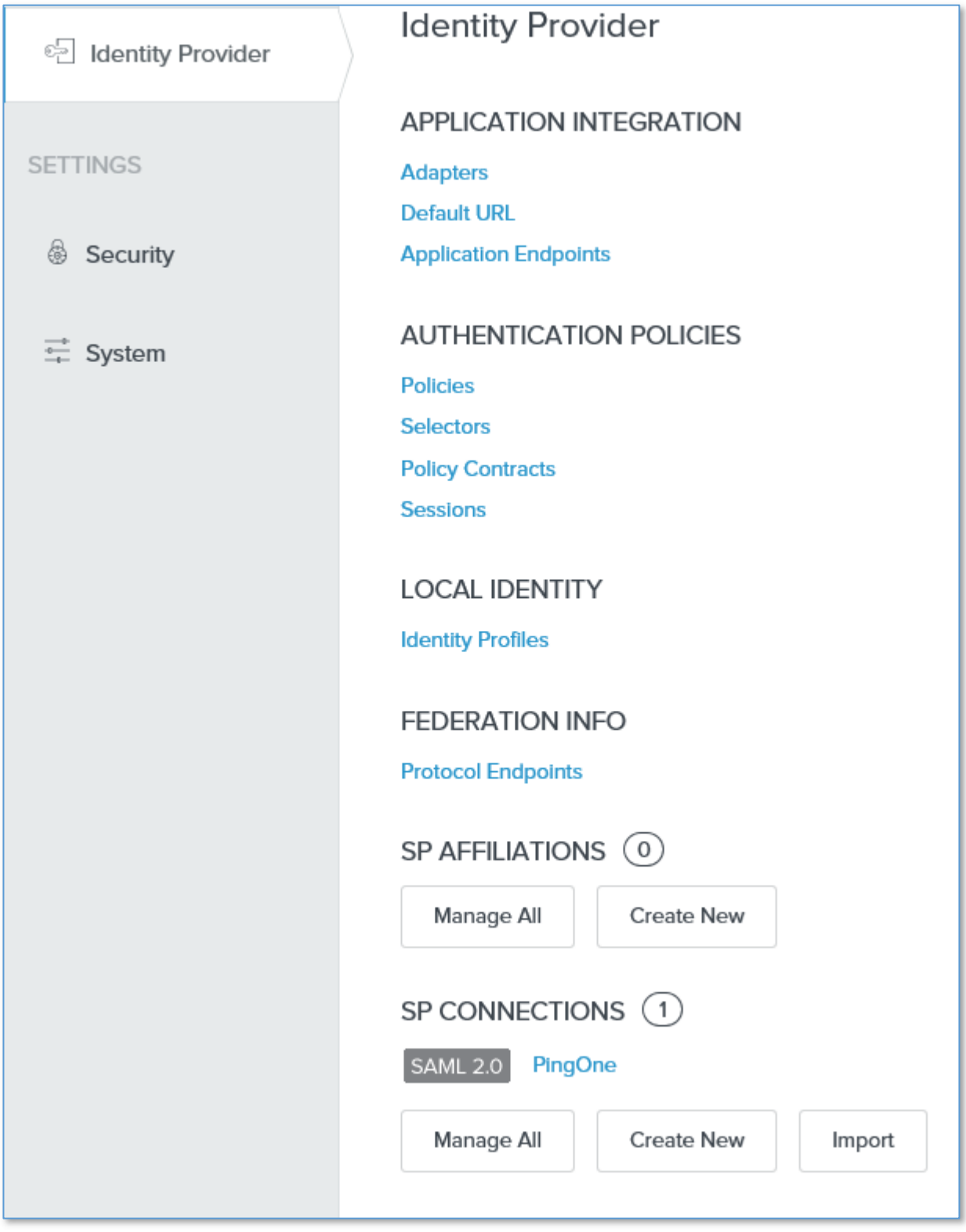
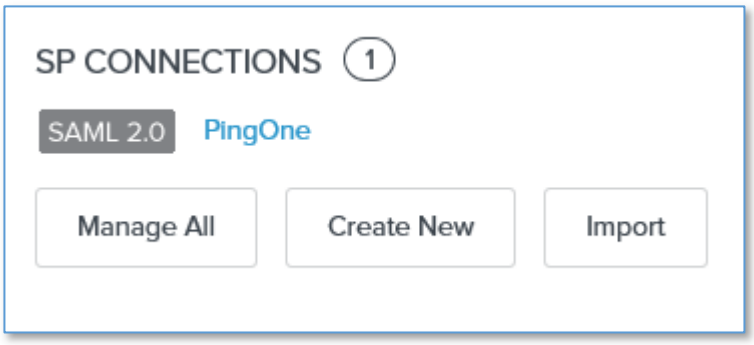
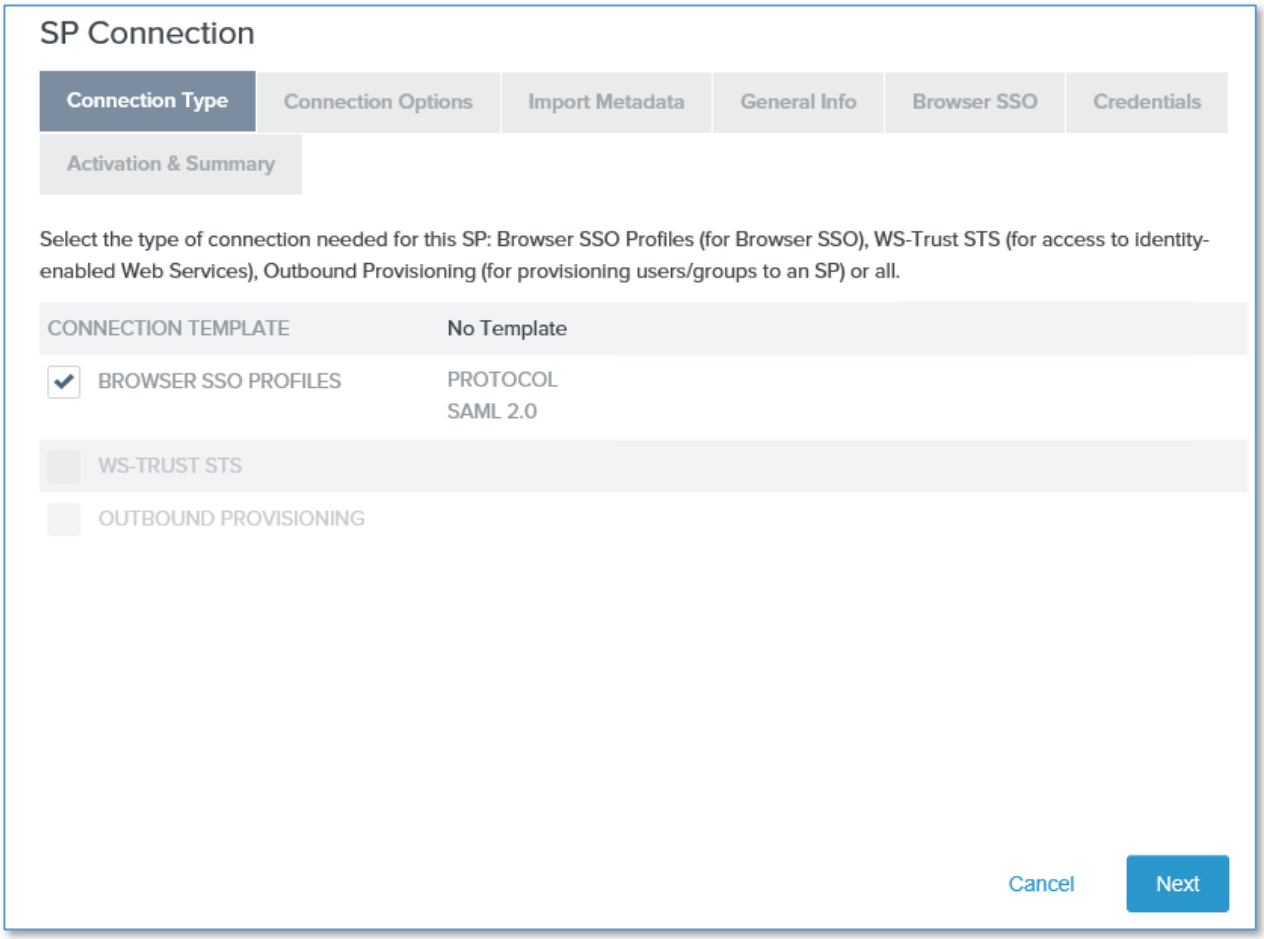
Content Collaboration: Single Sign-On Configuration Guide

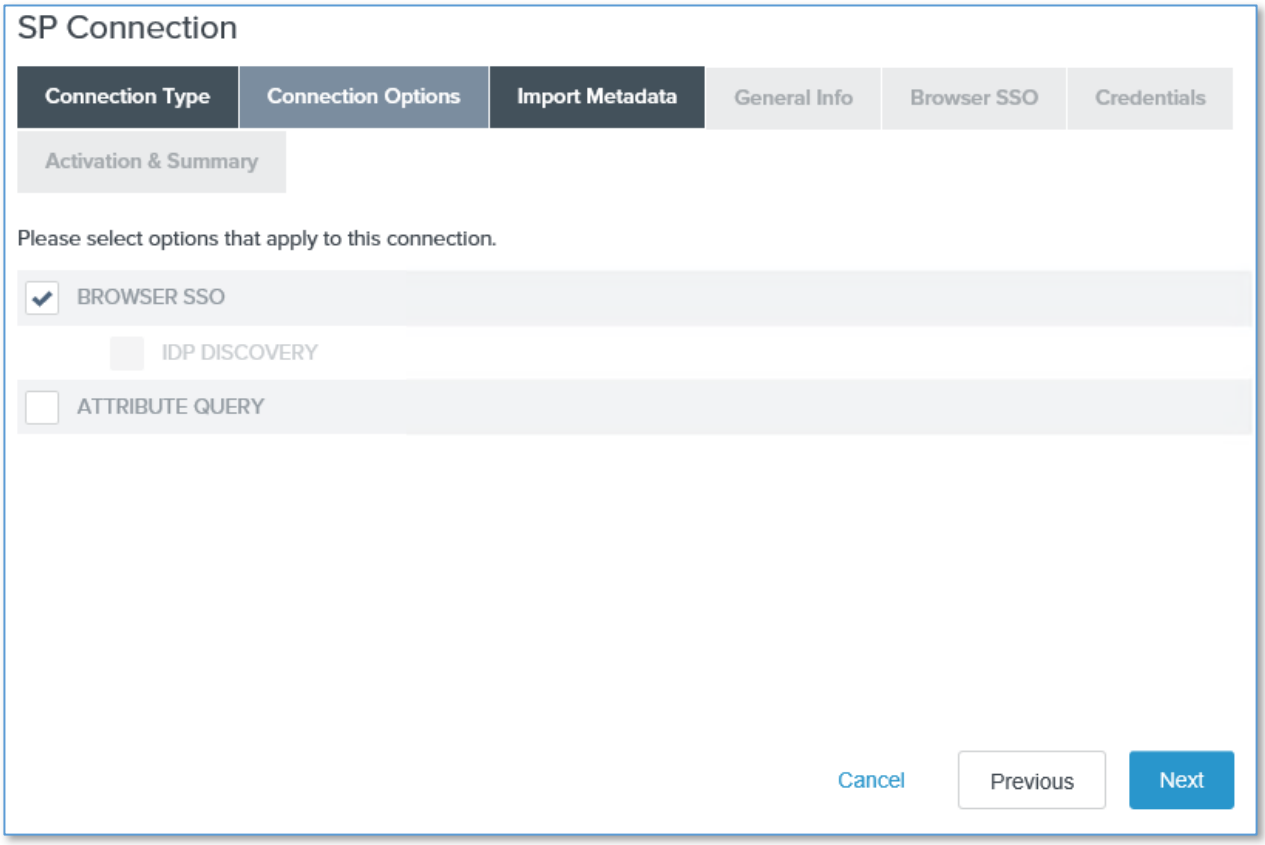
PingFederate

Last Revised: May 2019

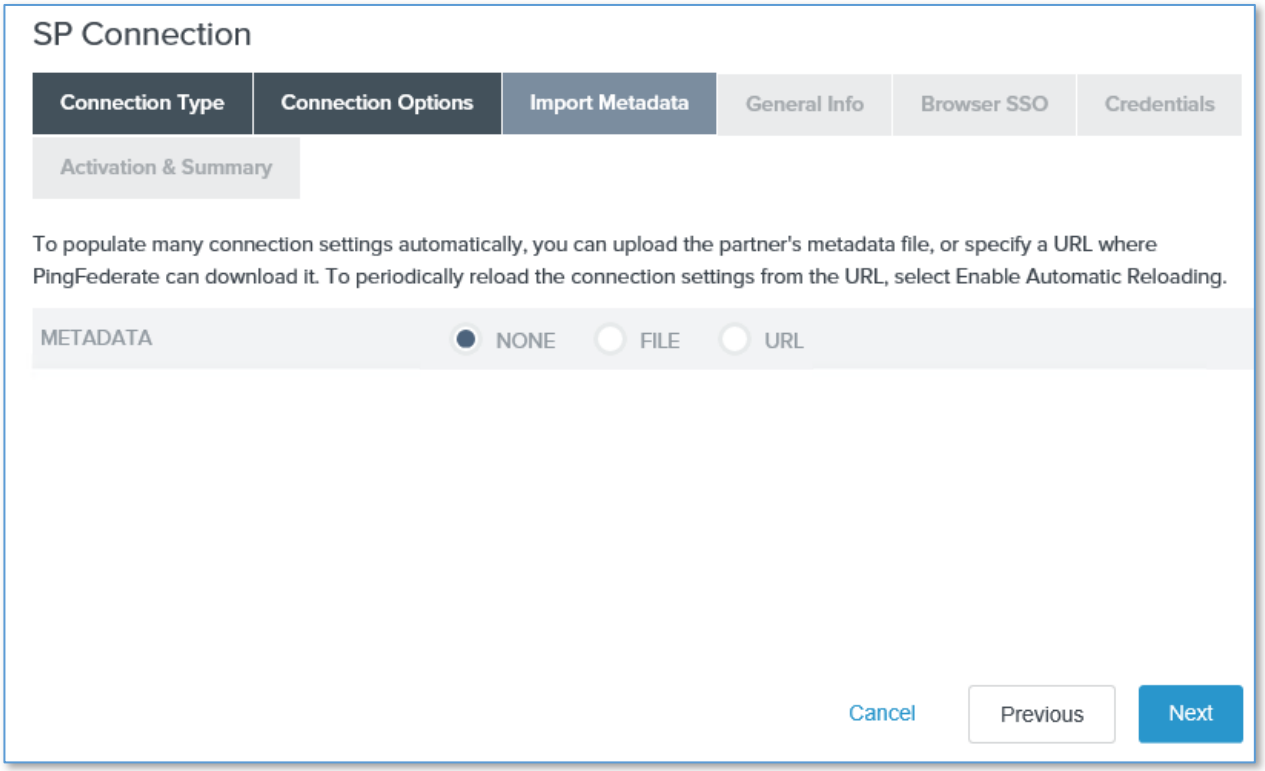
LEGAL NOTICE

Steps	Description
1.	Log in to the Ping administrative console. For example, login to https://pingfed.domain.com:9999/pingfederate/app
2.	Select **Identity Provider.** 

3.	Under **SP Connections** section and select **Create New**. 
4.	On the **Connection Type** tab, select **Browser SSO Profiles** and select **SAML 2.0** as the protocol type. Click **Next**. 
5.	On the **Connection Options** tab, select **Browser SSO**.

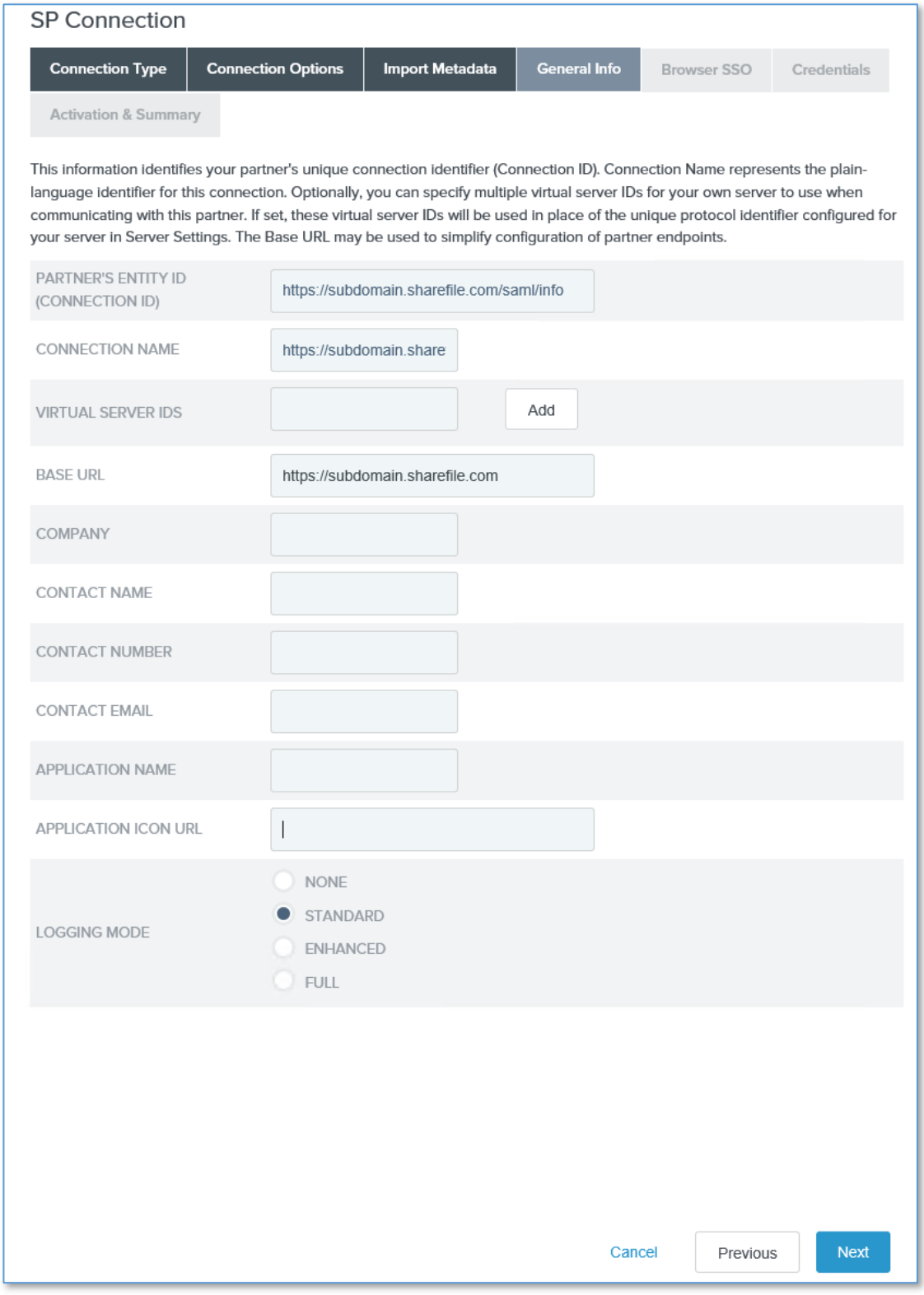


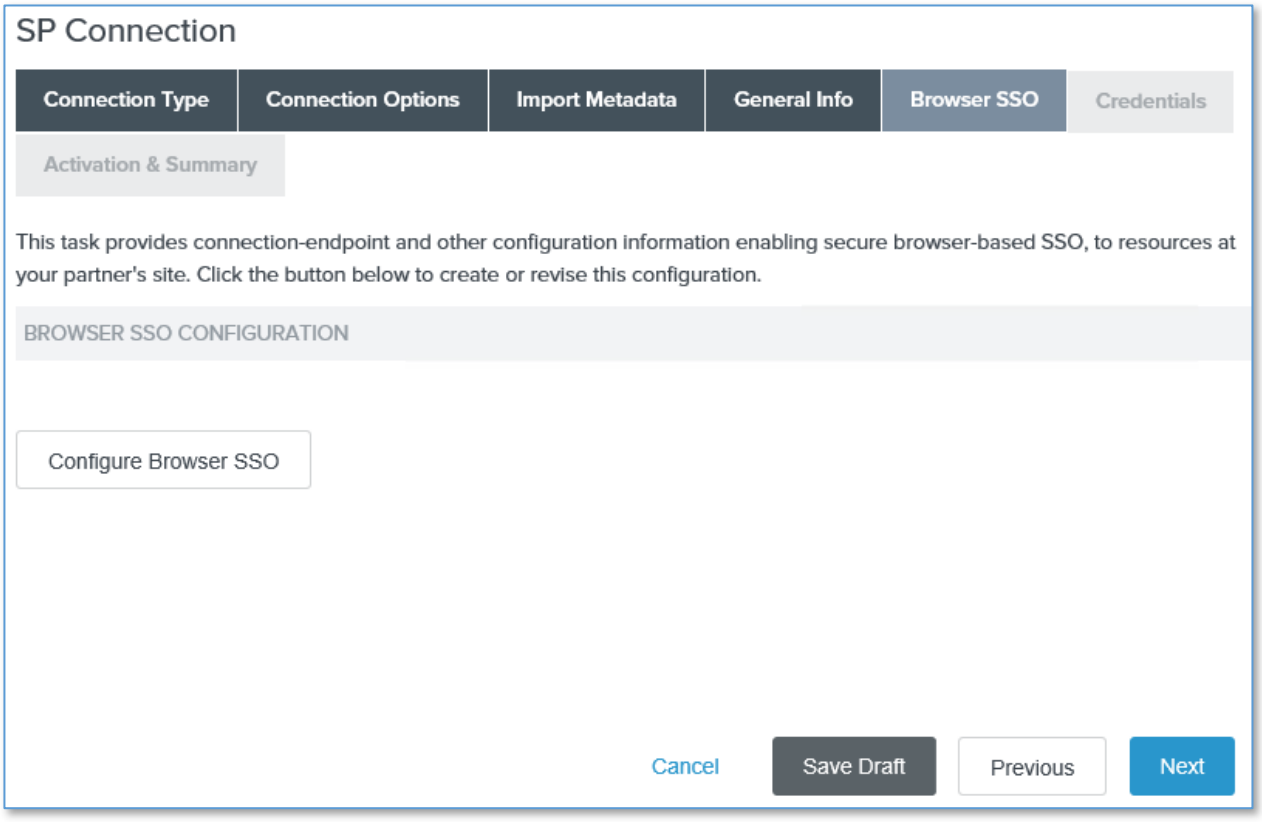
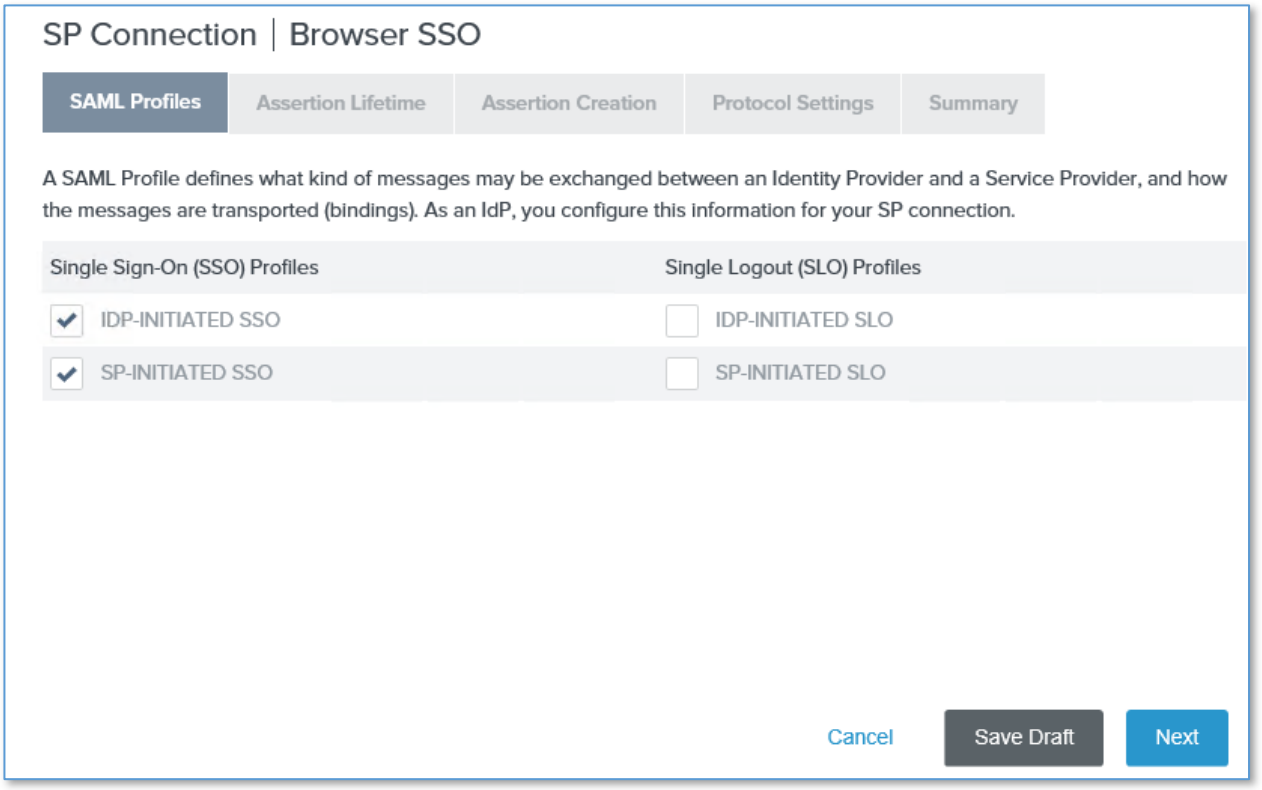
6. On the **Import Metadata** tab, select **None**.

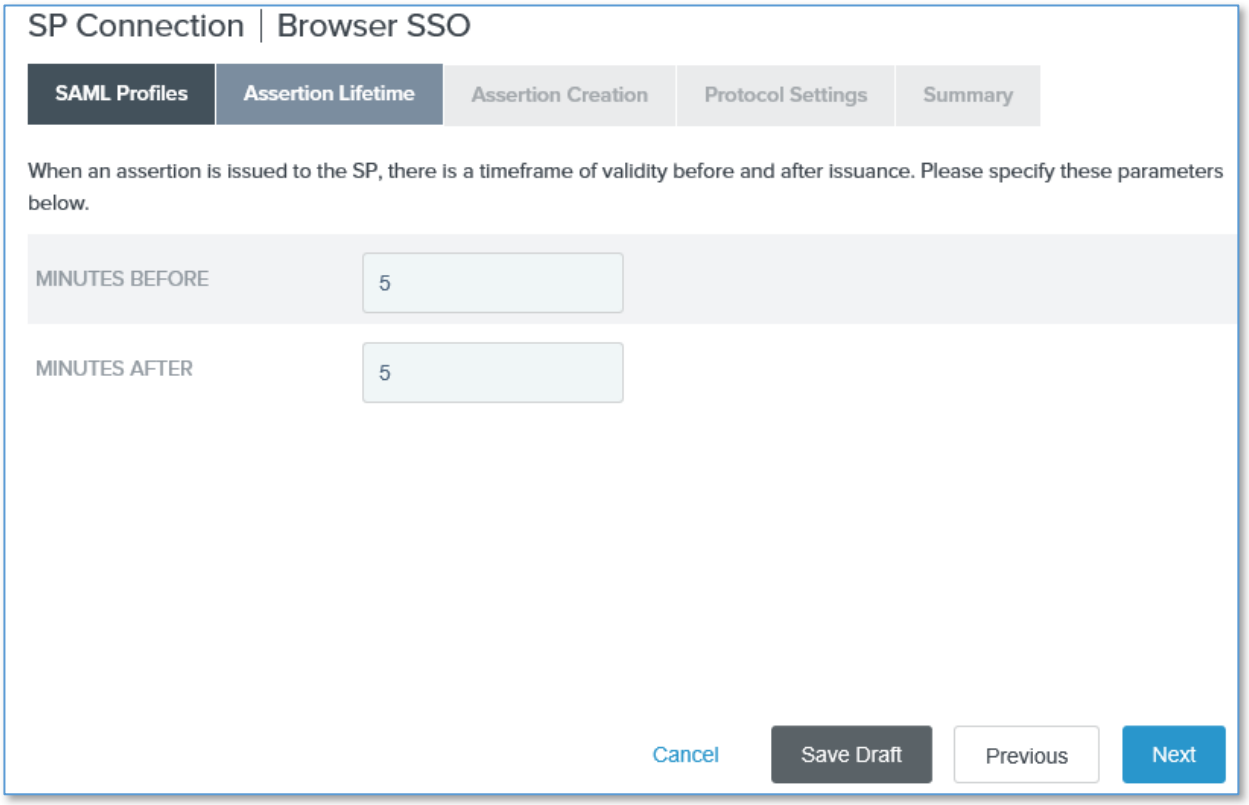


7. On the **General Info** tab, enter information in these required fields:

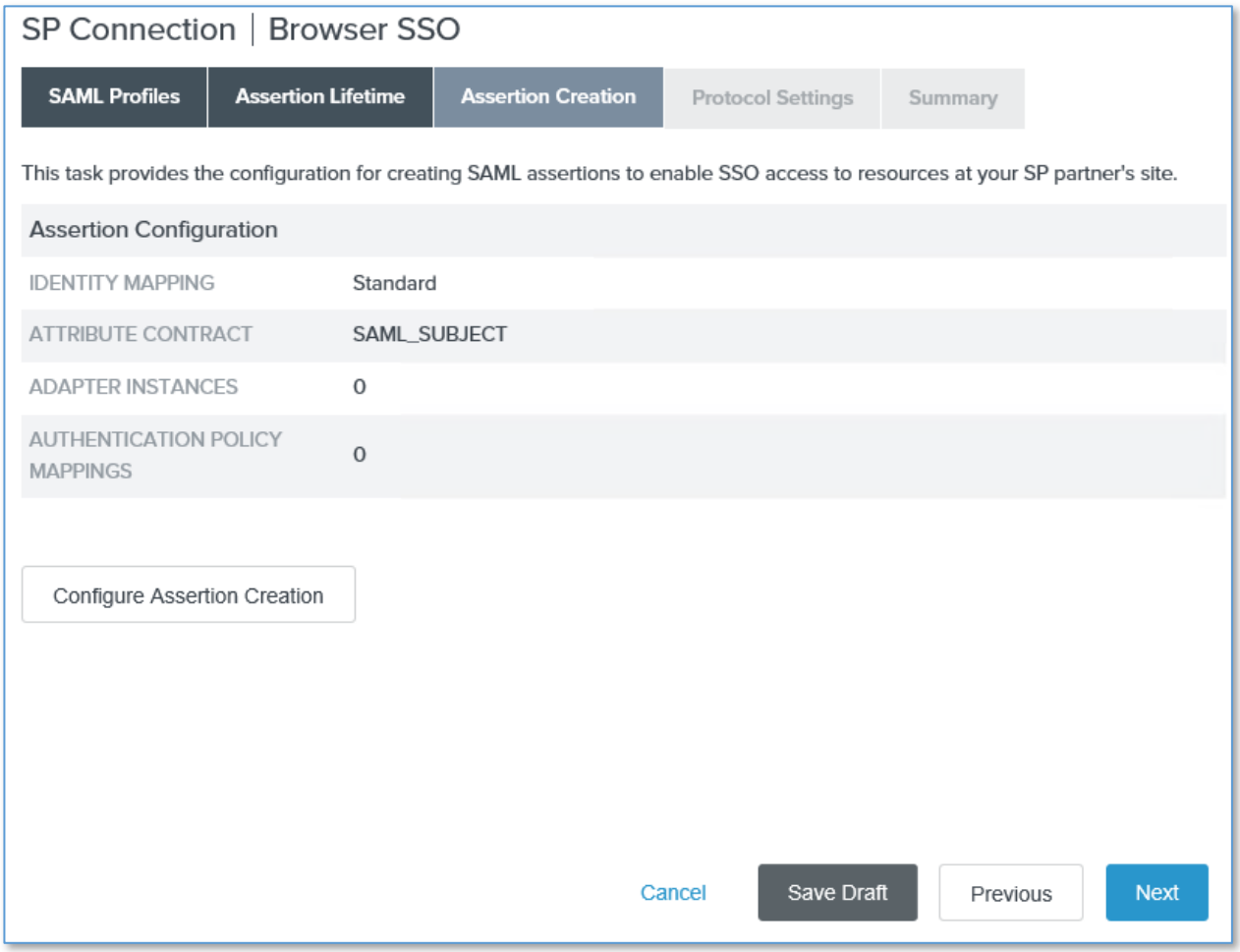
Partner's Entity ID: https://subdomain.sharefile.com/saml/info

	Connection Name: https://subdomain.sharefile.com **Base URL**: https://subdomain.sharefile.com 
8.	On the **Browser SSO** tab, click **Configure Browser SSO**.

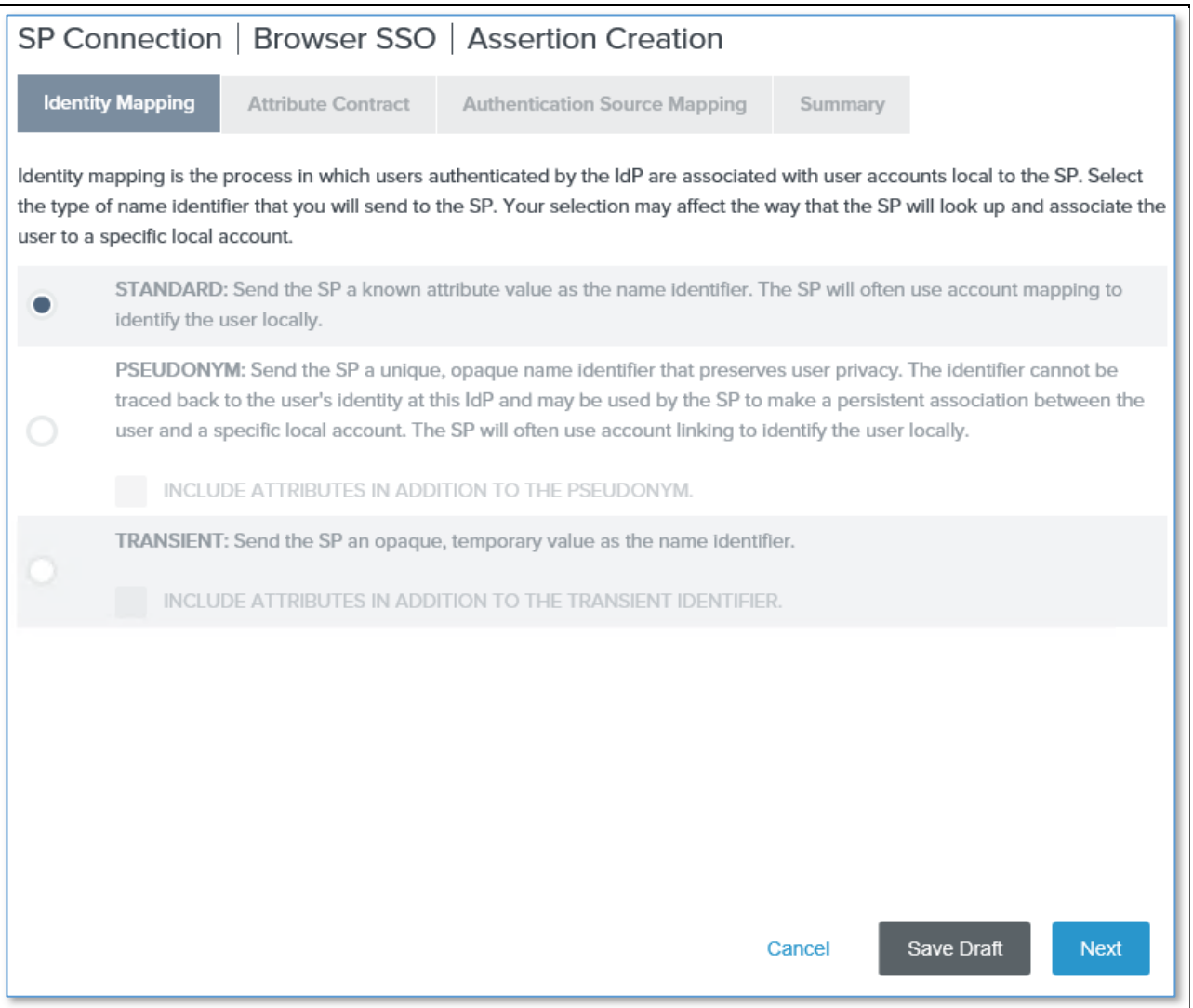
	
9.	In the **SAML Profiles** tab, select these options: **IDP-initiated SSO** and **SP-initiated SSO**. 
10.	In the **Assertion Lifetime** tab, keep the default values.

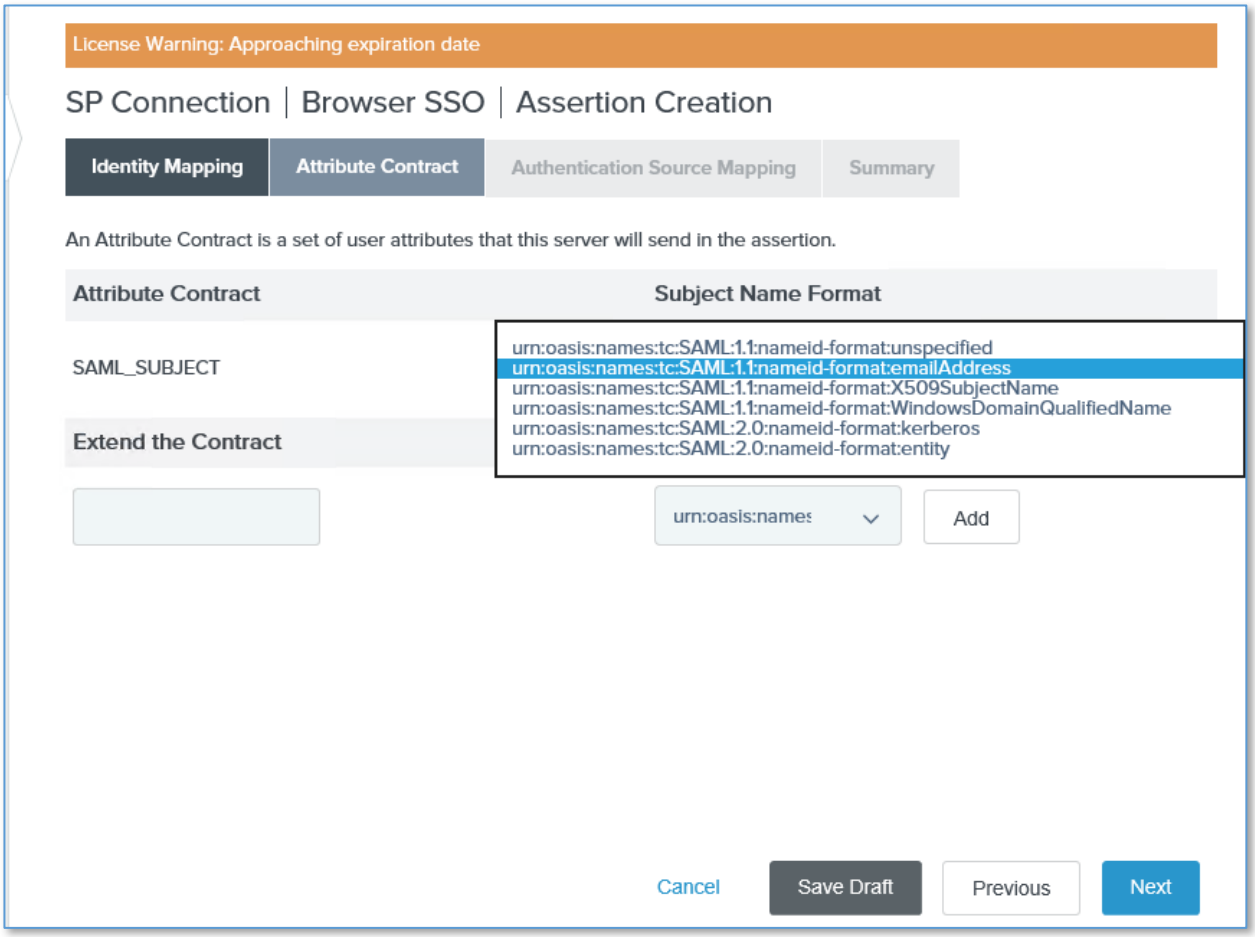


11. On the **Assertion Creation**, select **Configure Assertion Creation**.

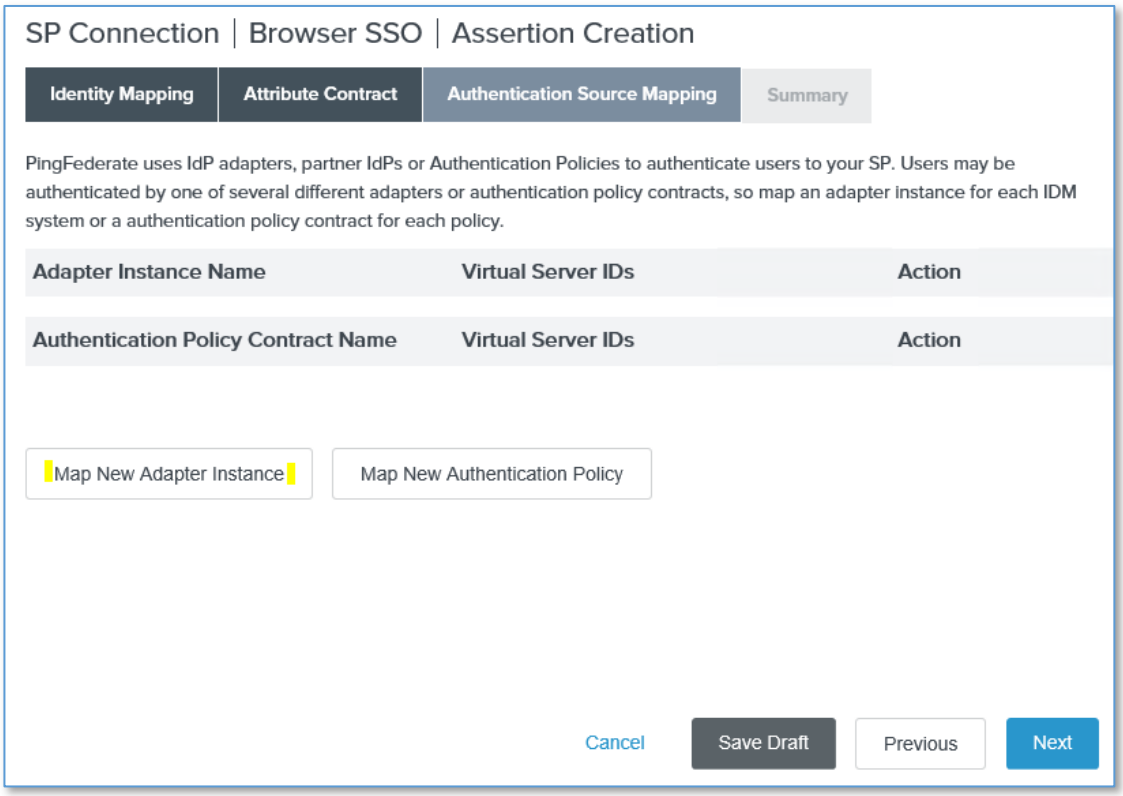


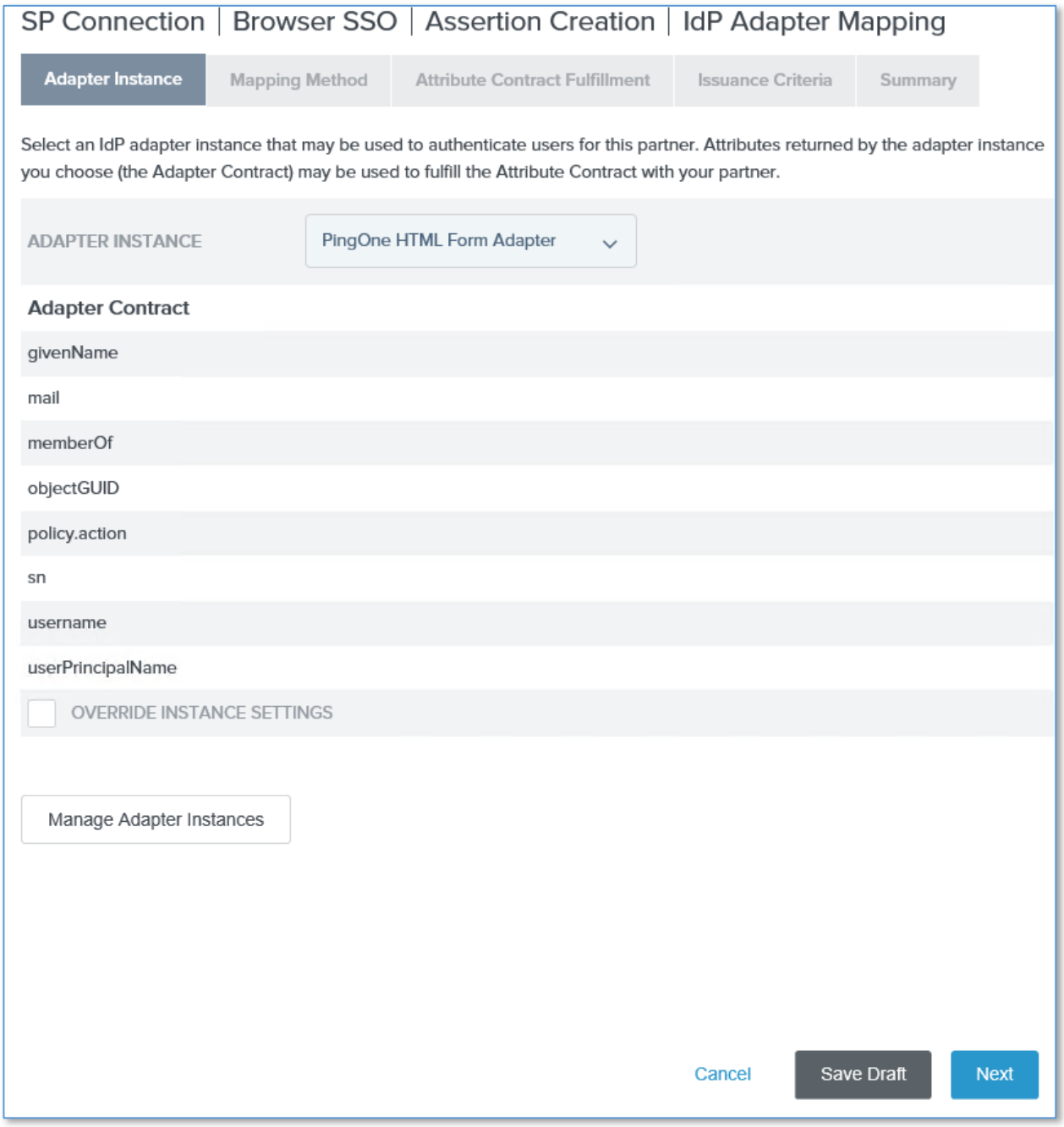
12. Choose the option **Standard** for **Identity Mapping**.

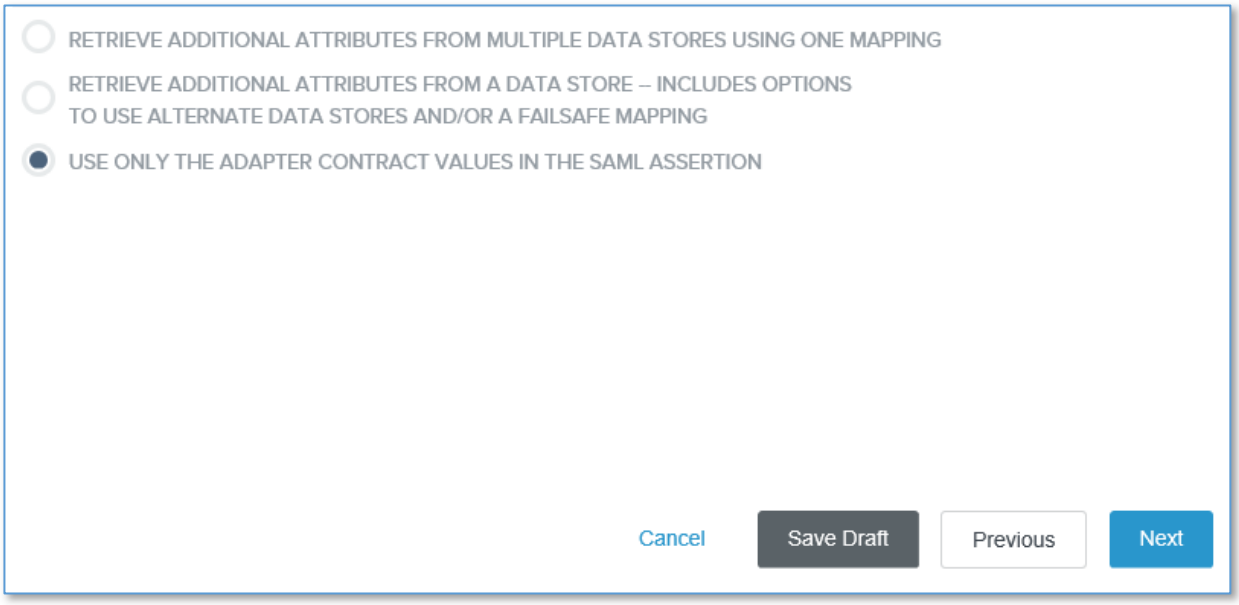
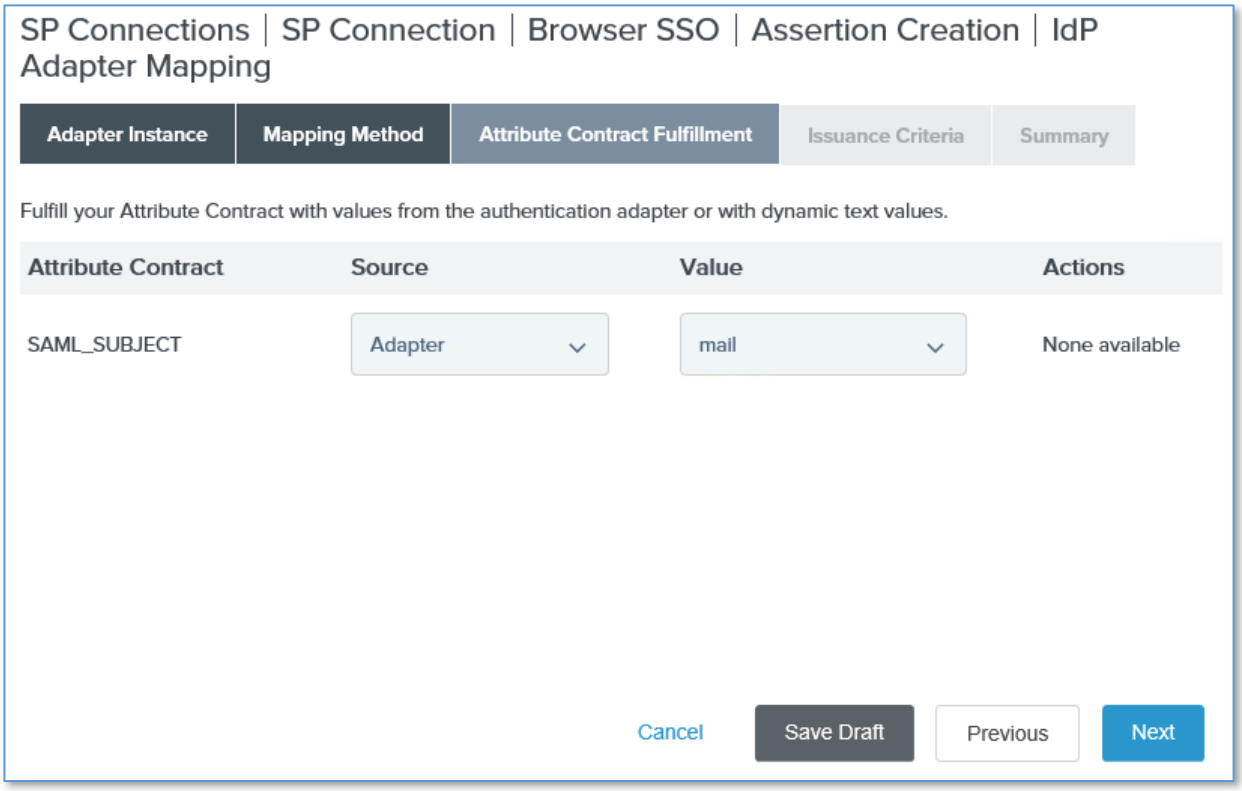
	
13.	In the **Attribute Contract** tab, set SAML_SUBJECT as the **Attribute Contract**. Set the **Subject Name Format** to **urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress**. ShareFile as the service provider requires email attribute as outgoing NameID format for SAML 2.0.

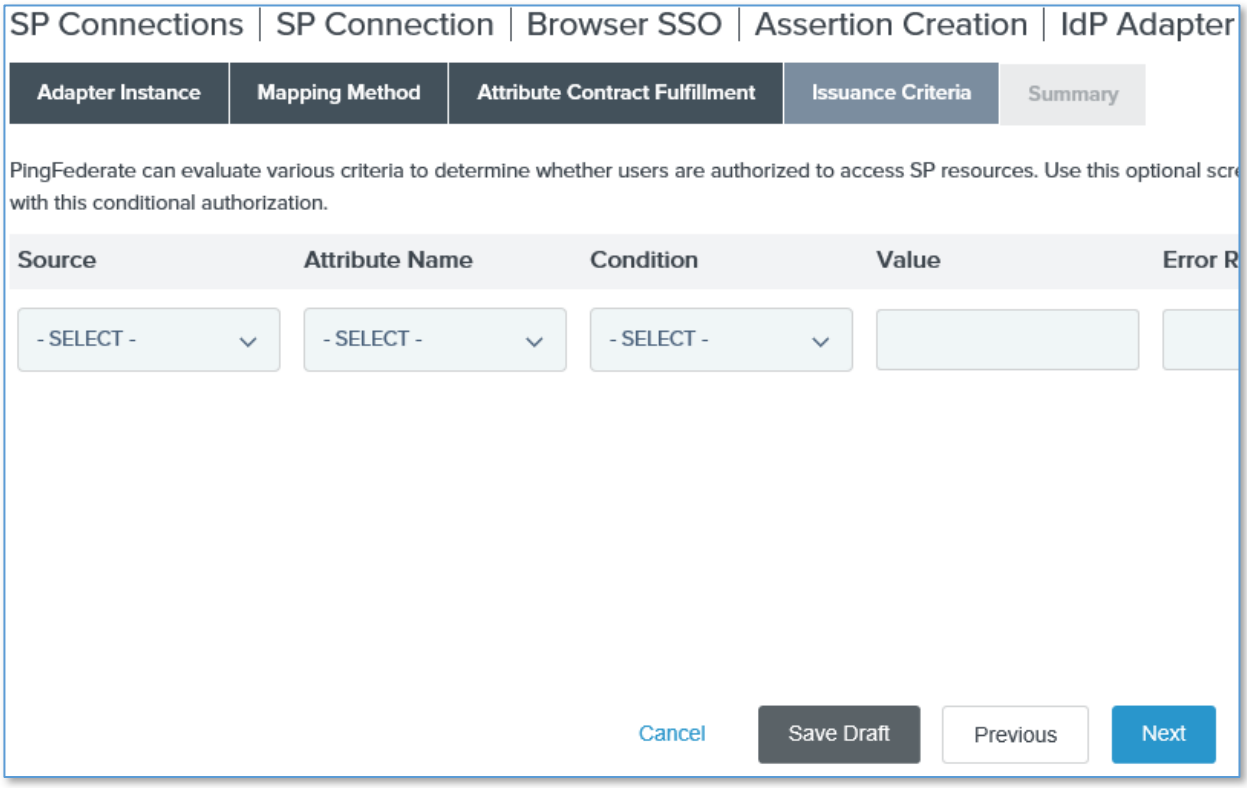


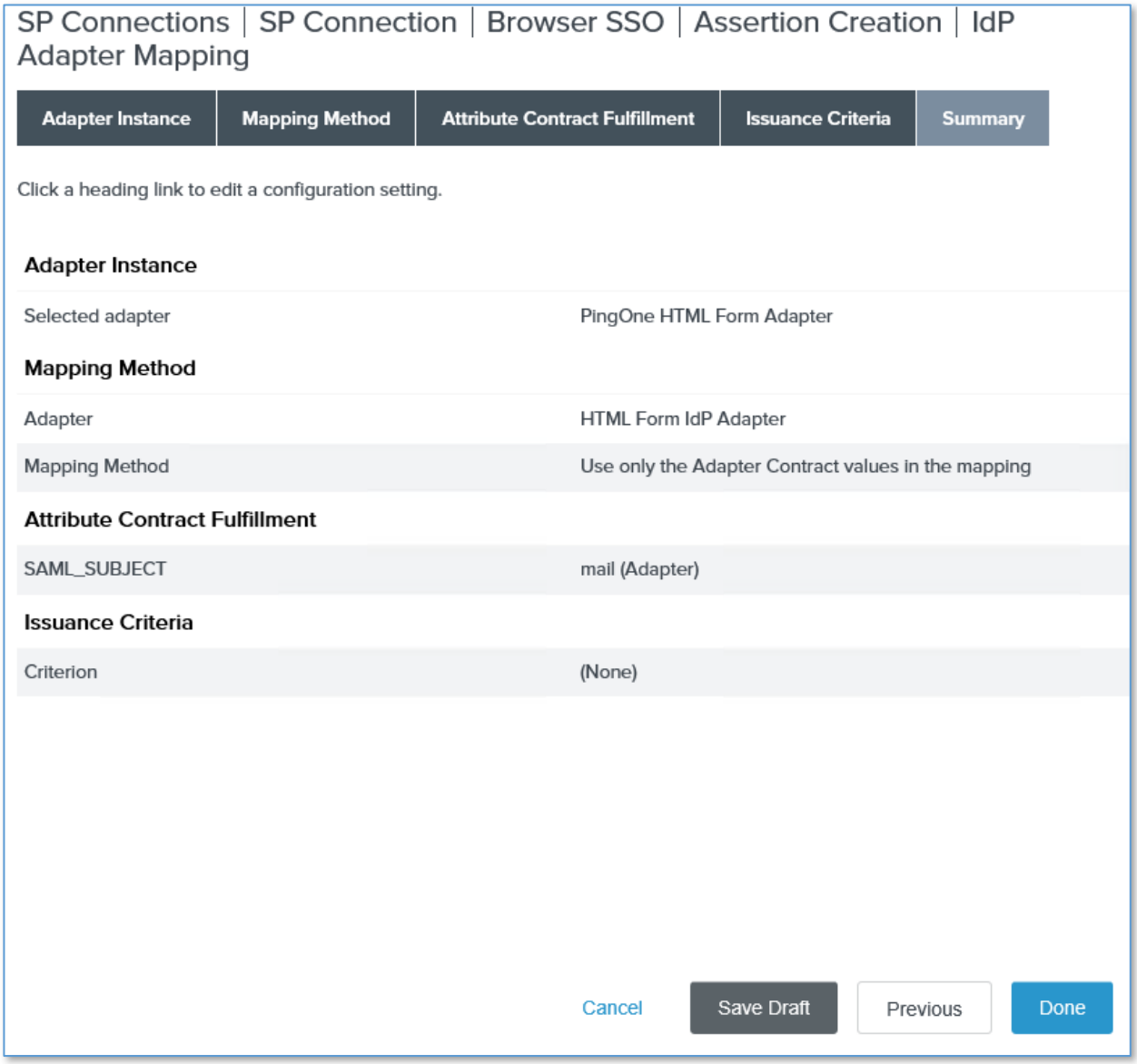
14. In the **Authentication Source Mapping** tab, select **Map New Adapter Instance.**

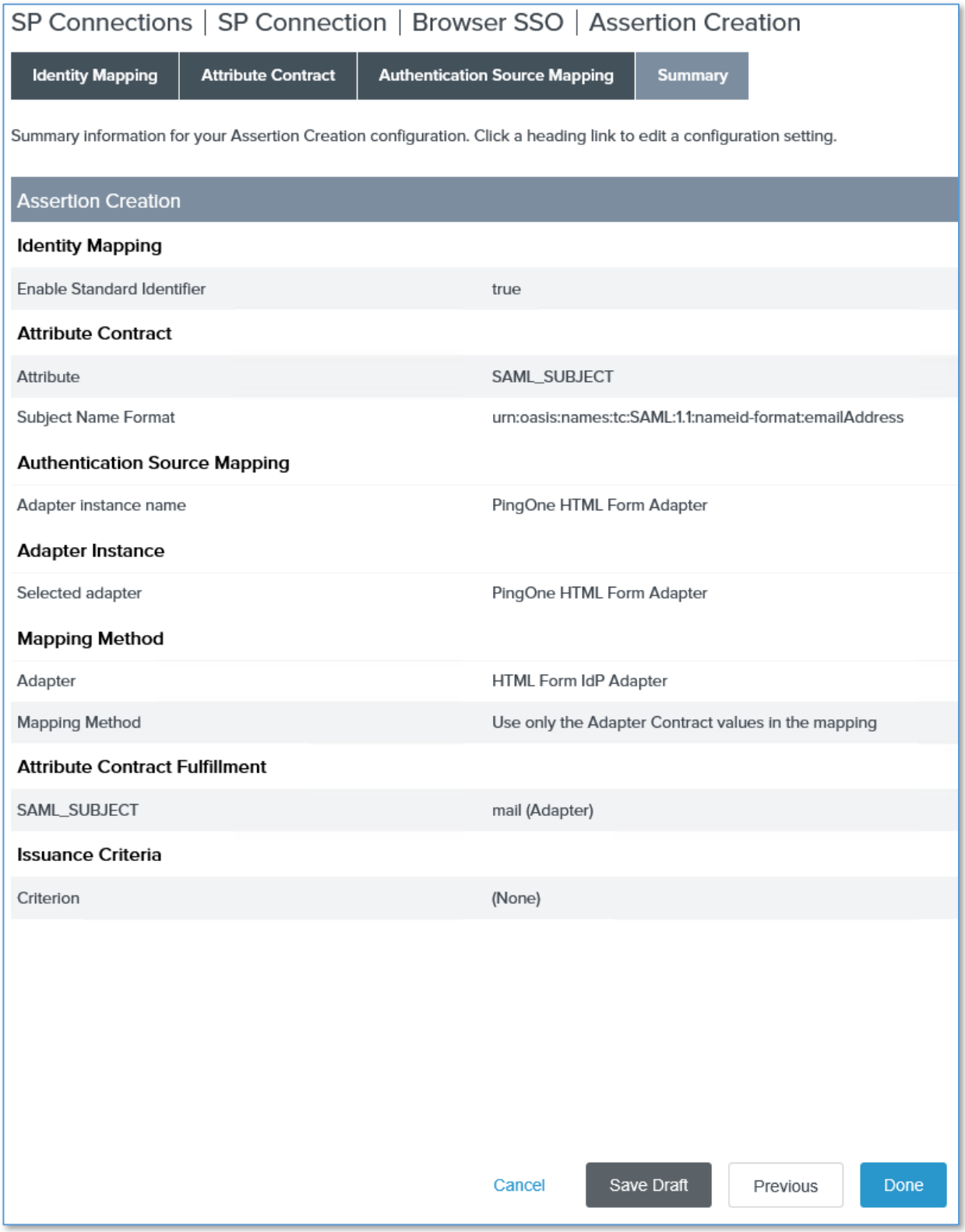


	that extends **email** as **NameID.**
15.	In Adapter Instance tab, in Adapter Instance select **PingONE HTML Form Adapter**. **The format of the adapter can be HTML Forms, Kerberos, or HTTP Basic. For the purpose of this article, HTML Forms is the adapter mapping used for this connection. 
16.	In the **Mapping Method** tab, choose the option **Use Only the Adapter Contract Values in the SAML Assertion.**

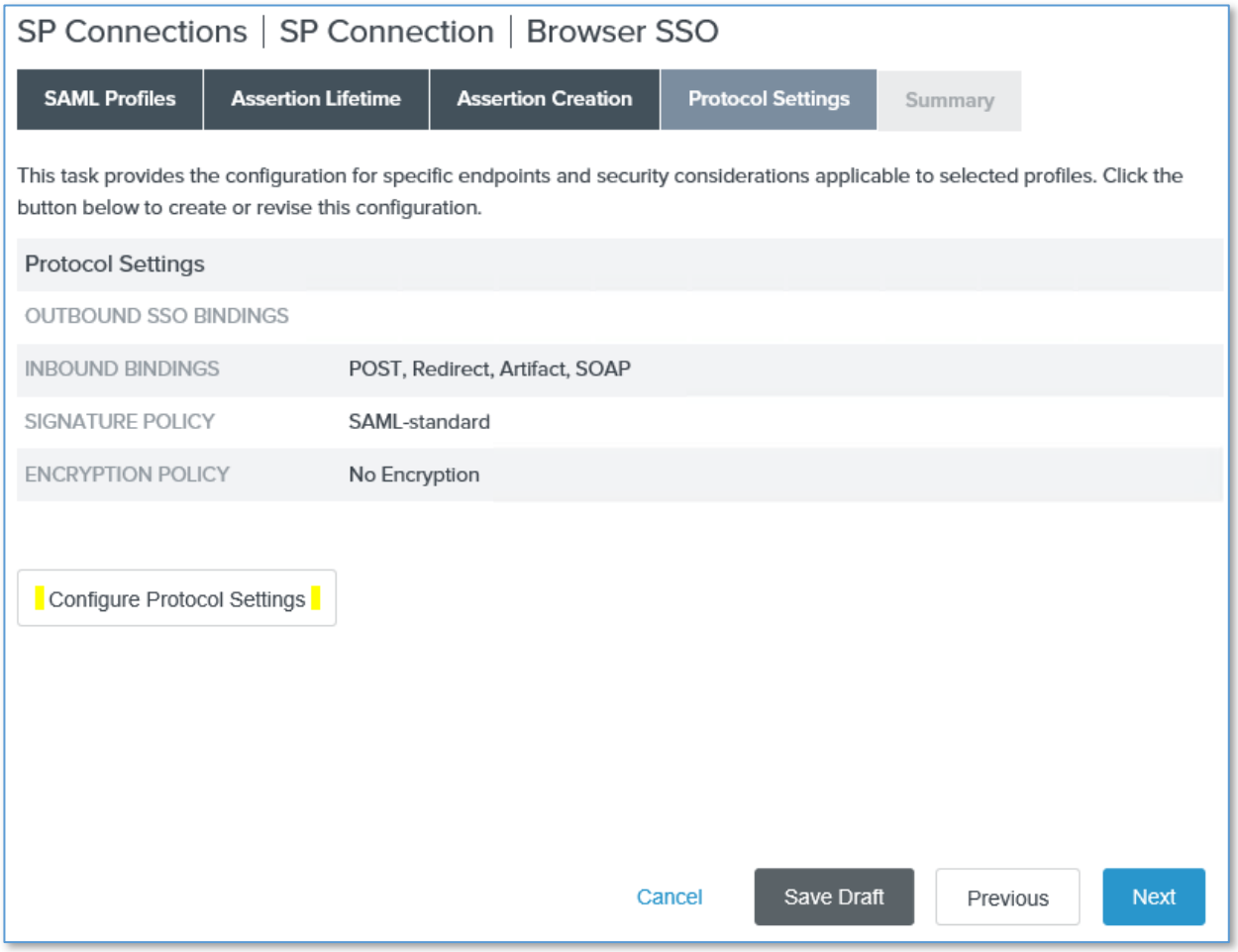
	
17.	In the **Attribute Contract Fulfillment** tab, choose the option **Adapter** for Source, and choose **mail** as Value. 
18.	In the **Issuance Criteria** tab, skip this section without any modifications by clicking **Next.**

	
19.	Once completed, verify the summary tabs matches the formatting.

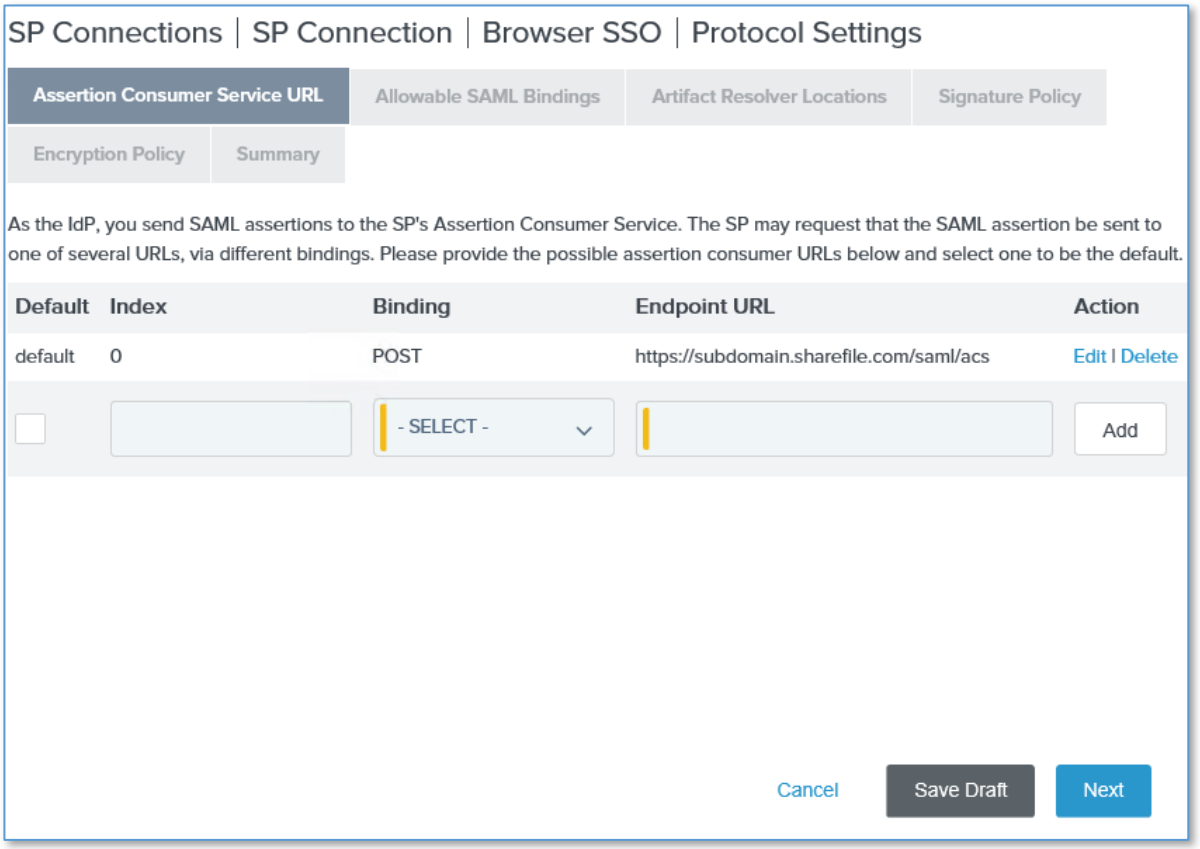

SP Connections | SP Connection | Browser SSO | Assertion Creation | IdP Adapter Mapping
Adapter Instance
Mapping Method
Attribute Contract Fulfillment
Issuance Criteria
Summary
Click a heading link to edit a configuration setting.
Adapter Instance
Selected adapter
PingOne HTML Form Adapter
Mapping Method
Adapter
HTML Form IdP Adapter
Mapping Method
Use only the Adapter Contract values in the mapping
Attribute Contract Fulfillment
SAML_SUBJECT
mail (Adapter)
Issuance Criteria
Criterion
(None)
Cancel
Save Draft
Previous
Done



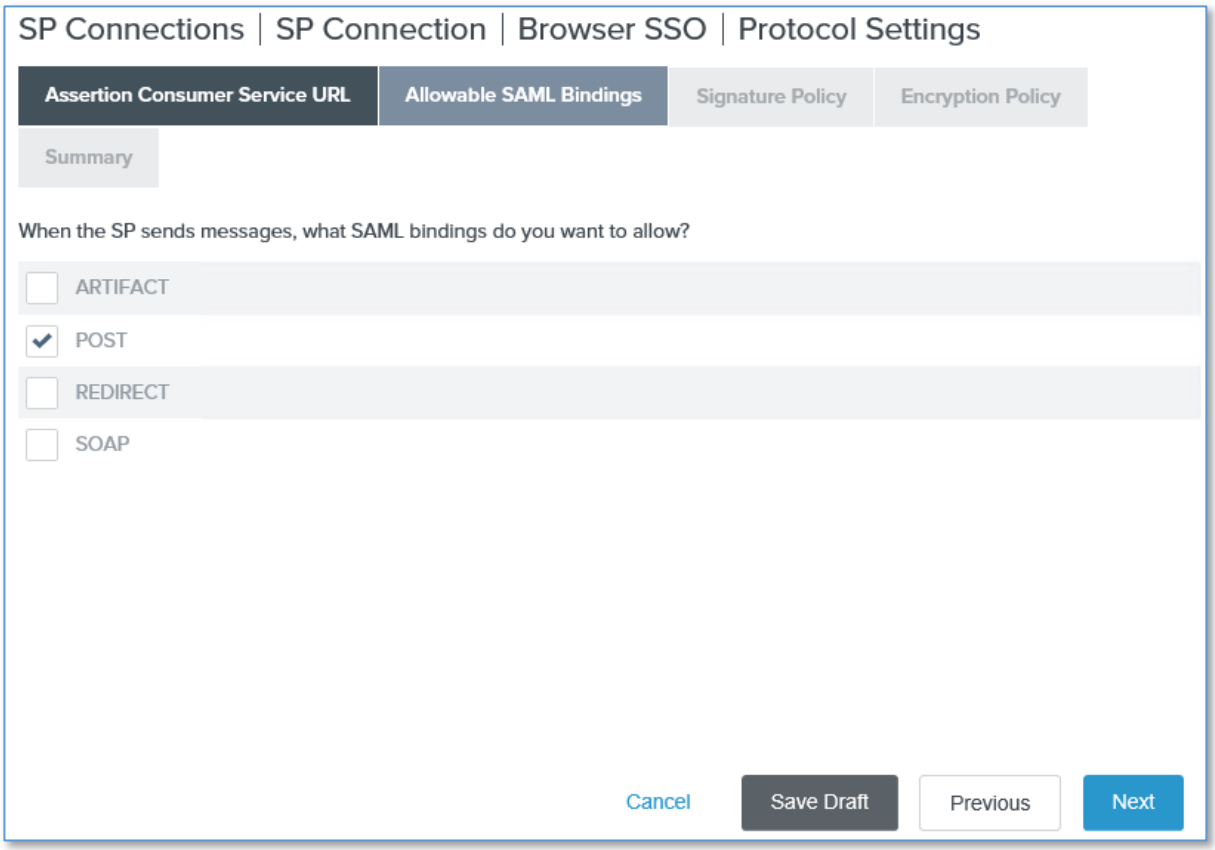
20.	In the **Protocol Settings,** select Configure Protocol Settings.

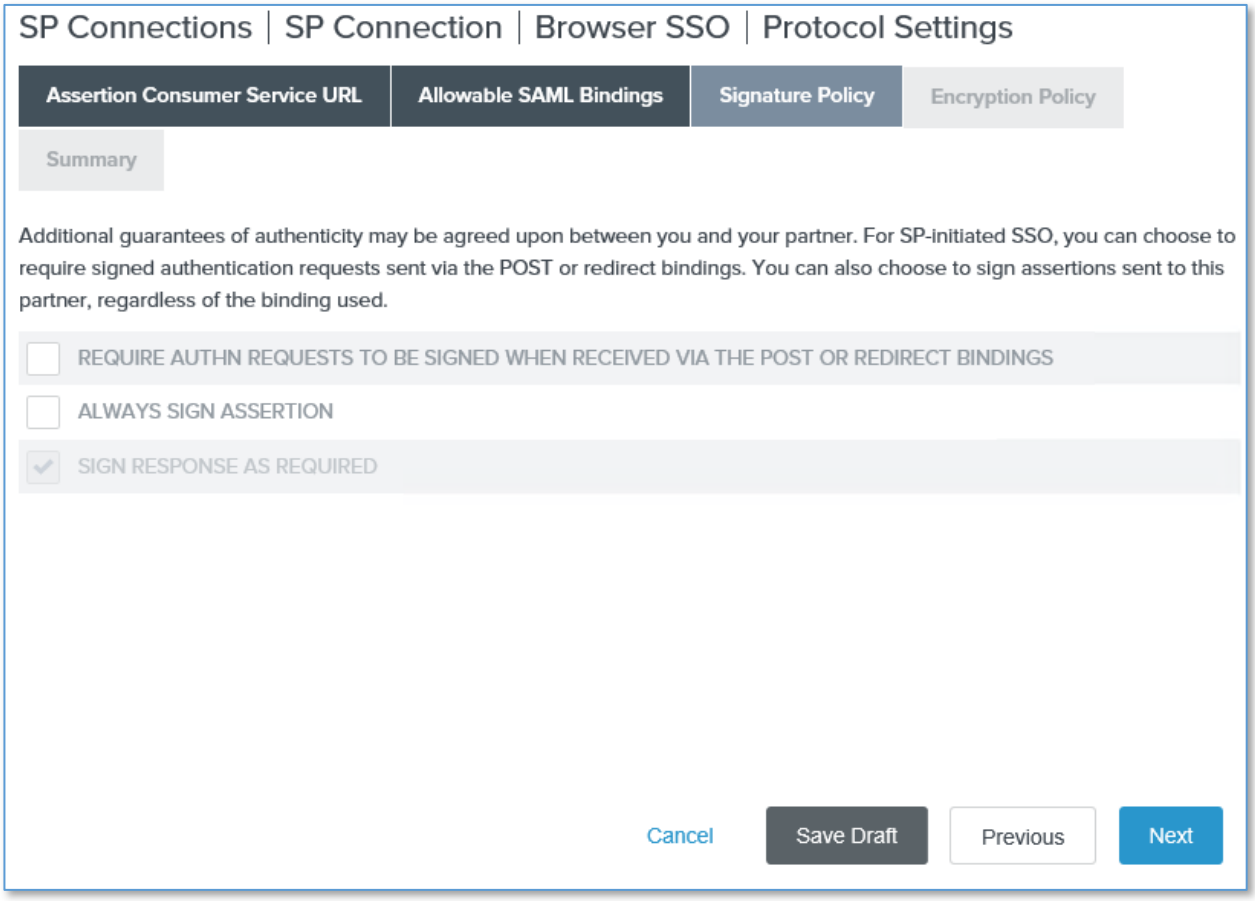


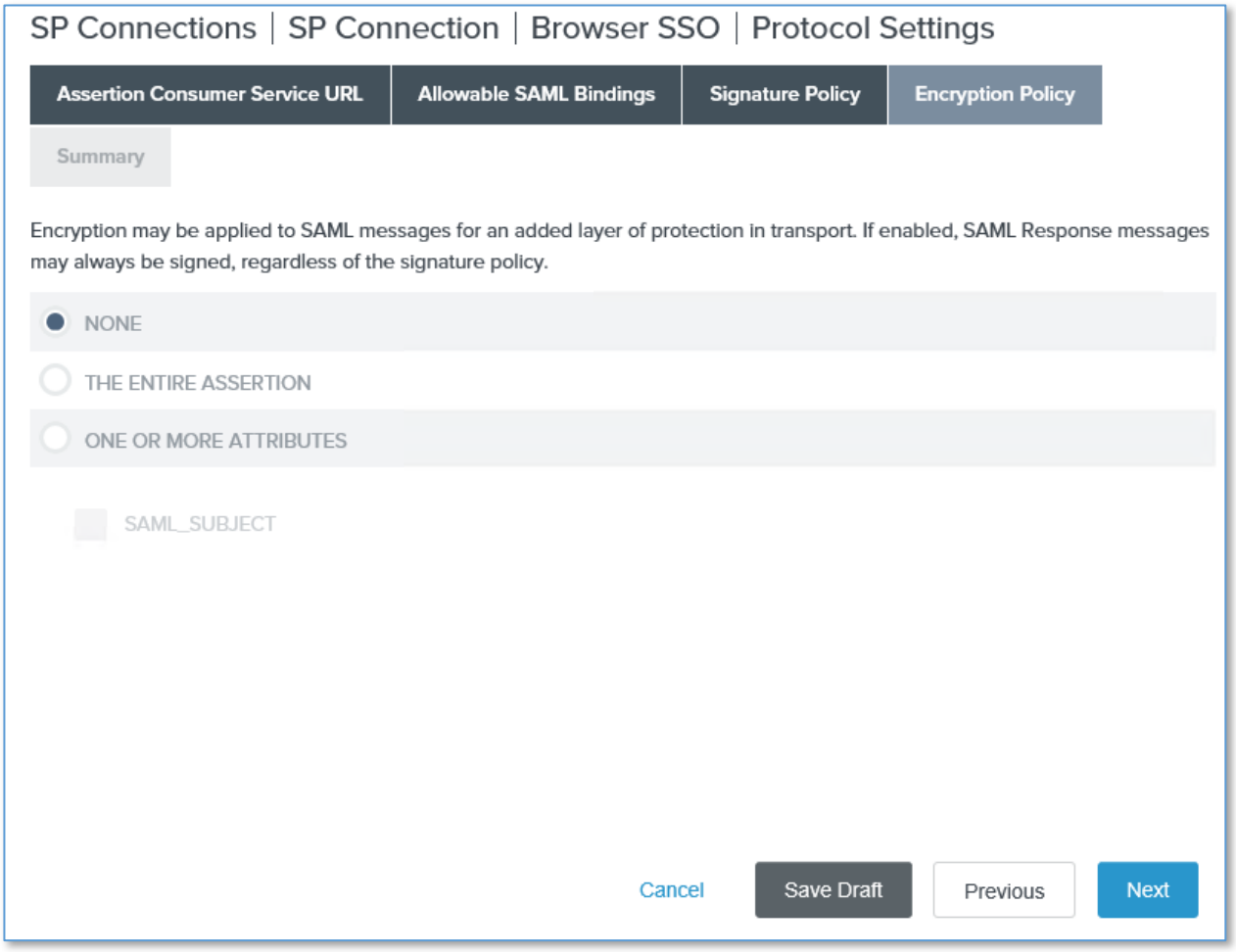
21.	In the **Assertion Consumer Service URL** tab, select Binding: **POST**. In the **Endpoint URL** enter: https://subdomain.sharefile.com/saml/acs Select **Add**.

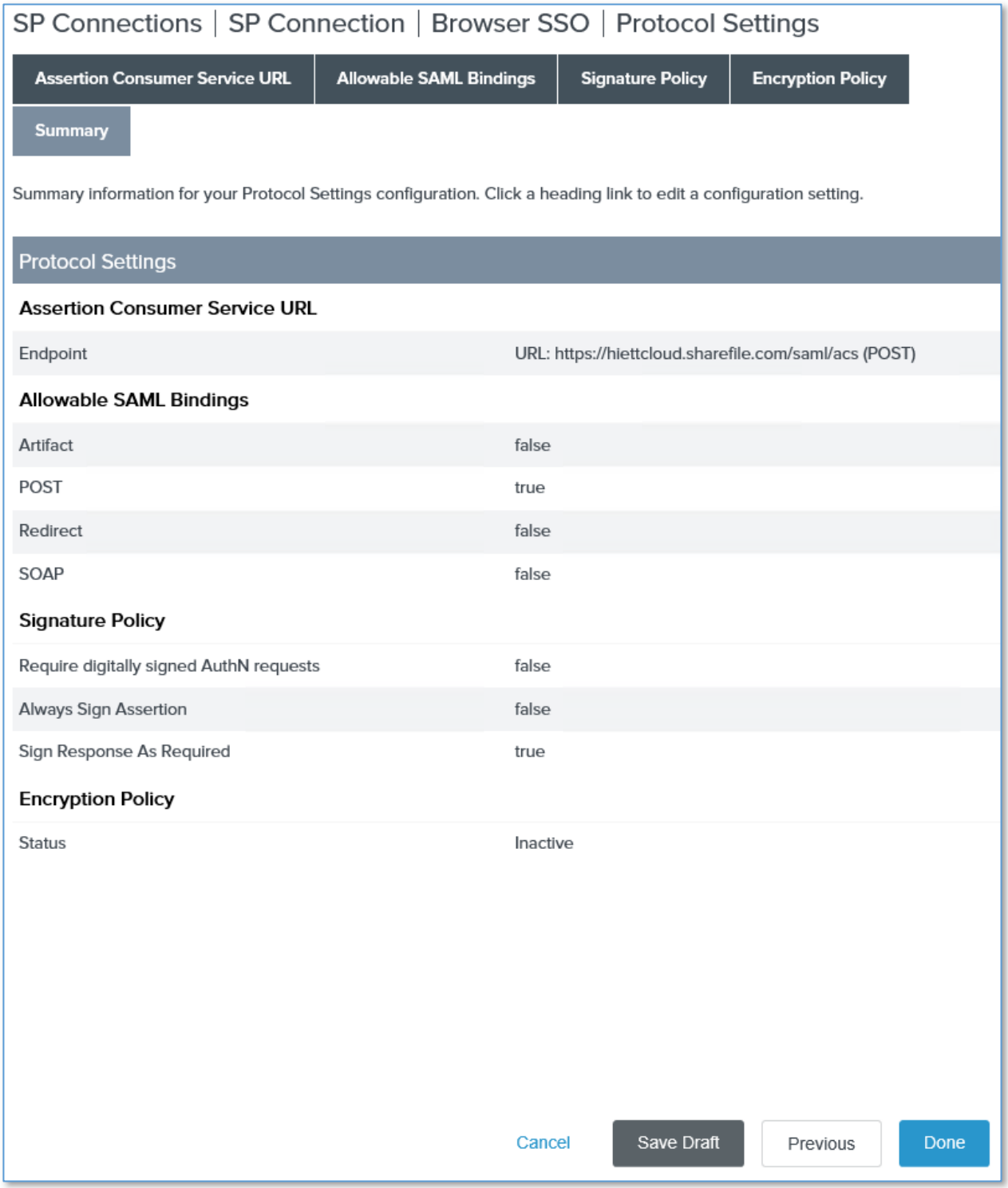


22. In the **Allowable SAML Bindings** tab, select only the **POST** option, de-selecting all other values.

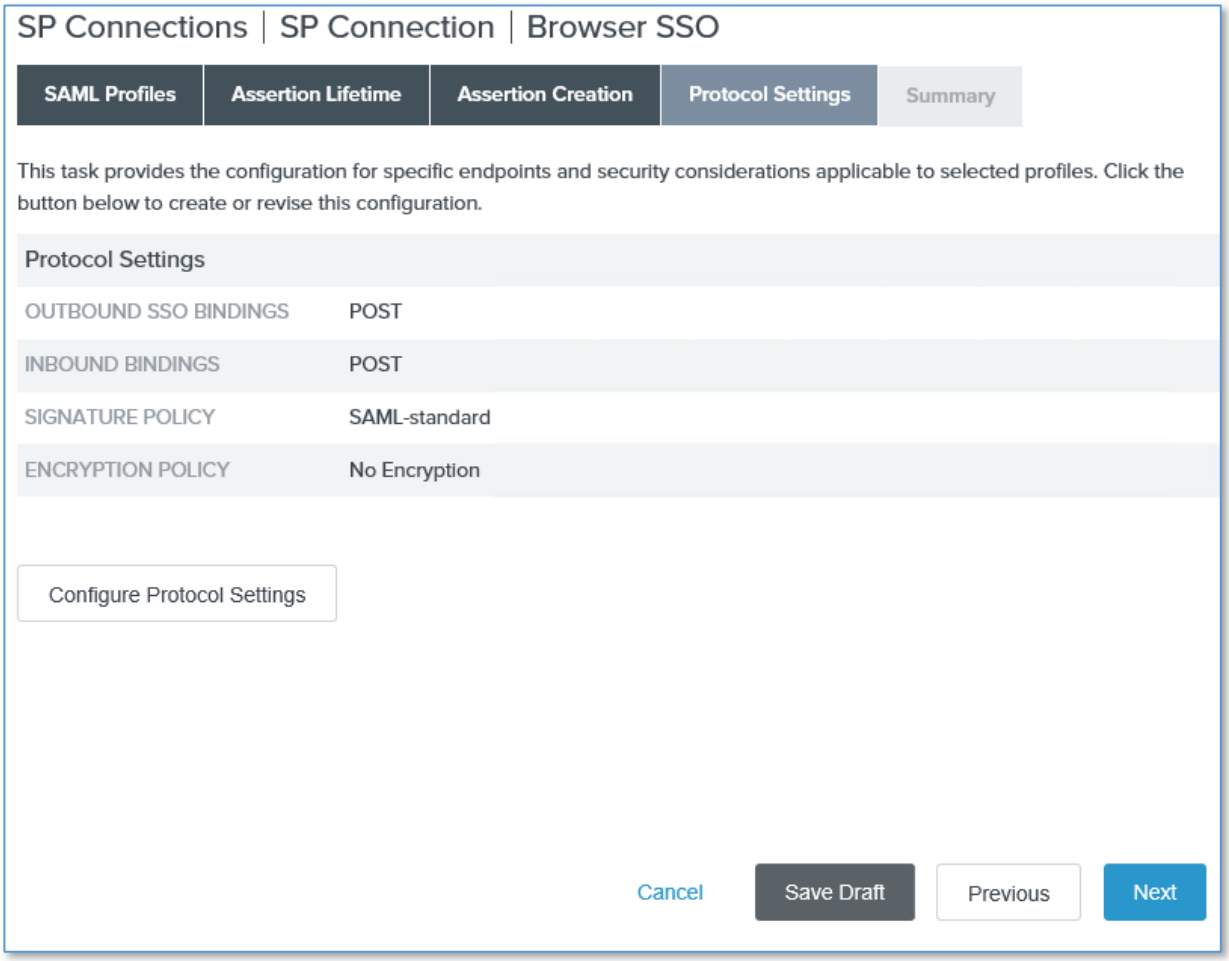


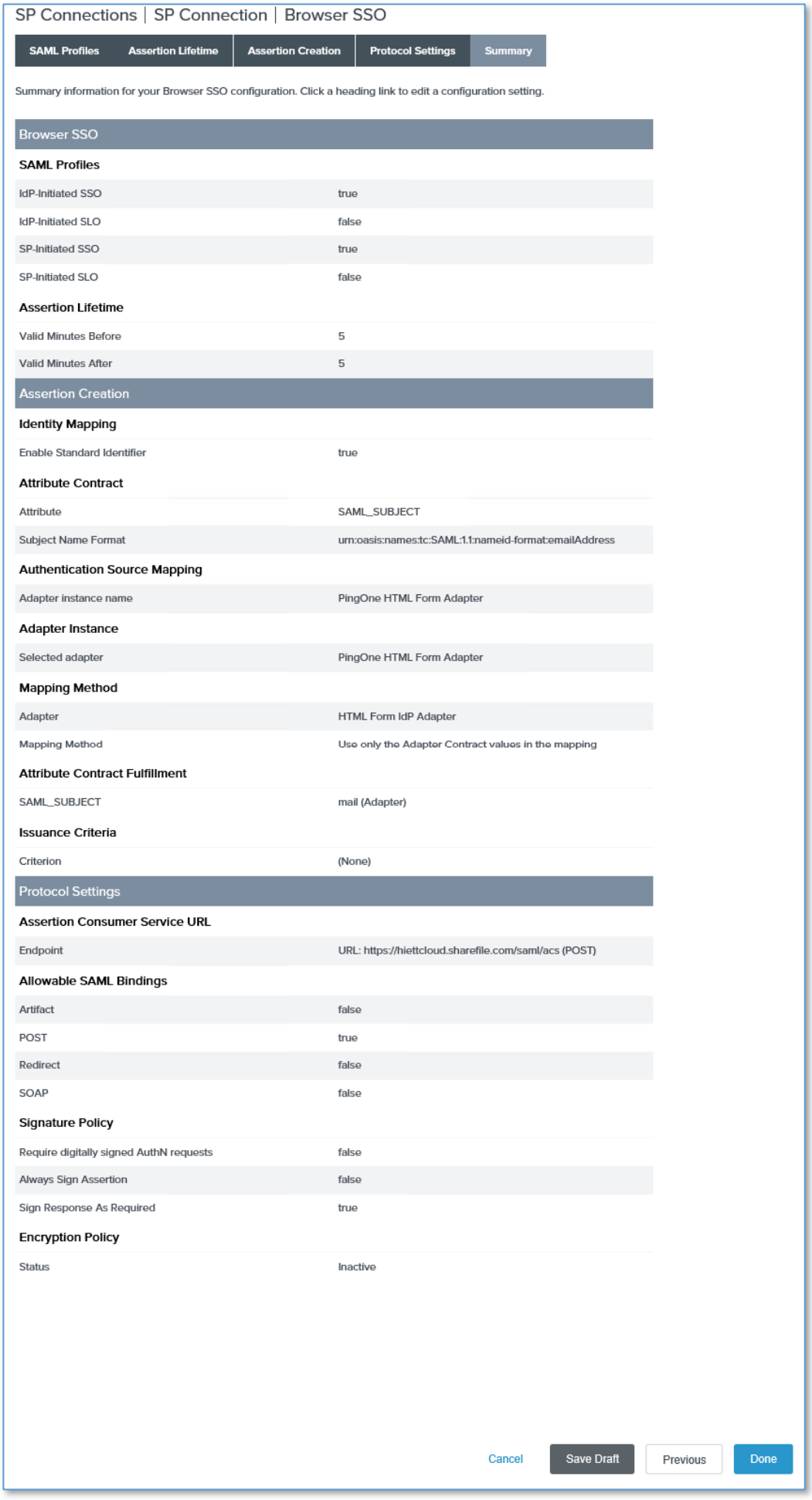
23.	In the **Signature Policy** tab, select **Next** without modifying default values. 
24.	In the **Encryption Policy** tab, select **None** as the value.

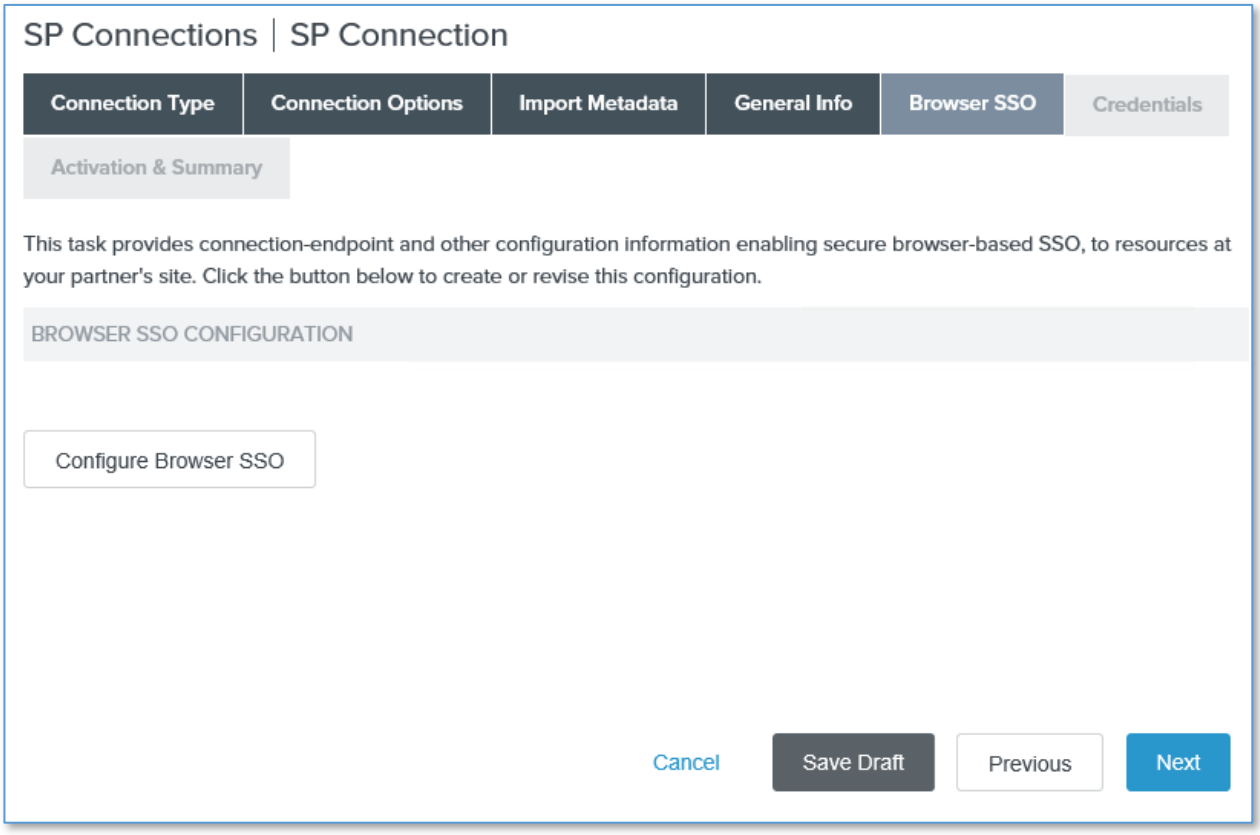
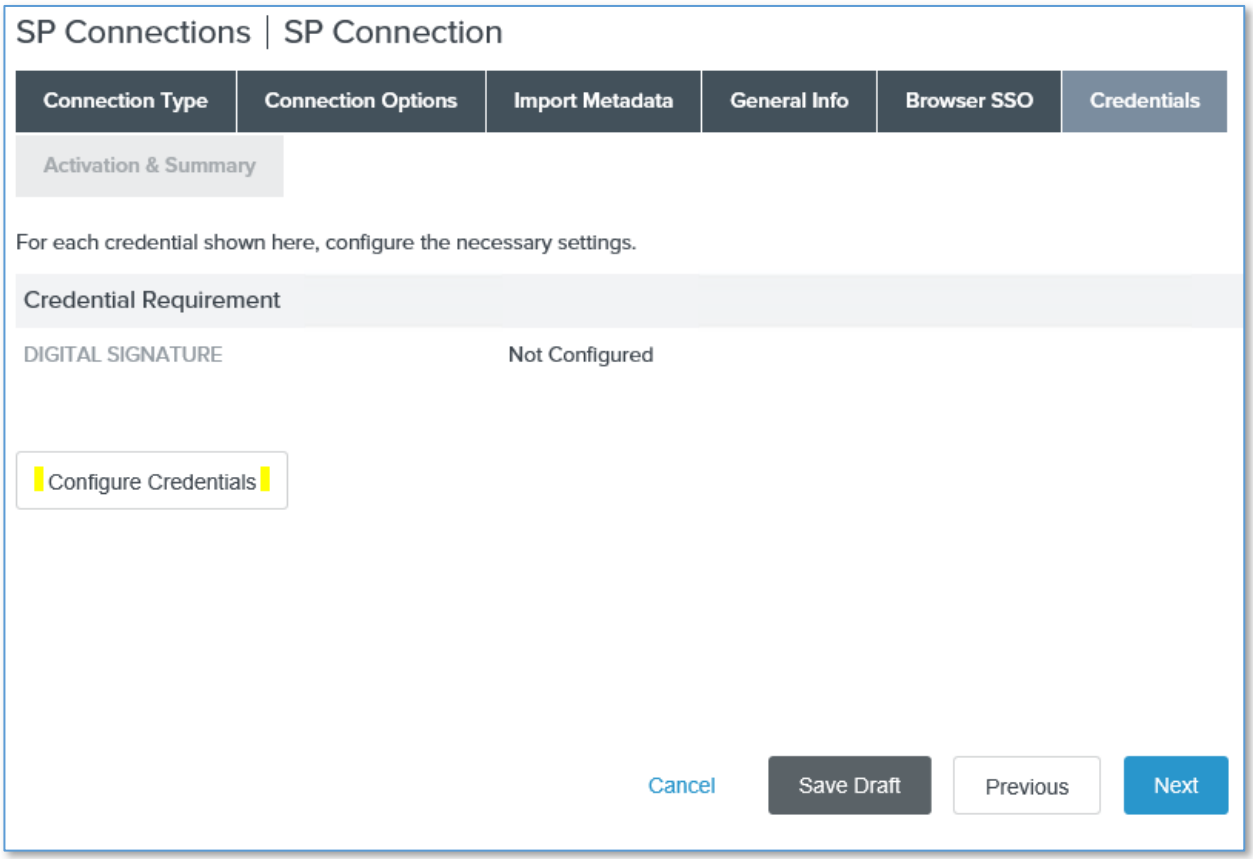
	
25.	Verify settings in Summary and select **Done**.

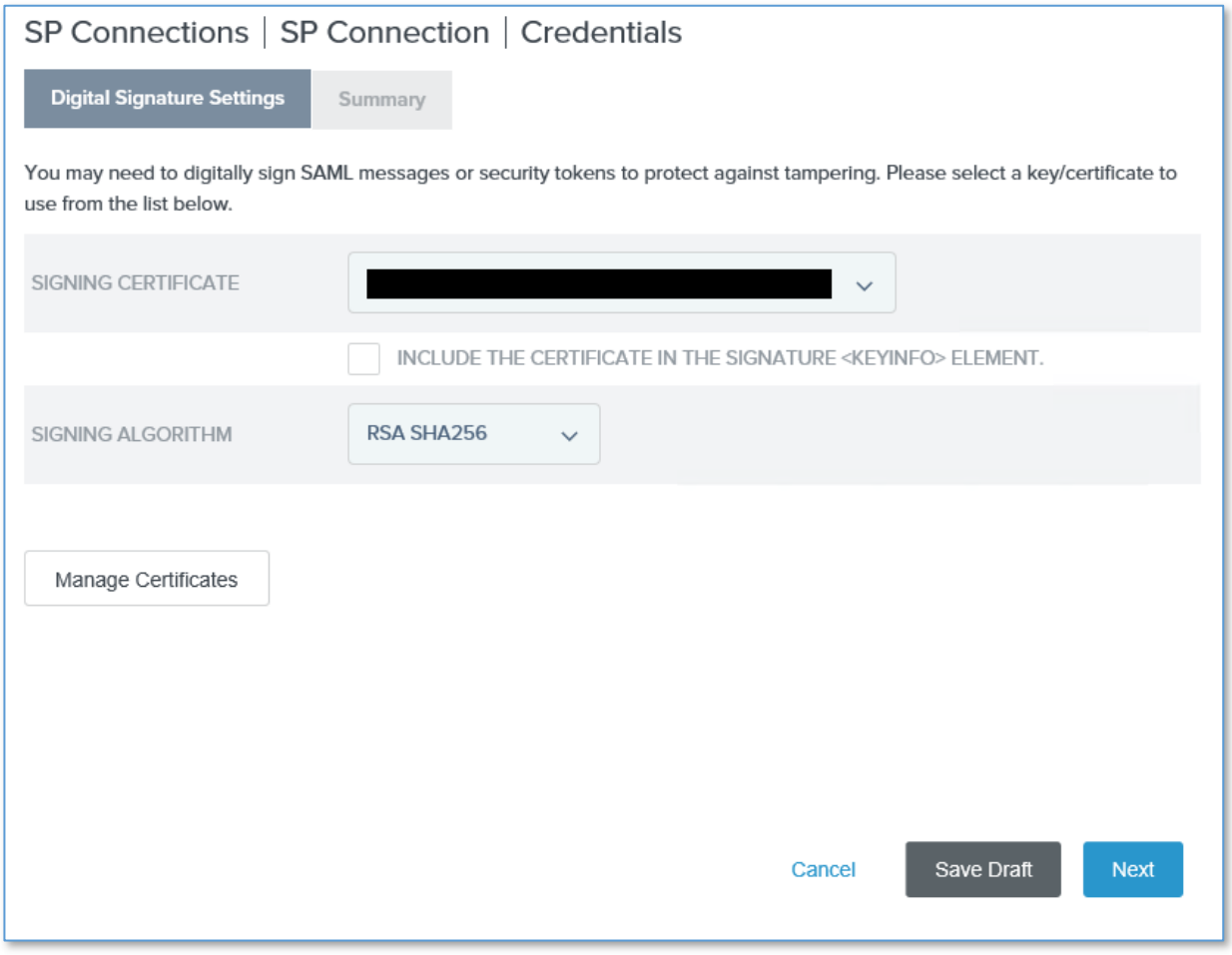


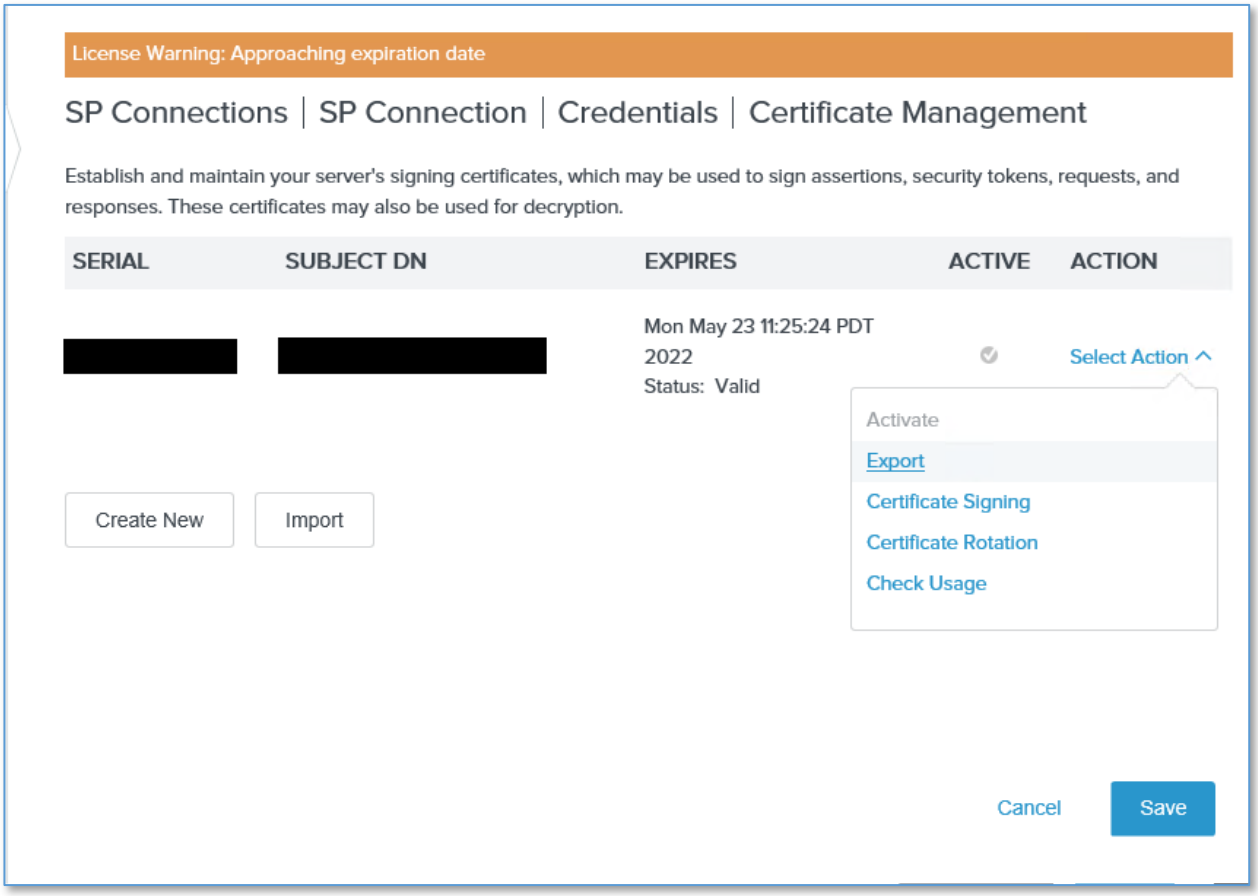
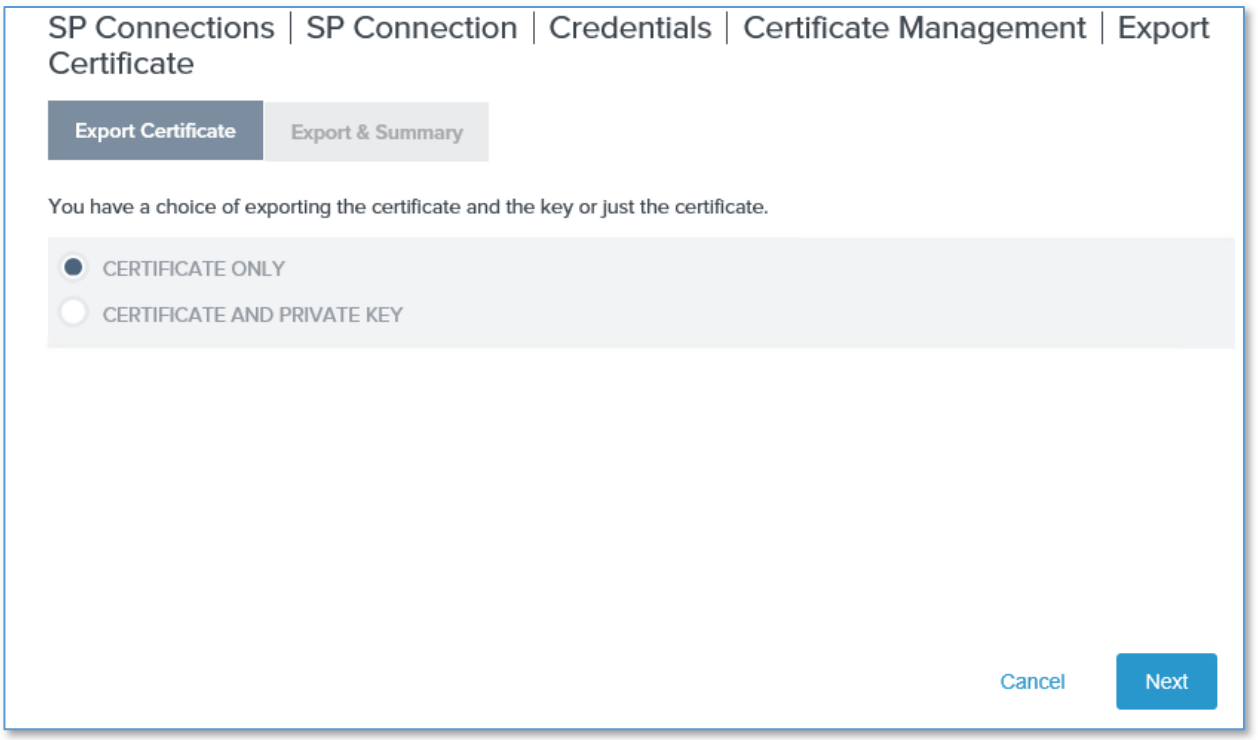
26.	Review Protocol Settings. Click **Next**.

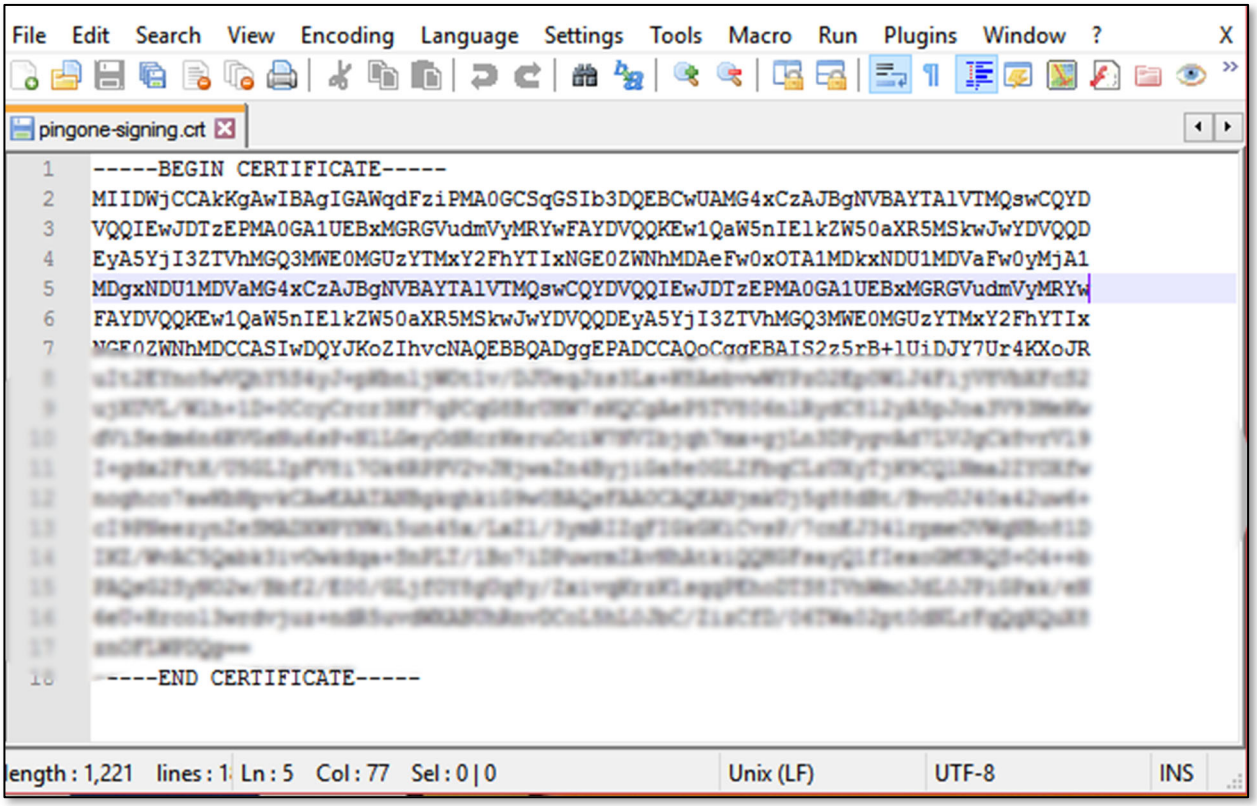
	
27.	Review Summary for Browser SSO configuration. Click **Done**.


SP Connections | SP Connection | Browser SSO
SAML Profiles
Assertion Lifetime
Assertion Creation
Protocol Settings
Summary
Summary information for your Browser SSO configuration. Click a heading link to edit a configuration setting.
Browser SSO
SAML Profiles
IdP-Initiated SSO
true
IdP-Initiated SLO
false
SP-Initiated SSO
true
SP-Initiated SLO
false
Assertion Lifetime
Valid Minutes Before
5
Valid Minutes After
5
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:emailAddress
Authentication Source Mapping
Adapter instance name
PingOne HTML Form Adapter
Adapter Instance
Selected adapter
PingOne HTML Form Adapter
Mapping Method
Adapter
HTML Form IdP Adapter
Mapping Method
Use only the Adapter Contract values in the mapping
Attribute Contract Fulfillment
SAML_SUBJECT
mail (Adapter)
Issuance Criteria
Criterion
(None)
Protocol Settings
Assertion Consumer Service URL
Endpoint
URL: https://hiettcloud.sharefile.com/saml/acs (POST)
Allowable SAML Bindings
Artifact
false
POST
true
Redirect
false
SOAP
false
Signature Policy
Require digitally signed AuthN requests
false
Always Sign Assertion
false
Sign Response As Required
true
Encryption Policy
Status
Inactive
Cancel
Save Draft
Previous
Done

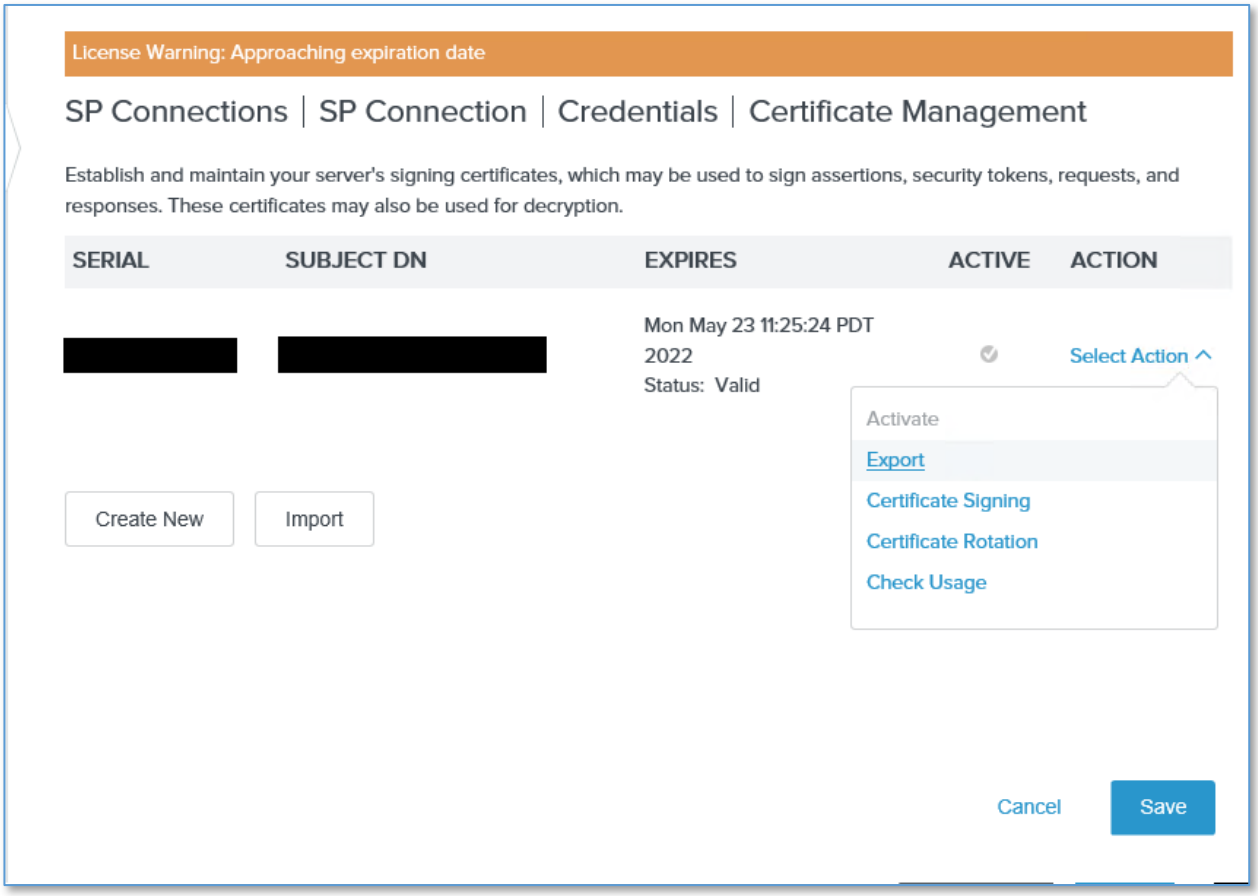
28.	Click **Next**. 
29.	In **Credentials** tab, click **Configure Credentials**. 

30.	In the **Digital Signature Settings** tab, for **Signing Certificate**, select the SSL certificate associated with your IDP. For the **Signing Algorithm**, select **RSA SHA256**. This is the certificate used for SAML requests. 

31.	Select **Manage Certificates**. From **Select Action**, select **Export**. 
32.	In the **Export Certificate** tab, select **Certificate Only** to export. Click **Export** again to download the .crt file. 
33.	Open the certificate (.crt) file in Notepad or any text editor.

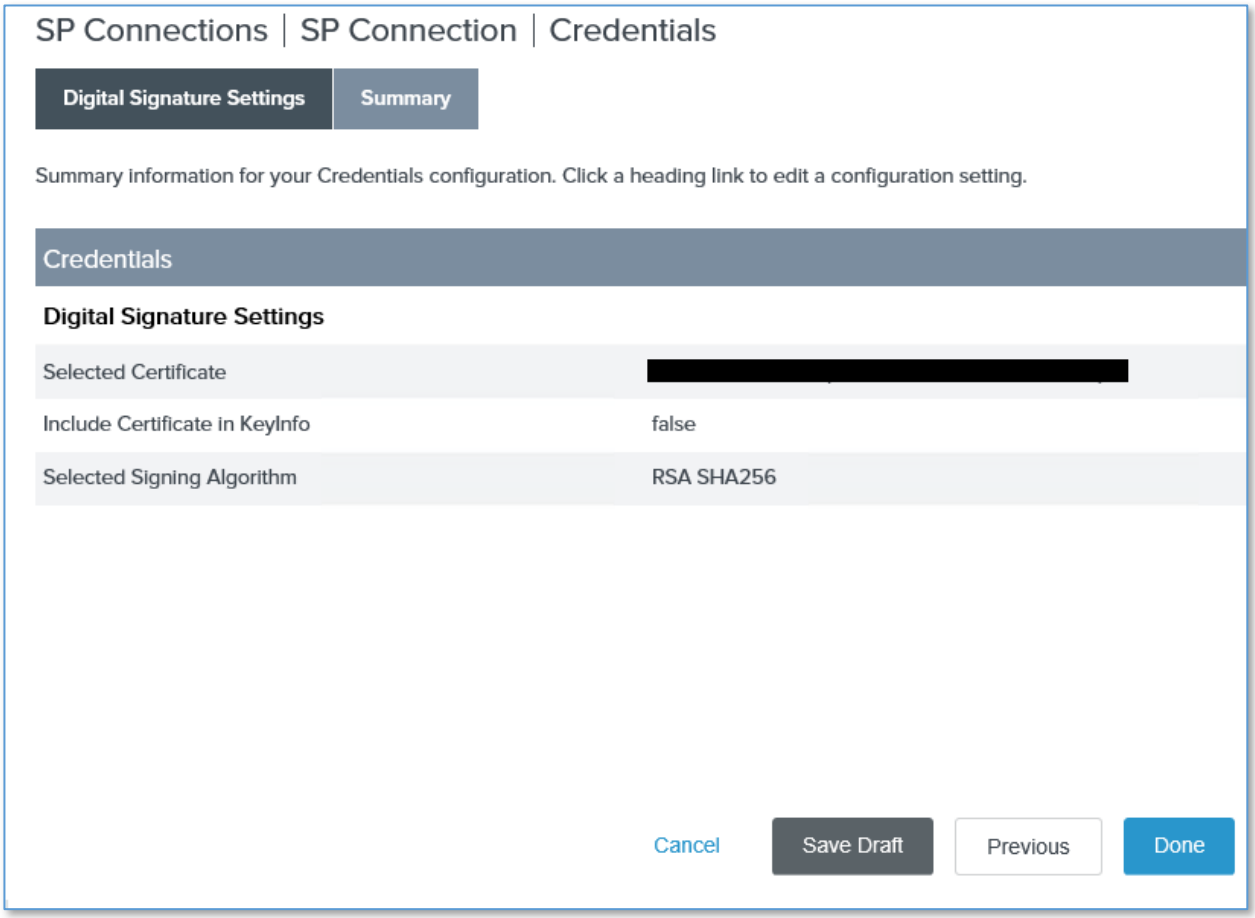


34. Click **Save** when done.

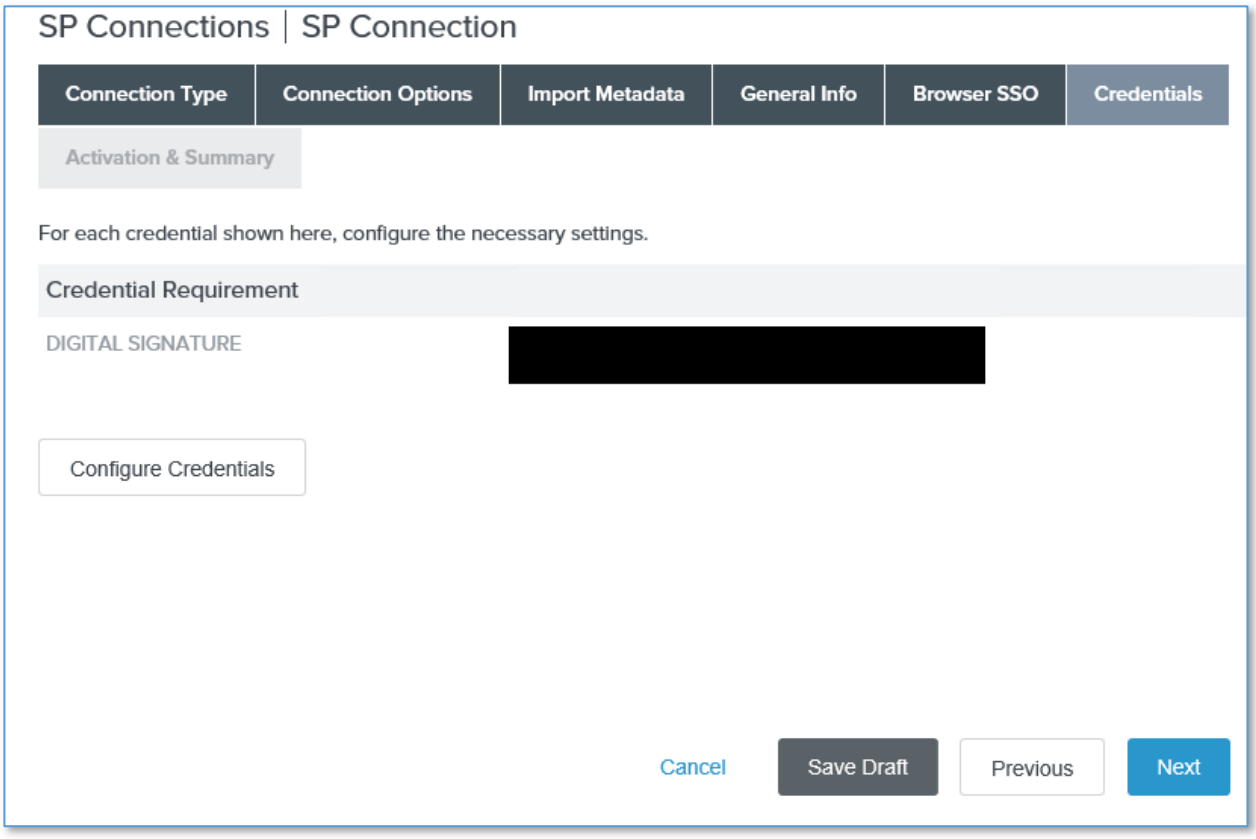


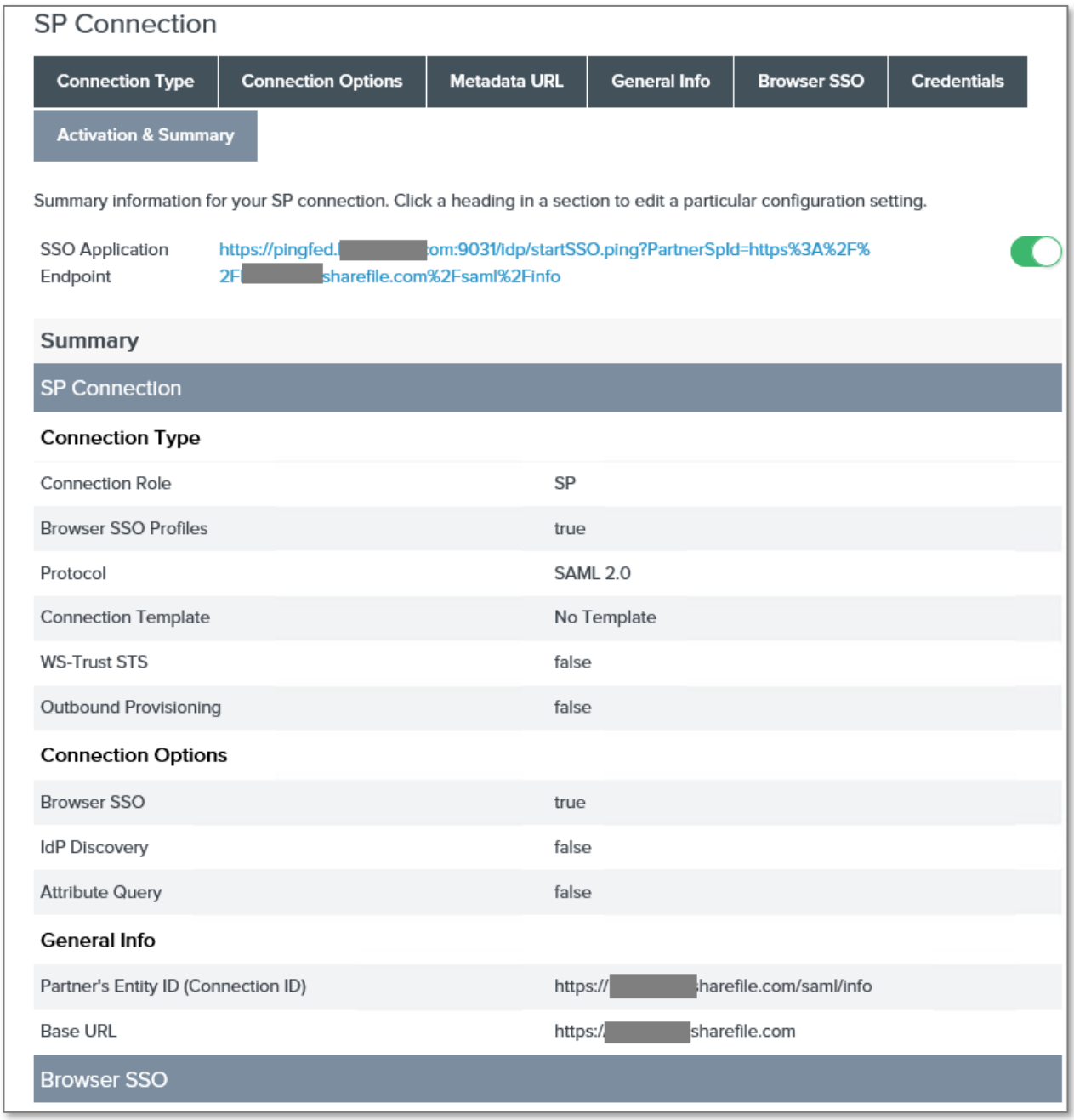
Review Summary for Digital Signature Settings. Click **Done**.

35.



36. Review Summary for Credentials. Click **Next**.

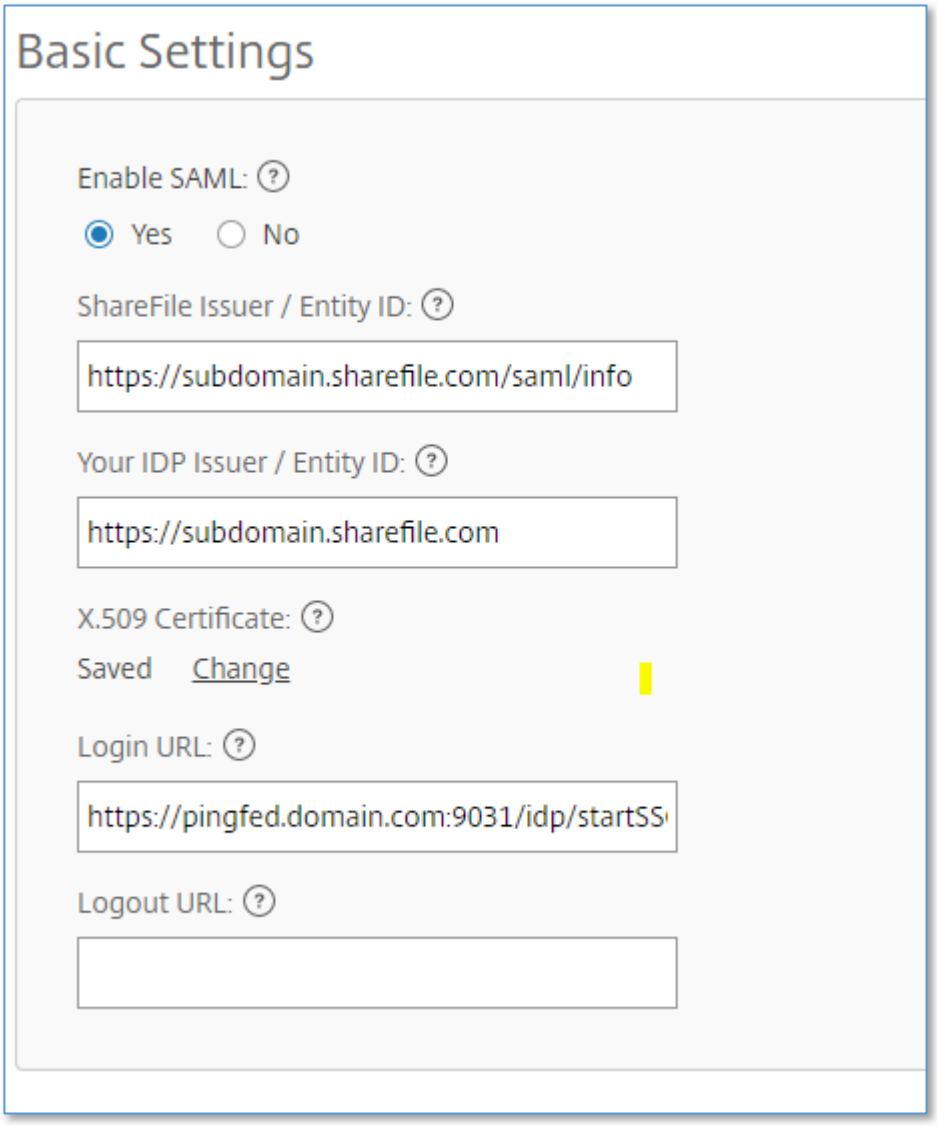


37.	Review **Activation and Summary**. Copy the **SSO Application Endpoint** URL. This will be used as the **Login URL** in the ShareFile Admin Settings. Click **Save**. https://ExternalDNSnameofyourPingFederate.com:9031/idp/startSSO.ping?PartnerSpId=https://subdomain.sharefile.com/saml/info 
38.	Go to your ShareFile account: https://subdomain.sharefile.com Login with Administrator account > **Settings** > **Admin Settings** > **Security** > **Login & Security Policy** > scroll down on this page to **Single sign on / SAML 2.0 Configuration.**
39.	Configure **Single sign on / SAML 2.0 Configuration** with the below:

Basic Settings

- **Enable SAML**: Select **Yes**
- **ShareFile Issuer / Entity ID**: https://subdomain.sharefile.com/saml/info
- **Your Issuer / Entity ID**: https://subdomain.sharefile.com/saml/info
- **X.509 Certificate**: Click **Change**, then copy and paste the certificate text from the **Certificate** file downloaded in the step above
- **Login URL**: Add login URL as the SSO Application Endpoint URL from PingFederate Server

  Example Login URL:
  https://ExternalDNSnameofyourPingFederate.com:9031/idp/startSSO.ping?PartnerSpId=https://subdomain.sharefile.com/saml/info
- **Logout URL**: Leave blank
  (When users log out of ShareFile, they will be redirected to ShareFile login page https://subdomain.sharefile.com.)



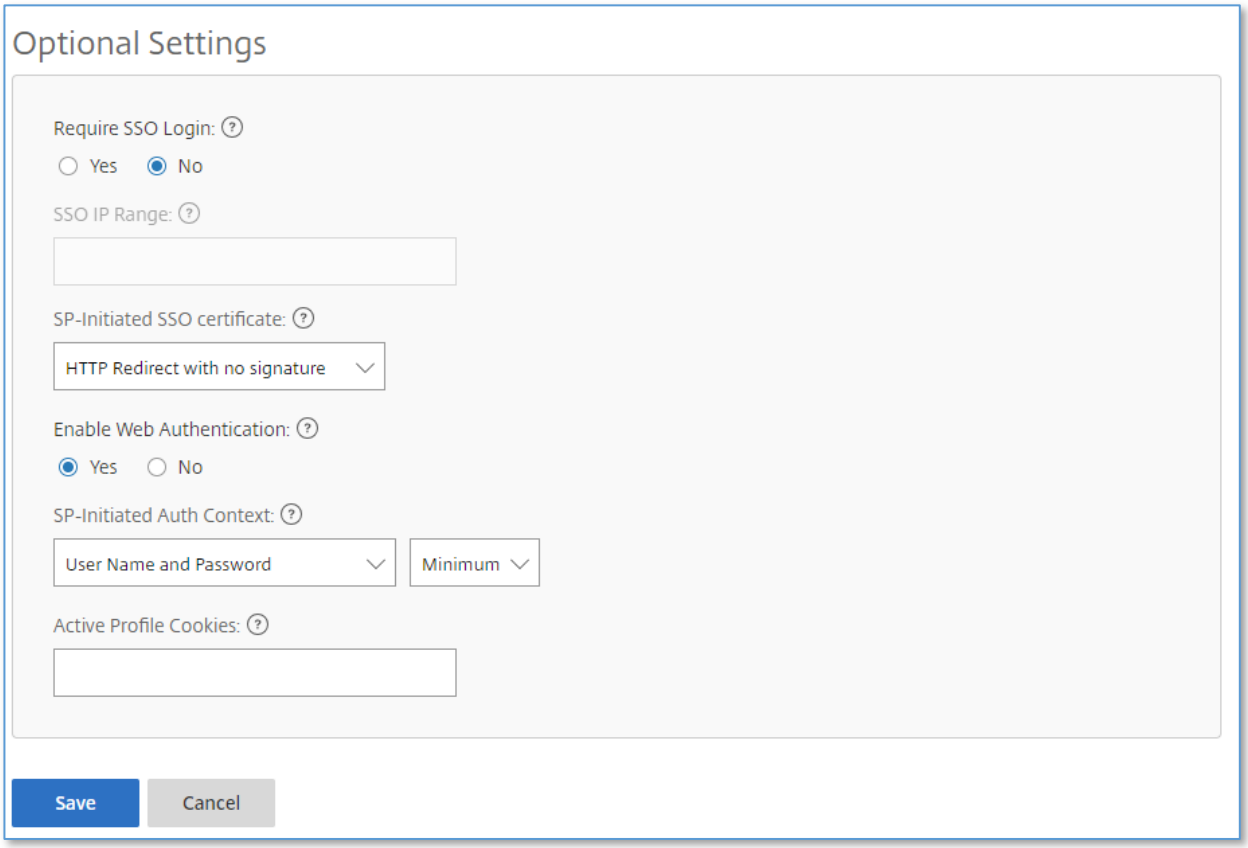
40.

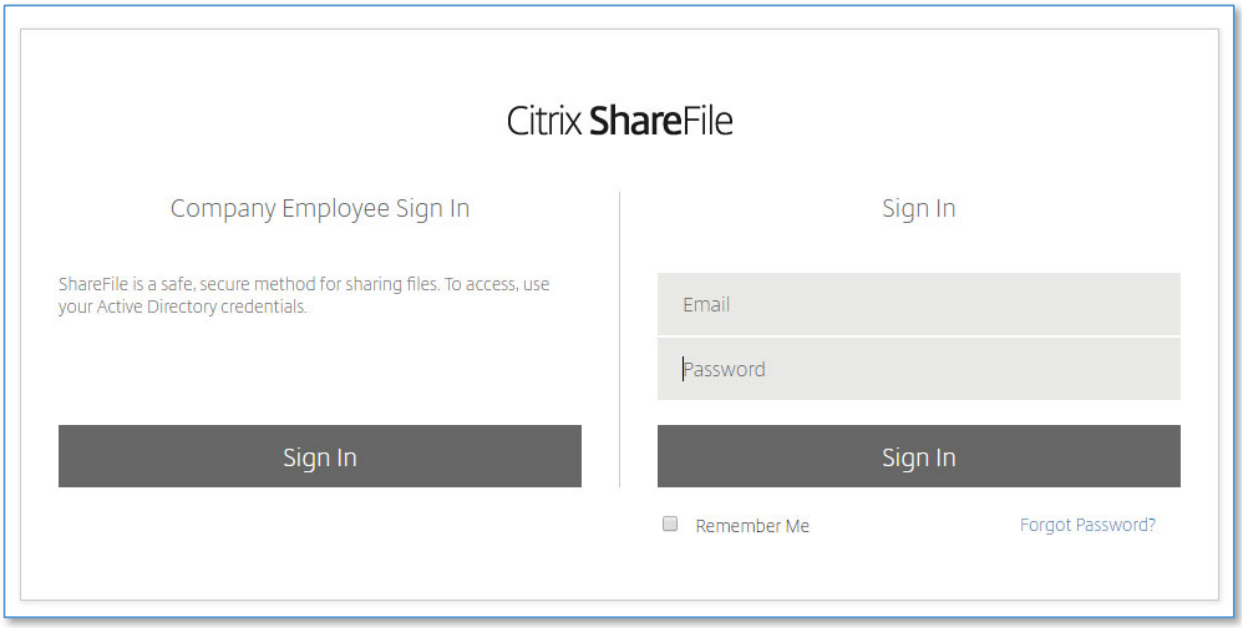
Optional Settings

- **Require SSO Login**: *Optional*
  After single-sign-on is successfully validated, checking **Yes** for this option will require all non-admin Employees to log in using PingFederate

  Admins will have the choice to login using PingFederate (on the left) or their email address as the username and a native ShareFile password (on the right).

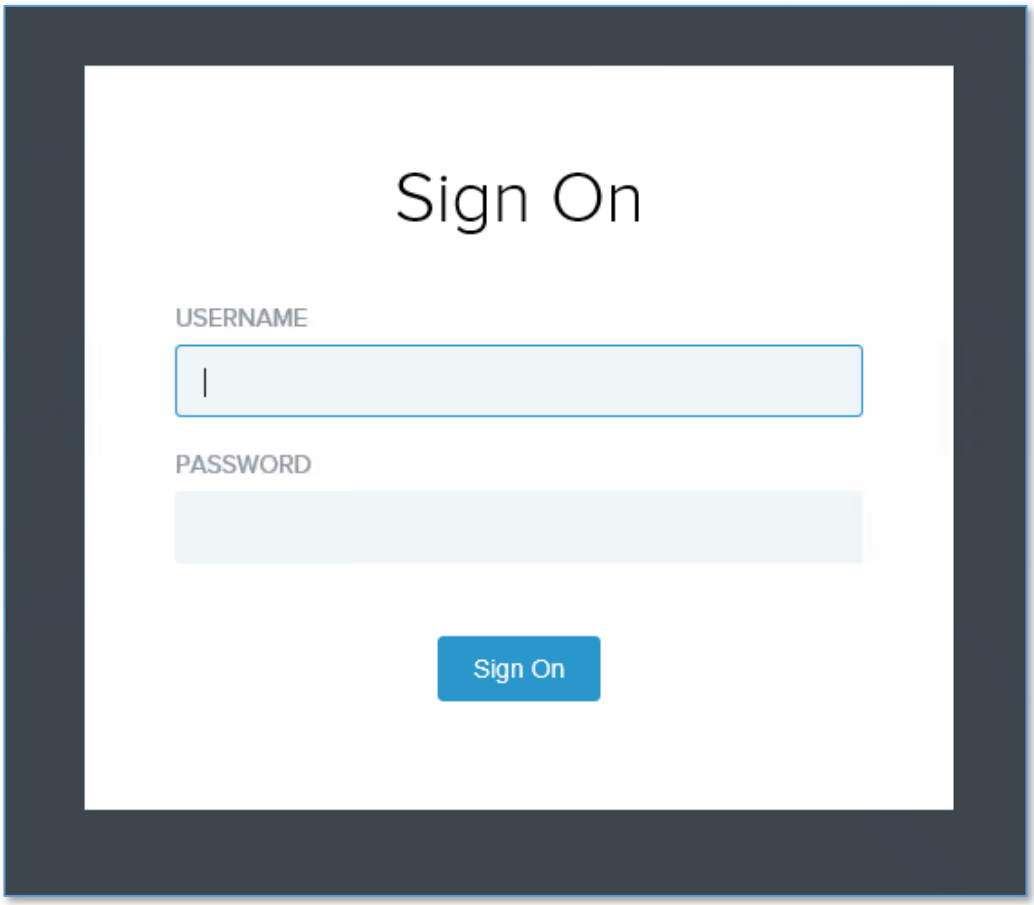
- **SSO IP Range**: *Optional*
  (Limit requiring non-admin Employees to login from a specific IP range. Employees outside of this specified range will not be required to use OneLogin to login.)

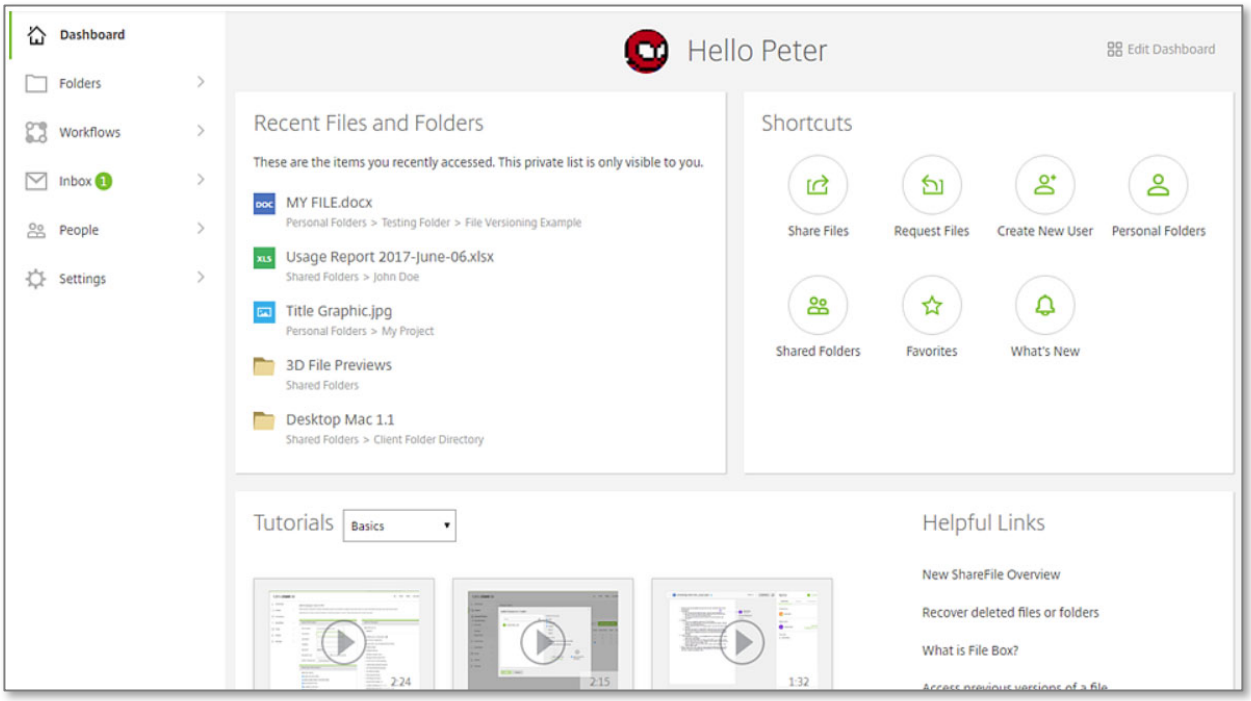
	○ **SP-initiated SSO Certificate**: Select **HTTP Redirect with no signature** ○ **Enable Web Authentication**: **Yes** (Choose **No** when you do not want to allow single sign on logins via a web browser. This means Windows authentication will need to be available. **No** is not recommended). ○ **SP-initiated Auth Context**: Select **User Name and Password**. ○ **Active Profile Cookies**: Leave blank ○ Click **Save** 
41.	Test successful authentication by going to your ShareFile URL: https://subdomain.sharefile.com ***Testing single-sign-on logins in private/incognito browser mode is best.* Click **Sign in** under **Company Employee Sign In**



****Make sure the user logging in with single sign-on has an Active Directory or Identity Provider email address that matches their email address in their ShareFile account.**

Sign in will redirect you PingFederate SSO Endpoint URL for sign in:



	Successful logins will authenticate users into their ShareFile account **Dashboard**. 
42.	Done!
43.	Common Errors: **User Not Valid For This Provider**: This generally indicates the email attribute sent to ShareFile (SP) does not match the email attribute of the user who logged into Ping Federate (IDP). Ensure the email attribute of the AD account exactly matches the email attribute of the ShareFile employee user account. **Failures redirect you to the ShareFile Login Page:** This could be any number of symptoms: ○ Review the settings from this article ○ Confirm the time settings of your server in relation to an NTP server. ○ Confirm the certificate you exported from Ping Federate exactly matches the certificate value you saved in ShareFile. ○ Ensure you are not encrypting SAML assertions or using unsupported protocols.