How to Sign in Saner through Ping Federate using SAML SSO

Pre-requisites for signing in via Ping Federate SSO

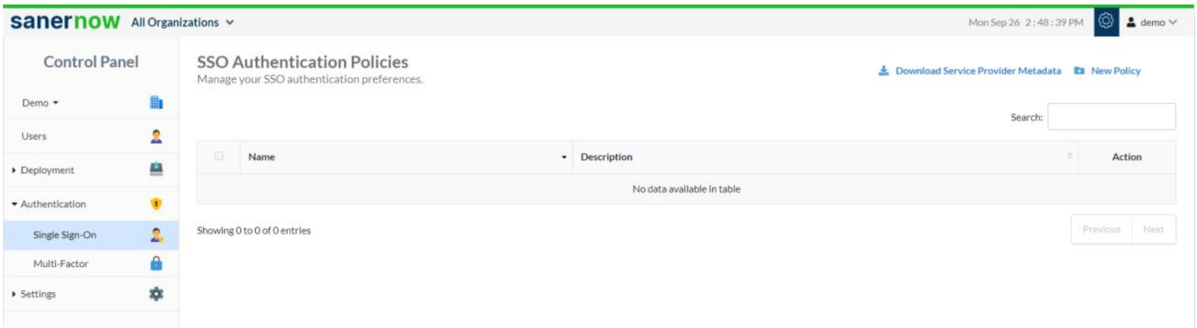
The following are the prerequisites to configure Ping Federate SSO

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

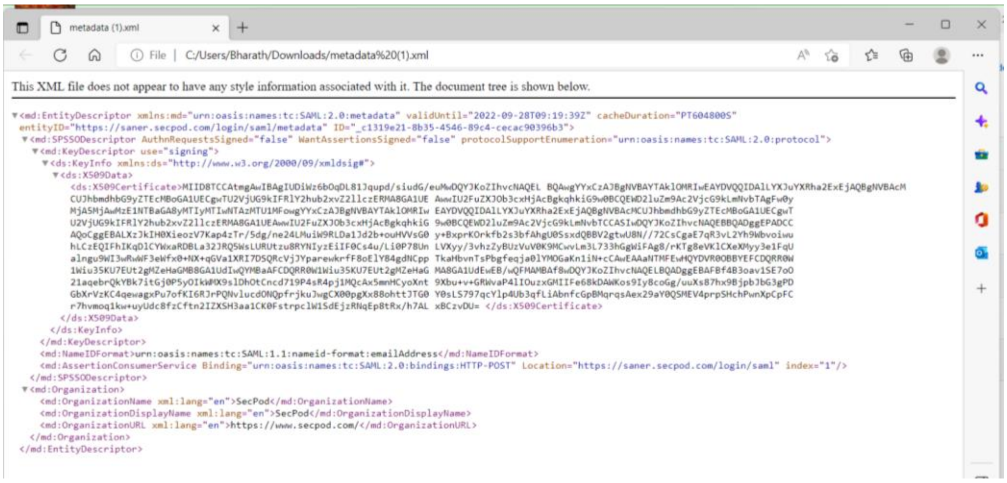
Follow the steps given below to retrieve the information mentioned above.

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.

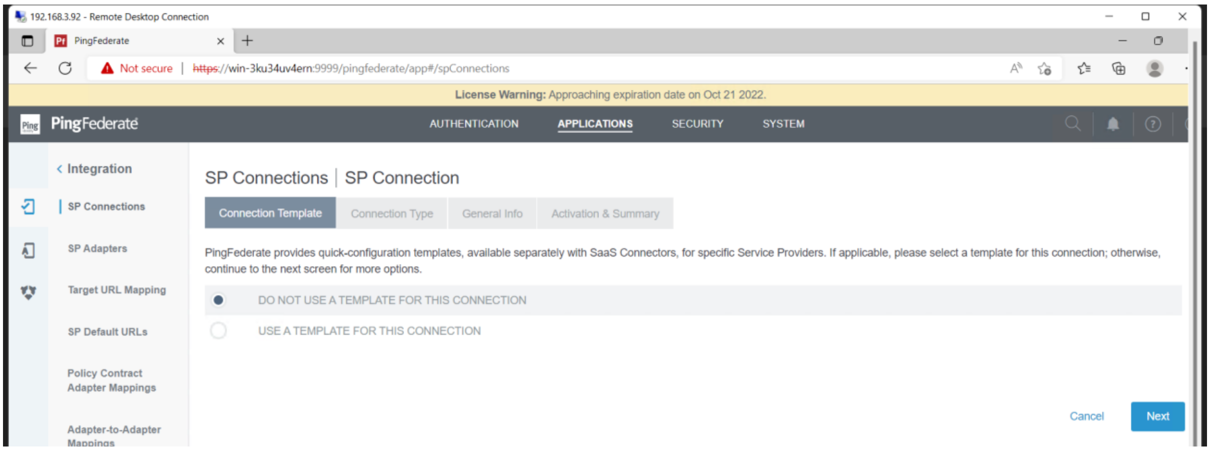


This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
▼<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 Ping Federate Admin Console.

8. Click **Applications,** Click on **SP connections** in the left menu.
9. Click on **Create Connections**



License Warning: Approaching expiration date on Oct 21 2022.

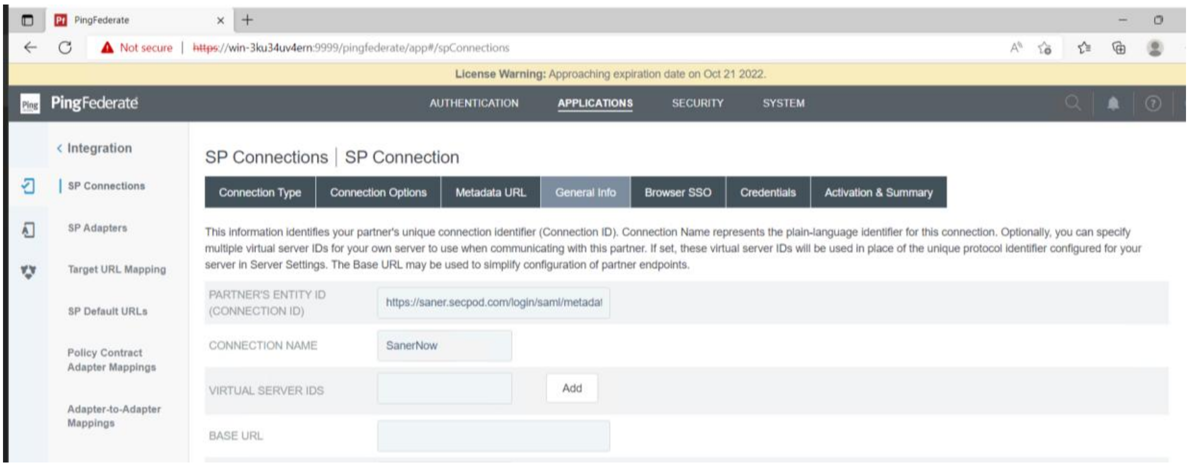
SP Connections | SP Connection

PingFederate provides quick-configuration templates, available separately with SaaS Connectors, for specific Service Providers. If applicable, please select a template for this connection; otherwise, continue to the next screen for more options.

● DO NOT USE A TEMPLATE FOR THIS CONNECTION

○ USE A TEMPLATE FOR THIS CONNECTION

10. Select browser SSO profile under Connection Type, click on Next
11. Select Browser SSO under Connection Options
12. Under Metadata URL click on Next
13. Under General Info, enter Saner entity ID in the Partner's entity ID field



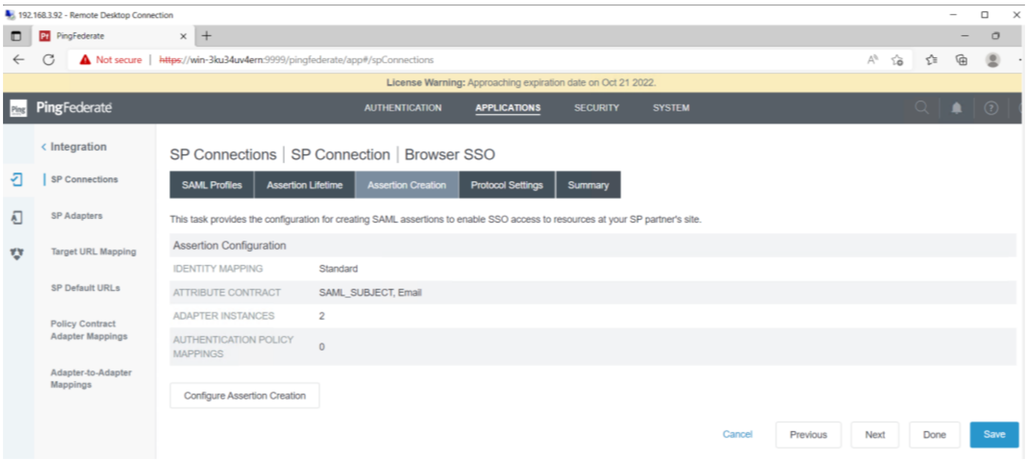
License Warning: Approaching expiration date on Oct 21 2022.

SP Connections | SP Connection

This information identifies your partner's unique connection identifier (Connection ID). Connection Name represents the plain-language identifier for this connection. Optionally, you can specify multiple virtual server IDs for your own server to use when communicating with this partner. If set, these virtual server IDs will be used in place of the unique protocol identifier configured for your server in Server Settings. The Base URL may be used to simplify configuration of partner endpoints.

PARTNER'S ENTITY ID (CONNECTION ID)	https://saner.secpod.com/login/saml/metadat
CONNECTION NAME	SanerNow
VIRTUAL SERVER IDS	
BASE URL	

14. Enter the connection name (Saner App), click on Next
15. Under Browser SSO, Configure Browser SSO
16. Under SAML profiles, enble IDP initiated SSO and SP initiated SSO, click on Next
17. Under Assertion Lifetime, click on Next
18. Under Assertion Creation, click on Configure Assertion Creation.
19. In identity mapping, select standard, and click on Next
20. Under Attribute contract, in the Attribute contract section, select Email address as SAML subject



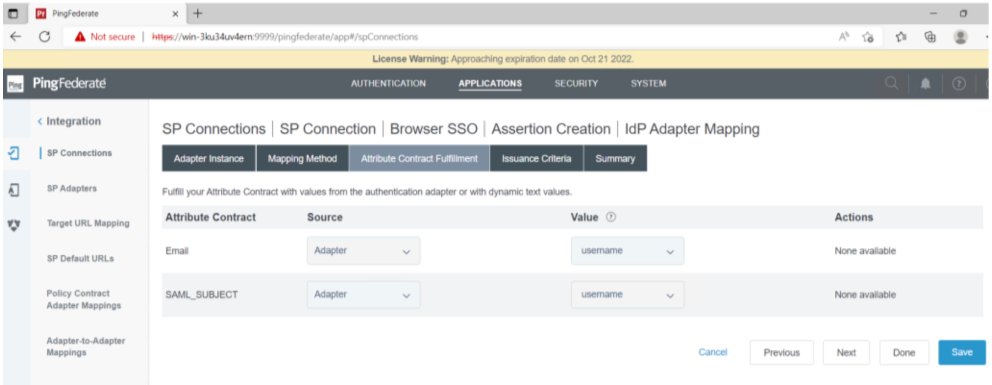
License Warning: Approaching expiration date on Oct 21 2022.

SP Connections | SP Connection | Browser SSO

This task provides the configuration for creating SAML assertions to enable SSO access to resources at your SP partner's site.

Assertion Configuration	
IDENTITY MAPPING	Standard
ATTRIBUTE CONTRACT	SAML_SUBJECT, Email
ADAPTER INSTANCES	2
AUTHENTICATION POLICY MAPPINGS	0

21. Under Extend the Contract, enter the name Email and basis as the attribute name format, click on Next



License Warning: Approaching expiration date on Oct 21 2022.

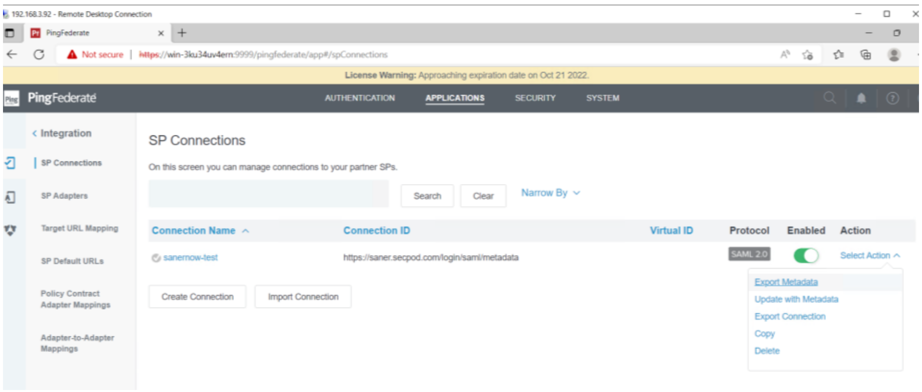
SP Connections | SP Connection | Browser SSO | Assertion Creation | IdP Adapter Mapping

Fulfill your Attribute Contract with values from the authentication adapter or with dynamic text values.

Attribute Contract	Source	Value	Actions
Email	Adapter	username	None available
SAML_SUBJECT	Adapter	username	None available

22. Under Authentication source mapping, select the Adapter instance to be used (User DB connection)
23. Click on Next
24. Verify the summary and click on done.
25. Under Assertion Creation, click on Next
26. Under Protocol Settings, click on Configure Protocol Settings
27. In Assertion Consumer Service URL section, for the default value, select post as binding, Index as 1, Saner metadata under Endpoint URL, click on Add. Click on Next
28. Select Post & Redirect under Allowable SAML Bindings. Click on Next
29. Under Signature Policy, enable all the checkboxes if requests has to be signed for authentication. Else, Click on Next
30. Under Encryption Policy, select None and Click on Next
31. Verify the summary and click on Done
32. Under Protocol Settings, click on Next
33. Verify the summary and click on Done
34. Under Browser SSO, click on Next
35. Under Browser, click on Configure Credentials
36. Under Digital Signature Settings, click on Manage Certificates, import Saner Certificate, click on Done
37. Under Digital Signature Settings, Click on Next
38. Under Signature Verification Settings, click on Manage Signature Verification Settings
39. Under Trust Model, create Unanchored, and Click on Next

40. Under Siganture Verification Certificate, click on Manage Certificate, import the digital verification certificate, and click on Done.
41. Under Signature Verification Certificate, click on Next.
42. Verify the summary and Click on Done.
43. Under Signature Verification Settings, click on Next.
44. Verify the Summary and click on Done
45. Under Credentials, Click on Next
46. Verify the Activation & Summary, scroll down and click on Save.
47. Click on Select Action for the connection added, and select export metadata and download the metada file.



License Warning: Approaching expiration date on Oct 21 2022.

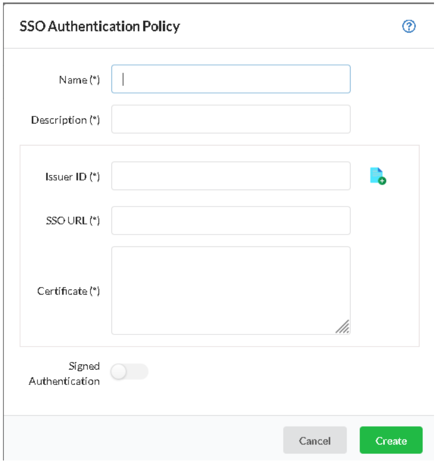
SP Connections

On this screen you can manage connections to your partner SPs.

Connection Name	Connection ID	Virtual ID	Protocol	Enabled	Action
sanernow-test	https://saner.secpod.com/login/saml/metadata		SAML 2.0	●	Select Action

48. Copy the Identity Provider Single Sign-On URL and identity provider issuer and the X.509 Certificate from the downloaded metadata and certificate file.
49. Return to the SSO authentication page in Saner.
50. Configure SSO in Saner using the downloaded certificate and copied URLs from Ping Federate 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 Ping Federate.
- Specify the required name and description for the SSO policy
- Enable signed authentication if you have configured it in Ping Federate
- Click on Create

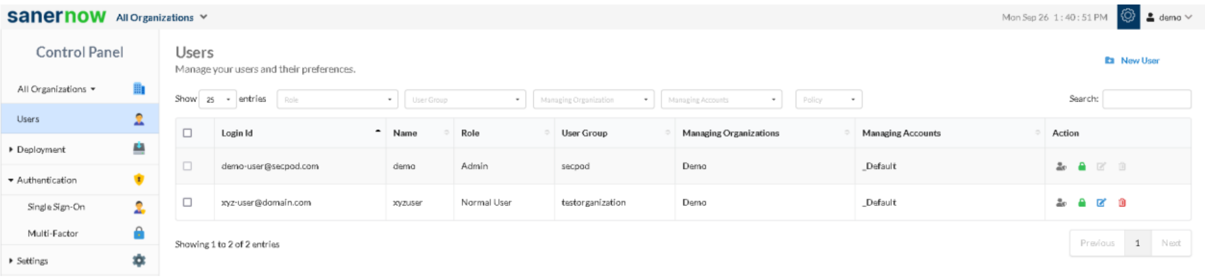
Steps to Assign users to the app in Ping Federate

As part of the IDP adapter selection in the above steps the User DB will be assigned to the application.

Assign SSO policy to Saner Existing Users

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

- Go to Control Panel. Click on Users.



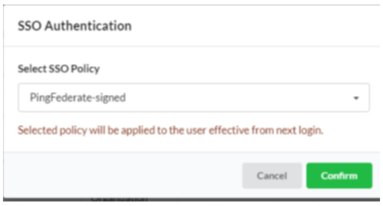
Users

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

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



SSO Authentication

Select SSO Policy

PingFederate-signed

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

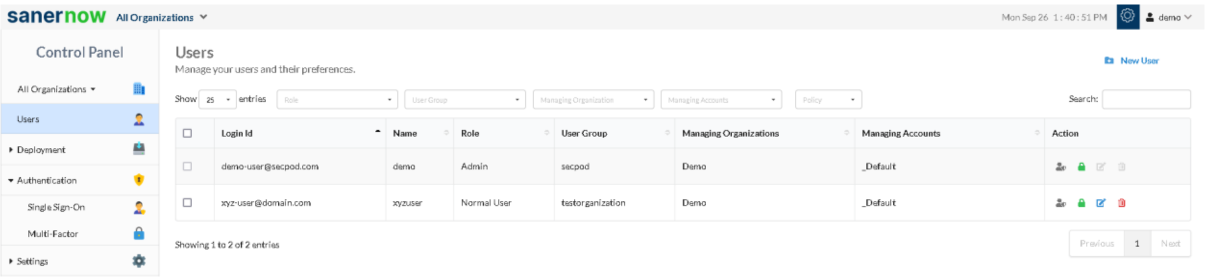
- Click on Confirm

How to apply SSO Policy to the New 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.



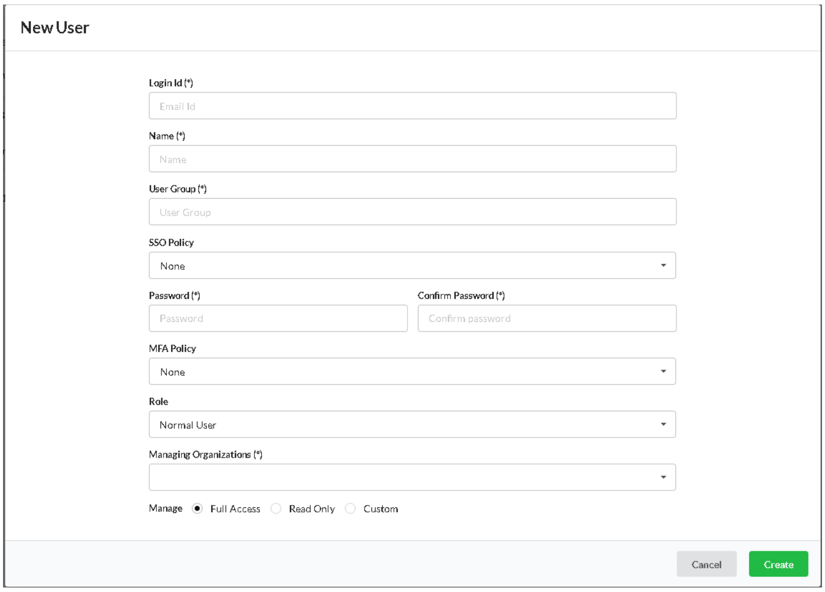
Users

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