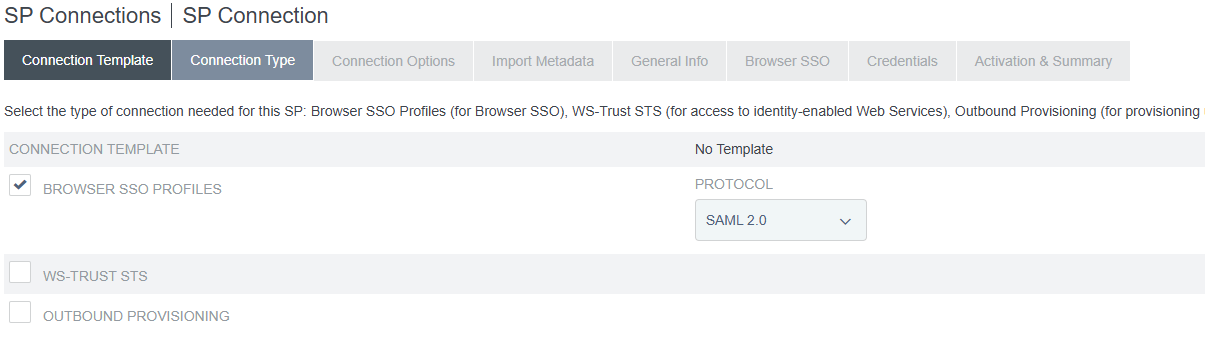
Steps to Integrate Atlassian Cloud SSO with Ping Federate.

1. Login in to PingFederate Admin Console .

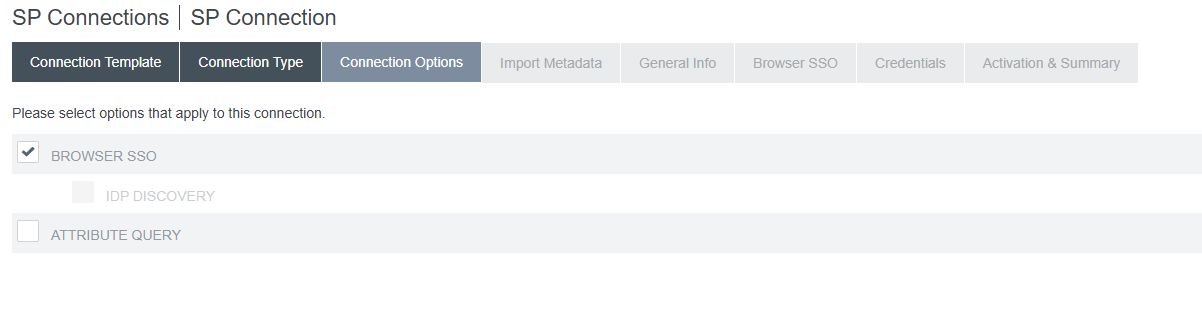
2. Navigate to Application--> Integration --> SP Connection > Create New SP Connection.

3. Under Connection Template , Select Browser SSO Profile

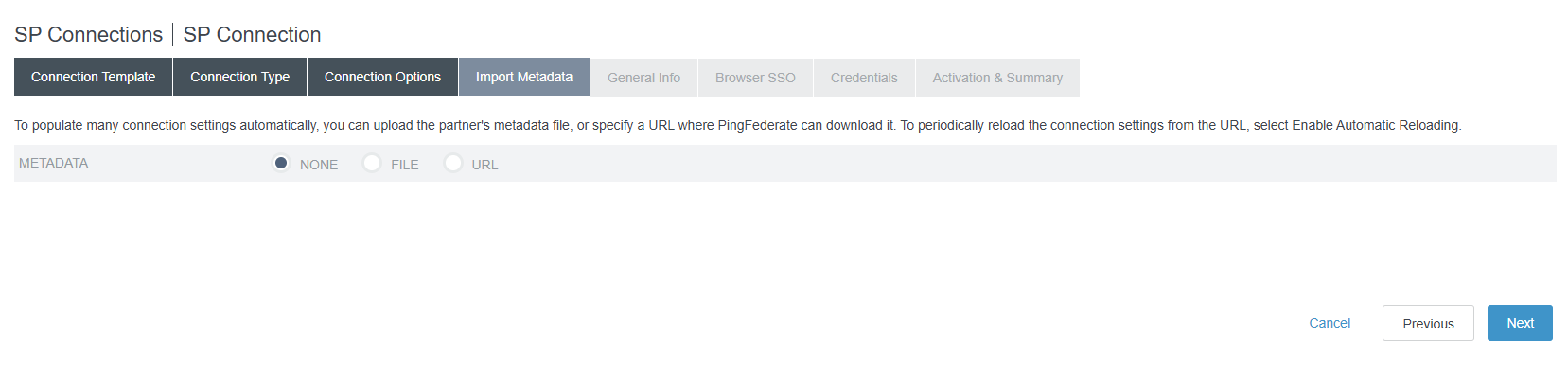


Click Next

4. Select Browser SSO under Connection Options



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

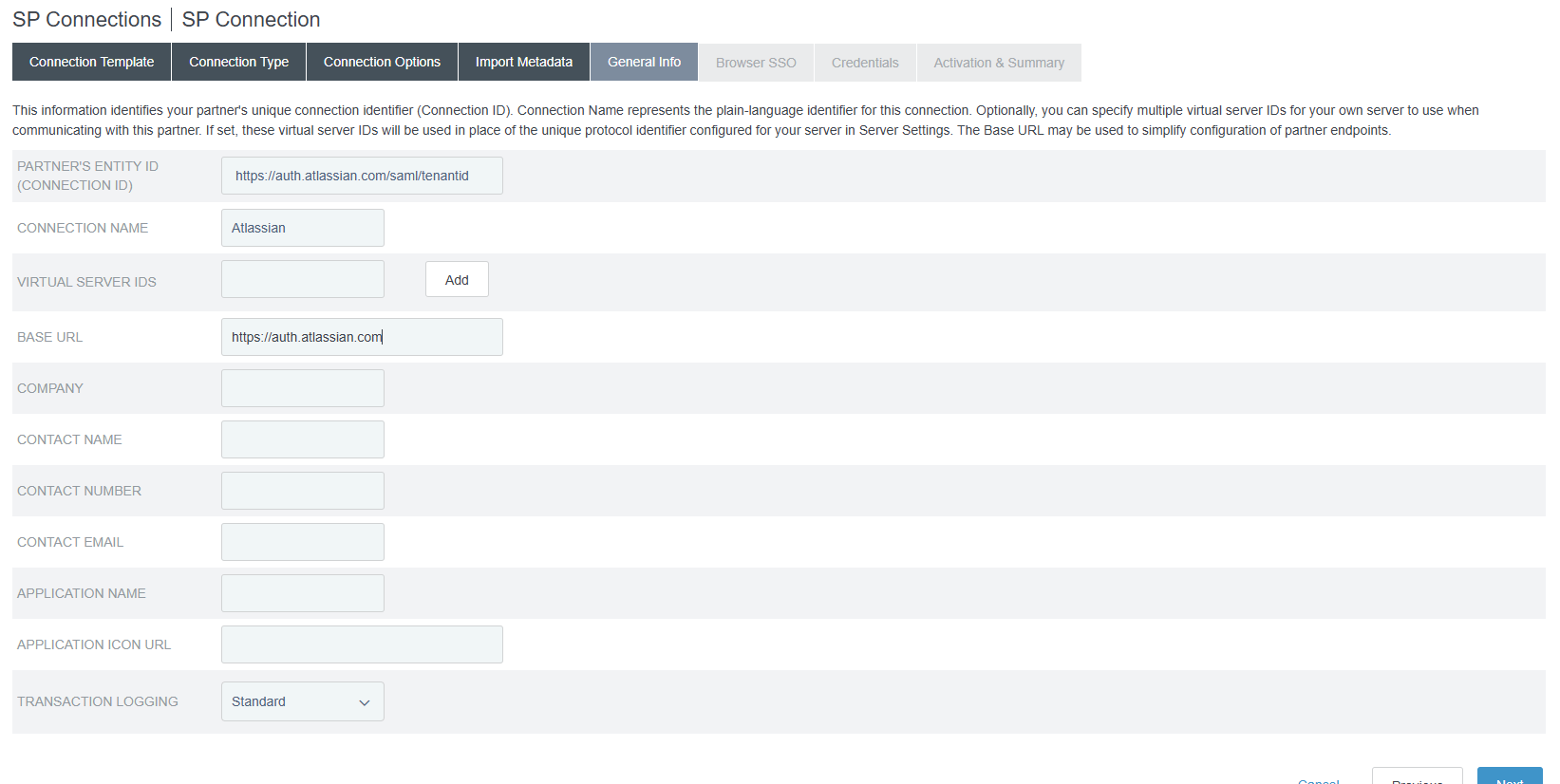


6. Under General Info , Fill in

Partner Entity ID : <https://auth.atlassian.com/saml/xxxxxx>

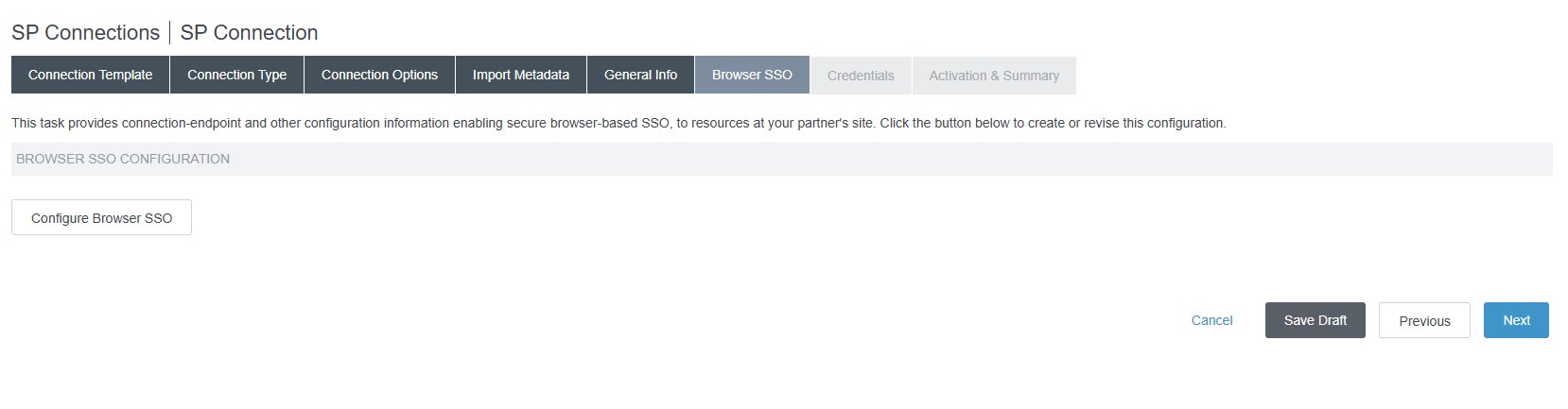
Note = Get the exact value From Atlassian Cloud Administration Page.

Base URL : https://auth.atlassian.com

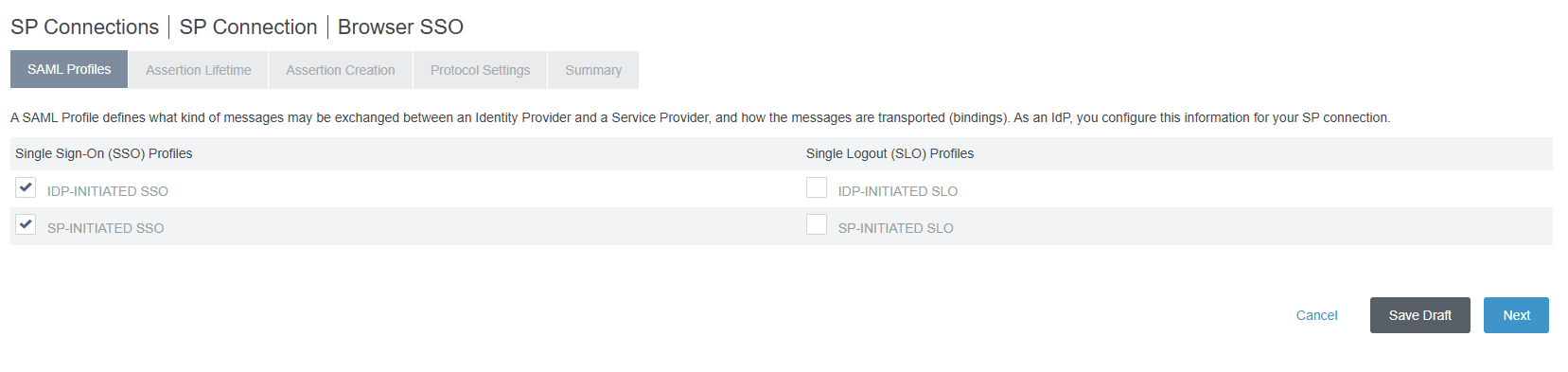


7. Click Next

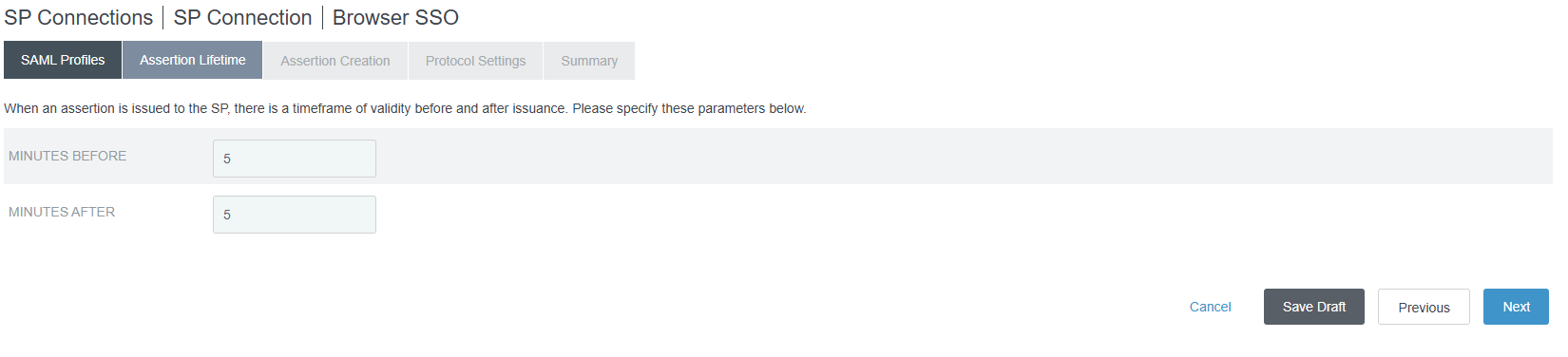
8. Under Browser SSO, Click Configure Browser SSO.



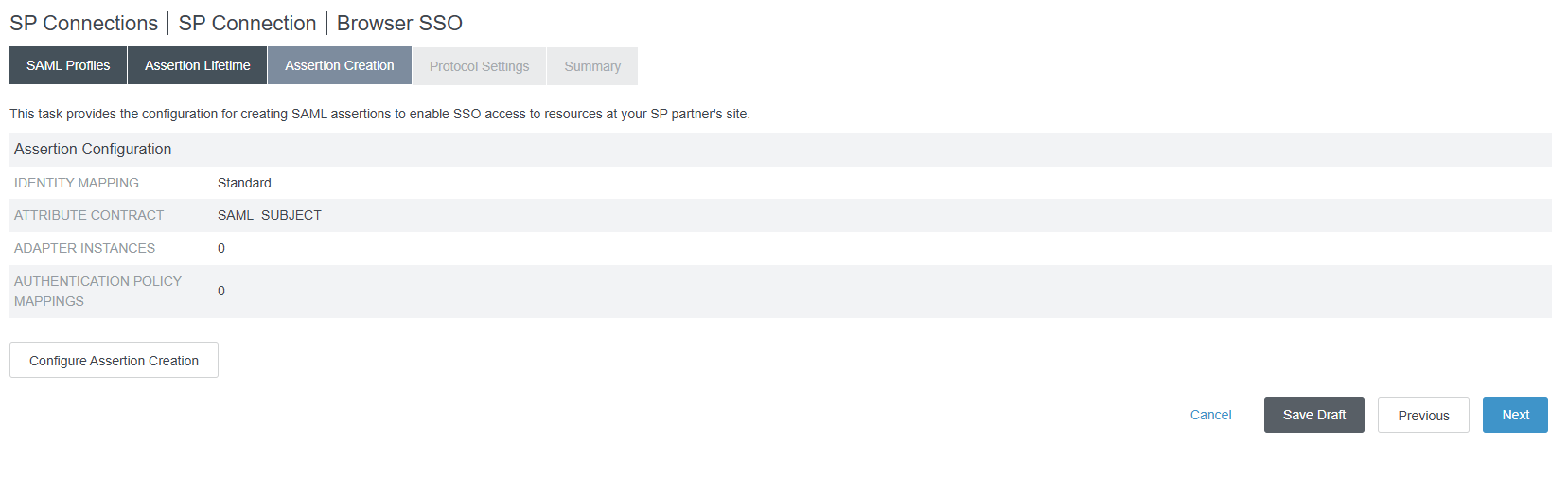
9. Select IDP-Initiated SSO and SP-Initiated SSO



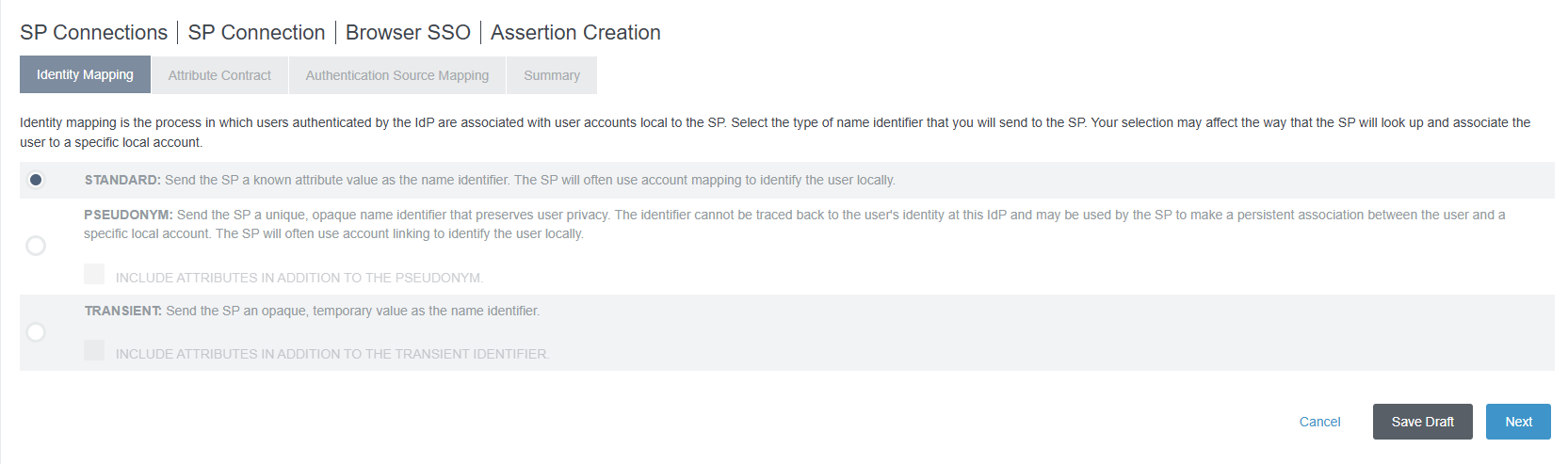
10. Leave Default values under Assertion Lifetime



11. Click Next.



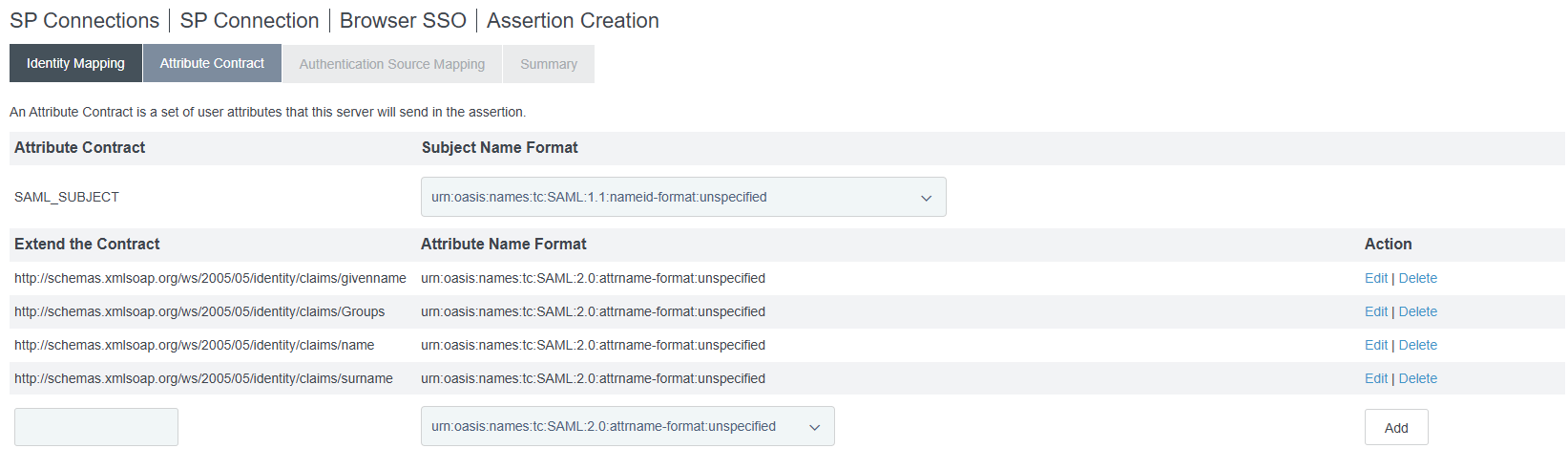
12. Click Configure Assertion Creation.



13. Chose Standard. Click Next.

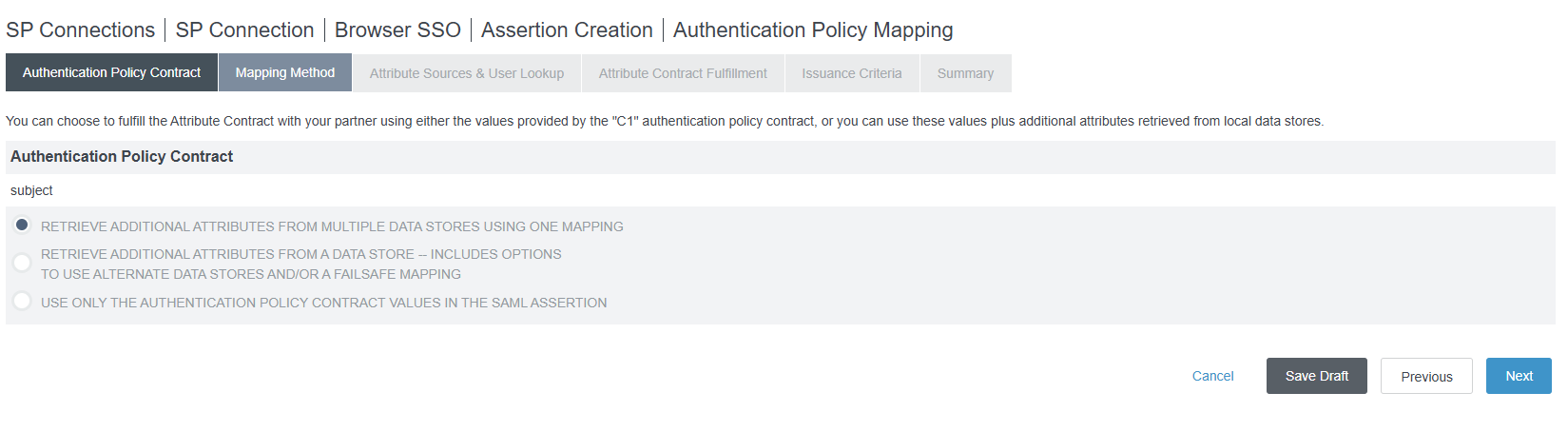
14. Under Attribute Contract Add below Attributes

|  |  |
| --- | --- |
| Attribute | Subject Name Format |
| SAML\_SUBJECT | urn:oasis:names:tc:SAML:2.0:attrname-format:emailAddress |
| http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname | urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified |
| <http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname> | urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified |
| http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name | urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified |
| http://schemas.xmlsoap.org/ws/2005/05/identity/claims/Groups | 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.

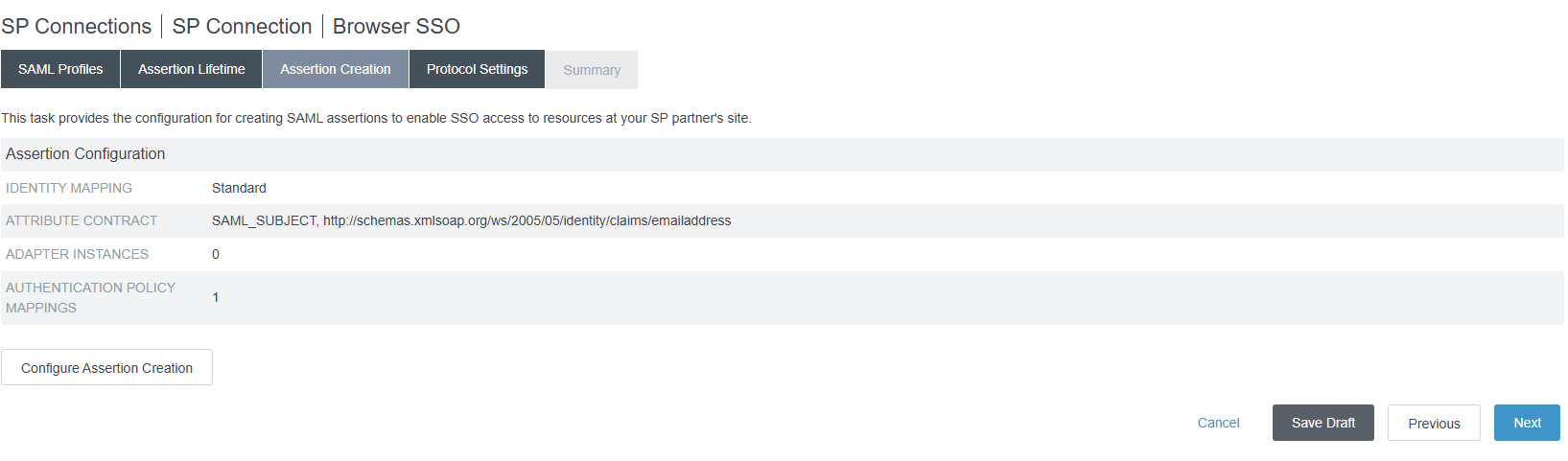


17. Under Attribute Contract Fulfillment Select

|  |  |
| --- | --- |
| Attribute Contract | Value |
| SAML\_SUBJECT | email |
| http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname | firstName |
| <http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname> | LastName |
| <http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name> | samAccountName/ Unique ID |
| http://schemas.xmlsoap.org/ws/2005/05/identity/claims/Groups | Write OGNL expression to pick up the Groups in ID that matches the Group Name in Atlassian |

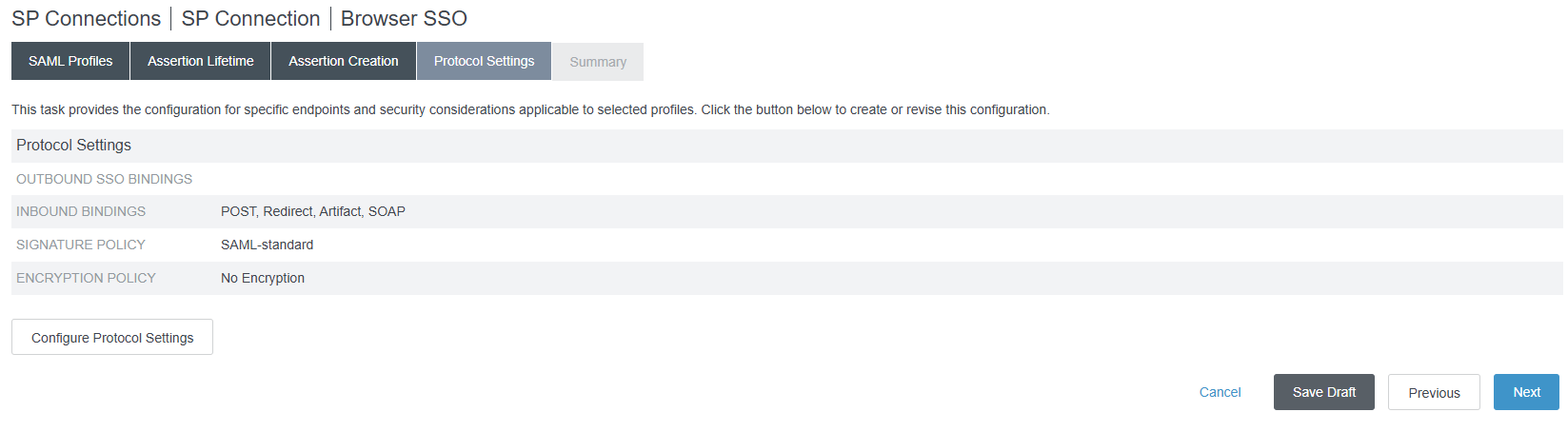
18. Select Issuance Criteria based on your Enterprise Choice.

19. Click Done.



Sample Screen as above will be shown.

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

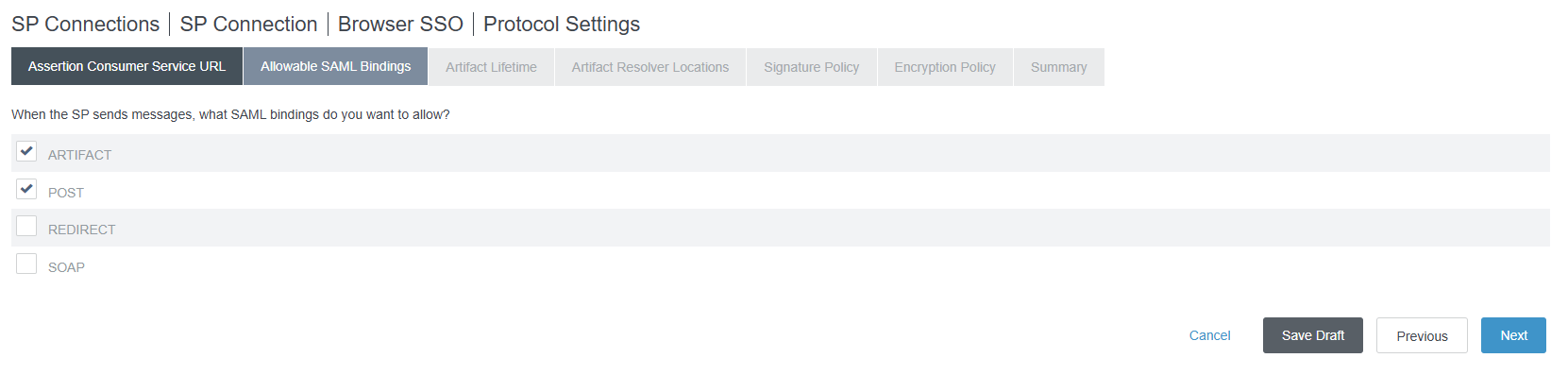


21. Click Configure Protocol Settings .

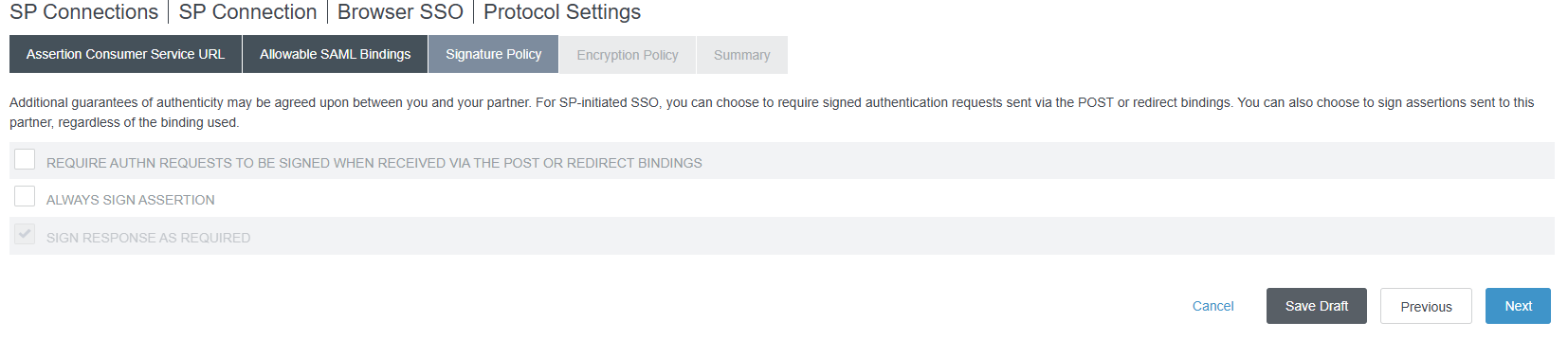
Select Artifact and Post under Bindings and enter <https://auth.atlassian.com/login/callback?connection=saml-tenantid> as Endpoint URL.

Click ADD

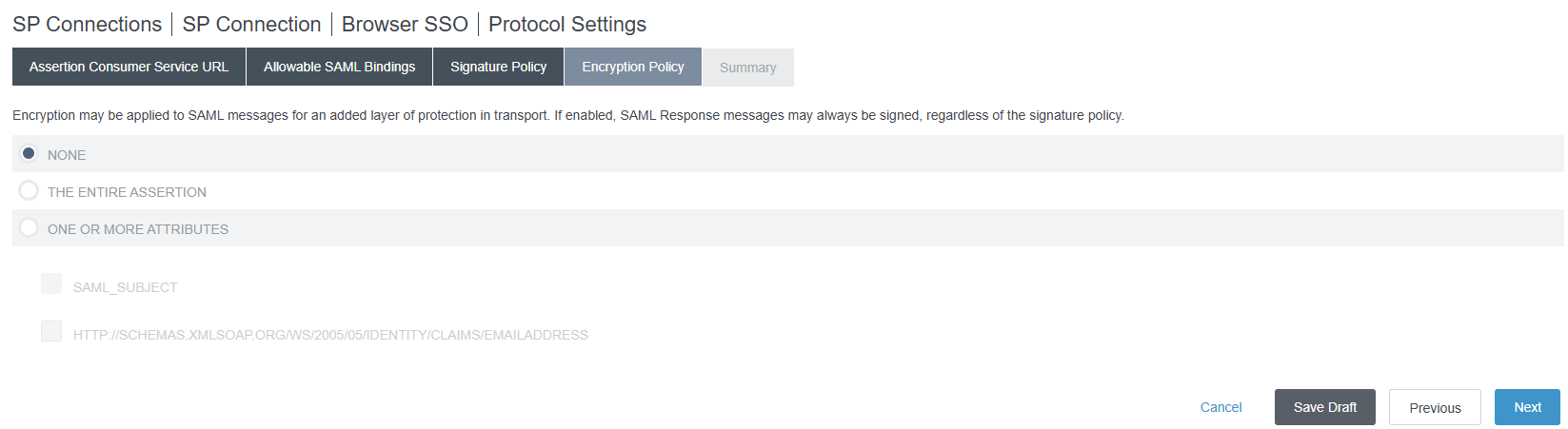
22. Choose Artifact and Post under Allowed SAML Bindings



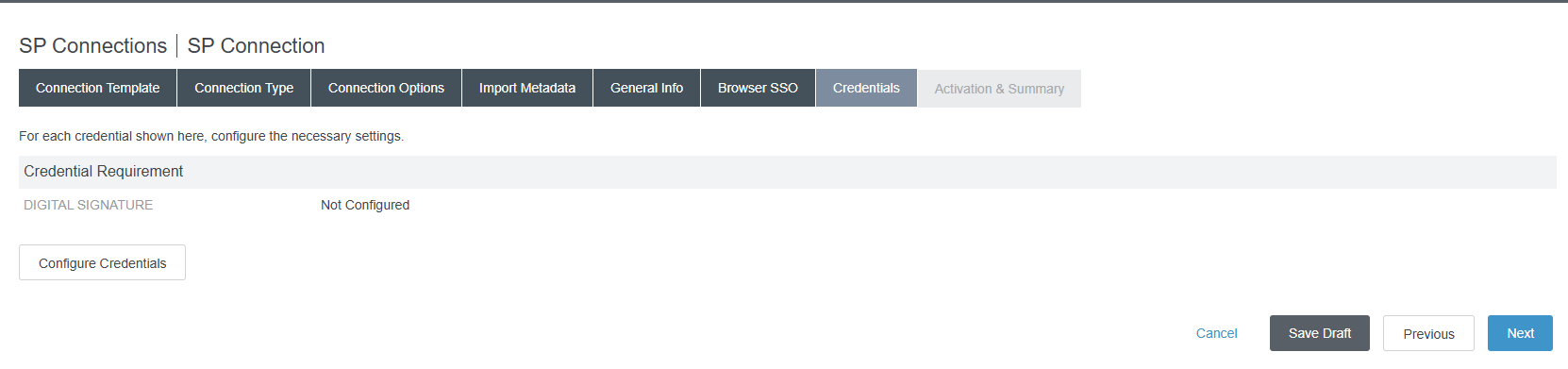
23. Select One of the following based on your Enterprise Requirement.



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

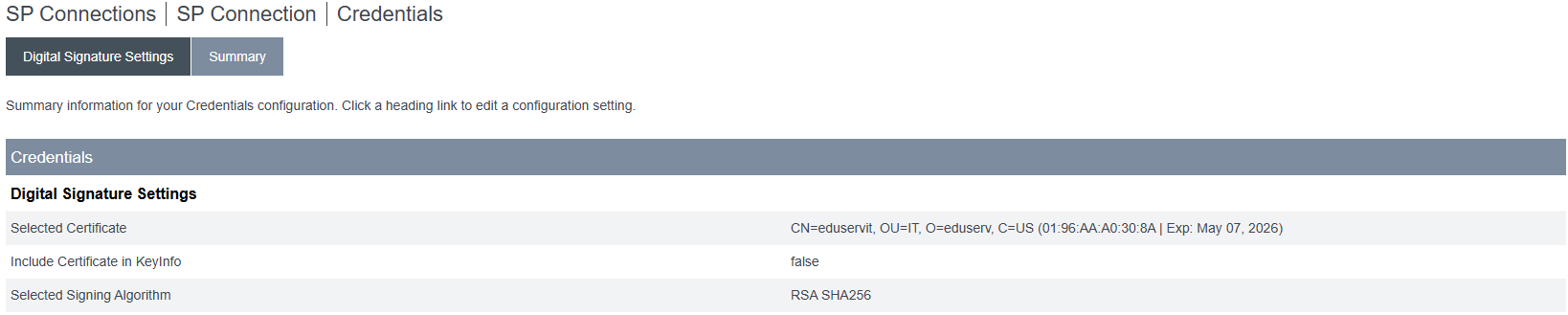


25. Click Next and Move to Credential Tab.



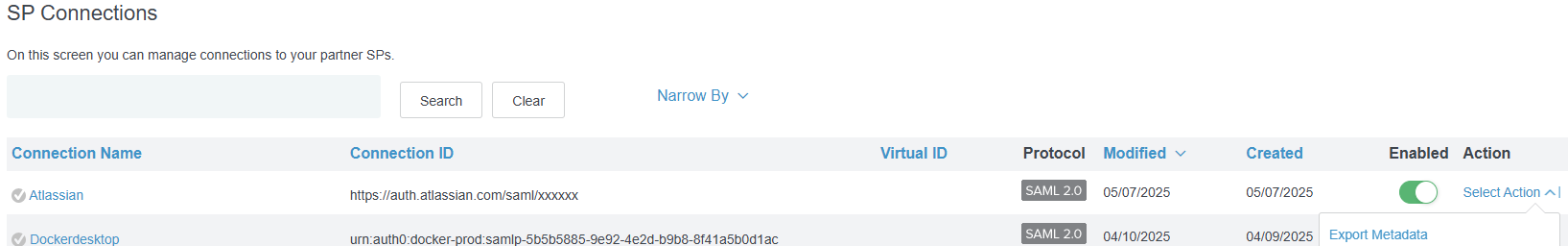
26. Click Configure Credentials.

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 Atlassian Cloud Application Admin.

Atlassian Cloud Setup :

1. Atlassian Cloud SAML SSO require the groups in Atlassian Cloud and Your Organization Group name to be similar. When SAML Assertion send the Groups it has to match the ones in Atlassian Cloud to enable Auto Sync.
2. Navigate to Atlassian Cloud Administration Page as Administrator to your Organization.
3. If you have multiple Sites, Choose the Site you like to enable SSO.
4. Navigate to Security 🡪 Enable SAML SSO.
5. Import the metadata from PingFederate.
6. This should import
   1. Service Provider URL
   2. Service Consumer URL
   3. Entity url
   4. Idp Entity ID
   5. IDP SSO URL
   6. Certificate from PingFederate.
7. This should enable the Single Signon Between your Atlassian Cloud and Ping Federate.