How to Sign in SanerNow through Ping Federate using SAML SSO

Pre-requisites for signing in via Ping Federate SSO

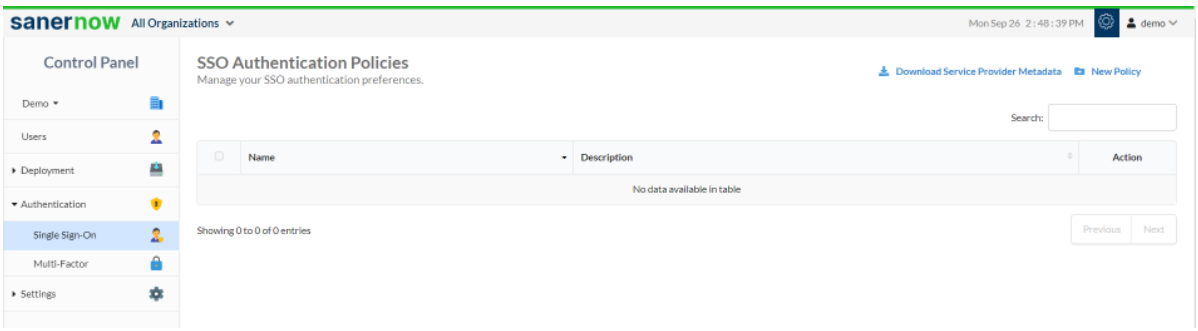
Following are the pre-requisites to configure Ping Federate SSO

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

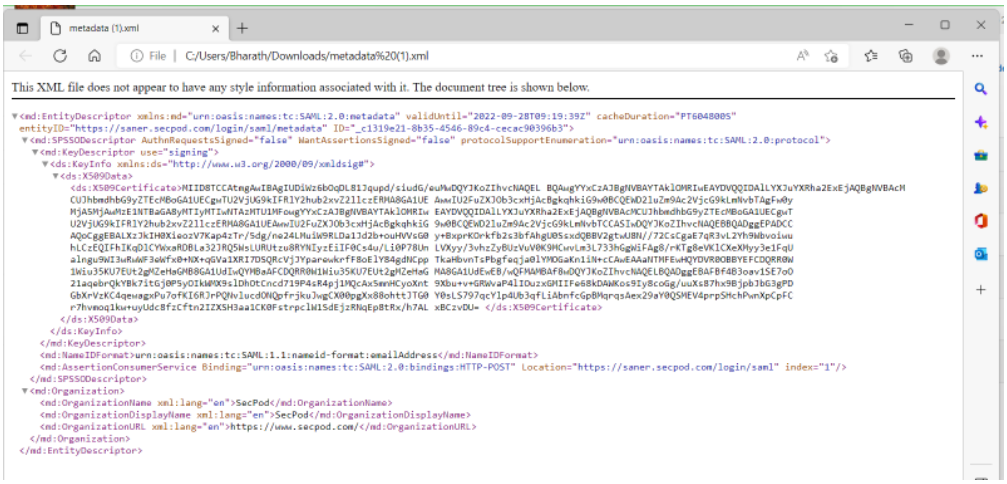
Follow the steps given below to retrieve the information mentioned above.

Steps to configure SAML-based SSO

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

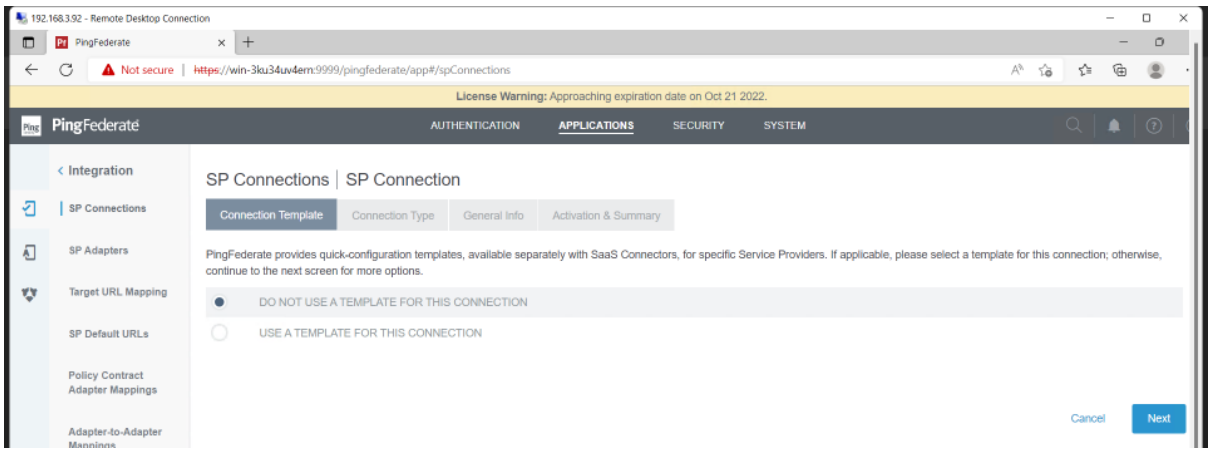


4. Click on **Download Service Provider metadata file**
5. Open the downloaded metadata file from your browser or a text editor.

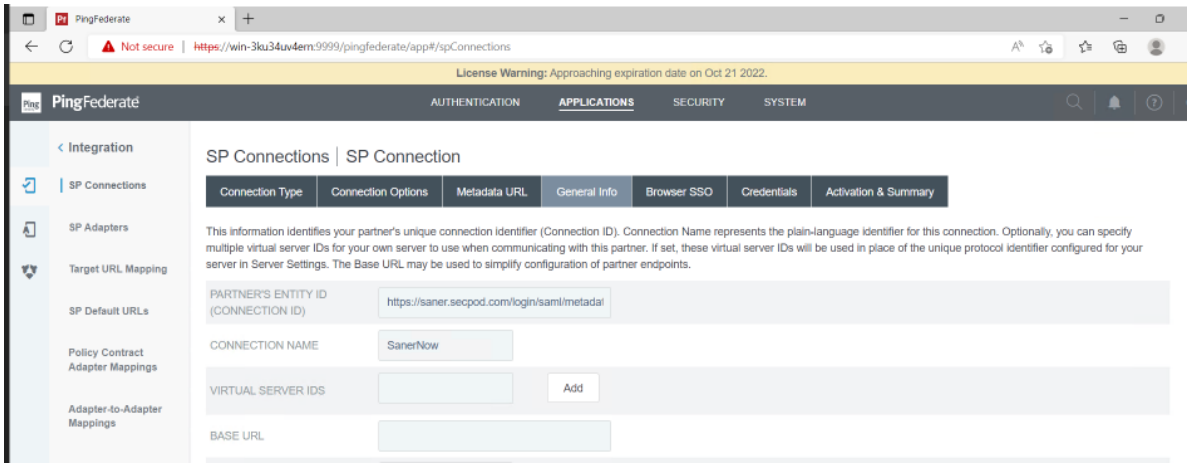


6. Copy and save the Entity ID and ACS URL from the metadata file you downloaded.
7. Sign in to your organization's Ping Federate Admin Console.
8. Click **Applications,** Click on **SP connections** in the left menu.
9. Click on **Create Connections**

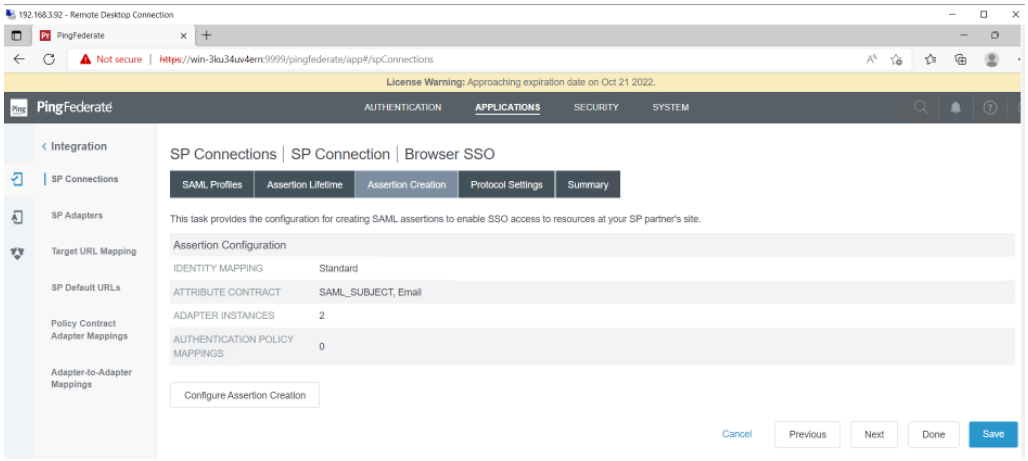
Copyright©2008-2022 SecPod Technologies. All Rights Reserved.



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 SanerNow entity ID in the Partner's entity ID field

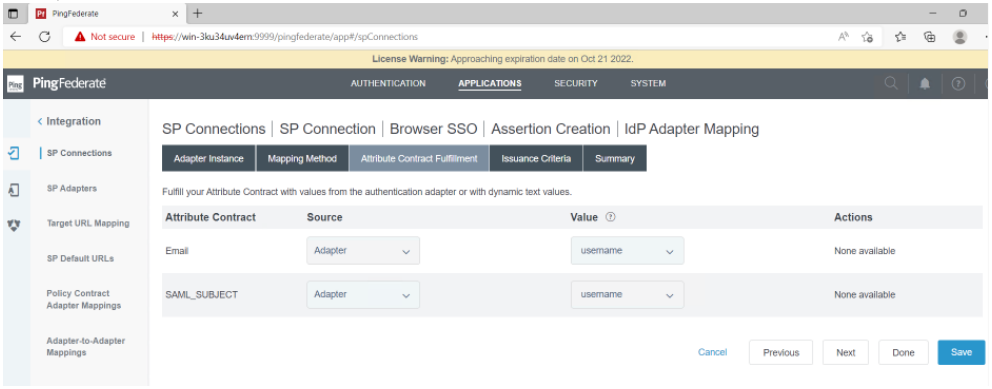


14. Enter the connection name (SanerNow App), click on Next
15. Under Browser SSO, Configure Browser SSO
16. Under SAML profiles, enble IDP initiated SSO and SP initiated SSO, click on Next
17. Under Assertion Lifetime, click on Next
18. Under Assertion Creation, click on Configure Assertion Creation.
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



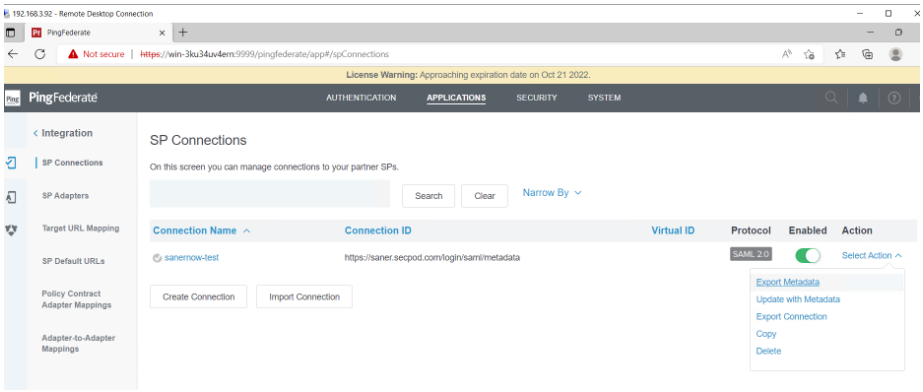
Copyright©2008-2022 SecPod Technologies. All Rights Reserved.

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



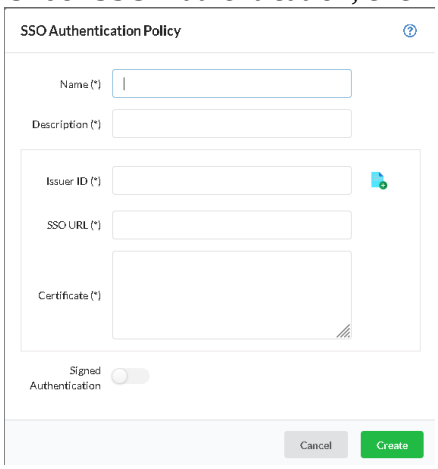
22. Under Authentication source mapping, select the Adapter instance to be used (User DB connection)
23. Click on Next
24. Verify the summary and click on done.
25. Under Assertion Creation, click on Next
26. Under Protocol Settings, click on Configure Protocol Settings
27. In Assertion Consumer Service URL section, for the default value, select post as binding, Index as 1, SanerNow 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 SanerNow 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.

Copyright©2008-2022 SecPod Technologies. All Rights Reserved.



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 SanerNow
50. Configure SSO in SanerNow using the downloaded certificate and copied URLs from Ping Federate by following the steps given below:

- Under SSO Authentication, click on new SSO policy.



- 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

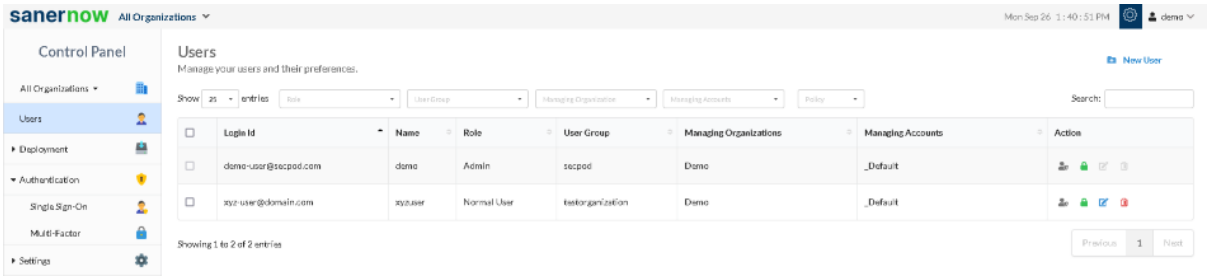
As part of the IDP adapter selection in the above steps the User DB will be assigned to the application.

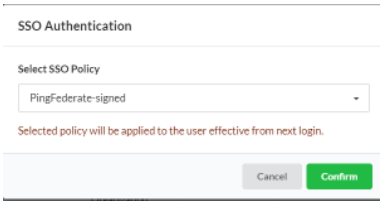
Assign SSO policy to SanerNow Existing Users

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

- Go to Control Panel. Click on Users.

Copyright©2008-2022 SecPod Technologies. All Rights Reserved.



- 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
- 

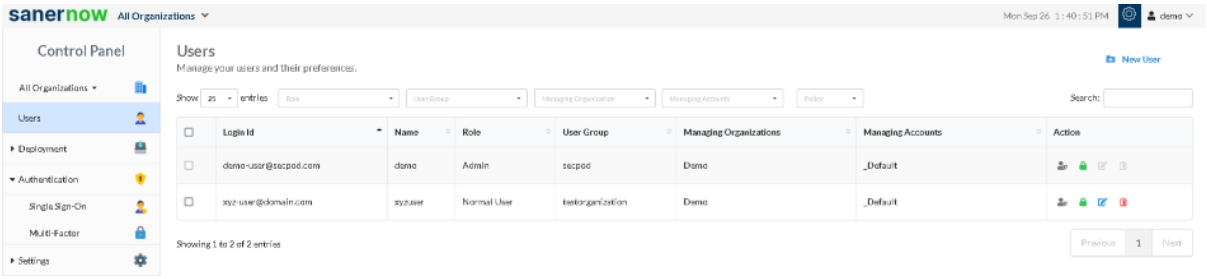
- Click on Confirm

How to apply SSO Policy to the New user

Step 1: Log in to SanerNow and then click Control Panel at the top-right to access the Control Panel page.

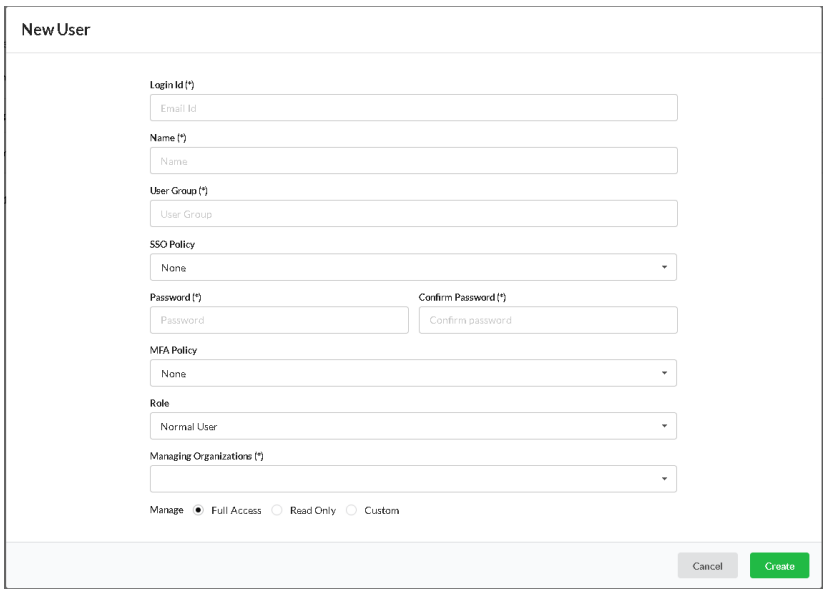
Step 2: **All Organizations** are selected from the drop-down by default on the control panel page. If the admin has created only one organization, the page will automatically select that organization and show its accounts.

Step 3: Click the Users section in the Control Panel.



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

Copyright©2008-2022 SecPod Technologies. All Rights Reserved.



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 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 SanerNow and will be signed in.

Via IdP-initiated flow:

1. Sign in to Ping Federate 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.

Copyright©2008-2022 SecPod Technologies. All Rights Reserved.