

# How to Sign in SanerNow through PingID using SAML SSO

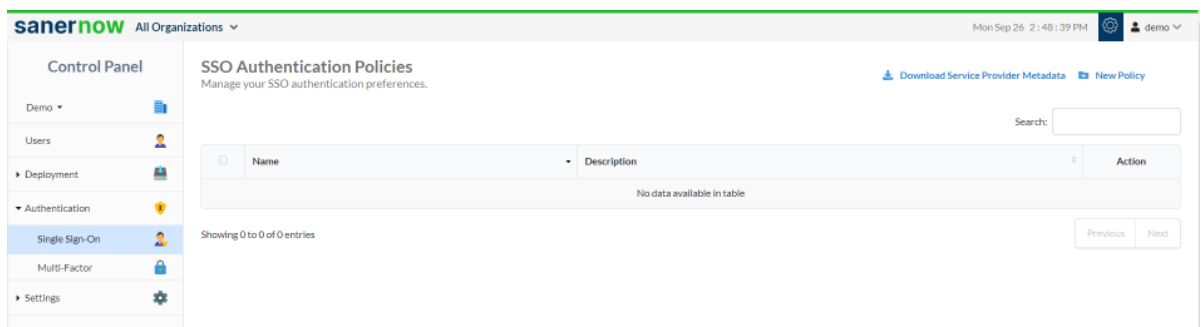
## Pre-requisites for signing in via PingID SSO

Following are the pre-requisites to configure PingID SSO

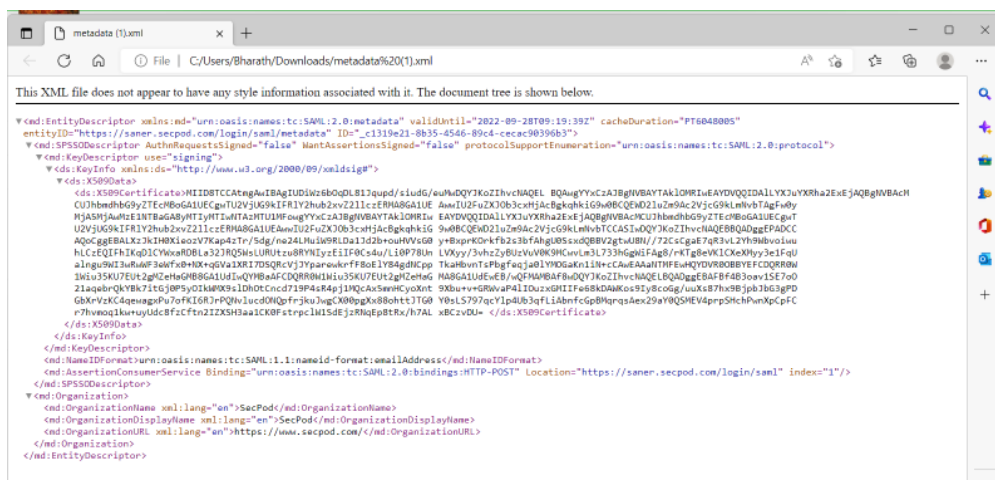
- Identity Provider Single Sign-On URL
- X.509 Certificate
- Issuer ID

## Steps to configure SAML-based SSO

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

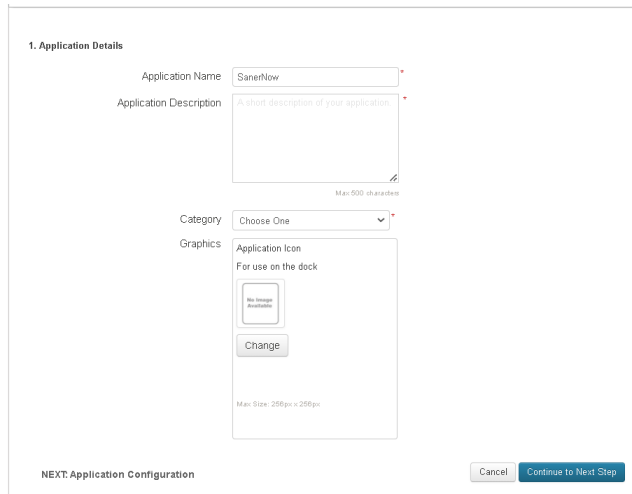


4. Click on **Download Service Provider metadata file**
5. Open the downloaded metadata file from your browser or a text editor.



6. Copy and save the Entity ID and ACS URL from the metadata file you downloaded.
7. Sign in to your organization's PingID Admin Console.
8. Click **Applications** in the Top menu.
9. Under My applications, Select SAML and Click on Add Applications. From the drop down select New SAML applications.

10. Under Application Details, enter the application name (eg: SanerNow App) for the app in the App Name field, enter the app description and select the category of the application.



1. Application Details

Application Name: SanerNow

Application Description: A short description of your application

Category: Choose One

Graphics: Application Icon (For use on the deck)

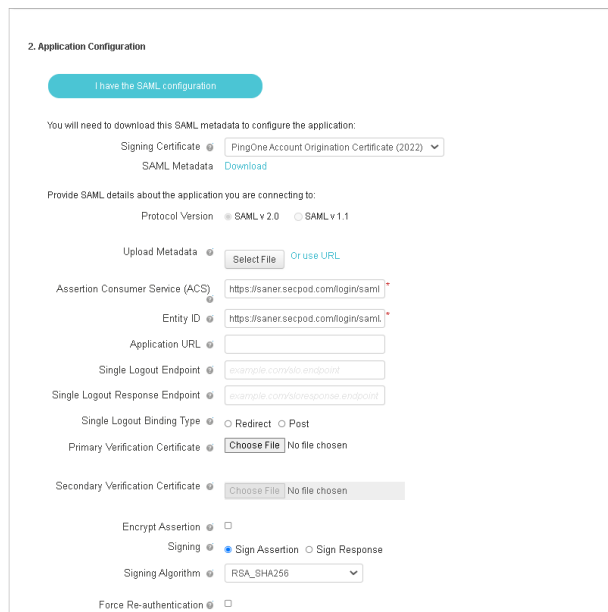
Change

Max Size: 256px x 256px

NEXT: Application Configuration

Cancel Continue to Next Step

11. Click on **Continue to Next Step**
12. Under Application Configuration, select **I have the SAML configuration option**
13. Enter the ACS URL, entity ID in the ACS URL field and the Entity ID field.



2. Application Configuration

I have the SAML configuration

You will need to download this SAML metadata to configure the application:

Signing Certificate: PingOne Account Origination Certificate (2022)

SAML Metadata: Download

Provide SAML details about the application you are connecting to:

Protocol Version: SAML v 2.0

Upload Metadata: Select File or use URL

Assertion Consumer Service (ACS): https://sanersecpod.com/login/saml

Entity ID: https://sanersecpod.com/login/saml

Application URL:

Single Logout Endpoint: example.com/slo/endpoint

Single Logout Response Endpoint: example.com/slo/response/endpoint

Single Logout Binding Type: Redirect Post

Primary Verification Certificate: Choose File No file chosen

Secondary Verification Certificate: Choose File No file chosen

Encrypt Assertion:

Signing: Sign Assertion Sign Response

Signing Algorithm: RSA\_SHA256

Force Re-authentication:

14. Scroll down and click on continue to Next.
15. Under SSO attribute mapping, Click on Add New Attribute.
16. Mention Email in the Application Attribute field, select the email under Literal value, and enable the Required field.

3. SSO Attribute Mapping

Map the necessary application provider (AP) attributes to attributes used by your identity provider (IdP).

Application Attribute	Identity Bridge Attribute or Literal Value	Required
1 Email	Email (Work) <input type="checkbox"/> As Literal Advanced	<input checked="" type="checkbox"/>

Add new attribute

NEXT: Group Access

Cancel Back **Continue to Next Step**

17. Click on **Continue to Next Step**

18. Under Group Access, Add the groups to which you need access to SanerNow applications.

19. Click on **Continue to Next Step**

20. Review the setup, download the metadata and the certificate file, and click on **Finish**



Single Sign-On (SSO) Relay State <https://pingone.com/1.0/12e689e3-be20-4e81-a61b-85300405bdcf>

Signing Certificate [Download](#)

SAML Metadata [Download](#)

SAML Metadata URL <https://admin-api.pingone.com/latest/metadata/707b6a14-79bc-42a4-8e33-6a739de5de01>

21. From the downloaded metadata and certificate file, copy the Identity Provider Single Sign-On URL and identity provider issuer and copy the X.509 Certificate.

22. Return to the SSO authentication page in SanerNow

23. Configure SSO in SanerNow using the downloaded certificate and copied URLs from PingID 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

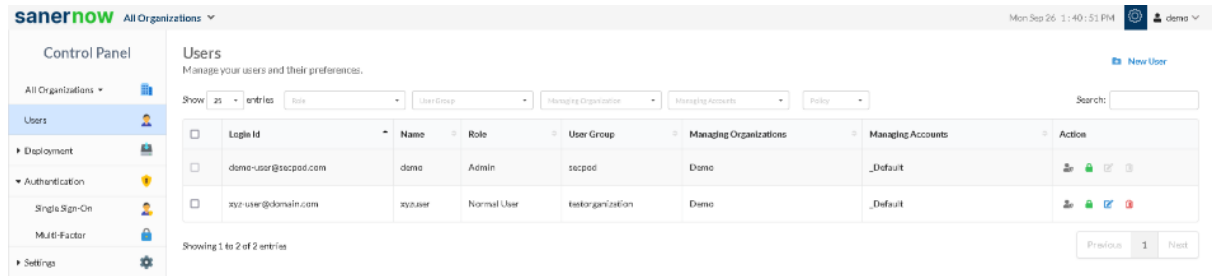
Cancel Create

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

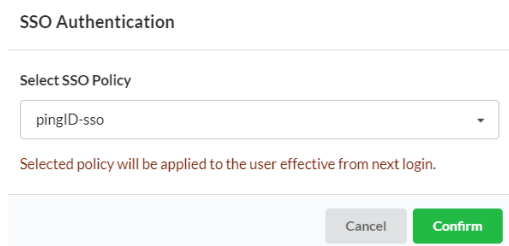
## Assign SSO policy to SanerNow Users

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

- Go to Control Panel. Click on Users.



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



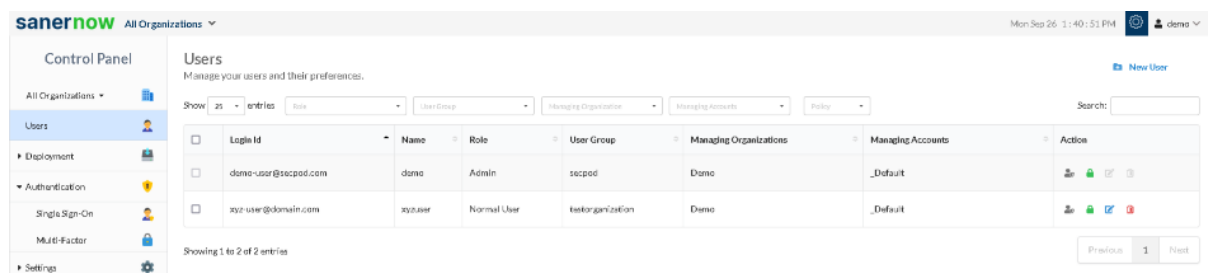
- Click on Confirm

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