How to Sign in Saner through Okta using SAML SSO

Pre-requisites for signing in via Okta SSO

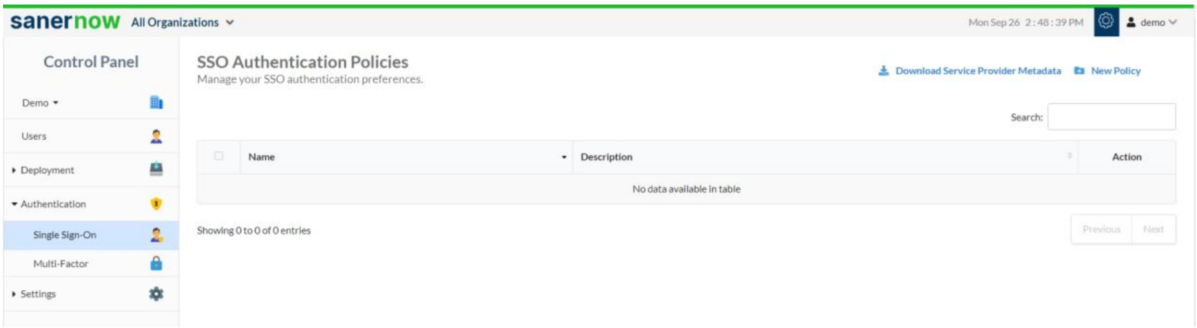
Following are the pre-requisites to configure Okta SSO

- 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**



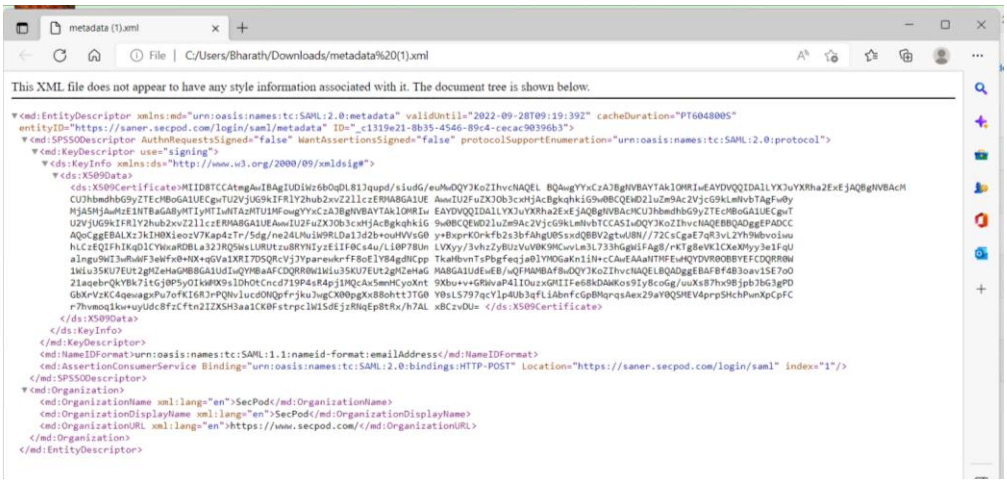
SSO Authentication Policies

Manage your SSO authentication preferences.

□	Name	Description	Action
No data available in table			

Showing 0 to 0 of 0 entries

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

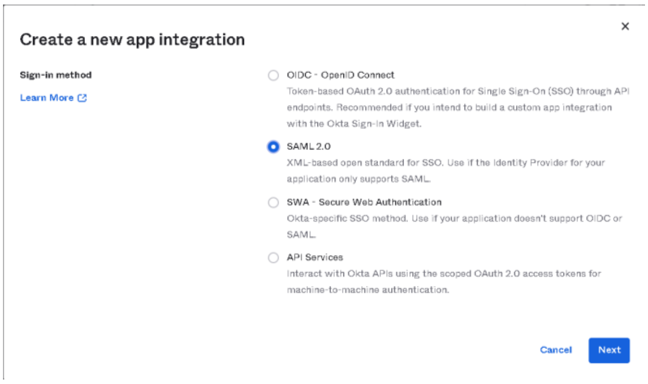


This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
▼<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" validUntil="2022-09-28T09:19:39Z" cacheDuration="PT604800S"
 entityID="https://saner.secpod.com/login/saml/metadata" ID="_c1319e21-8b35-4546-89c4-cecac90396b3">
  ▼<md:SPSSODescriptor AuthnRequestsSigned="false" WantAssertionsSigned="false" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    ▼<md:KeyDescriptor use="signing">
      ▼<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        ▼<ds:X509Data>
            <ds:X509Certificate>MIID8TCCAtmgAwIBAgIUDiWz6bOqDL81Jqupd/siudG/euMwDQYJKoZIhvcNAQEL BQAwgYYxCzAJBgNVBAYTAk1OMRIwEAYDVQQIDAlLYXJuYXRha2ExEjAQBgNVBAcM
            CUJhbmdhbG9yZTEcMBoGA1UECgwTU2VjUG9kIFRlY2hub2xvZ2llczERMA8GA1UE AwwIU2FuZXJOb3cxHjAcBgkqhkiG9w0BCQEWD2luZm9Ac2VjcG9kLmNvbTAgFw0y
            MjA5MjAwMzE1NTBaGA8yMTIyMTIwNTAzMTU1MFowgYYxCzAJBgNVBAYTAk1OMRIw EAYDVQQIDAlLYXJuYXRha2ExEjAQBgNVBAcMCUJhbmdhbG9yZTEcMBoGA1UECgwT
            U2VjUG9kIFRlY2hub2xvZ2llczERMA8GA1UEAwwIU2FuZXJOb3cxHjAcBgkqhkiG 9w0BCQEWD2luZm9Ac2VjcG9kLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCC
            AQoCggEBALXzJkIH0XieozV7Kap4zTr/5dg/ne24LMuiW9RLDa1Jd2b+ouHVVsG0 y+BxprKOrkfb2s3bfAhgU0SsxdQBBV2gtwU8N//72CsCgaE7qR3vL2Yh9Wbvoiwu
            hLCzEQIFhIKqD1CYWxaRDBLa32JRQ5WsLURUtzu8RYNIyzEiIF0Cs4u/Li0P78Un LVXyy/3vhzZyBUzVuV0K9MCwvLm3L733hGgWiFAg8/rKTg8eVKlCXeXMyy3e1FqU
            alngu9WI3wRwWF3eWfx0+NX+qGVa1XRI7DSQRcVjJYparewkrfF8oElY84gdNCpp TkaHbvnTsPbgfeqja0lYMOGaKn1iN+cCAwEAAaNTMFEwHQYDVR0OBBYEFCDQRR0W
            1Wiu35KU7EUt2gMZeHaGMB8GA1UdIwQYMBaAFCDQRR0W1Wiu35KU7EUt2gMZeHaG MA8GA1UdEwEB/wQFMAMBAf8wDQYJKoZIhvcNAQELBQADggEBAFBf4B3oav1SE7oO
            21aqebrQkYBk7itGj0P5yOIkWMX9slDhOtCncd719P4sR4pj1MQcAx5mnHCyoXnt 9Xbu+v+GRWvaP4lIOuzxGMIIFe68kDAWKos9Iy8coGg/uuXs87hx9BjpbJbG3gPD
            GbXrVzKC4qewagxPu7ofKI6RJrPQNvlucdONQpfrjkuJwgCX00pgXx88ohttJTG0 Y0sLS797qcYlp4Ub3qfLiAbnfcGpBMqrqsAex29aY0QSMEV4prpSHchPwnXpCpFC
            r7hvmoq1kw+uyUdc8fzCftn2IZXSH3aa1CK0FstrpclW1SdEjzRNqEp8tRx/h7AL xBCzvDU= </ds:X509Certificate>
          </ds:X509Data>
        </ds:KeyInfo>
      </md:KeyDescriptor>
      <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</md:NameIDFormat>
      <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://saner.secpod.com/login/saml" index="1"/>
    </md:SPSSODescriptor>
  ▼<md:Organization>
      <md:OrganizationName xml:lang="en">SecPod</md:OrganizationName>
      <md:OrganizationDisplayName xml:lang="en">SecPod</md:OrganizationDisplayName>
      <md:OrganizationURL xml:lang="en">https://www.secpod.com/</md:OrganizationURL>
    </md:Organization>
</md:EntityDescriptor>
```

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

Sign-in method

Learn More

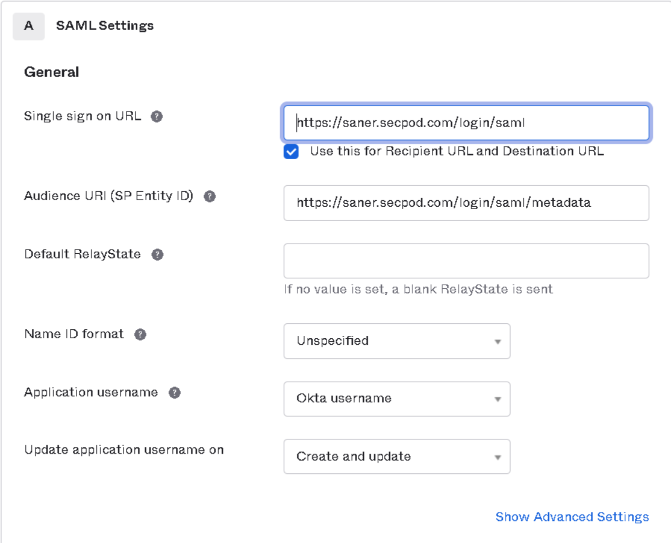
○ OIDC - OpenID Connect
Token-based OAuth 2.0 authentication for Single Sign-On (SSO) through API endpoints. Recommended if you intend to build a custom app integration with the Okta Sign-In Widget.

● 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.

10. Under General settings, enter the application name (eg: Saner 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: https://saner.secpod.com/login/saml

☑ Use this for Recipient URL and Destination URL

Audience URI (SP Entity ID): https://saner.secpod.com/login/saml/metadata

Default RelayState:

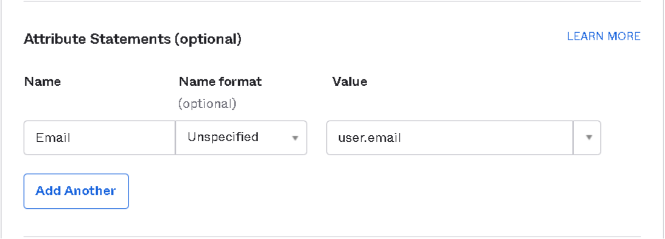
If no value is set, a blank RelayState is sent

Name ID format: Unspecified

Application username: Okta username

Update application username on: Create and update

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.

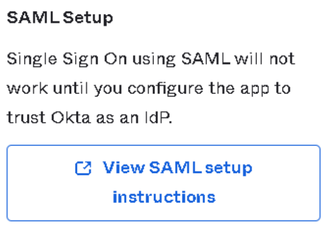


Attribute Statements (optional)

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

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.

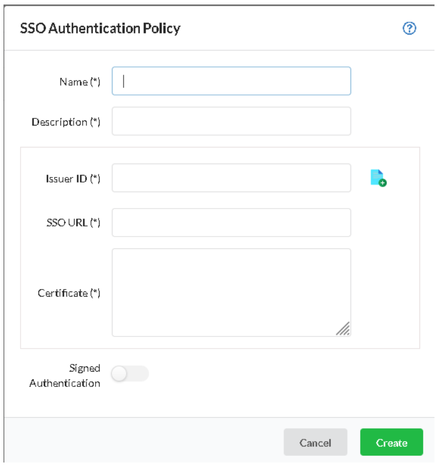


SAML Setup

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

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 Saner
19. 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

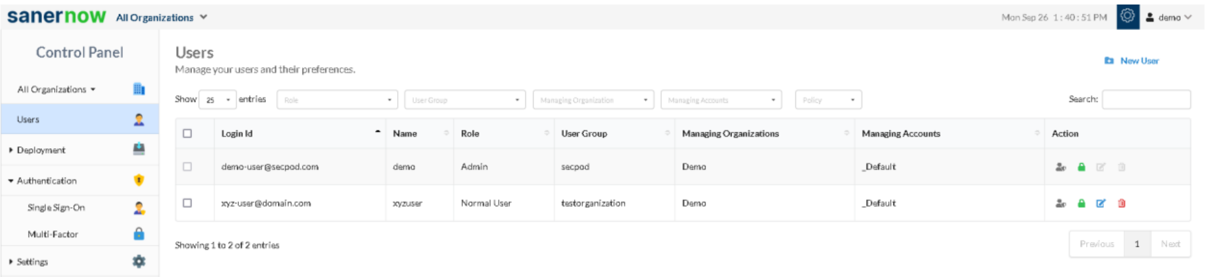
Steps to Assign users to the app in Okta

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.



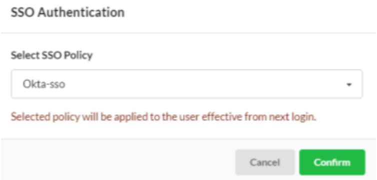
Users

Manage your users and their preferences.

□	Login Id	Name	Role	User Group	Managing Organizations	Managing Accounts	Action
□	demo-user@secpod.com	demo	Admin	secpod	Demo	_Default	
□	xyz-user@domain.com	xyzuser	Normal User	testorganization	Demo	_Default	

Showing 1 to 2 of 2 entries

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



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

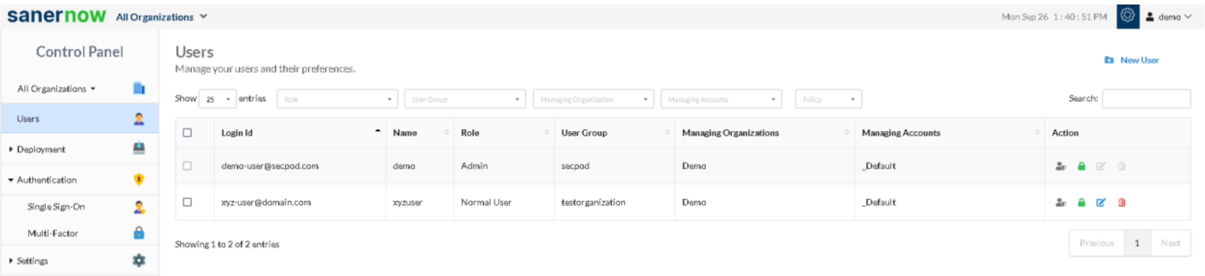
- Click on Confirm

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.



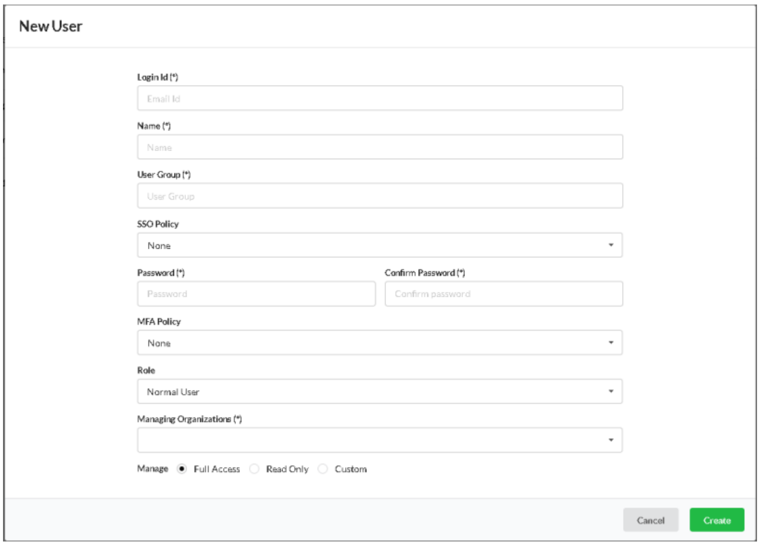
Users

Manage your users and their preferences.

□	Login Id	Name	Role	User Group	Managing Organizations	Managing Accounts	Action
□	demo-user@secpod.com	demo	Admin	secpod	Demo	_Default	
□	xyz-user@domain.com	xyzuser	Normal User	testorganization	Demo	_Default	

Showing 1 to 2 of 2 entries

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



New User

Login Id (*): Email Id

Name (*): Name

User Group (*): User Group

SSO Policy: None

Password (*): Password

Confirm Password (*): Confirm password

MFA Policy: None

Role: Normal User

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: 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.