How to Sign in Saner through PingID using SAML SSO

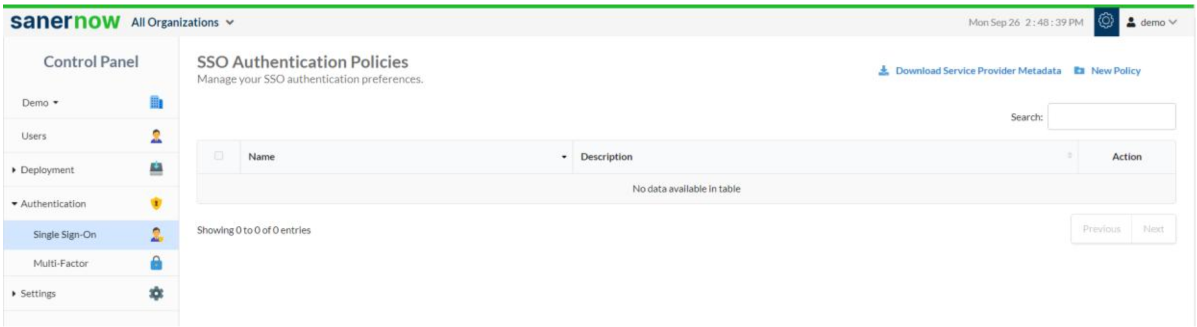
Pre-requisites for signing in via PingID SSO

The following are the prerequisites to configure PingID SSO

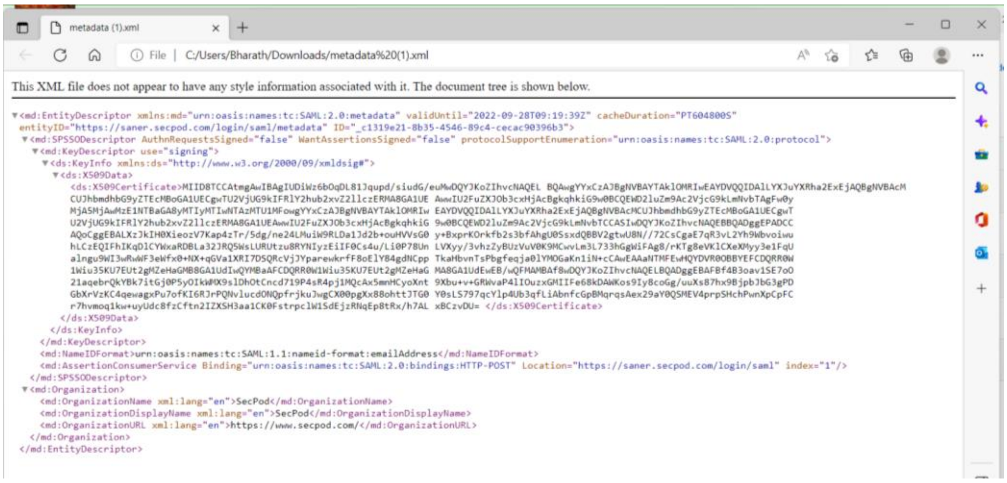
- Identity Provider Single Sign-On URL
- X.509 Certificate
- Issuer ID

Steps to configure SAML-based SSO

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



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

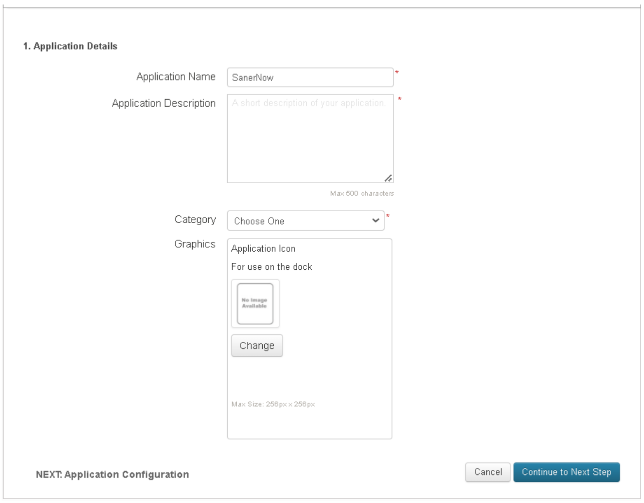


This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
▼<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 BQAwgYYxCzAJBgNVBAYTAklOMRIwEAYDVQQIDAlLYXJuYXRha2ExEjAQBgNVBAcM
       CUJhbmdhbG9yZTEcMBoGA1UECgwTU2VjUG9kIFRlY2hub2xvZ2llczERMA8GA1UE AwwIU2FuZXJOb3cxHjAcBgkqhkiG9w0BCQEWD2luZm9Ac2VjcG9kLmNvbTAgFw0y
       MjA5MjAwMzE1NTBaGA8yMTIyMTIwNTAzMTU1MFowgYYxCzAJBgNVBAYTAklOMRIw EAYDVQQIDAlLYXJuYXRha2ExEjAQBgNVBAcMCUJhbmdhbG9yZTEcMBoGA1UECgwT
       U2VjUG9kIFRlY2hub2xvZ2llczERMA8GA1UEAwwIU2FuZXJOb3cxHjAcBgkqhkiG 9w0BCQEWD2luZm9Ac2VjcG9kLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCC
       AQoCggEBALXzJkIH0XieozV7Kap4zTr/5dg/ne24LMuiW9RLDa1Jd2b+ouHVVsG0 y+BxprKOrkfb2s3bfAhgU0SsxdQBBV2gtwU8N//72CsCgaE7qR3vL2Yh9Wbvoiwu
       hLCzEQIFhIKqDlCYWxaRDBLa32JRQ5WsLURUtzu8RYNIyzEiIF0Cs4u/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 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: Saner App) for the app in the App Name field, enter the app description and select the category of the application.

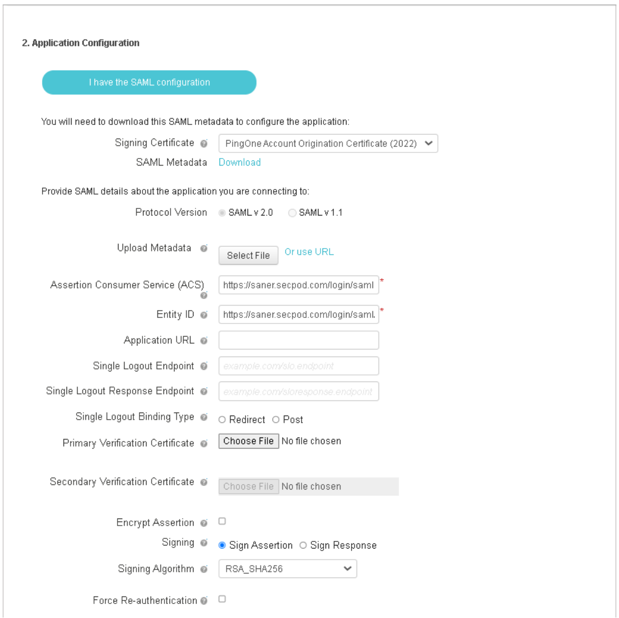


1. Application Details

Application Name	SanerNow *
Application Description	A short description of your application. * Max 500 characters
Category	Choose One *
Graphics	Application Icon For use on the dock Change Max Size: 256px x 256px

NEXT: Application Configuration

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

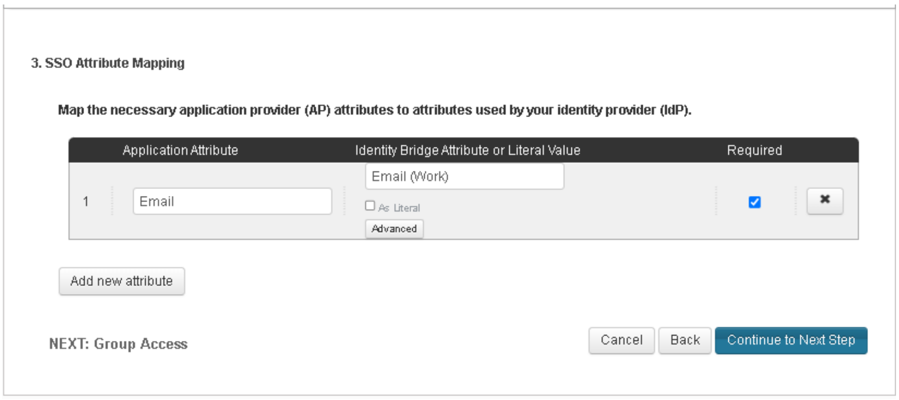
You will need to download this SAML metadata to configure the application:

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 ○ SAML v 1.1
Upload Metadata	Select File Or use URL
Assertion Consumer Service (ACS)	https://saner.secpod.com/login/saml *
Entity ID	https://saner.secpod.com/login/saml. *
Application URL	
Single Logout Endpoint	example.com/slo.endpoint
Single Logout Response Endpoint	example.com/sloresponse.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

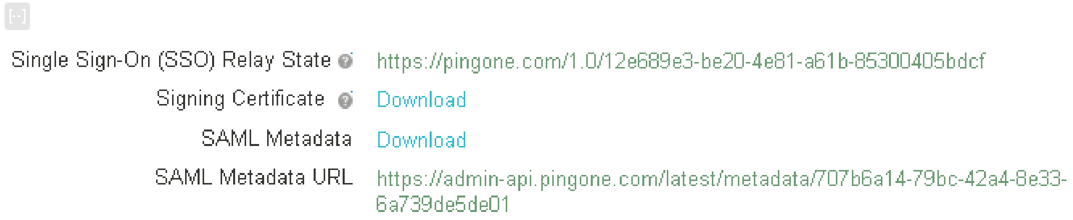
Map the necessary application provider (AP) attributes to attributes used by your identity provider (IdP).

	Application Attribute	Identity Bridge Attribute or Literal Value	Required	
1	Email	Email (Work) □ As Literal Advanced	☑	✖

Add new attribute

NEXT: Group Access

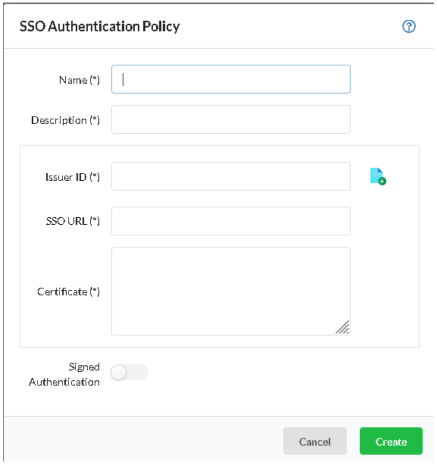
17. Click on **Continue to Next Step**
18. Under Group Access, Add the groups to which you need access to Saner applications.
19. Click on **Continue to Next Step**
20. Review the setup, download the metadata and the certificate file, and click on **Finish**



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 metada 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 Saner.
23. Configure SSO in Saner 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 (*)

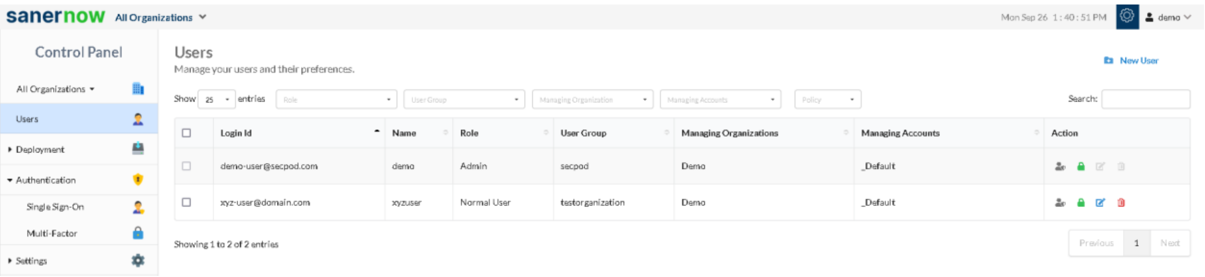
Signed Authentication

- 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 Saner Users

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

- Go to Control Panel. Click on Users.



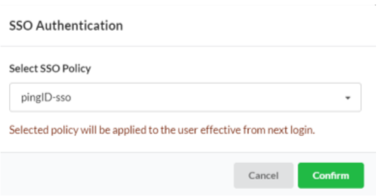
Users

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



Select SSO Policy: pingID-sso

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

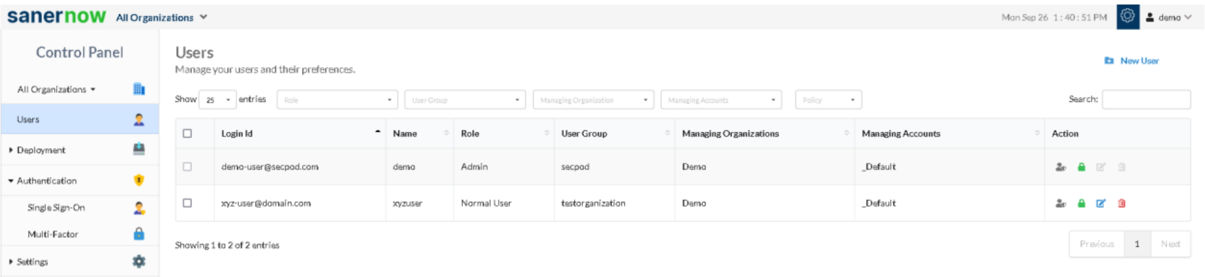
- Click on Confirm

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.



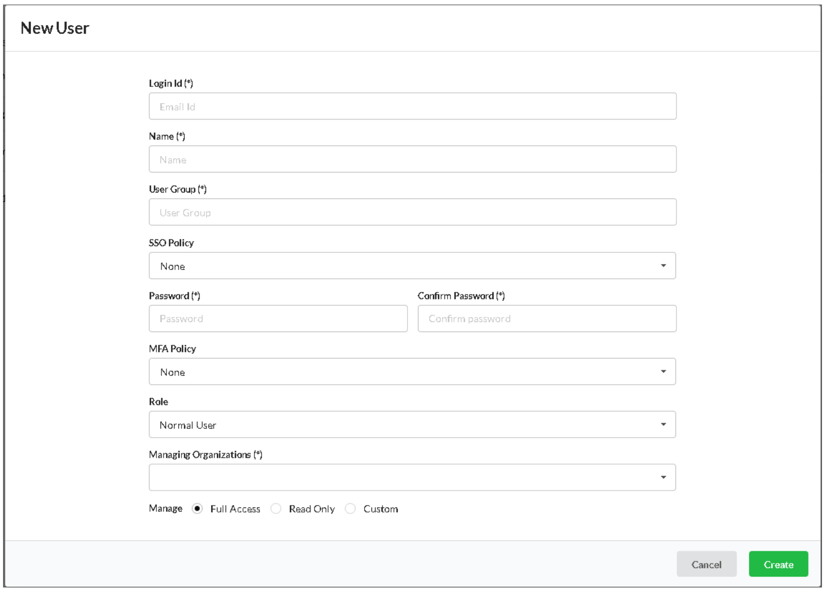
Users

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 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 Saner and will be signed in.

Via IdP-initiated flow:

1. Sign in to PingID 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.