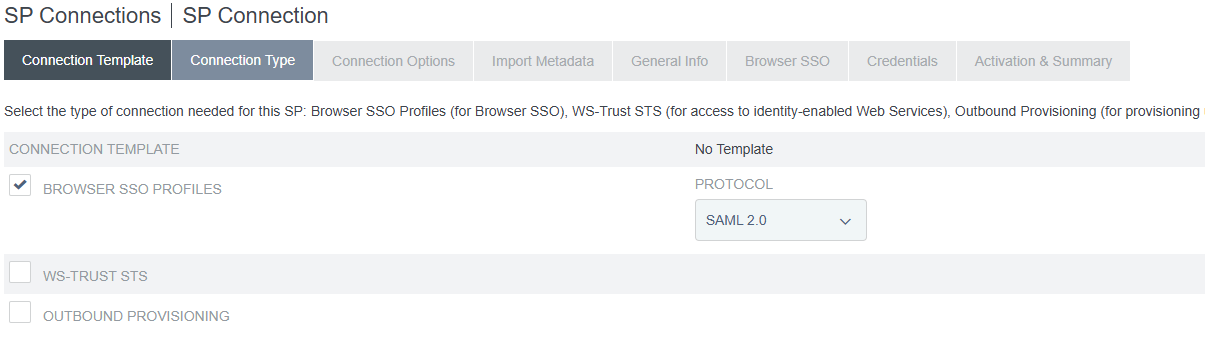
Steps to Integrate Docker Desktop SSO with Ping Federate

1. Login in to PingFederate Admin Console .

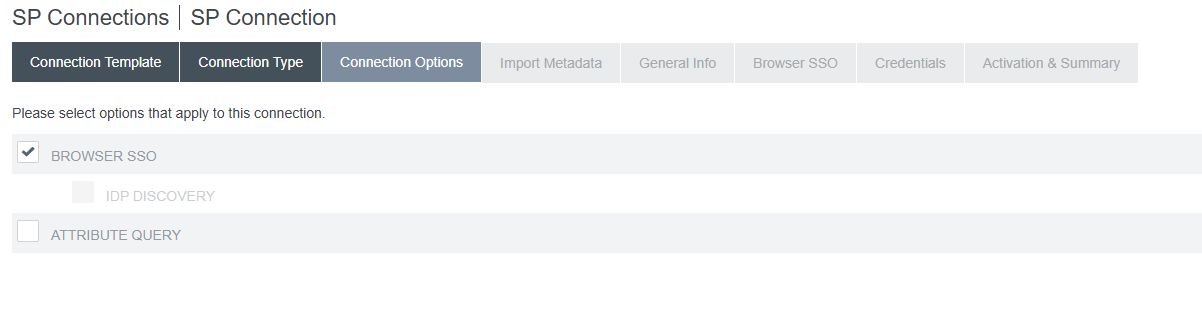
2. Navigate to Application--> Integration --> SP Connection > Create New SP Connection.

3. Under Connection Template , Select Browser SSO Profile

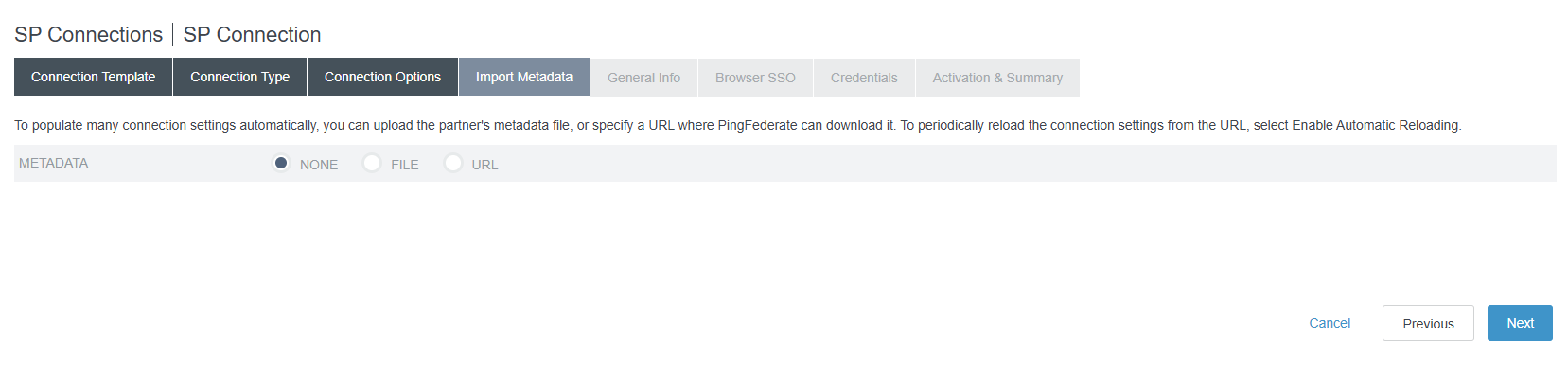


Click Next

4. Select Browser SSO under Connection Options



5. Pick None in Import Meta Data if Metadata file is not there.

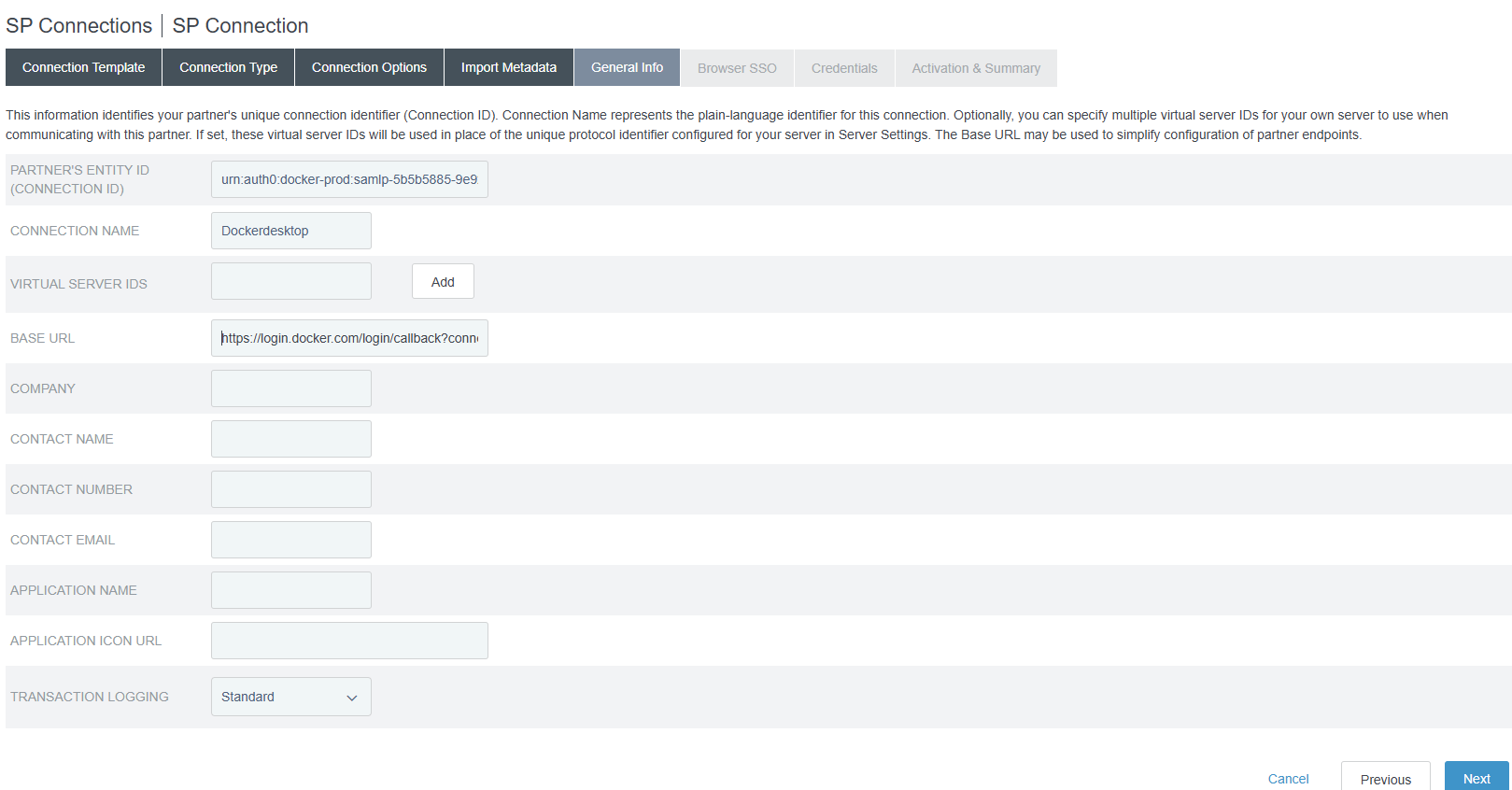


6. Under General Info , Fill in

Partner Entity ID : urn:auth0:docker-prod:samlp-TenantID

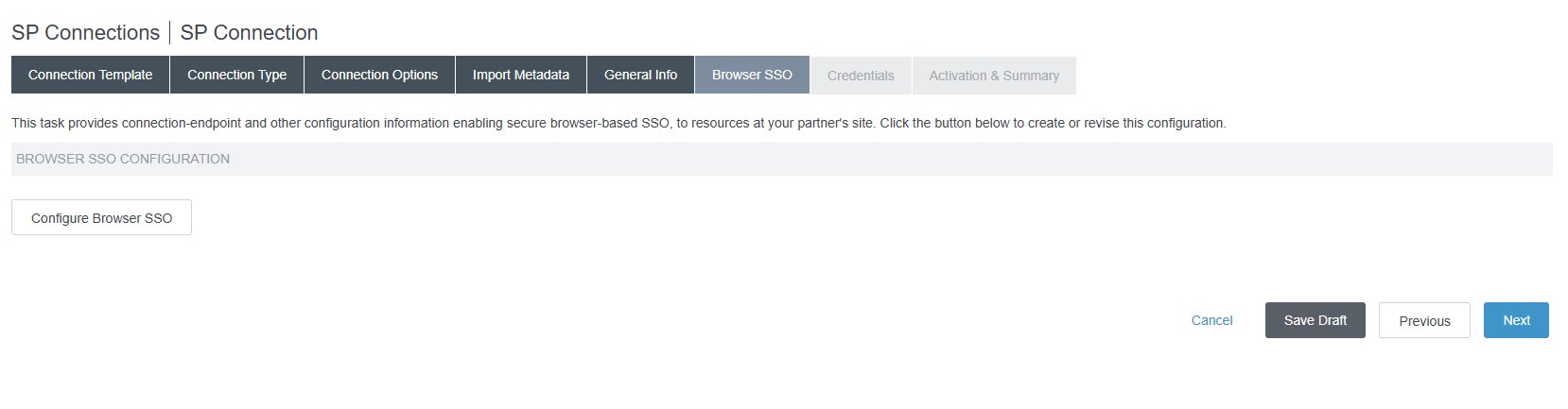
Note = Get the exact value From Docker Administration Consle.

Base URL : https://login.docker.com/login/callback?connection=samlp-TenantID

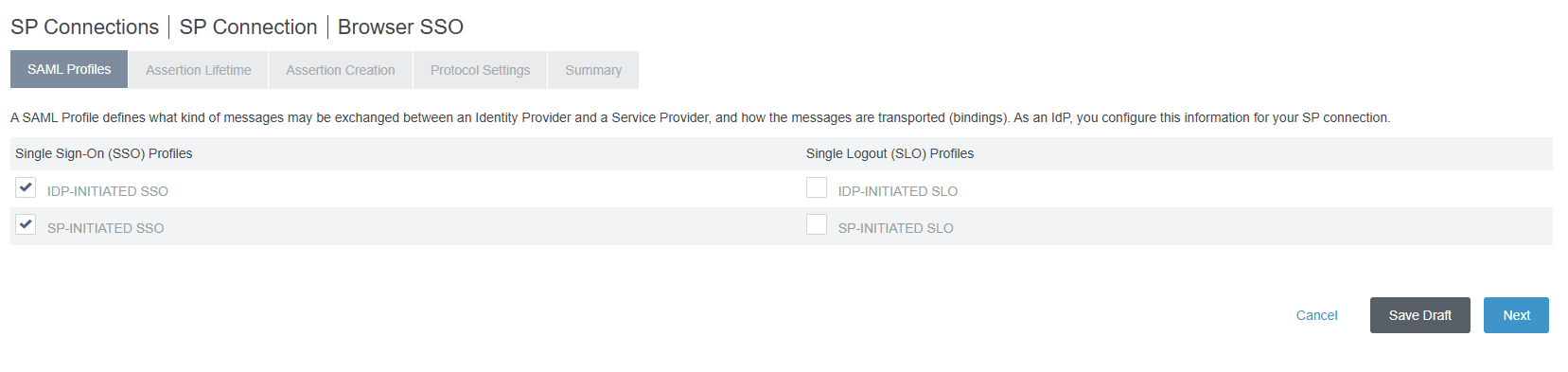


7. Click Next

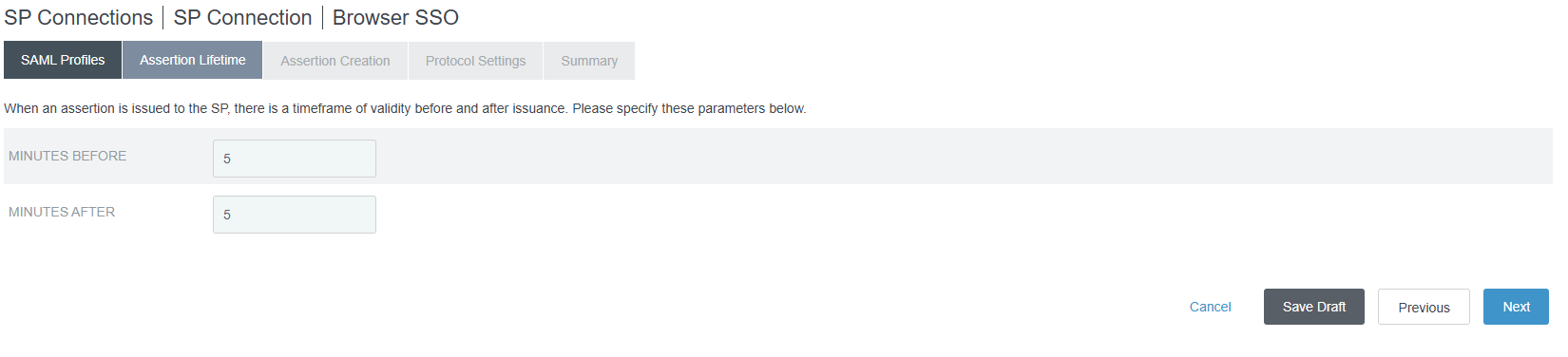
8. Under Browser SSO, Click Configure Browser SSO.



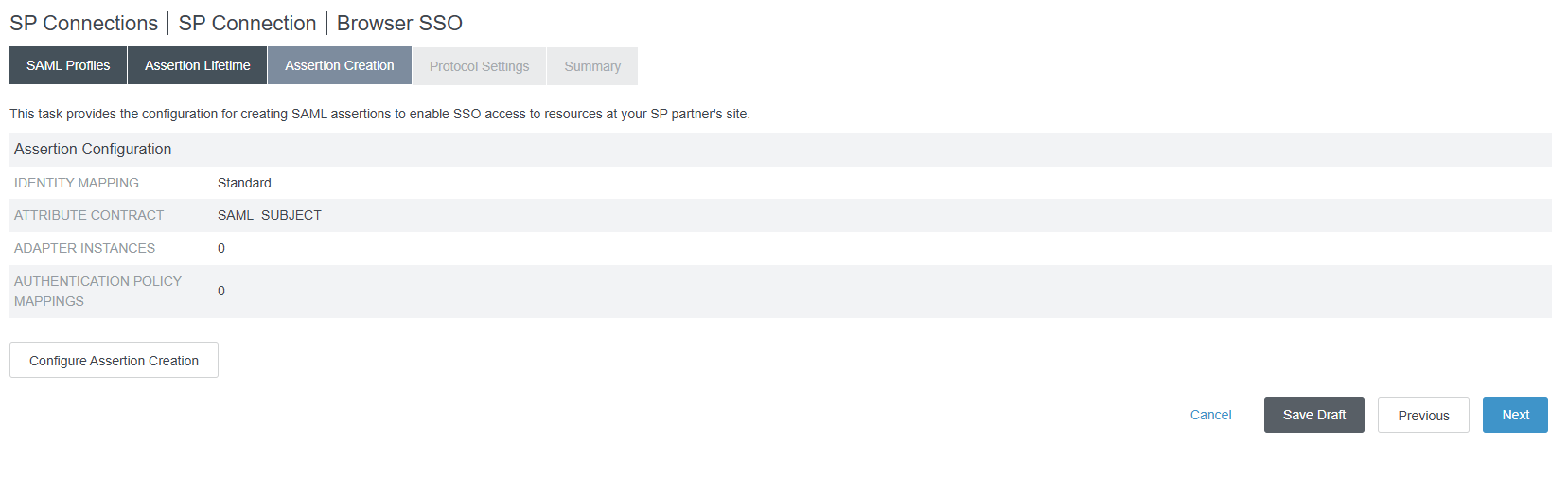
9. Select IDP-Initiated SSO and SP-Initiated SSO



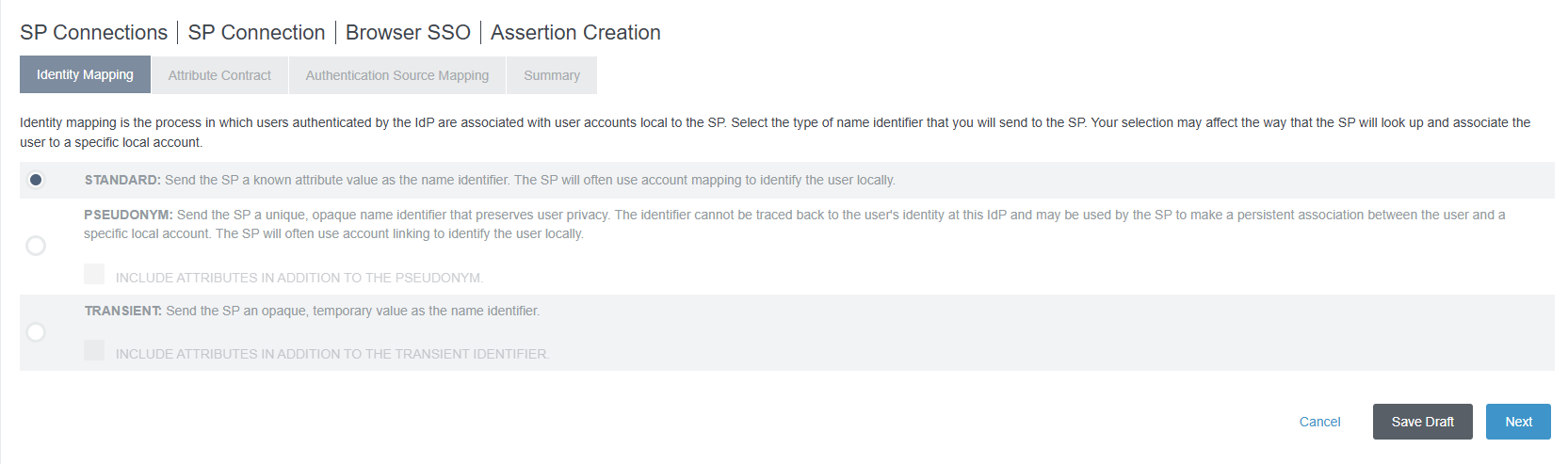
10. Leave Default values under Assertion Lifetime



11. Click Next.



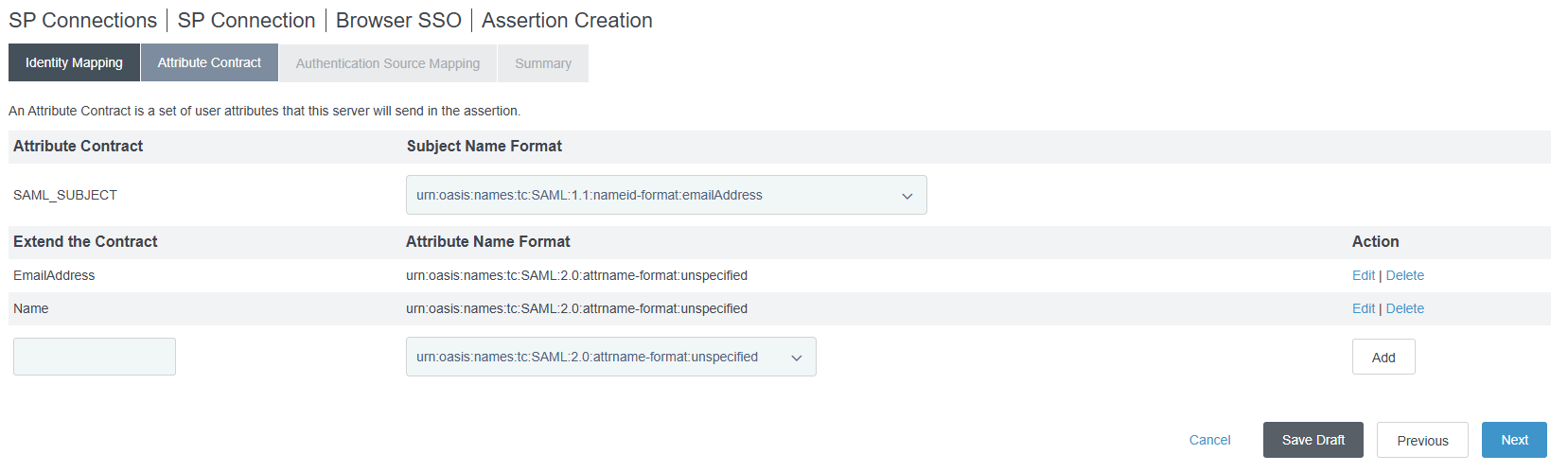
12. Click Configure Assertion Creation.



13. Chose Standard. Click Next.

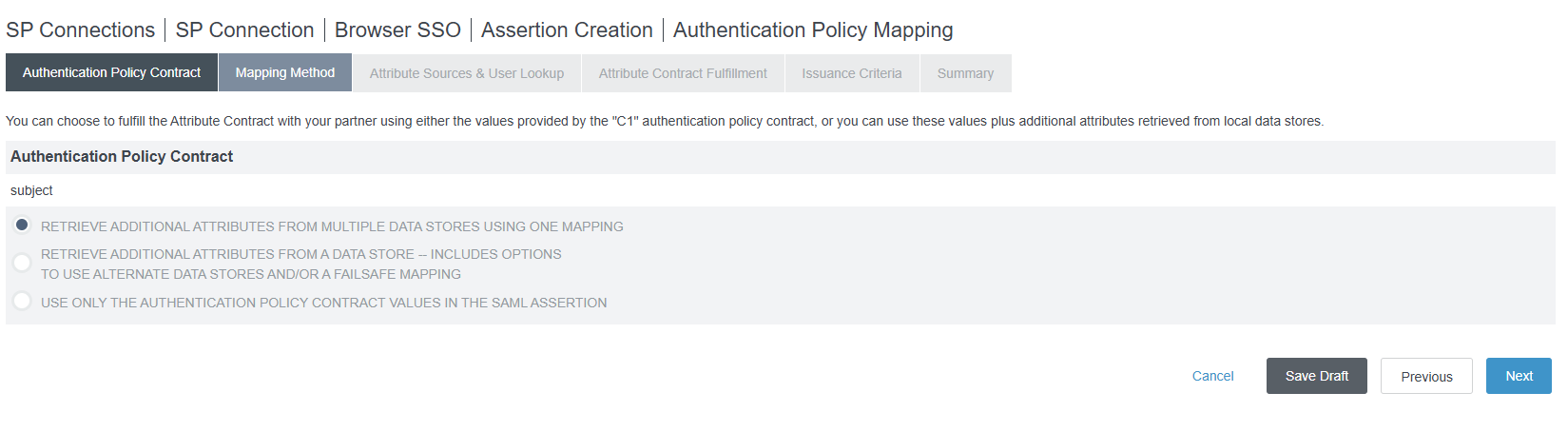
14. Under Attribute Contract Add below Attributes

|  |  |
| --- | --- |
| Attribute | Subject Name Format |
| SAML\_SUBJECT | urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress |
| EmailAddress | urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified |
| Name | urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified |



15. Click Map New Authentication Policy and Choose the Authentication Policy of your Enterprise.

16. Based on the Attributes Available in Contract , Choose one of the below.



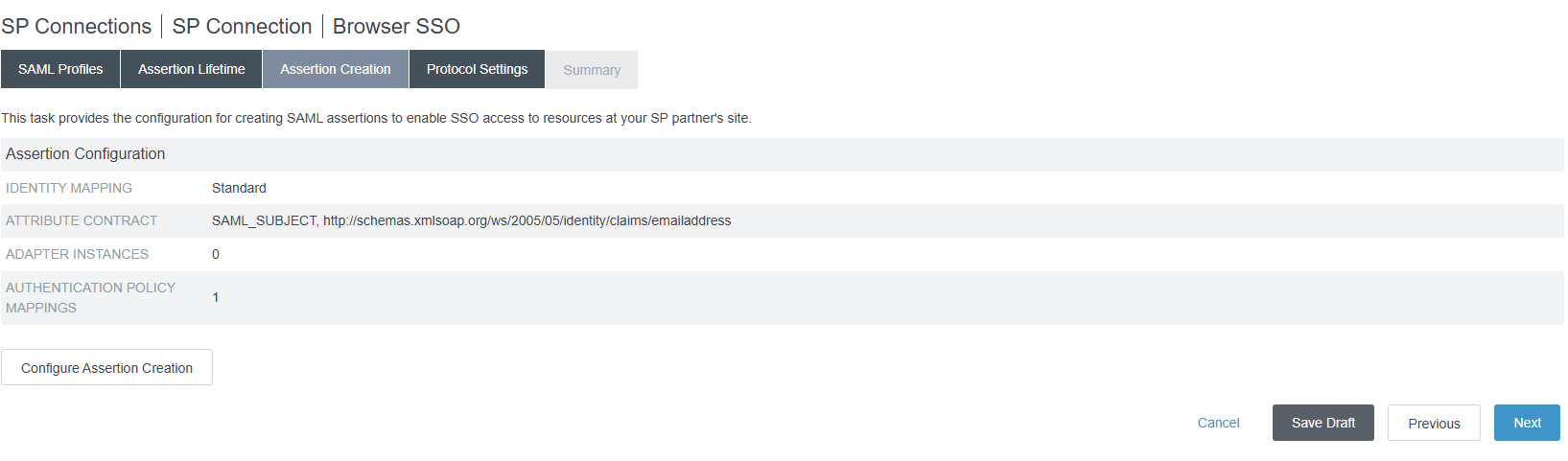
17. Under Attribute Contract Fulfillment Select

<http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress>

|  |  |
| --- | --- |
| Attribute Contract | Value |
| SAML\_SUBJECT | email |
| EmailAddress | email |
| Name | #value=#firstName.toString()+" "+#lastName.toString() |

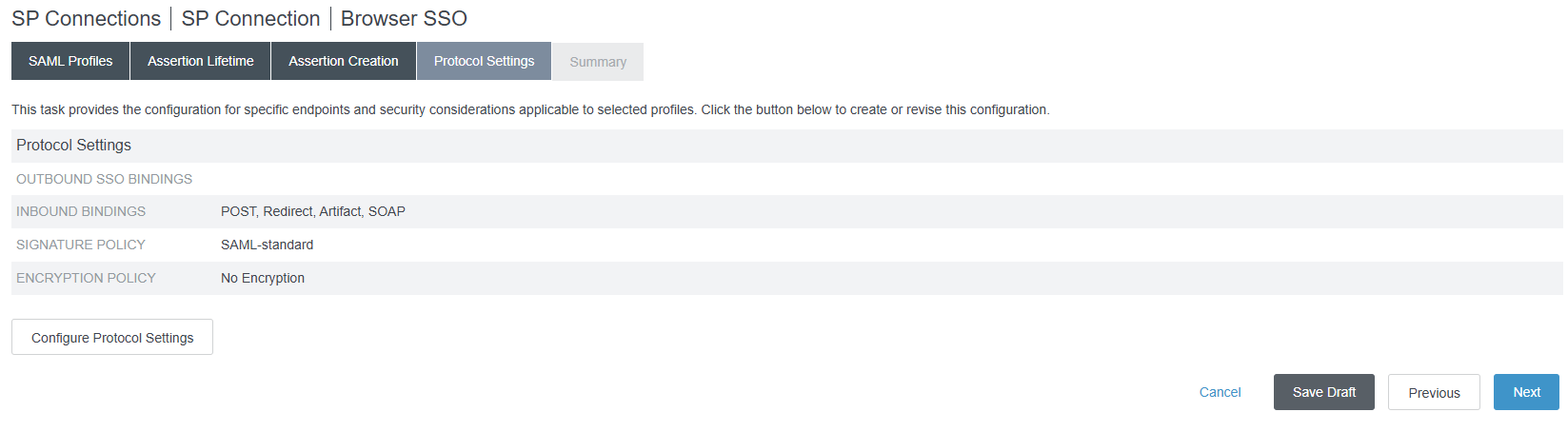
18. Select Issuance Criteria based on your Enterprise Choice.

19. Click Done.



Sample Screen as above will be shown.

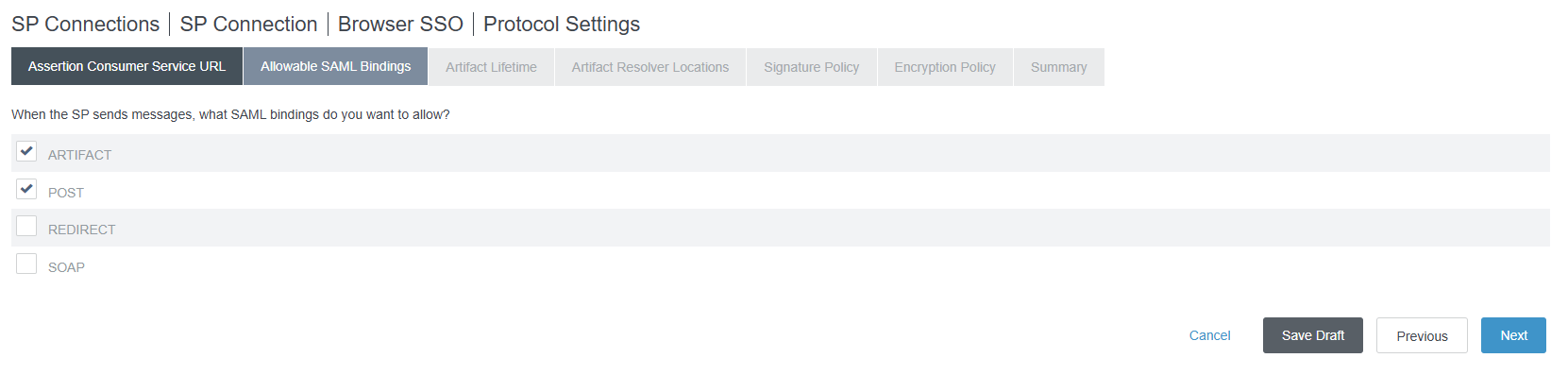
20. Click Next. This will take you to Protocol Settings Page.



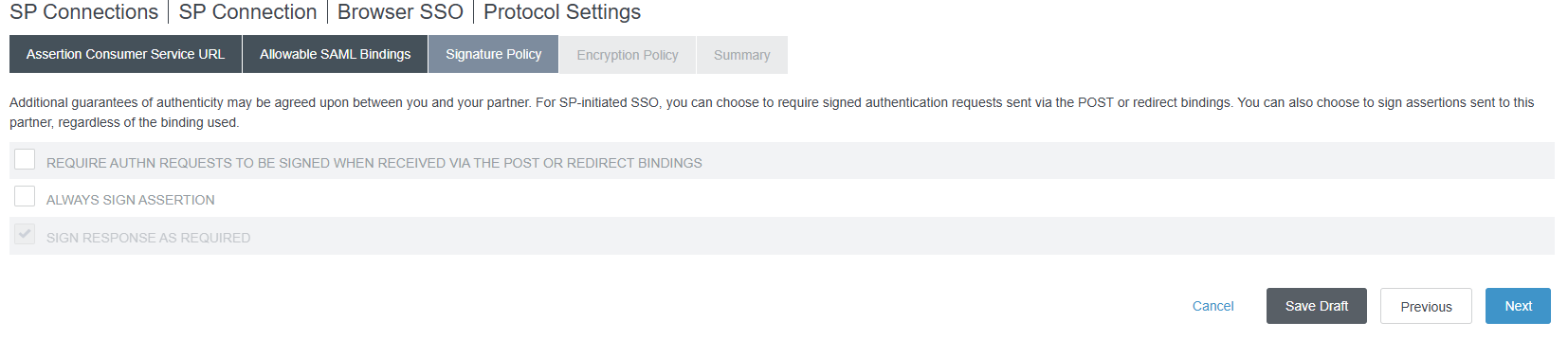
21. Click Configure Protocol Settings .

Select Artifact and Post under Bindings and enter <https://login.docker.com/login/callback?connection=samlp-tenantid> as Endpoint URL. Click ADD

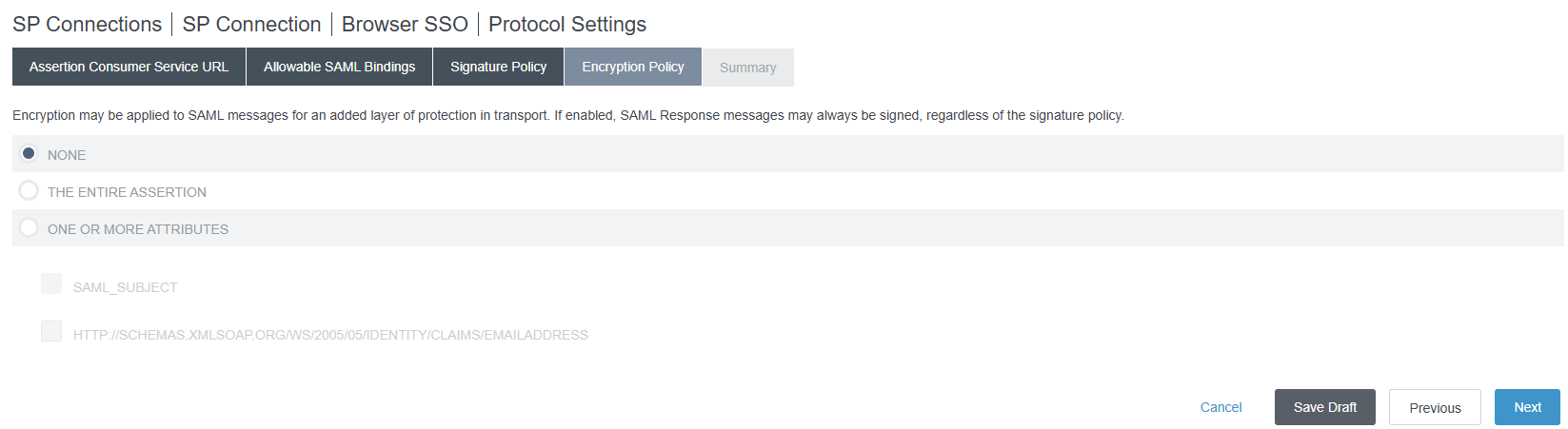
22. Choose Artifact and Post under Allowed SAML Bindings



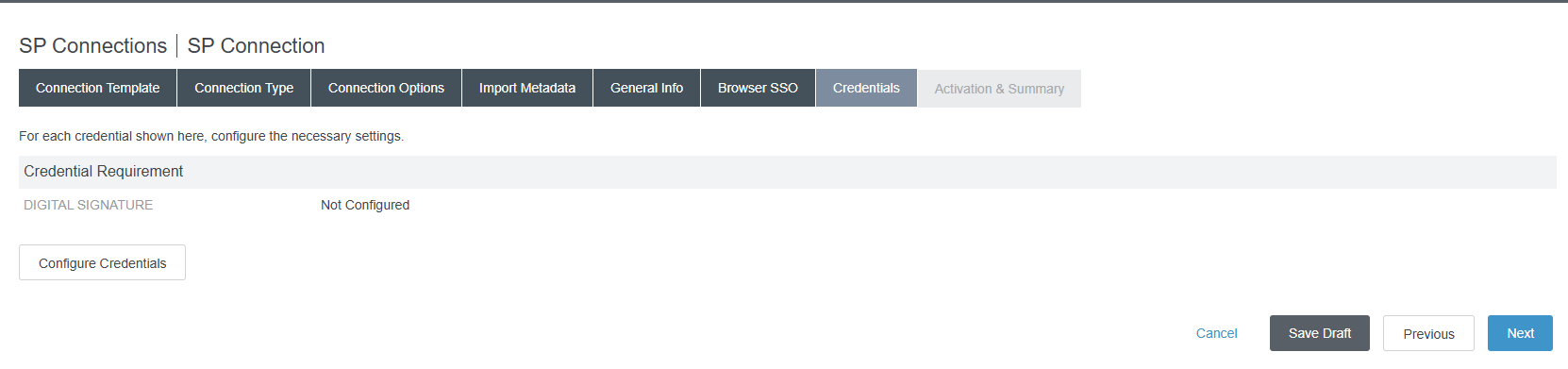
23. Select One of the following based on your Enterprise Requirement.



24. Select None for Mentorship for Encryption. Choose based on your Enterprise Needs.

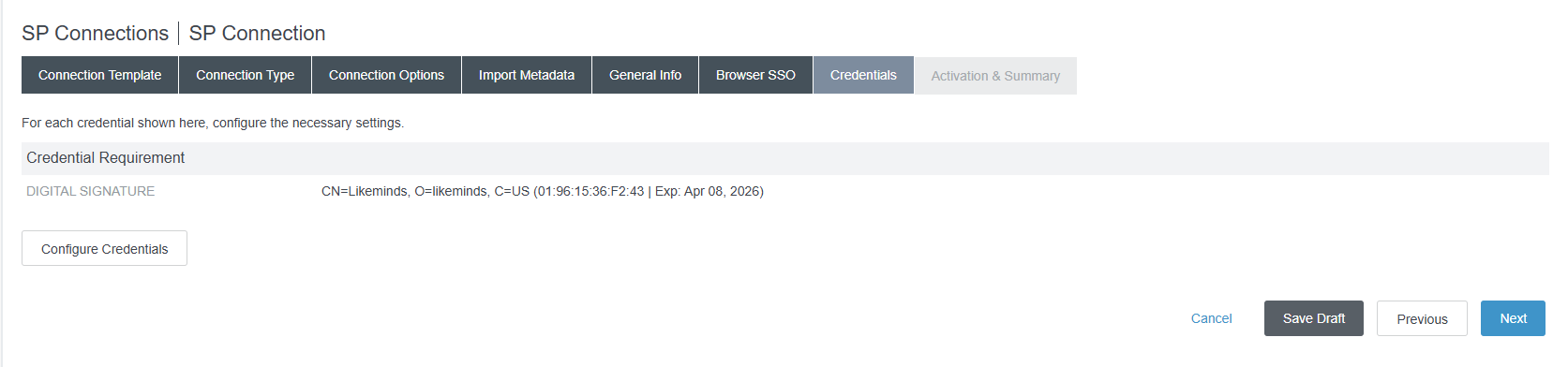


25. Click Next and Move to Credential Tab.



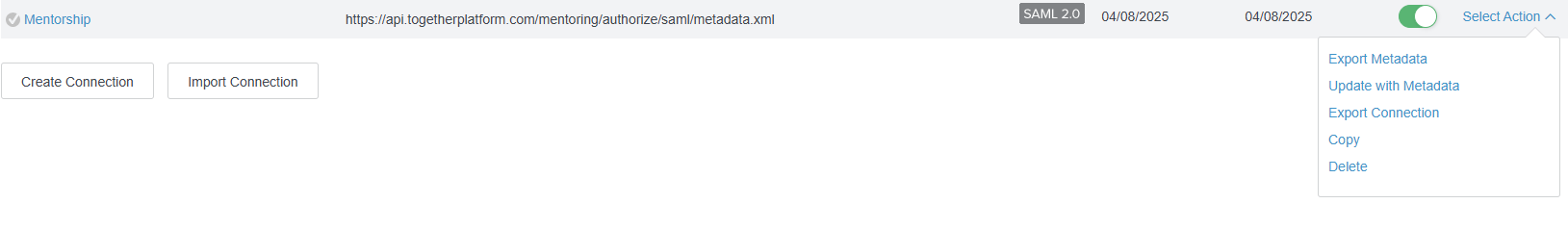
26. Click Configure Credentials.

27. Select the Digital Certificate of your Enterprise.



28. Click Save on the SP Connection Summery page.

29. Select the SP Connection and Export the Metadata.



30. Share the Metadata with the Docker Application Admin.

31. Follow the steps in to setup together platform and import Metadata

https://docs.docker.com/security/for-admins/single-sign-on/connect/