

Cookbook for PingFederate

SAML provides single sign-on capability for users accessing their services hosted in a cloud environment. Generally, a service provider such as Office 365 is federated with an identity provider such as PingFederate for authentication. The user gets authenticated by PingFederate and obtains a SAML token for accessing applications in a cloud environment, such as Office 365. This guide serves as step-by-step configuration manual for users using PingFederate as an authentication provider in a cloud environment.

Prerequisites for PingFederate

- Configure the following components in PingFederate:
 - Step 1a. Adding an LDAP Store
 - Step 1b. Creating a Password Credential Validator
 - Step 1c. Creating an Adapter
 - Step 1d. Creating a Signing Certificate
- Fetching the PingFederate metadata file

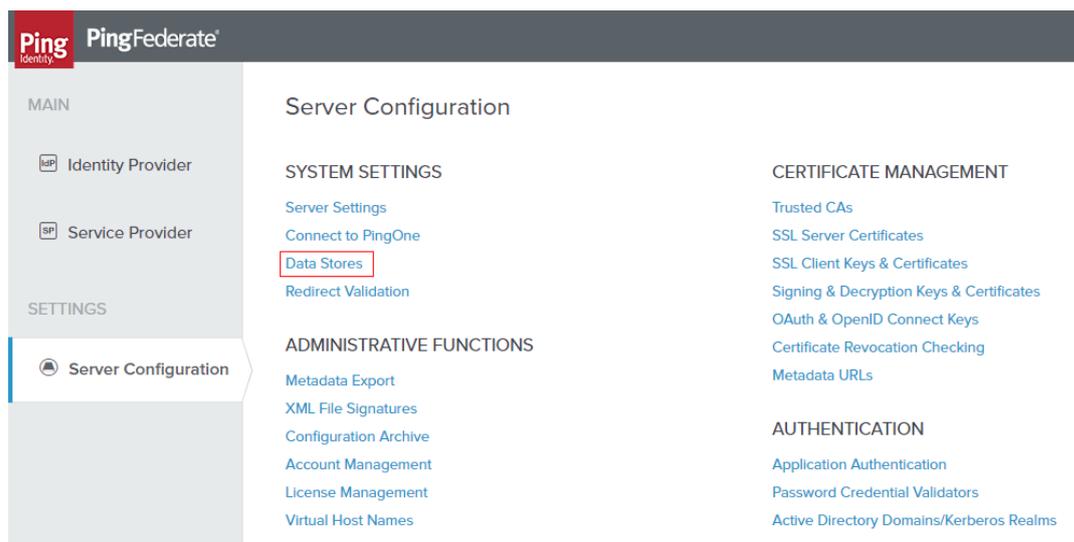
Configuring the components in PingFederate

Step 1a. Adding an LDAP Store

PingFederate lets you add an existing LDAP Datastore.

Procedure

1. Login to PingFederate with admin credentials.
2. Click **Server Configuration > Data Stores**.



3. Click **Add New Data Store**.
4. Enter the following details for Data Store and click **Save**.

Field	Value
Hostname	dc.example.com
User DN	domain\administrator
Password	Enter an appropriate password

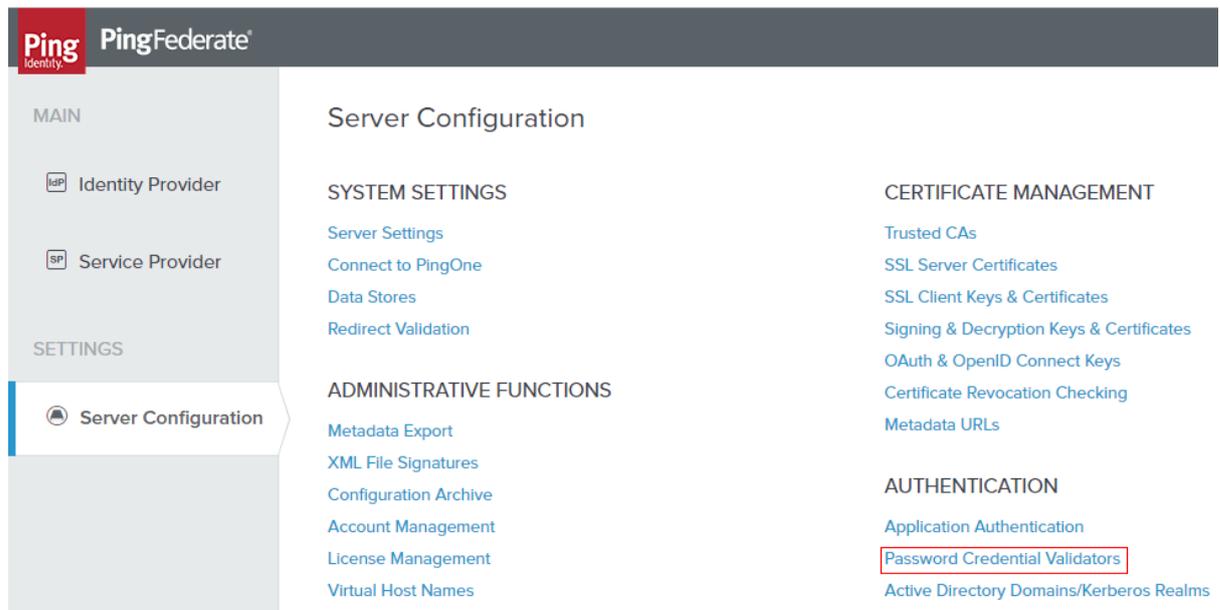
LDAP Data Store is added. The same Data Store is referred to in **Create a Validator**.

Step 1b. Creating a Password Credential Validator

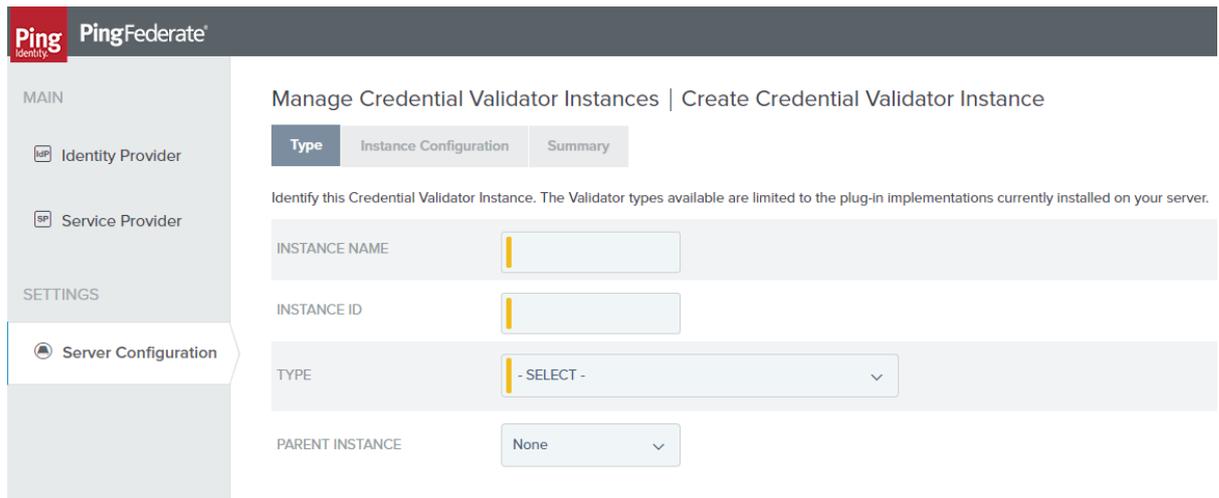
A validator authenticates the user. A user can authenticate in multiple ways with PingFederate such as AD authentication (sync users in AD), local user authentication (create local users in PingFederate), and so on.

Procedure

1. Login to PingFederate with admin credentials.
2. Click **Server Configuration > Password Credential Validator**.



3. Click **Create New Instance**. The **Manage Credential Validator Instance** page opens.



4. Enter the following details in the new instance and click **Next**.

Field	Value
Instance Name	Enter an appropriate instance name
Instance ID	Enter an ID
Type	Select LDAP Username and Password Credential Validator from the drop-down list.

5. Select the appropriate values for LDAP and click **Next**.

Field	Value
LDAP Datastore	dc.example.com
Search Base	DC=example,DC=com
Search Filter	userPrincipalName=\${username}
Scope of Search	Subtree

6. Click **Next > Done**.

The Validator is created. You must use this validator while creating the federation data.

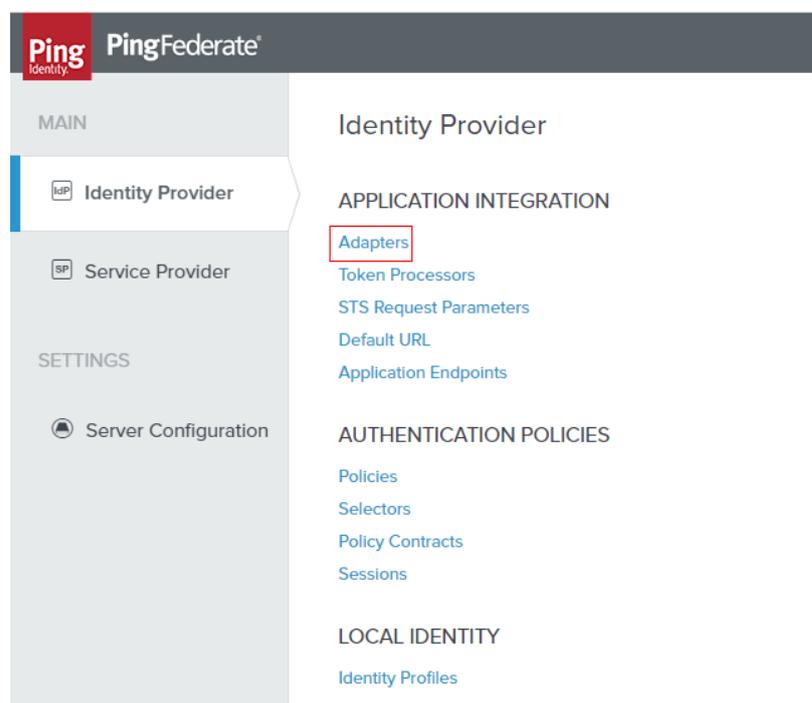
Step 1c. Creating an Adapter

An adapter is a simulator for the authentication page. It can be form-based or pop-up based. PingFederate uses terms such as HTMLFORM for form-based and httpBasic for pop-up based adapters. You must create a new adapter instance.

Procedure

1. Login to PingFederate with admin credentials.

2. Click **Identity Provider > Adapters > Create New Instance**.



3. Enter the following details for the new instance and click **Next**.

Field	Value
Instance Name	Enter an appropriate instance name
InstanceID	Enter an ID
Type	HTML Form IDP Adapter

4. On the next screen, select the validator created using **Creating a Password Credential Validator** and click **Update**.
5. click **Next > Next** again and on the Adapter Attributes tab, select **Pseudonym**. Click **Next**.
6. Click **Configure Adapter Contract**.
7. Click **Adapter Contract Fulfillment** and select **Source** as Adapter. Click **Next > Next > Done**.

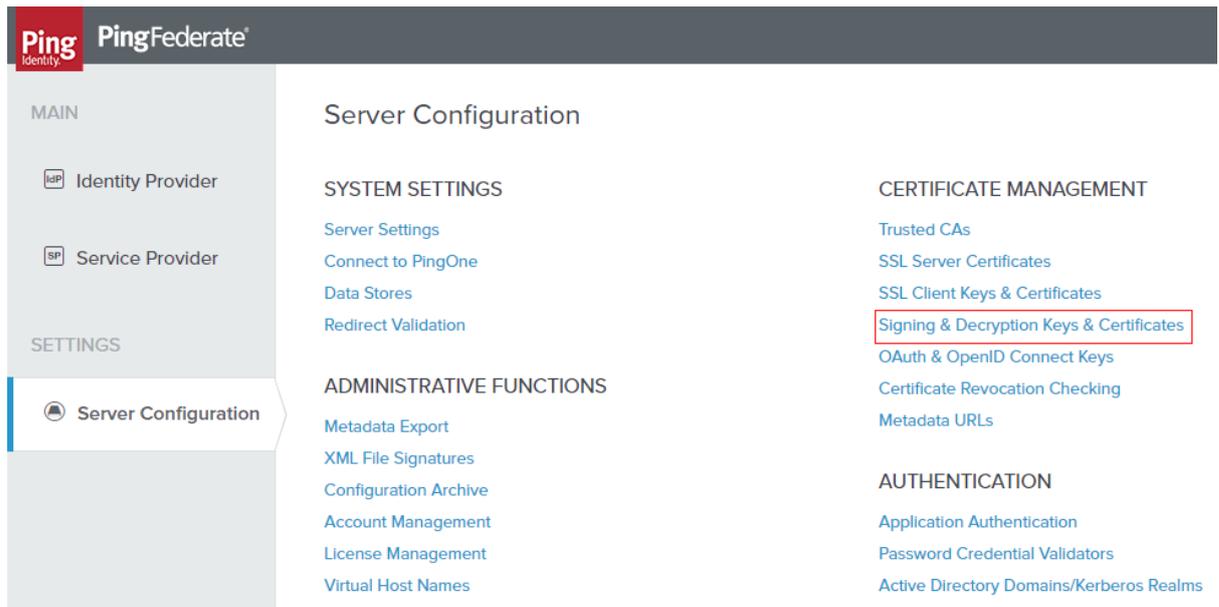
An Adapter is created. You must use this adapter while creating the federation pair.

Step 1d. Creating a Signing Certificate

If you are using any self-signed certificate as a signing certificate, you must upload the same certificate to PingFederate such that the uploaded certificate is used as a signing certificate.

Procedure

1. Login to PingFederate with admin credentials.
2. Click **Server Configuration > Signing & Decryption Keys & Certificates**.



3. Click **Import** if you already have the signing certificates.
4. Click **Choose File** and browse to import the **p12 certificate**.
5. Enter the password and click **Next**.
6. Click **Save**.

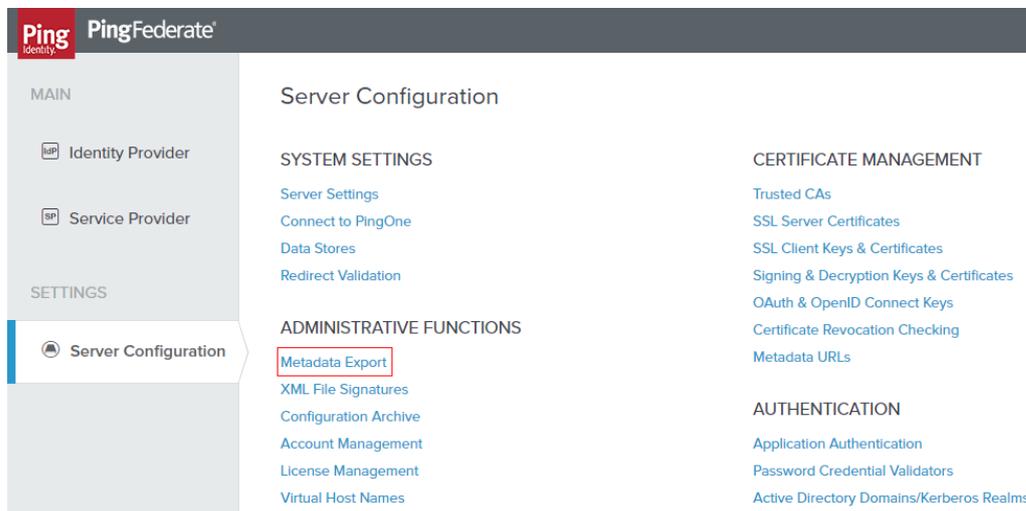
A signing certificate is created. You must use the same exported certificate while creating federation pairs in Access.

Fetching the metadata file for PingFederate

You must export and save the metadata for PingFederate to configure the federated pair.

Procedure

1. Login to PingFederate with admin credentials.
2. Click **Server Configuration > Metadata Export**.



3. Select **I am the Identity Provider** and click **Next**.
4. On the **Metadata Mode** tab, select "**Select information to include in Metadata manually**" and click **Next**.
5. Select **SAML 2.0** as the protocol and click **Next**.
6. On **Attribute Contract**, click **Next**.
7. On the **Signing Key** tab, select the signing key user for the service provider configuration and click **Next**.
8. On **Metadata Signing** tab, click **Next**.
9. On **XML Encryption Certificate**, click **Next**.
10. On the **Export & Summary** tab, review the export details and click **Export**. Save this **metadata.xml** file.

Configuring PingFederate in MobileIron Access

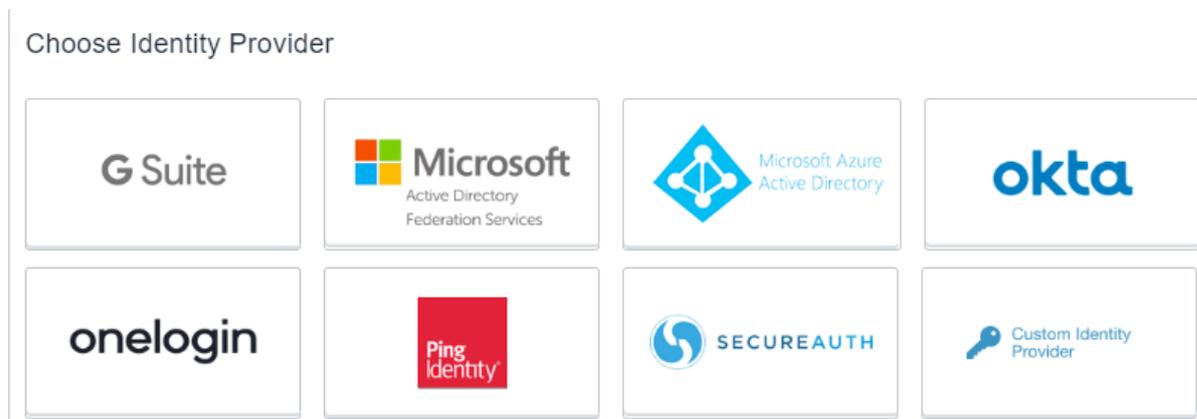
You must configure an appropriate service provider in Access and then proceed to configure PingFederate as your identity provider.

Prerequisites

- Ensure that you have completed **Step 1a to Step 1d** in PingFederate.
- Ensure that you have the metadata file for the service provider and for PingFederate (identity provider).

Procedure

1. Login to MobileIron Access administrative portal with admin credentials.
2. Click **Profile > Federation**.
3. Click **Add Pair > Federated Pair**.
4. Select the appropriate service provider from the catalog and click **Next** to configure the desired service provider.
5. Click **Next** to configure PingFederate.
6. Select **PingIdentity** as the identity provider.



7. Select the Access Signing Certificate from the drop-down list else click **Advanced Options to Generate certificate or Add new certificate**.
8. Use one of the following methods to upload the metadata information from PingFederate.

- Select **Upload Metadata** and click **Choose file** to upload the metadata.xml file downloaded in [#Fetching the metadata file for PingFederate](#).
 - Select **Add Metadata** and enter the following details from the metadata.xml file.
 - Extract the **Entity ID URL** and the Base64 Encoded Certificate from the metadata file.
 - Enter the same URL for the **Entity ID, POST SSO URL, and Redirect SSO URL**.
 - Enter the **Base64 Encoded Certificate** for Signing.
9. Click **Done**.
10. On the Federation page, download **Access IDP Metadata (Upload to SP)** and **Access SP Metadata (Upload to IDP)** as proxy metadata files.

Updating PingFederate configuration

You must update PingFederate with the proxy metadata file for the configuration to complete.

Procedure

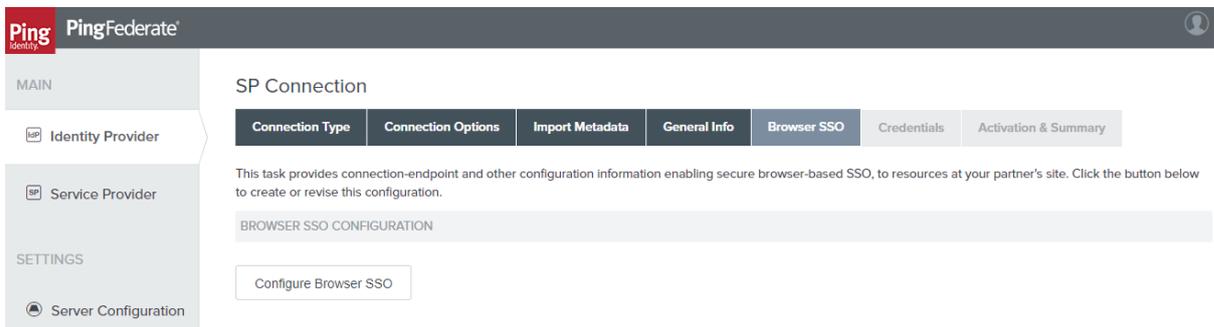
1. Login to PingFederate portal with admin credentials.
2. Click **Identity Provider > Create New**.
3. Select **Browser SSO Profiles** (SAML 2.0 is selected by default) as the connection type and click **Next**.

The screenshot shows the 'SP Connection' configuration page in the PingFederate portal. The left sidebar has 'Identity Provider' selected under 'MAIN'. The main content area has tabs for 'Connection Type', 'Connection Options', 'Import Metadata', 'General Info', 'Browser SSO', 'Credentials', and 'Activation & Summary'. The 'Connection Type' tab is active, displaying instructions to select a connection type. Under 'CONNECTION TEMPLATE', 'No Template' is selected. Under 'BROWSER SSO PROFILES', the checkbox is checked, and the 'PROTOCOL' dropdown is set to 'SAML 2.0'. The 'WS-TRUST STS' and 'OUTBOUND PROVISIONING' checkboxes are unchecked.

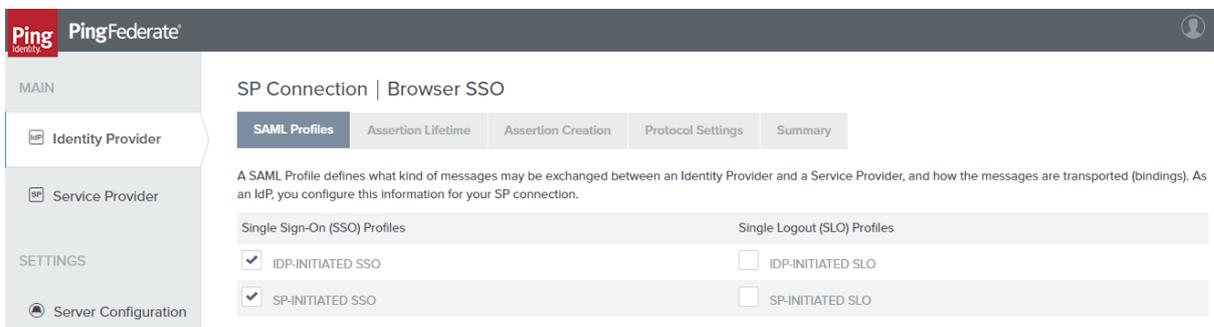
4. Select **File** to import metadata and click **Choose File**. Upload the **Access SP Metadata (Upload to IDP)** metadata file that you downloaded in [#Configuring PingFederate in MobileIron Access](#) and click **Next**.

The screenshot shows the 'SP Connection' configuration page with the 'Import Metadata' tab selected. The 'METADATA' section has three radio button options: 'NONE', 'FILE', and 'URL'. The 'FILE' option is selected. Below the radio buttons, it says 'No file selected' and there is a 'Choose file' button. The other tabs ('Connection Type', 'Connection Options', 'General Info', 'Browser SSO', 'Credentials', 'Activation & Summary') are visible but not active.

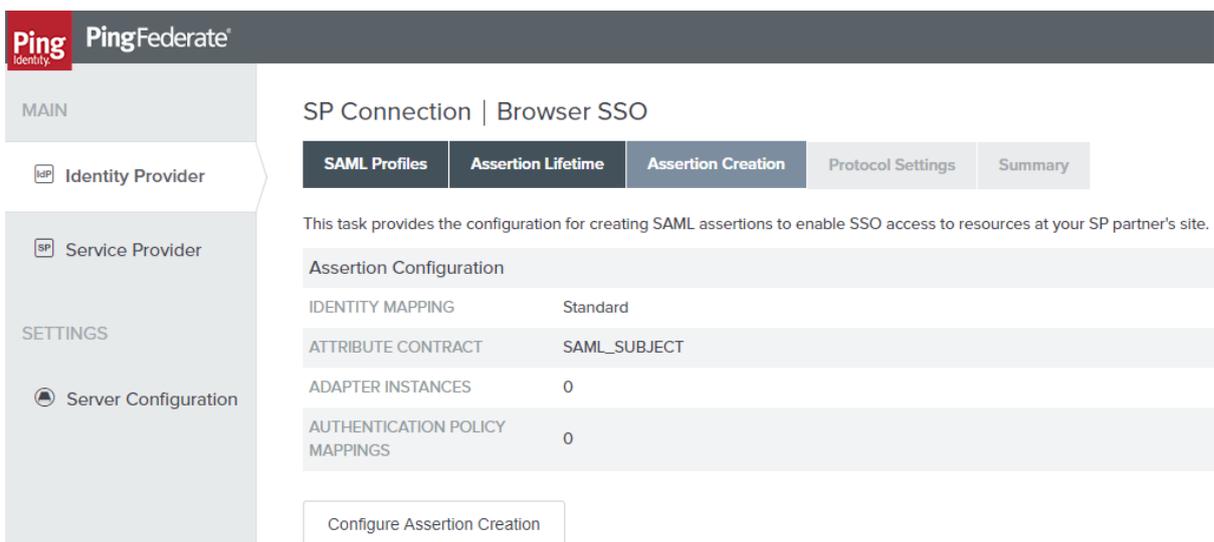
- Review **Metadata Summary** and click **Next**.
- On the **General Info** tab, click **Next**.
- On the **Browser SSO** tab, click **Configure Browser SSO**.



- On the **SAML Profiles** tab, select **IDP-Initiated SSO** and **SP-Initiated SSO**. Click **Next**.



- On the **Assertion Lifetime** tab, click **Next**.
- On the **Assertion Creation** tab, click **Configure Assertion Creation**.



- On the **Identity Mapping** tab, select **Standard** and click **Next**.

The screenshot shows the 'Identity Mapping' tab in the PingFederate configuration interface. The breadcrumb trail is 'SP Connection | Browser SSO | Assertion Creation'. The left sidebar shows 'MAIN' with 'Identity Provider' selected and 'Service Provider' below it, and 'SETTINGS' with 'Server Configuration' selected. The main content area has a sub-breadcrumb 'Identity Mapping' and a description: 'Identity mapping is the process in which users authenticated by the IdP are associated with user accounts local to the SP. Your selection may affect the way that the SP will look up and associate the user to a specific local account.' There are three radio button options: 'STANDARD' (selected), 'PSEUDONYM', and 'TRANSIENT'. Each option has a checkbox for 'INCLUDE ATTRIBUTES IN ADDITION TO THE [OPTION] IDENTIFIER'.

12. On **Attribute Contract** tab, extend the Contract and configure IDPEmail as urn:oasis:names:tc:SAML:2.0:attrname-format:basic and SAML_NAME_FORMAT as urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified.

The screenshot shows the 'Attribute Contract' tab. The breadcrumb trail is 'SP Connection | Browser SSO | Assertion Creation'. The left sidebar is the same as in the previous screenshot. The main content area has a sub-breadcrumb 'Attribute Contract' and a description: 'An Attribute Contract is a set of user attributes that this server will send in the assertion.' There are two sections: 'Attribute Contract' with a dropdown for 'Subject Name Format' set to 'urn:oasis:names:tc:SAML:1:nameid-format:unspecified', and 'Extend the Contract' with a dropdown for 'Attribute Name Format' set to 'urn:oasis:names:tc:SAML:2.0:attrname-format:basic' and an 'Add' button.

13. On **Authentication Source Mapping** page, click **Map New Adapter Instance** and select the **Adapter**.

The screenshot shows the 'Authentication Source Mapping' tab. The breadcrumb trail is 'SP Connection | Browser SSO | Assertion Creation'. The left sidebar is the same as in the previous screenshots. The main content area has a sub-breadcrumb 'Authentication Source Mapping' and a description: 'PingFederate uses IdP adapters, partner IdPs or Authentication Policies to authenticate users to your SP. Users may be authenticated by one of several different adapters or authentication policy contracts, so map an adapter instance for each IDM system or a authentication policy contract for each policy.' There are two tables: one for 'Adapter Instance Name' and one for 'Authentication Policy Contract Name', both with columns for 'Virtual Server IDs' and 'Action'. At the bottom, there are two buttons: 'Map New Adapter Instance' (highlighted with a red box) and 'Map New Authentication Policy'.

14. On **Mapping Method**, click **Next**.

15. Configure **Attribute Contract Fulfilment**. Select source as Adapter and choose username as value.

PingFederate

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

Adapter Instance | Mapping Method | **Attribute Contract Fulfillment** | Issuance Criteria | Summary

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

Attribute Contract	Source	Value	Actions
SAML_SUBJECT	Adapter	- SELECT -	None available

16. On **Issuance Criteria** page, click **Next**.

PingFederate

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

Adapter Instance | Mapping Method | Attribute Contract Fulfillment | **Issuance Criteria** | Summary

PingFederate can evaluate various criteria to determine whether users are authorized to access SP resources. Use this optional screen to configure the criteria for use with this conditional authorization.

Source	Attribute Name	Condition	Value	Error Result	Action
- SELECT -	- SELECT -	- SELECT -			Add

17. Review the summary and click **Done**. Return to **Authentication Source Mapping**. Ensure that the adapter is listed on the page.

PingFederate

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

Adapter Instance | Mapping Method | Attribute Contract Fulfillment | Issuance Criteria | **Summary**

Click a heading link to edit a configuration setting.

Adapter Instance

Selected adapter: anAdapter

Mapping Method

Adapter: HTML Form IdP Adapter

Mapping Method: Use only the Adapter Contract values in the mapping

Attribute Contract Fulfillment

SAML_SUBJECT: username (Adapter)

Issuance Criteria

Criterion: (None)

18. Review the summary and click **Done**. Return to **Browser SSO**.

Ping PingFederate

MAIN

Identity Provider

Service Provider

SETTINGS

Server Configuration

SP Connection | Browser SSO | Assertion Creation

Identity Mapping | Attribute Contract | Authentication Source Mapping | Summary

Summary information for your Assertion Creation configuration. Click a heading link to edit a configuration setting.

Assertion Creation

Identity Mapping

Enable Standard Identifier	true
----------------------------	------

Attribute Contract

Attribute	SAML_SUBJECT
Subject Name Format	urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified

Authentication Source Mapping

Adapter Instance name	anAdapter
-----------------------	-----------

Adapter Instance

Selected adapter	anAdapter
------------------	-----------

Mapping Method

Adapter	HTML Form IdP Adapter
Mapping Method	Use only the Adapter Contract values in the mapping

Attribute Contract Fulfillment

SAML_SUBJECT	username (Adapter)
--------------	--------------------

Issuance Criteria

Criterion	(None)
-----------	--------

Copyright © 2003-2018
Ping Identity Corporation
All rights reserved
Version 9.3.2

19. Under **Credentials**, click **Configure Credentials** and select the Signing Certificate for this connection.
20. Review the configuration and click **Save**. Ensure that the connection is marked as **Active**.