

How to Sign in SanerNow through Okta using SAML SSO

Pre-requisites for signing in via Okta SSO

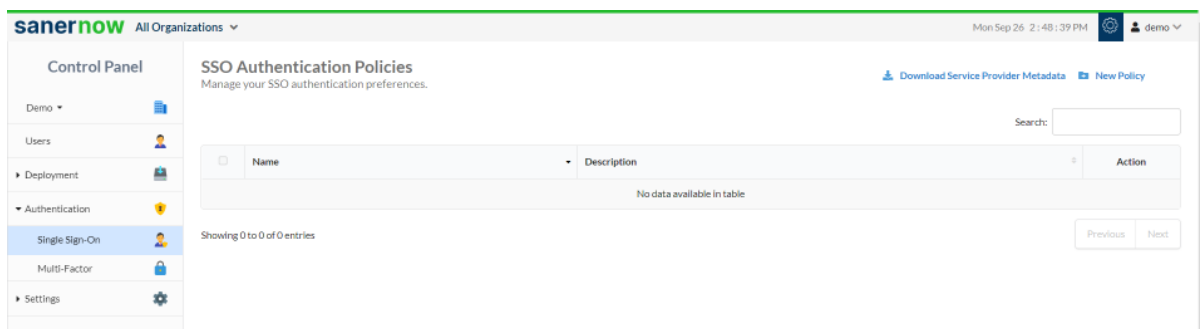
Following are the pre-requisites to configure Okta SSO

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

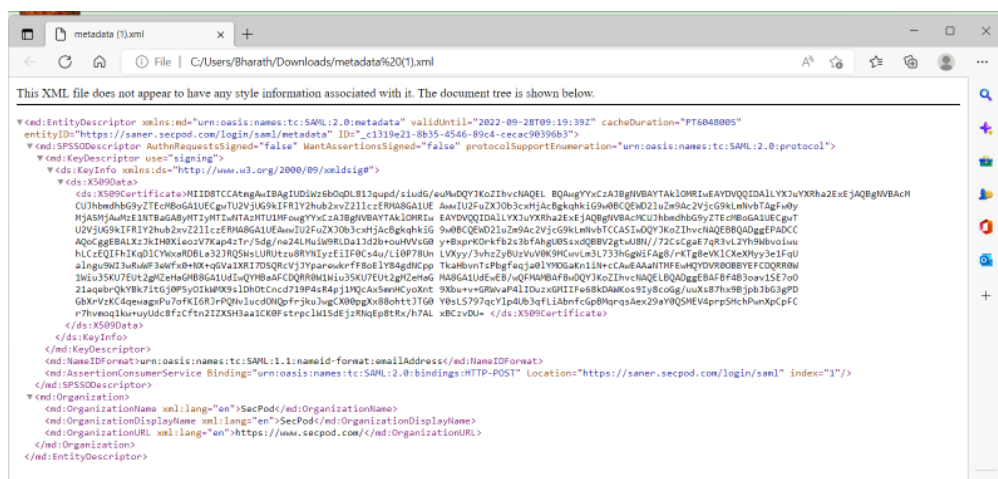
Follow the steps given below to retrieve the information mentioned above.

Steps to configure SAML-based SSO

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

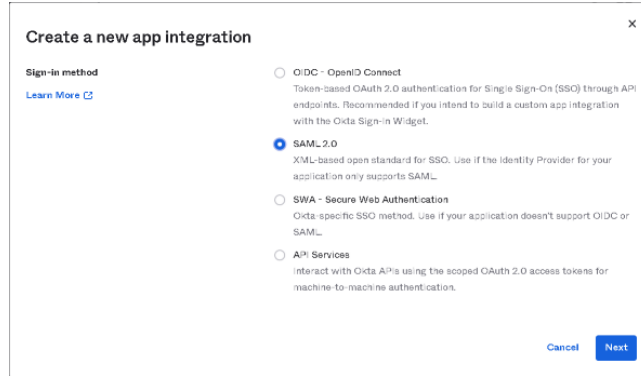


4. Click on **Download Service Provider metadata file**
5. Open the downloaded metadata file from your browser or a text editor.



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, then click on **Applications**.

9. Click **Create App Integration**, select **SAML 2.0**, and click **Next**.



Create a new app integration [X]

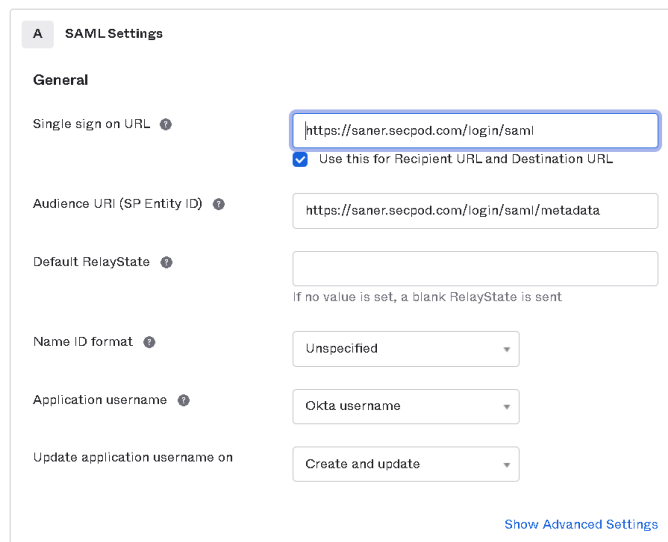
Sign-in method
[Learn More](#)

- OpenID Connect
Token-based OAuth 2.0 authentication for Single Sign-On (SSO) through API endpoints. Recommended if you intend to build a custom app integration with the Okta Sign-in Widget.
- SAML 2.0**
XML-based open standard for SSO. Use if the Identity Provider for your application only supports SAML.
- SWA - Secure Web Authentication
Okta specific SSO method. Use if your application doesn't support OIDC or SAML.
- API Services
Interact with Okta APIs using the scoped OAuth 2.0 access tokens for machine-to-machine authentication.

Cancel **Next**

10. Under General settings, enter the application name (eg: SanerNow App) for the app in the App Name field, then click **Next**.

11. Enter the ACS URL in the Single sign-on URL field and the Entity ID in the Audience URI (SP Entity ID) field.



A SAML Settings

General

Single sign on URL
 Use this for Recipient URL and Destination URL

Audience URI (SP Entity ID)

Default RelayState
 If no value is set, a blank RelayState is sent

Name ID format

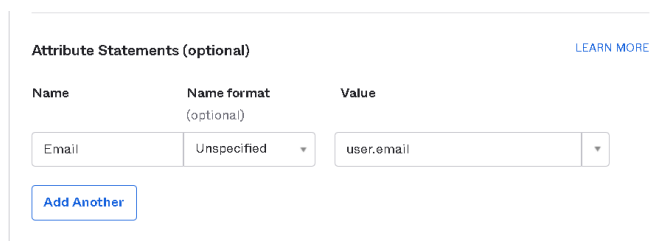
Application username

Update application username on

[Show Advanced Settings](#)

12. Select **EmailAddress** in the name ID format field.

13. Under Attribute statements, add an attribute with an Email in the Name field and user.email in the value field. Then click Next.



Attribute Statements (optional) [LEARN MORE](#)

Name	Name format (optional)	Value
Email	Unspecified	user.email

[Add Another](#)

14. Select the option **I'm an Okta customer adding an internal app**, and then click **Finish**.

15. On the next page, go to the **Sign On** tab.

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

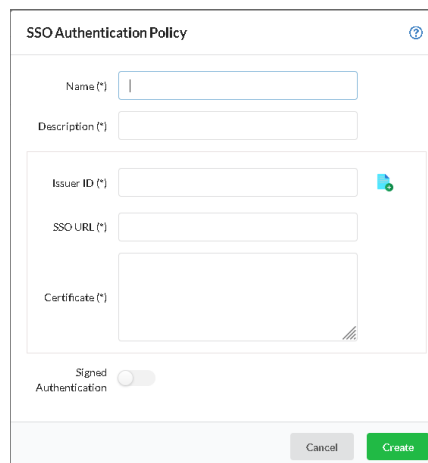
SAML Setup

Single Sign On using SAML will not work until you configure the app to trust Okta as an IdP.

[View SAML setup instructions](#)

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

- Under SSO Authentication, click on new SSO policy.



The screenshot shows the 'SSO Authentication Policy' configuration form. It contains the following fields and controls:

- Name (*)**: A text input field.
- Description (*)**: A text input field.
- Issuer ID (*)**: A text input field with a small blue icon to its right.
- SSO URL (*)**: A text input field.
- Certificate (*)**: A large text area for pasting the certificate.
- Signed Authentication**: A toggle switch, currently turned off.
- Buttons**: 'Cancel' and 'Create' buttons at the bottom right.

- 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

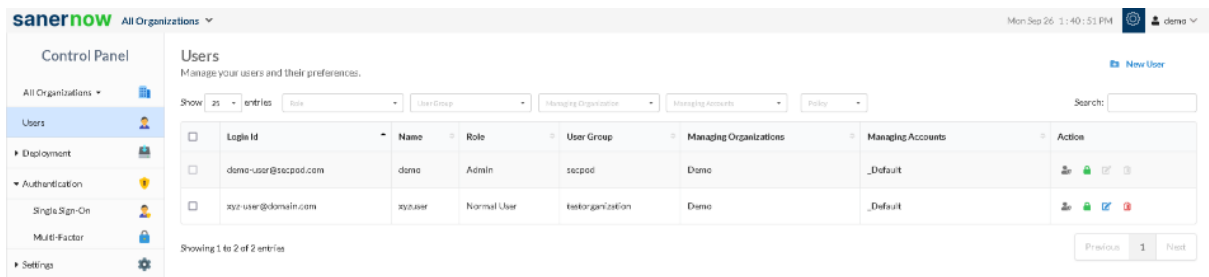
Your users in Okta can use this newly configured SanerNow app to sign in to SanerNow. Before that, ensure that you assign your users to this app. Follow the instructions in the following Okta article to assign your users to the app.

<https://help.okta.com/en/prod/Content/Topics/Provisioning/lcm/lcm-assign-app-user.htm>

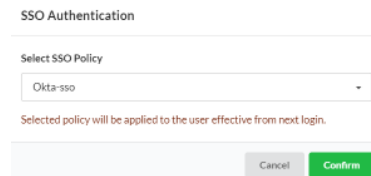
Assign SSO policy to SanerNow Users

Note: Before assigning the users, ensure that the User login ID in SanerNow 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



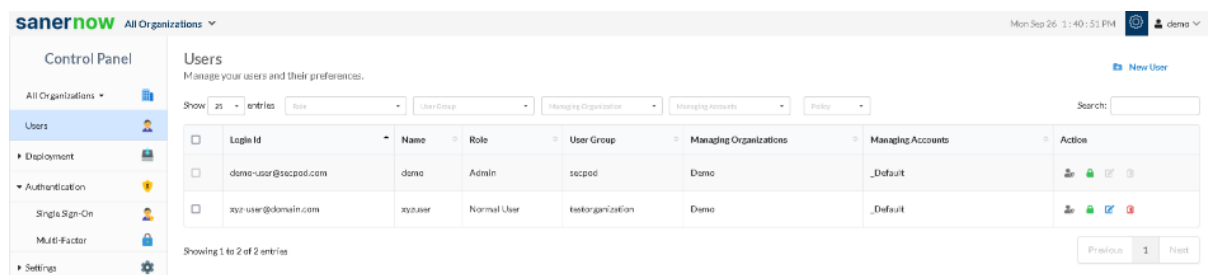
- Click on Confirm

How to apply SSO Policy to the New 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.

The screenshot shows a 'New User' form with the following fields and options:

- Login Id (*)**: Text input field with placeholder 'Email Id'.
- Name (*)**: Text input field with placeholder 'Name'.
- User Group (*)**: Text input field with placeholder 'User Group'.
- SSO Policy**: Dropdown menu with 'None' selected.
- Password (*)**: Text input field with placeholder 'Password'.
- Confirm Password (*)**: Text input field with placeholder 'Confirm password'.
- MFA Policy**: Dropdown menu with 'None' selected.
- Role**: Dropdown menu with 'Normal User' selected.
- Managing Organizations (*)**: Dropdown menu.
- Manage**: Radio buttons for 'Full Access' (selected), 'Read Only', and 'Custom'.
- Buttons**: 'Cancel' and 'Create' buttons at the bottom right.

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 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 SanerNow and will be signed in.

Via IdP-initiated flow:

1. Sign in to Okta 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.