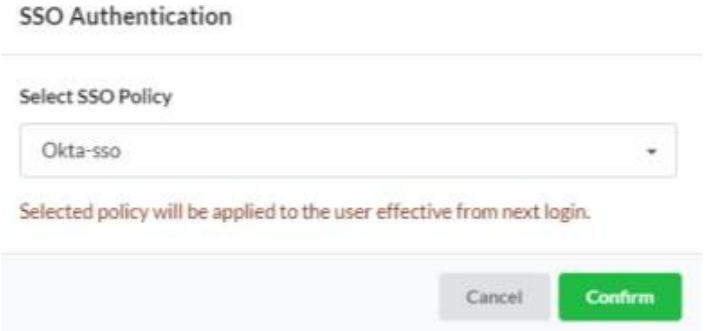
Assign SSO policy to Saner Users

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

- Go to Control Panel. Click on Users.



- Select the users to whom Okta policy should be applied
- Under Actions, select “Enforce SSO authentication” button

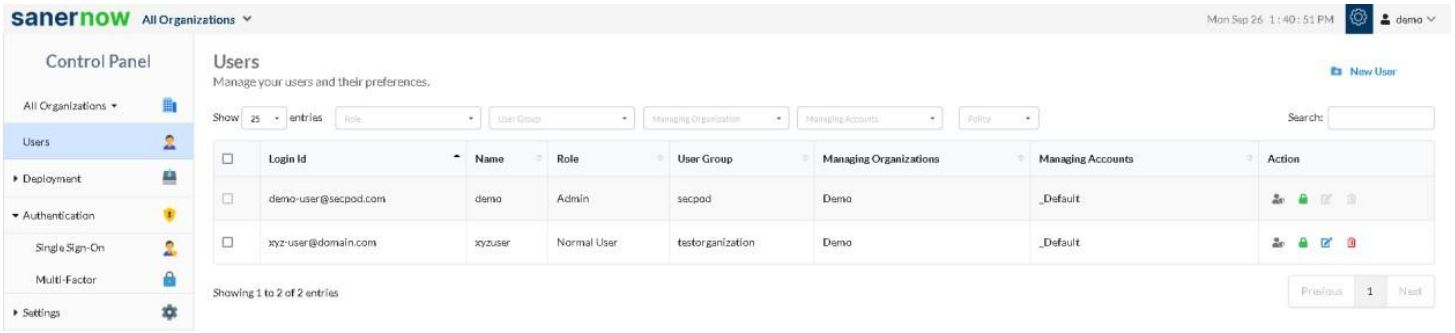


- Select the Okta policy from the drop-down
- Click on Confirm

How to apply SSO Policy to the New Saner user

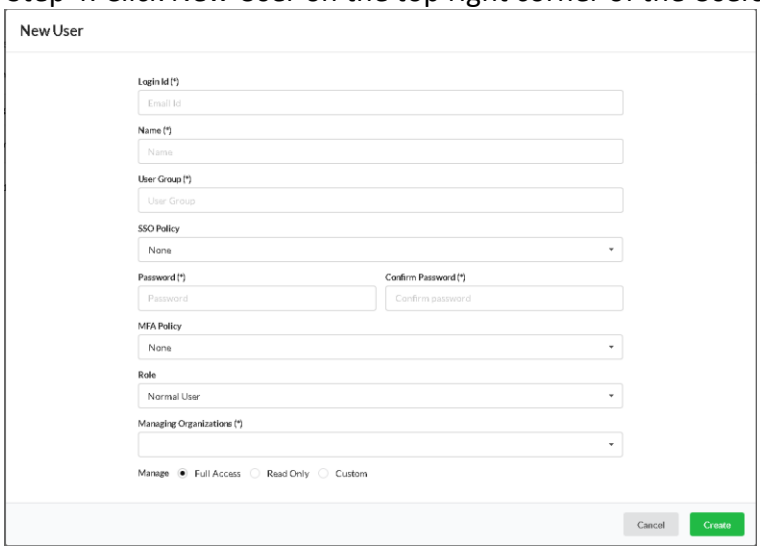
Step 1: Log in to Saner and then click Control Panel at the top-right to access the Control Panel page.

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 Okta for authentication.
3. If you have not already signed in to Okta, enter your Okta 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 Okta 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.