hStream™

PingFederate (SAML) Configuration

Auth0 Self Service — Connecting PingFederate as a SAML identity provider for Single Sign-On into HealthStream.

September 2026

Before You Begin

! Do not delete or remove your existing SSO connection in PingFed while completing this guide. Keeping it active lets us fall back to it if anything below needs troubleshooting, and your users see no disruption in the meantime.

! This upgrade runs entirely behind the scenes. Anyone currently signing in through your existing SSO connection will not notice any difference until HealthStream switches your account over to the new connection after a successful test.

! Open your existing PingFed SSO connection in a separate browser tab before you start. Several steps below ask you to copy values — attribute mapping and the access group — directly from it.

WHAT WE'LL COVER

Seven Steps to a Working SAML Connection

1. **Create SP Connection**

   Start a new Service Provider connection in PingFederate.

2. **Browser SSO**

   Configure the Browser SSO profile for SP-initiated sign-on.

3. **Assertion Creation**

   Map the user attributes PingFederate will send to Auth0.

4. **Protocols**

   Review SAML 2.0 protocol settings and the ACS endpoint.

5. **Credentials**

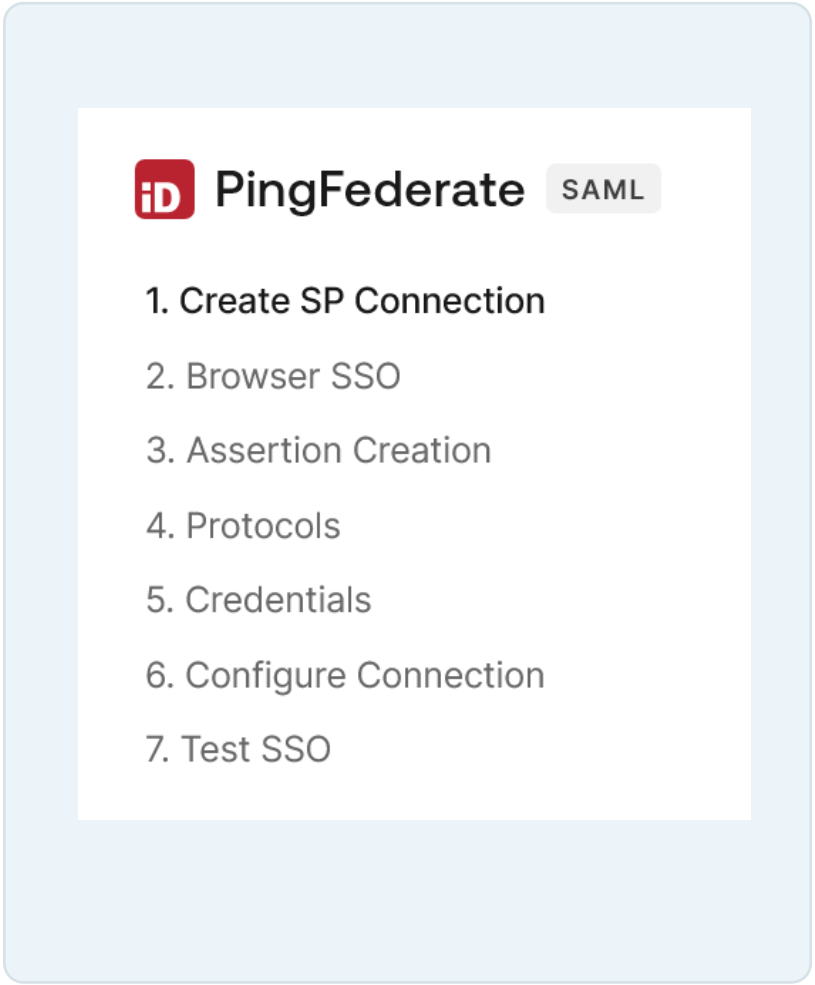
   Select the signing certificate PingFederate will use.

6. **Configure Connection**

   Bring the PingFederate metadata into Auth0 Self Service.

7. **Test SSO**

   Sign in through PingFederate and confirm the test is successful.

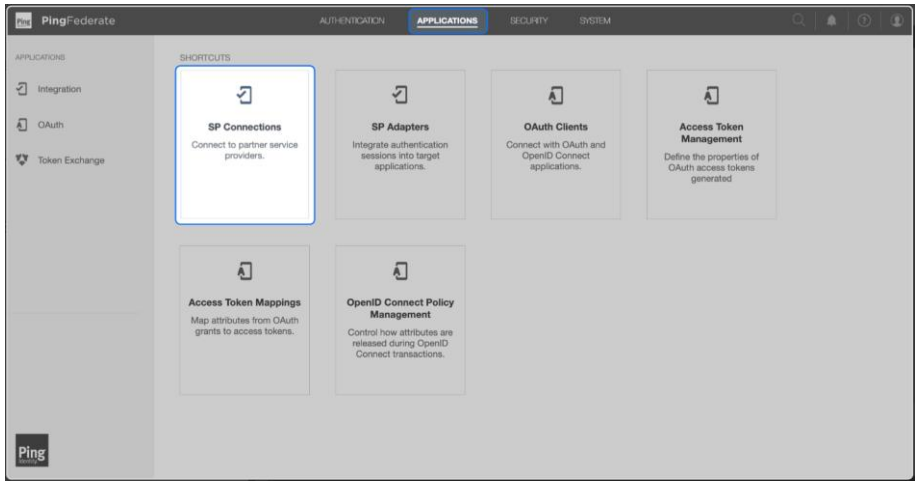


Auth0 Self Service progress panel

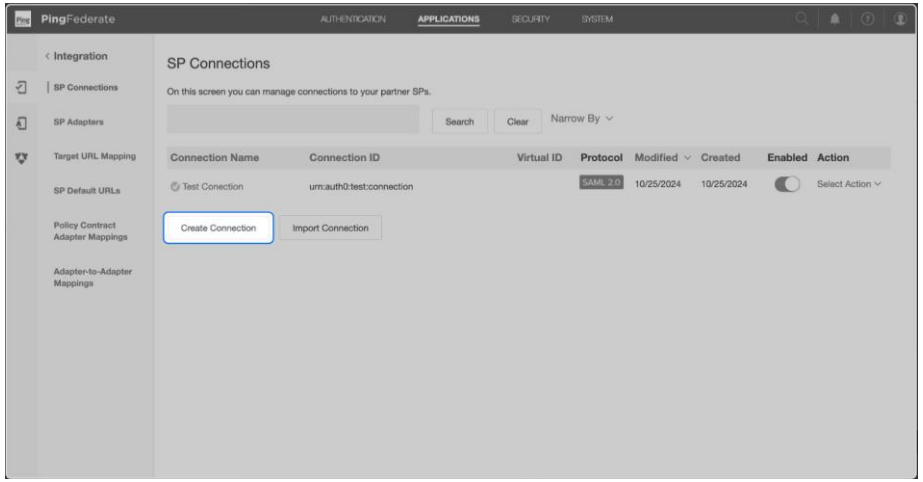
1

Navigate to SP Connections

- To connect your PingFederate tenant as an identity provider, you must create a SAML SP connection.
- Log in to the PingFederate Administrative Console.
- Select Applications in the top navigation, then SP Connections.
- Select Create Connection.



SP Connections

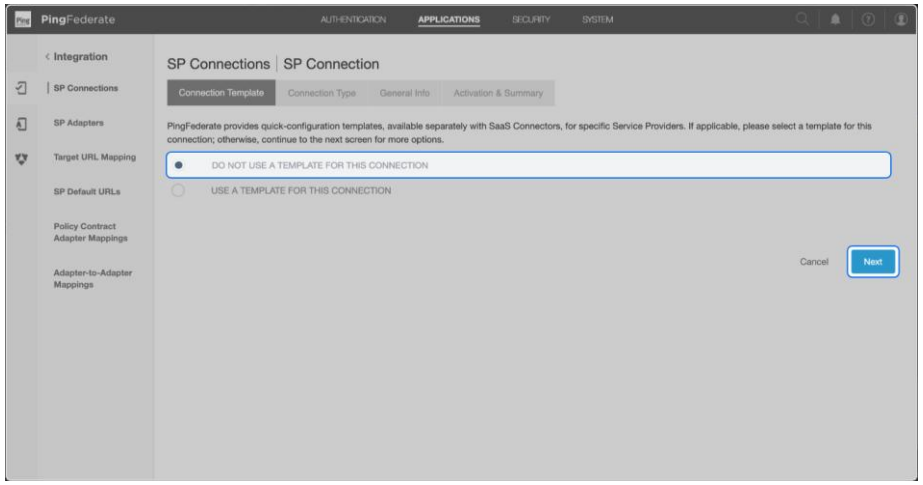


Create a new connection

1

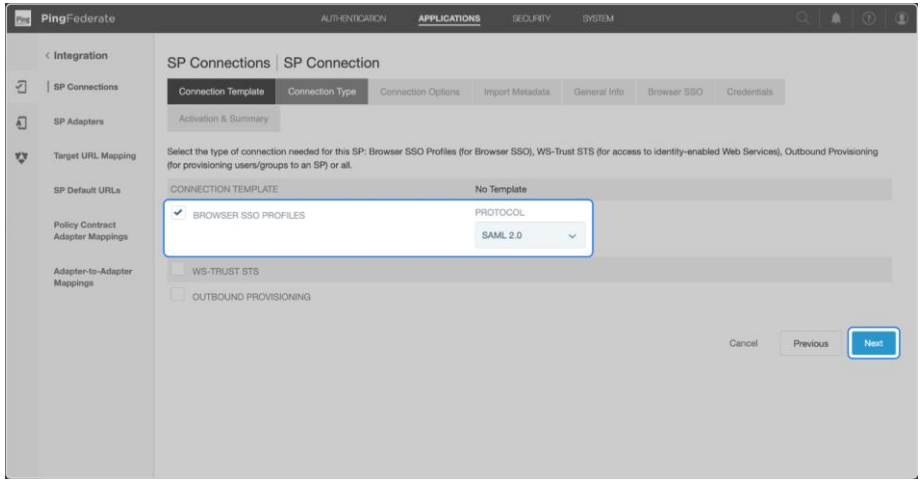
Choose the Connection Type

- Select “Do not use a template for this connection”, then Next.



Do not use a template

- Select Browser SSO Profiles and SAML 2.0 as the Protocol, then click Next.



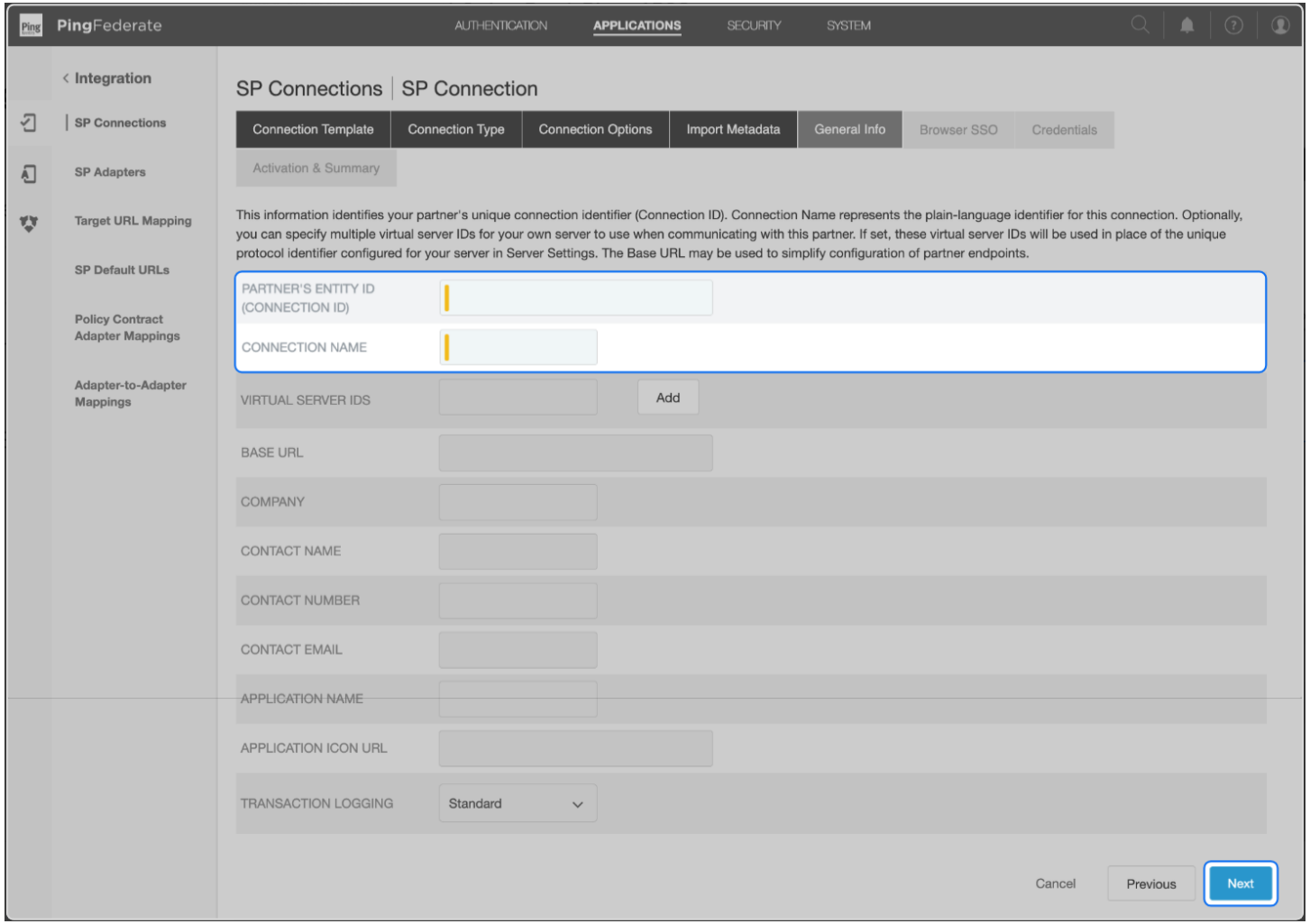
Browser SSO Profiles — SAML 2.0

Enter General Info

1

- Proceed to the General Info page.

- Enter the Partner's Entity ID provided by Auth0 Self Service.
- Enter a custom Connection Name, then select **Next.**

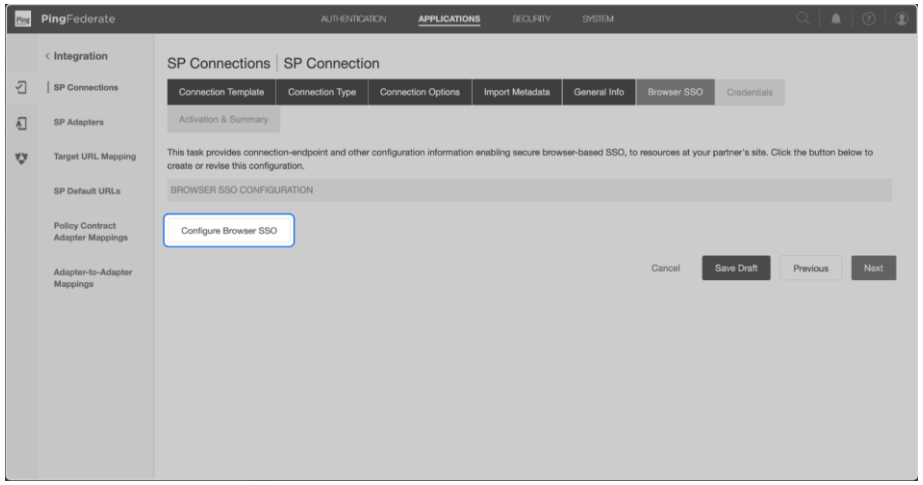


General Info — Partner's Entity ID & Connection Name

2

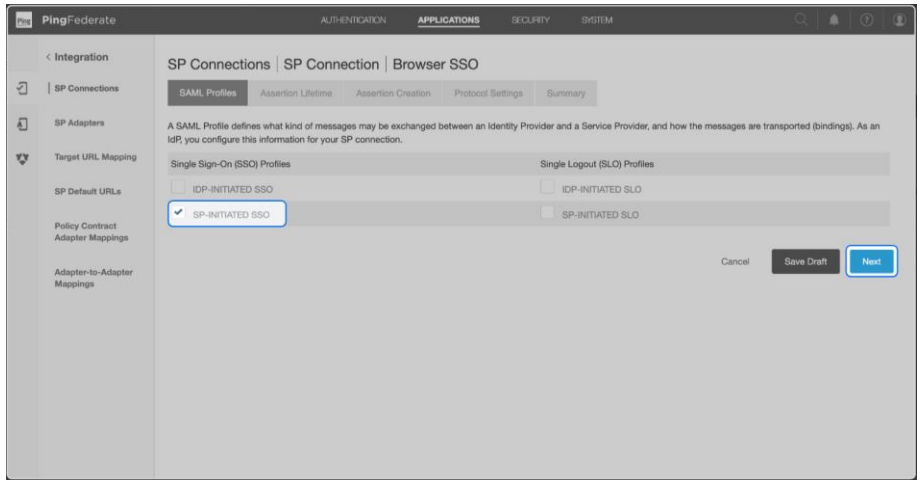
Configure Browser SSO

- To connect your PingFederate tenant as an identity provider, you must configure Browser SSO.
- You should now be on the Browser SSO page. Select Configure Browser SSO.



Configure Browser SSO

- Under Single Sign-On (SSO) Profiles, select SP-INITIATED SSO, then click Next.

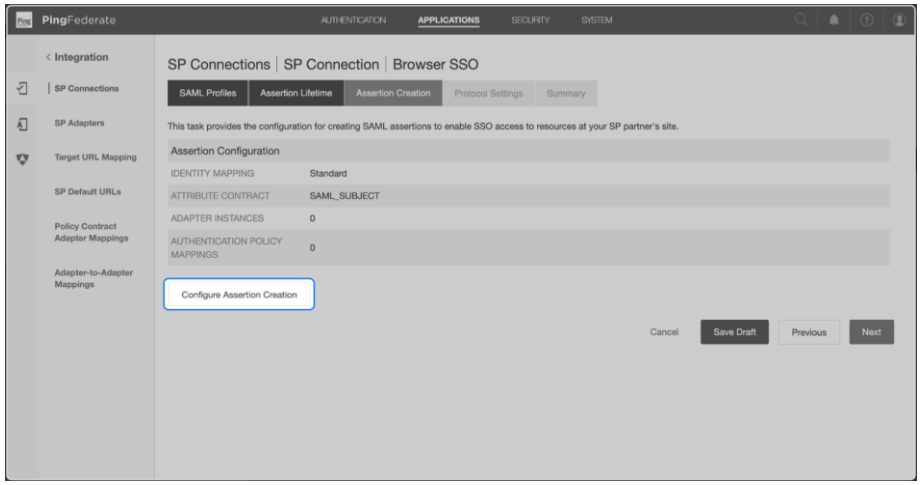


SSO Profiles — SP-Initiated SSO

3

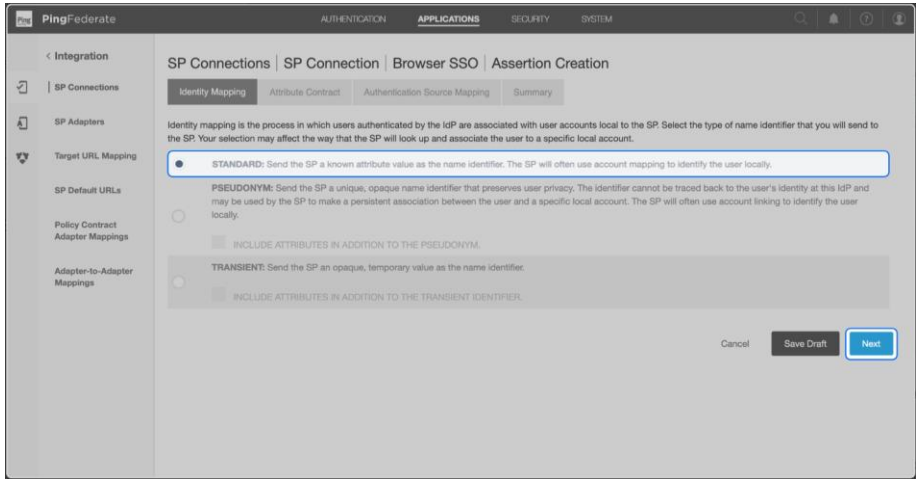
Configure Assertion Creation

- To connect your PingFederate tenant as an identity provider, you must configure assertion creation.
- Proceed to the Assertion Creation page and select Configure Assertion Creation.



Configure Assertion Creation

- On the Identity Mapping page, make sure STANDARD is selected, then click Next.



Identity Mapping — STANDARD

Know What Auth0 Requires

3

Before building the attribute contract, check the Auth0 Self Service portal for the required and optional attributes it expects from PingFederate.

Required attributes

- **name** (First & Last Name)
- **email**
- **preferred_username** (User ID)
- **family_name** (Last Name)
- **given_name** (First Name)

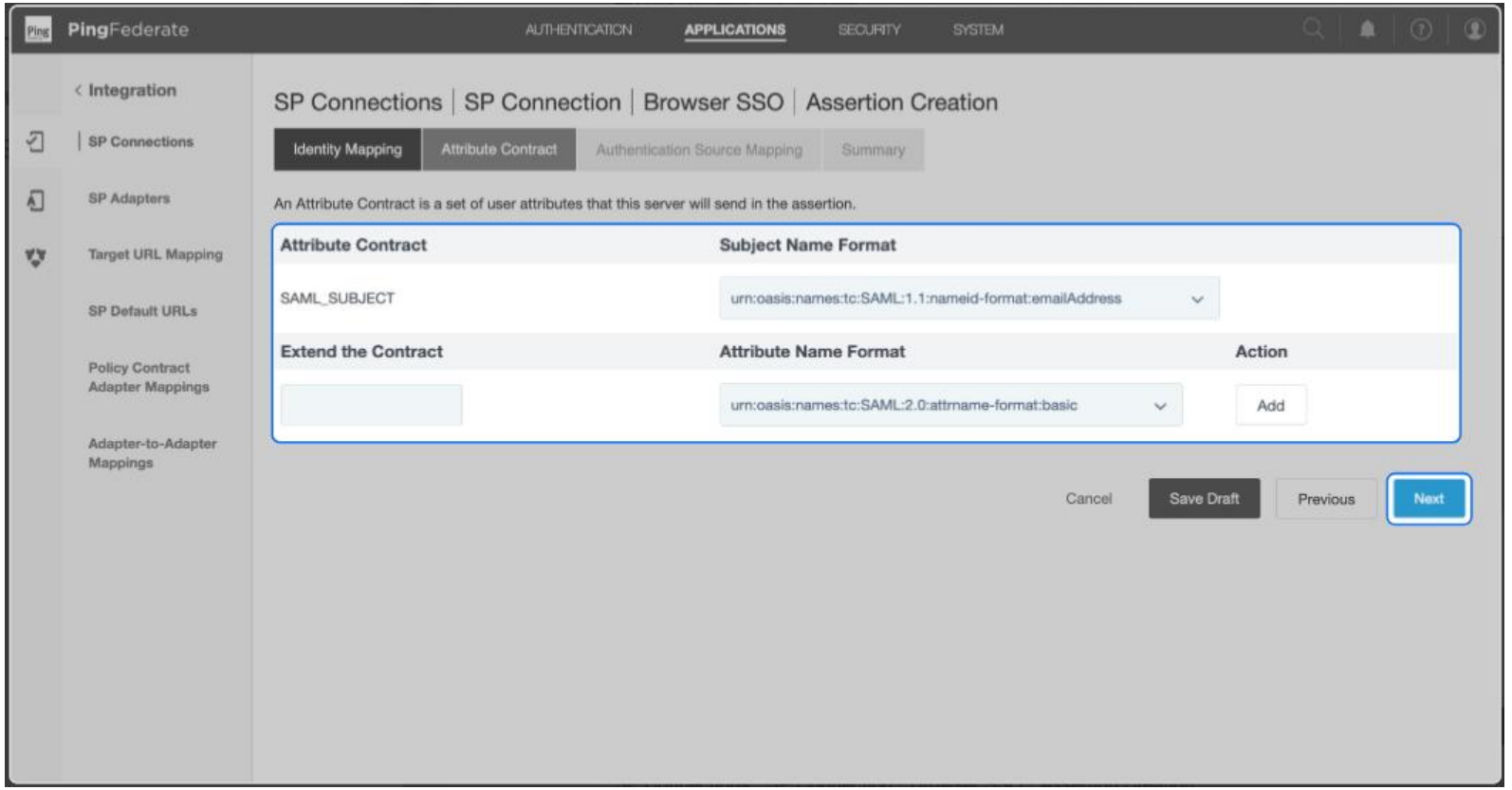
Optional attributes

- Mobile Phone Number
- Role
- UPN
- User's groups

Extend the Attribute Contract

3

- On the Attribute Contract page, set SAML_SUBJECT to urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress.
- Under Extend the Contract, enter each attribute and map it to the relevant Attribute Name Format.
- Click Add for each attribute, then Next.

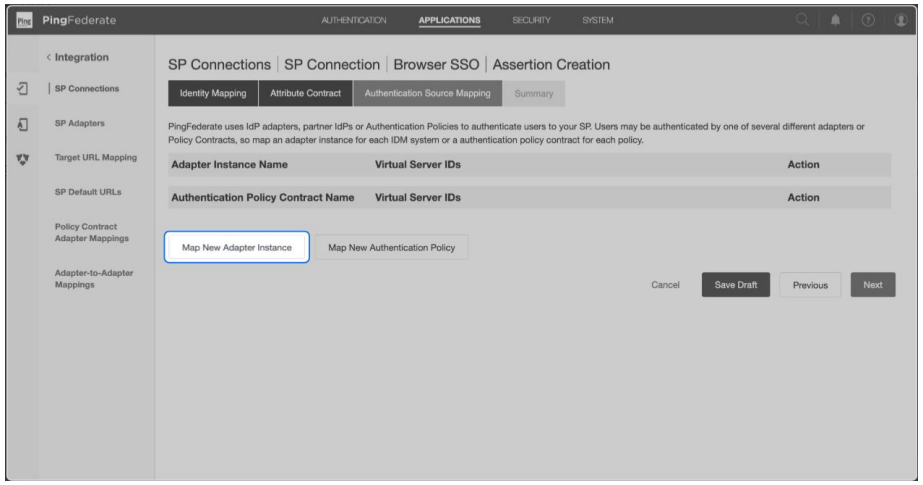


Attribute Contract — SAML_SUBJECT & extended attributes

3

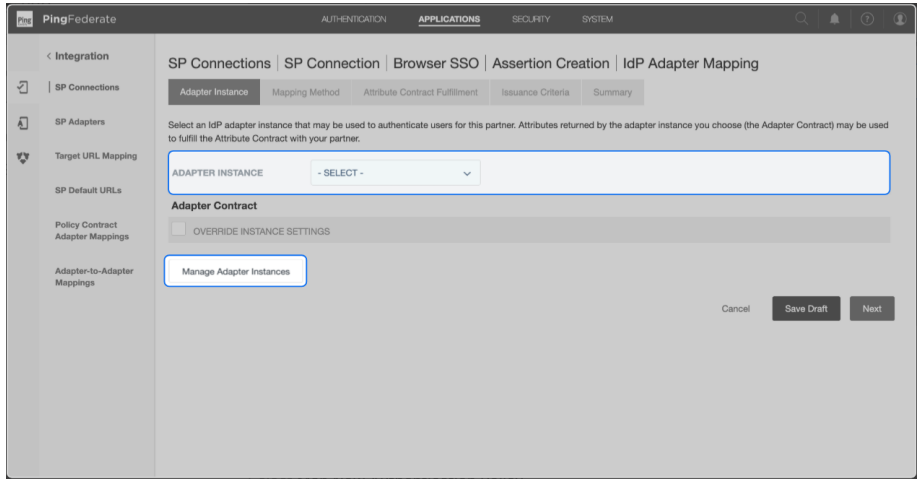
Map an Adapter Instance

- On the Authentication Source Mapping page, select Map New Adapter Instance.



Map New Adapter Instance

- Select an existing Adapter Instance, or create a new one.
- Proceed with configurations relevant to your organization's authentication requirements, then select Done.

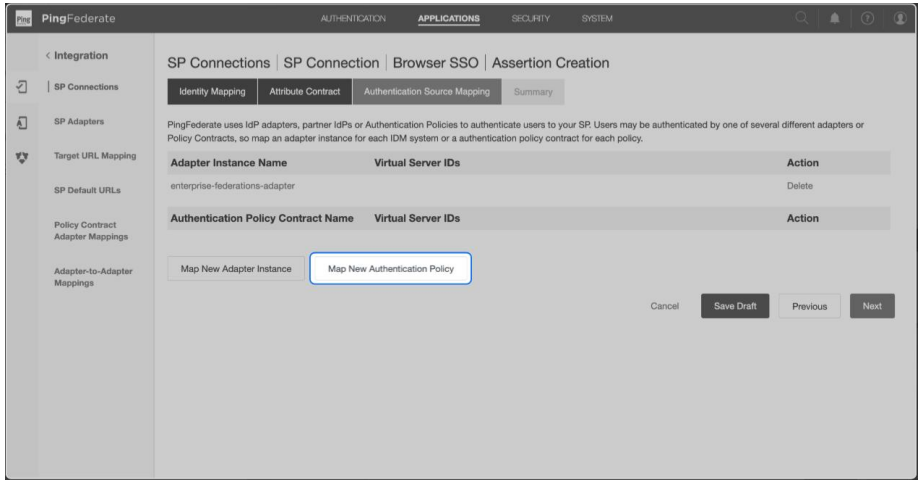


Select or create an Adapter Instance

3

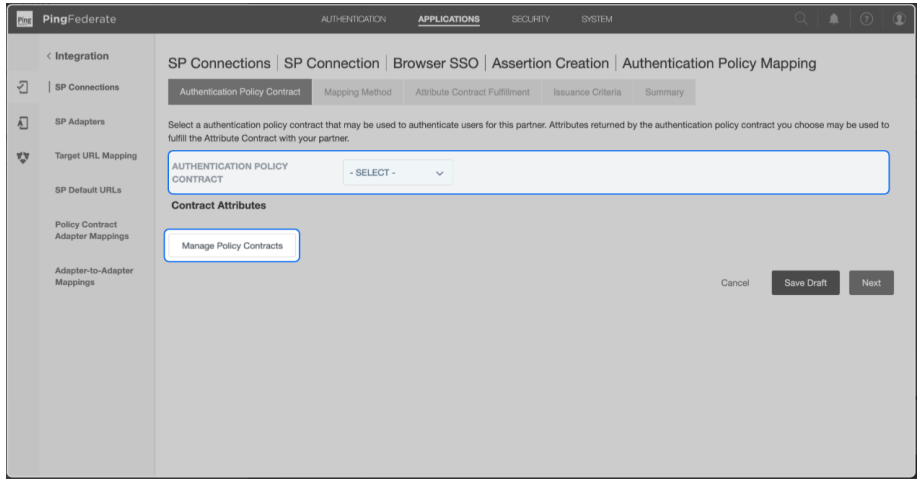
Map an Authentication Policy Contract

- Back on the Authentication Source Mapping page, select Map New Authentication Policy.



Map New Authentication Policy

- Select an existing Authentication Policy Contract, or create a new one by selecting Manage Policy Contracts.

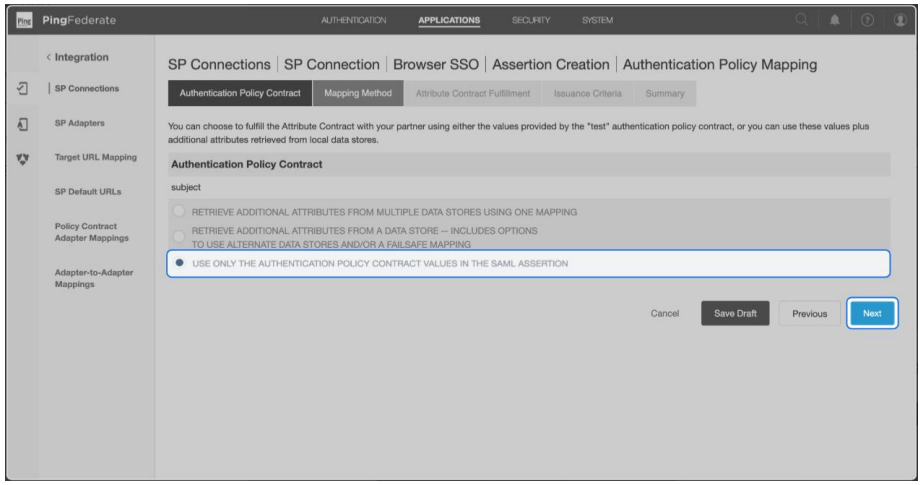


Select or manage a Policy Contract

3

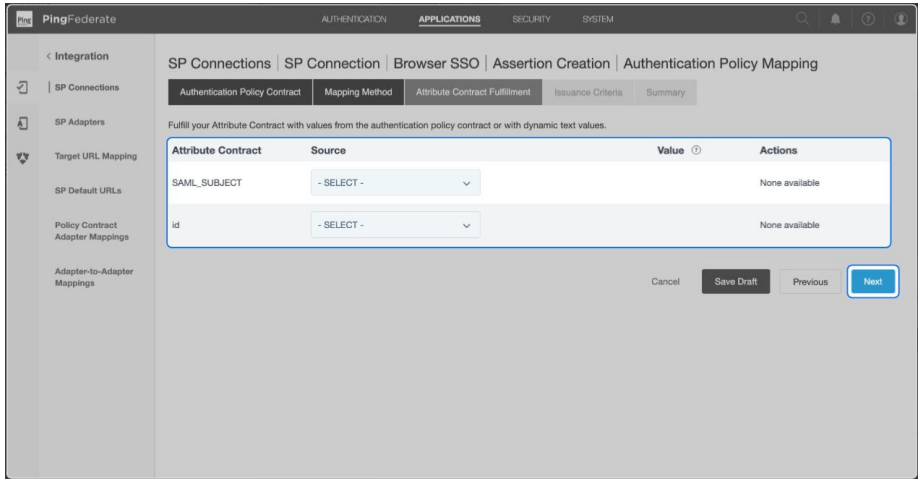
Complete the Attribute Contract

- On the Mapping Method page, make sure “Use only the Authentication Policy Contract values in the SAML assertion” is selected, then click Next.



Mapping Method

- On the Attribute Contract Fulfillment page, map each Attribute Contract to the corresponding Value. **Note:** Reference the required values from page 9.
- Select Next, then proceed to the Summary and select Done.

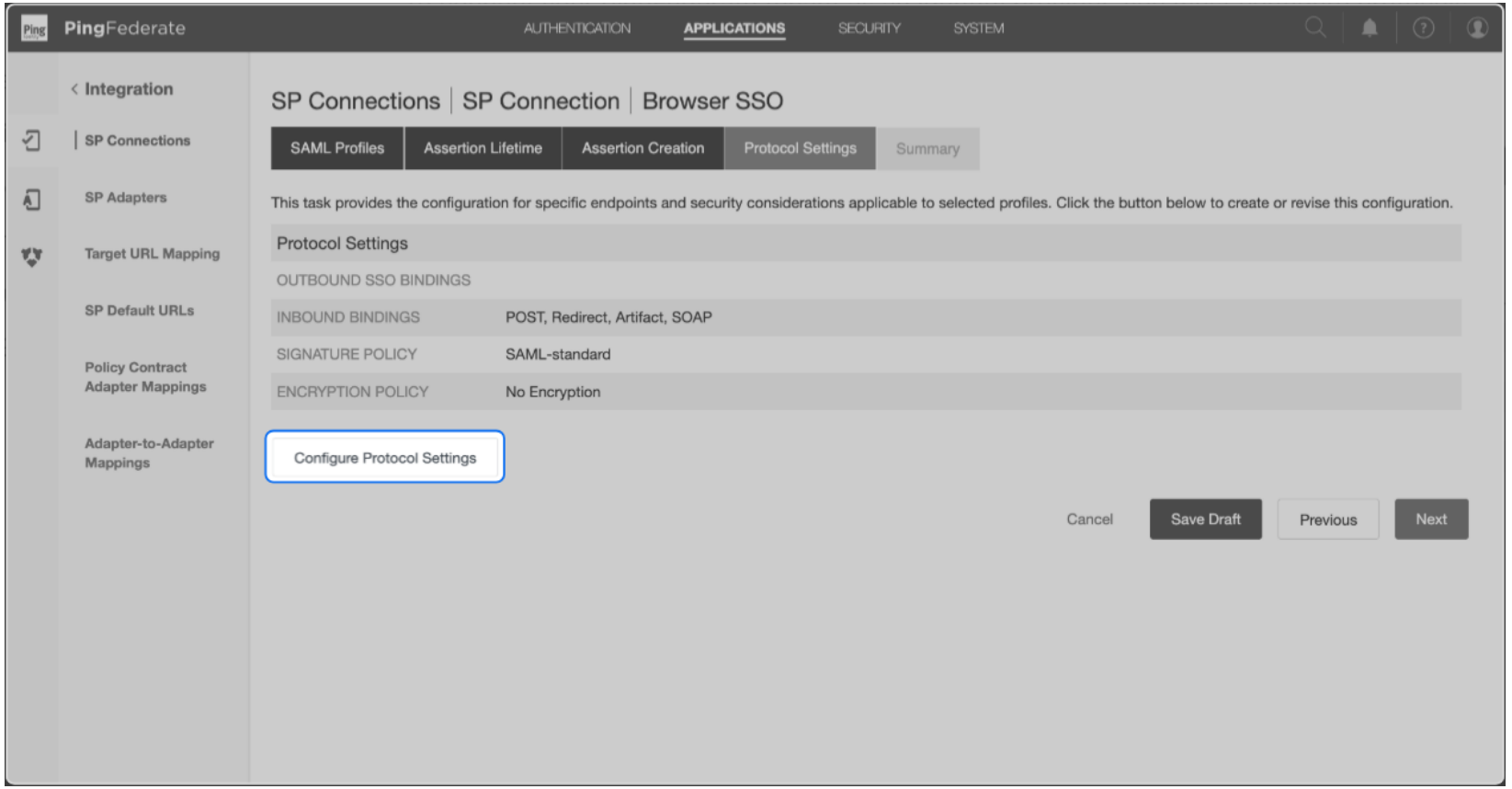


Attribute Contract Fulfillment

Configure Protocol Settings

4

- To connect your PingFederate tenant as an identity provider, you must configure protocols.
- Click Next to the Protocol Settings page, then select Configure Protocol Settings.
- Review the protocol configuration to verify SAML 2.0 is selected and response signing requirements meet your organization's standards.

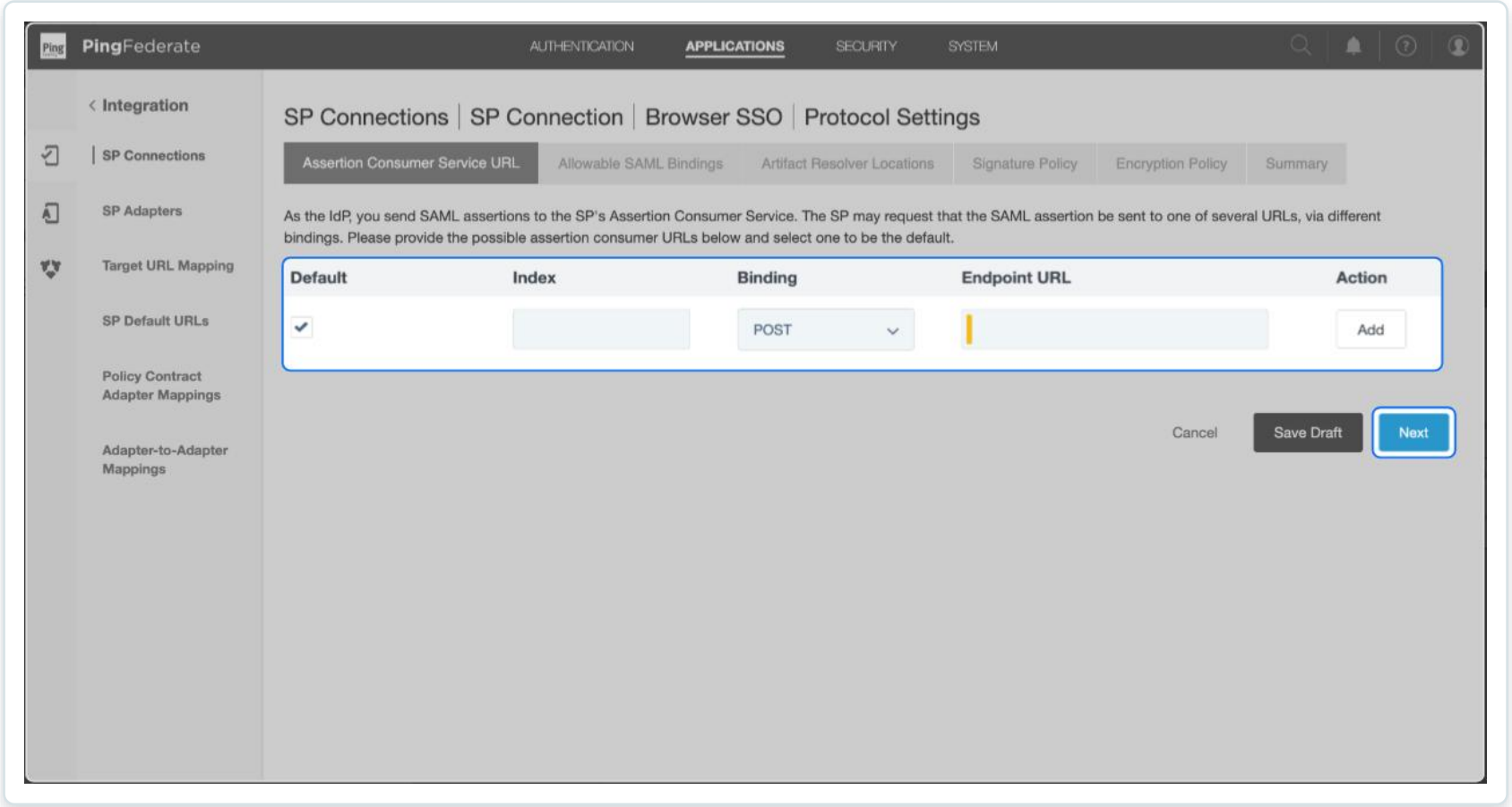


Protocol Settings

Set the Assertion Consumer Service URL

4

- You should now be on the Assertion Consumer Service URL page.
- Select Default, set the Binding to POST, and enter the Endpoint URL provided by Auth0 Self Service.
- Select Add, then Next.

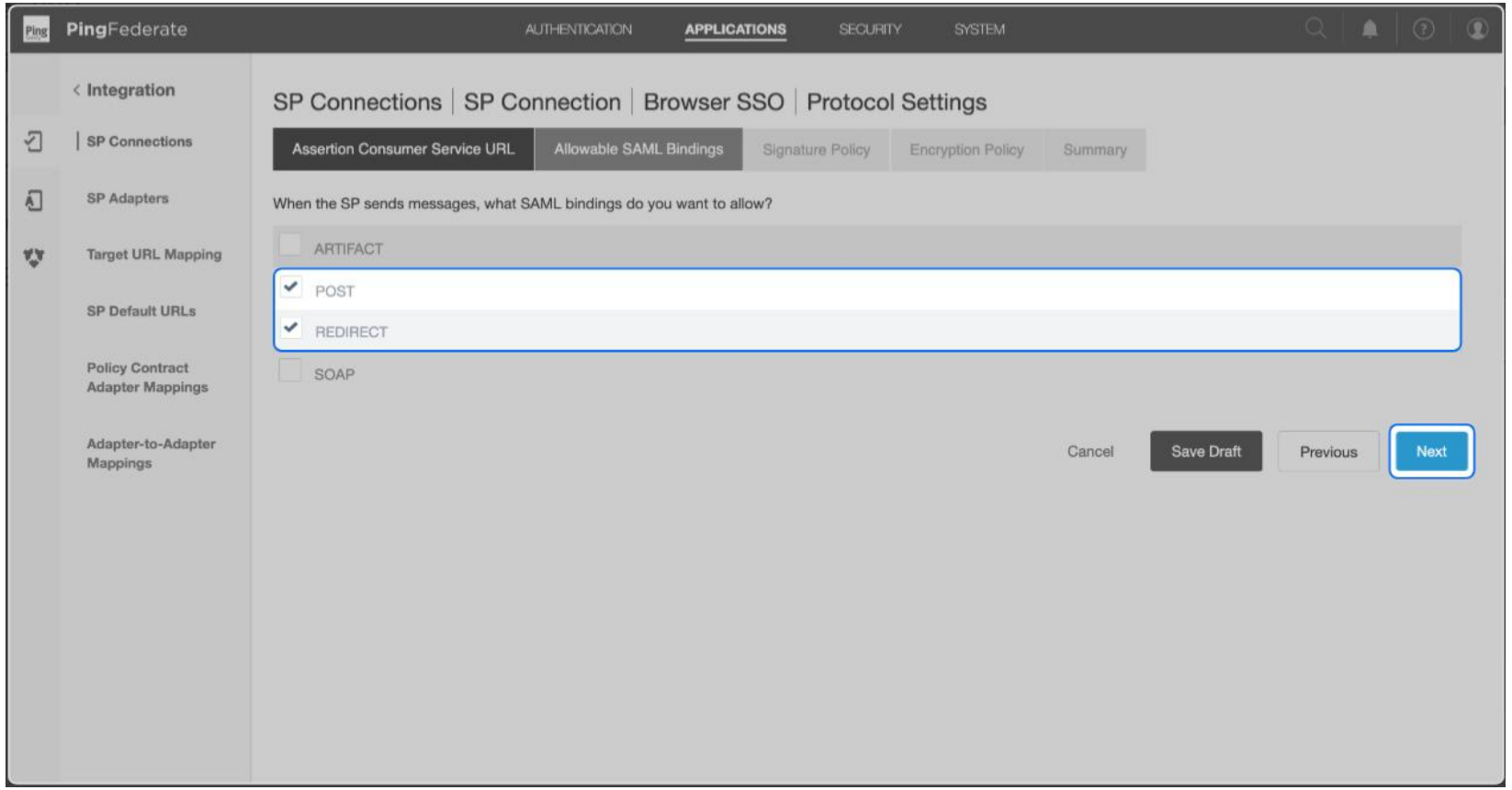


Assertion Consumer Service URL

Set the Allowable SAML Bindings

4

- On the Allowable SAML Bindings page, select only POST and REDIRECT.
- Select Next, then proceed to the Summary and select Done.
- You should now be back in Browser SSO configuration. Proceed to the Summary, then select Done.

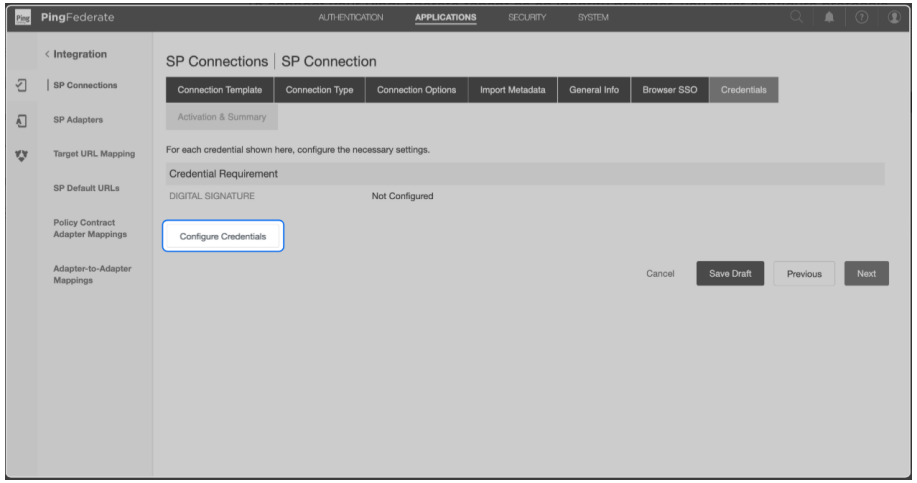


Allowable SAML Bindings — POST & REDIRECT

5

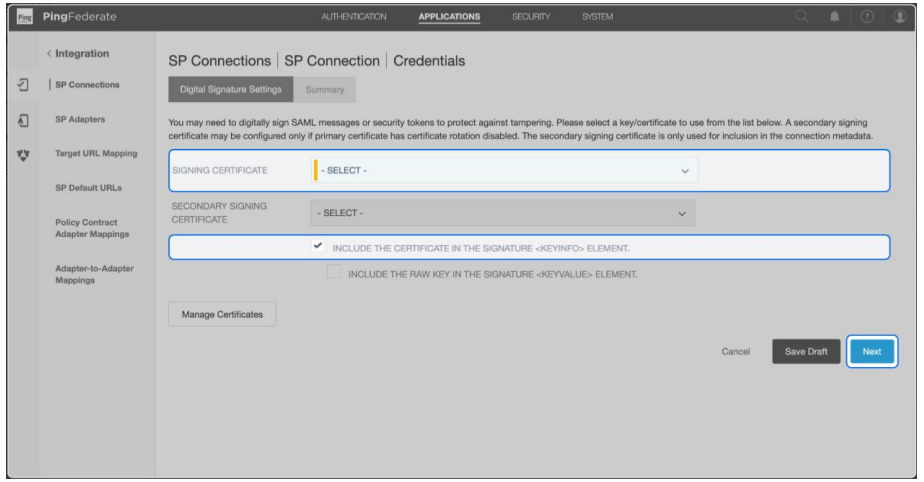
Configure the Signing Certificate

- Click Next to the Credentials page, then select Configure Credentials.



Configure Credentials

- In Digital Signature Settings, select your Signing Certificate and select “Include the certificate in the signature <KeyInfo> element”.
- Select Next, then proceed to the Summary and select Done.
- You should now be in SP Connection configuration. Proceed to Activation & Summary, then select Save.

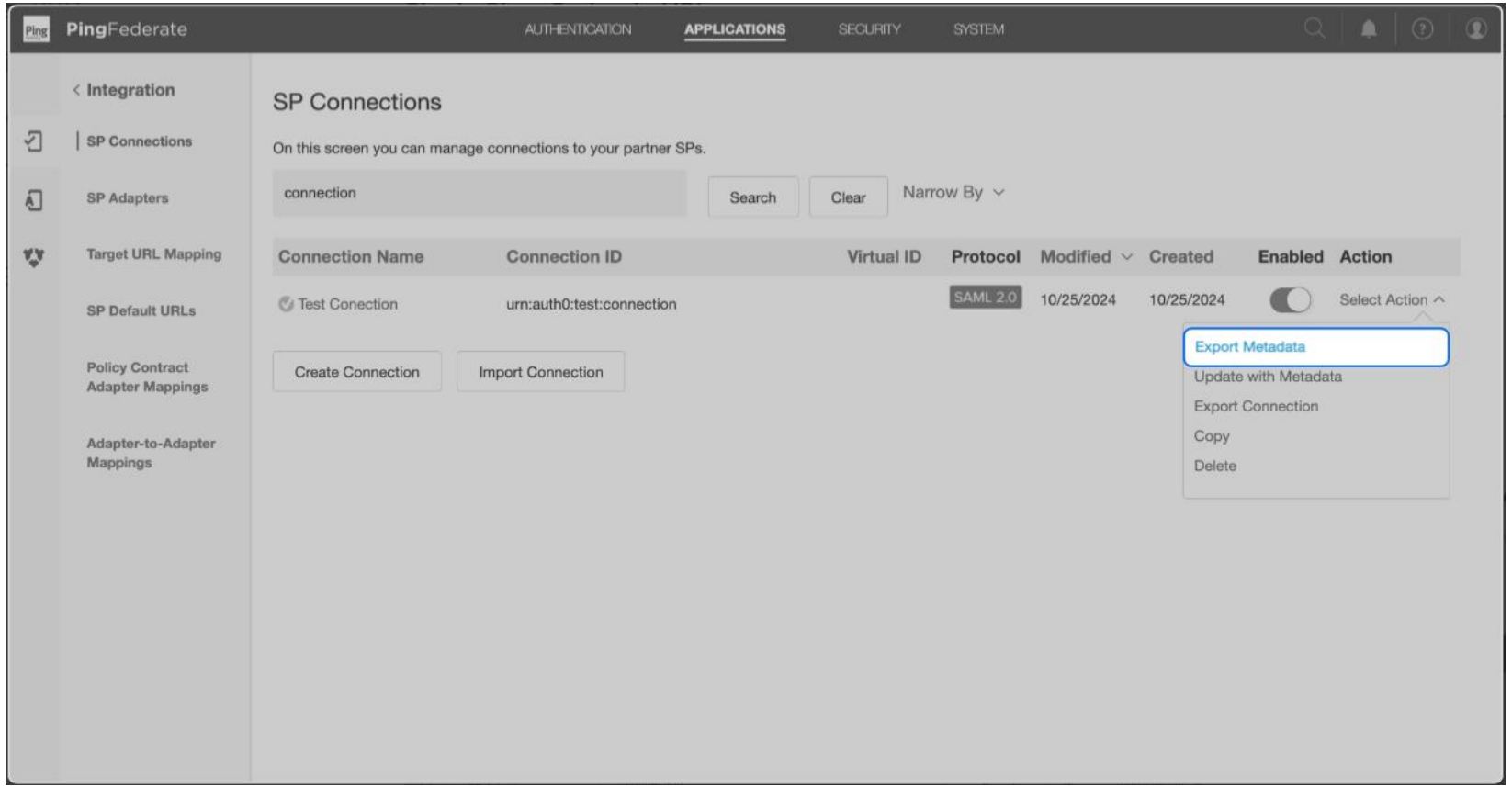


Digital Signature Settings

Find the SAML Login URL

6

- To obtain the Single Sign-On Login URL, navigate to the SP Connections page.
- Select Export Metadata.
- Look for the SingleSignOnService assertion tag in the metadata and copy the associated URL.

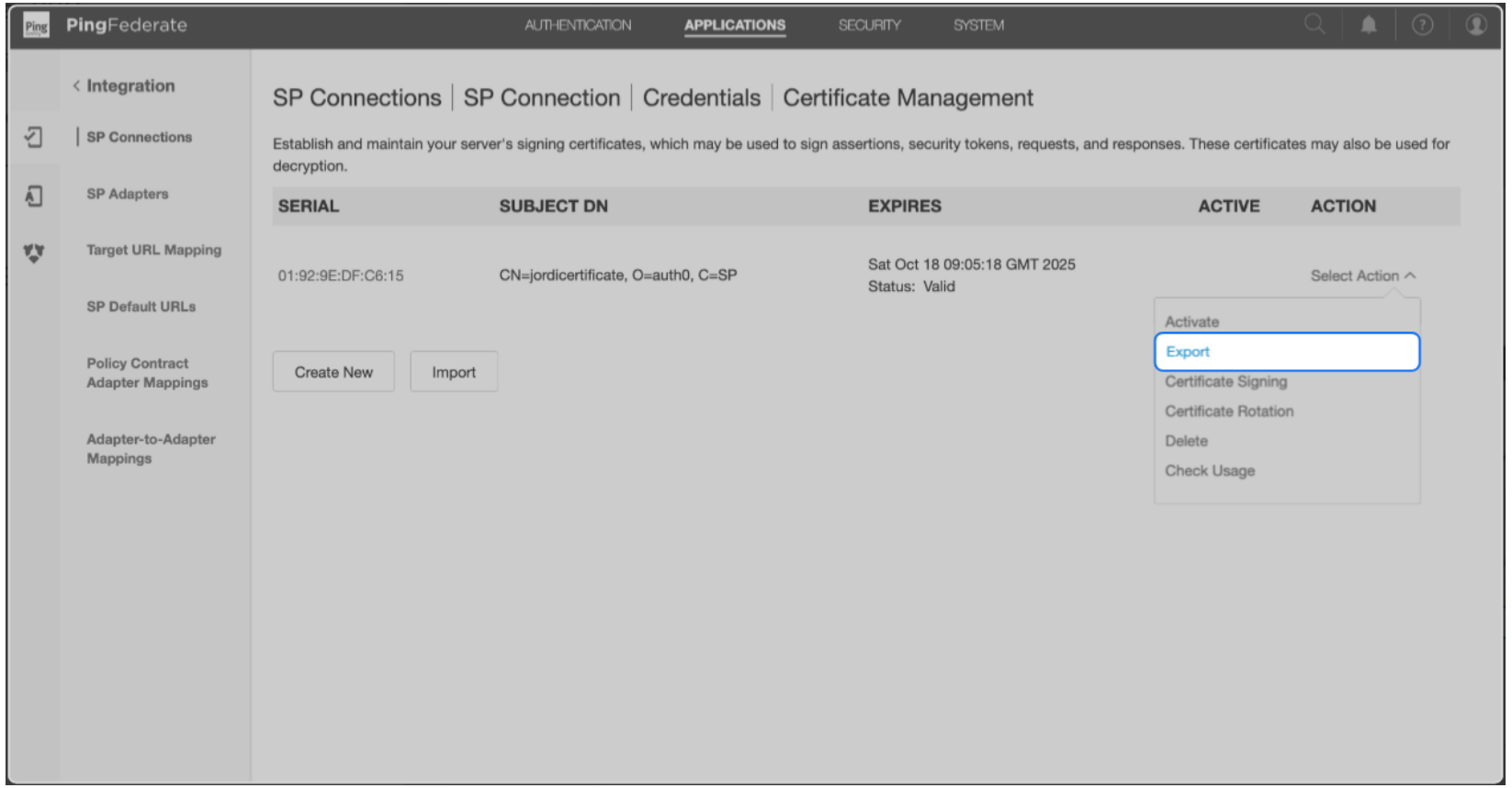


SP Connections — Export Metadata

6

Export the Signing Certificate

- From the Signing Certificate, navigate to SP Connections › SP Connection › Credentials › Certificate Management.
- Select Export.
- After entering the values in Auth0, select Validate or Save. If validation is successful, continue to the final step.



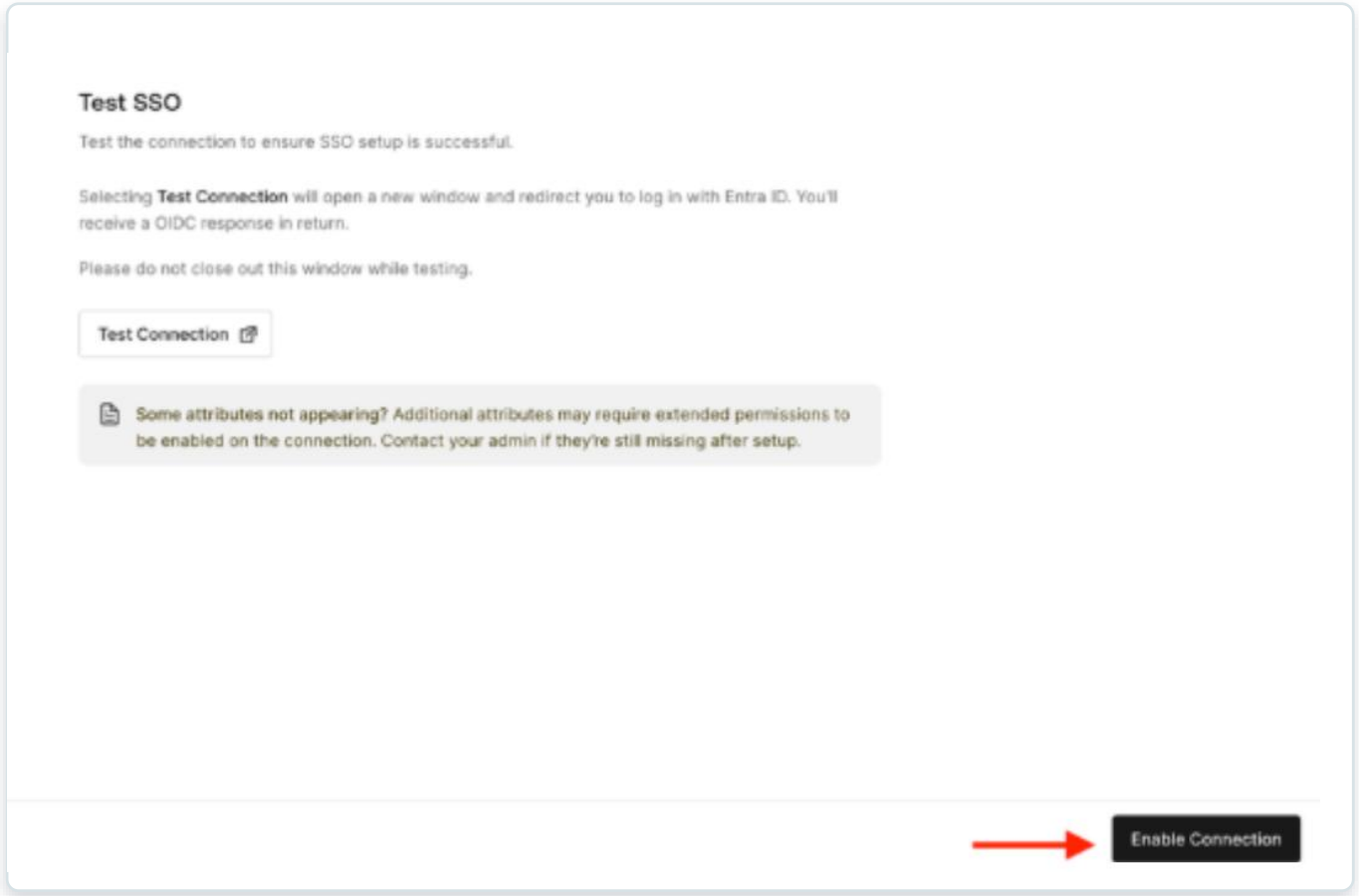
Certificate Management — Export

Enable & Test Connection

7

- **Step 1 : Click on the Test Connection button**

- **Step 2 : Enable the Connection**



Auth0 Self Service — Enable Connection

BEFORE YOU GO LIVE

Common Validation Checklist

Verify the following before rolling out SSO to all users.

- ✓ SP Connection created in PingFederate
- ✓ Assertion attributes mapped
- ✓ Signing certificate selected
- ✓ Test user assigned
- ✓ Browser SSO configured
- ✓ SAML protocol settings reviewed
- ✓ Metadata entered into Auth0

Thank You

Your PingFederate SAML connection is now configured using Auth0 Self Service. Users can now authenticate with their PingFederate credentials and access HealthStream through a secure Single Sign-On experience.

For additional assistance, contact the HealthStream Platform team or consult your organization's PingFederate administration documentation.