Value-Added Module (VAM)

PingFederate 2FA VAM Deployment Guide

SECUREAUTH

Copyright Information

Document Revision History

Version	Date	Notes
0.1	12-October-2017	Initial draft
1.0	24-May-2018	First draft completed
1.1	31-July-2018	Redaction of first draft
1.2	10-October-2018	Redaction of second draft
1.3	13-November-2018	Push-to-Accept and Time-Based OTP added
1.4	22-January-2019	Support of Email2 and Phone2

For information on support for this module, contact your SecureAuth support or sales representative:

Email: support@secureauth.com inside-sales@secureauth.com

Phone:	+1-949-777-6959
	+1-866- 859-1526
Website:	https://www.secureauth.com/support
	https://www.secureauth.com/contact

Contents

Introduction

This integration between the SecureAuth® Identity Platform (formerly known as SecureAuth IdP) and Ping Identity relies on a SecureAuth PingFederate two-factor authentication (2FA) value-added module (VAM). It is a piece of software that enables PingFederate to perform 2FA through the Identity Platform API.

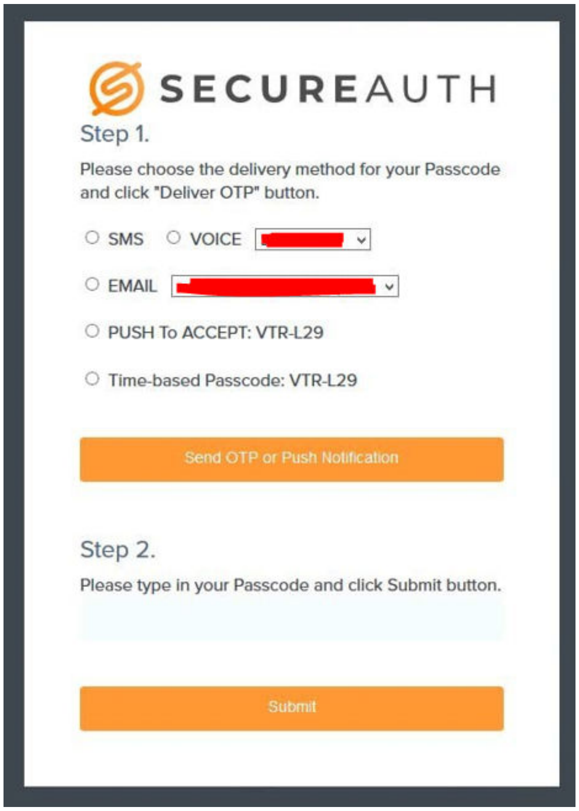
Along with standard multi-factor authentication, the VAM has additional functionality of Adaptive Authentication and Device Recognition, Push to Accept Notifications and Time-Based Passcodes (OATH). Once deployed and configured, a PingFederate server can take advantage of all the advanced security features the Identity Platform provides.

The following MFA and adaptive authentication methods are supported:

- OTP via Phone1, Phone2
- OTP via Email1, Email2
- Time-based Passcode (OATH)
- Mobile Login Request (Push To Accept)

These features are supported by following actions:

- 1 – Skip MFA
- 2 – Hard stop
- 3 – Redirect



Step 1.

Please choose the delivery method for your Passcode and click "Deliver OTP" button.

○ SMS ○ VOICE [redacted]

○ EMAIL [redacted]

○ PUSH To ACCEPT: VTR-L29

○ Time-based Passcode: VTR-L29

Step 2.

Please type in your Passcode and click Submit button.

System information

- Applies to PingFederate server version 8.3 and later
- To configure the multi-factor authentication (MFA) and adaptive authentication features, see the list of guides in the References section.
- Alternatively, you can integrate the Identity Platform with PingFederate using SAML SSO.

Configuration

This section outlines the steps to configure the SecureAuth PingFederate Two-Factor Authentication (2FA) VAM in PingFederate 8.3. The PingFederate 2FA VAM is a piece of software that enables the Identity Platform to talk with a PingFederate server through an exchange of SAML code.

To set up the integration, download the deployment package and do each group of tasks in this order

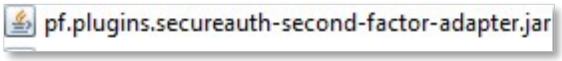
1. Set up the environment
2. Create a password credential validator
3. Create the HTML Form Adapter
4. Configure the Identity Platform for API
5. Create the SecureAuth 2FA adapter
6. Create the SecureAuth composite adapter
7. Create service provider (SP) connections
8. Configure the HTML Form Adapter Logout
9. Test the configured SecureAuth 2FA functionality

Set up the environment

It is required to set up the PingFederate environtment to use the 2FA VAM adapter.

To set up the PingFederate environment

1. Place the **pf.plugins.secureauth-second-factor-adapter.jar** in the following deploy folder: …\pingfederate-8.3.2\pingfederate\server\default\deploy



pf.plugins.secureauth-second-factor-adapter.jar

2. Copy the jar files (as shown in the image example) to the following deploy directory:

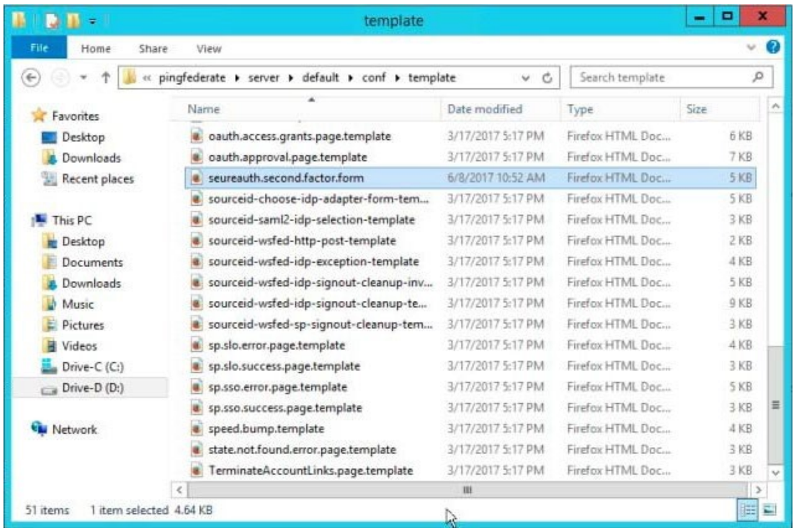
   …\pingfederate-8.3.2\pingfederate\server\default\deploy

   You can find these files under “dependency-jars” in the downloaded deployment package.

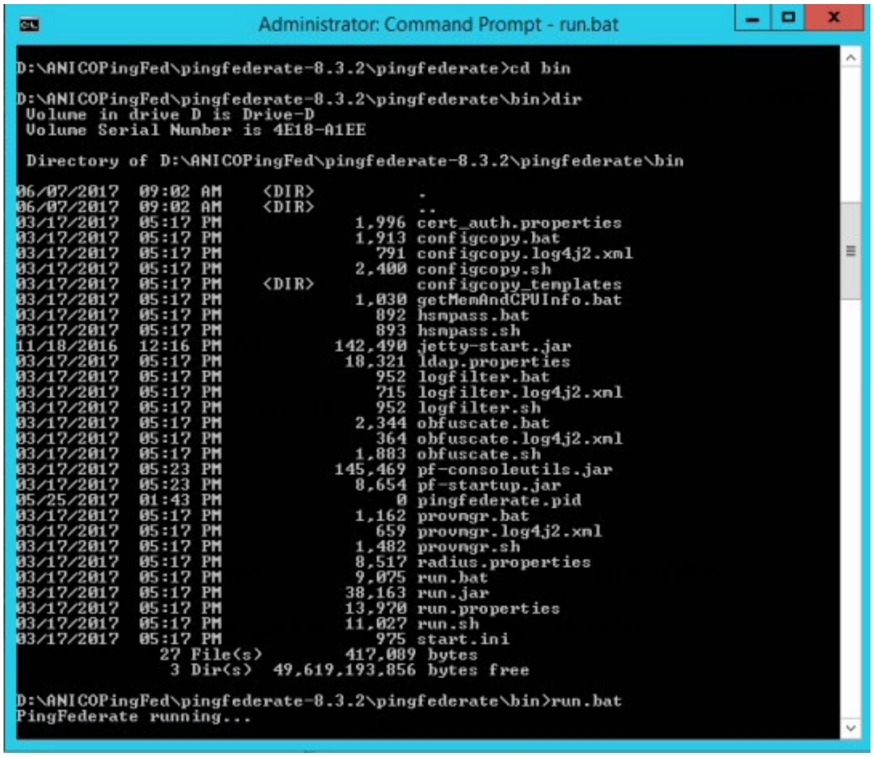
aopalliance-repackaged-2.5.0-b30.jar
common-mfa-14.4.7.jar
gson-2.2.4.jar
hk2-api-2.5.0-b30.jar
hk2-locator-2.5.0-b30.jar
hk2-utils-2.5.0-b30.jar
jackson-annotations-2.7.0.jar
jackson-core-2.7.3.jar
jackson-databind-2.7.3.jar
jackson-jaxrs-base-2.3.3.jar
jackson-jaxrs-json-provider-2.3.3.jar
jackson-module-jaxb-annotations-2.3.3.jar
javassist-3.20.0-GA.jar
javax.annotation-api-1.2.jar

javax.inject-2.5.0-b30.jar
javax.servlet-api-3.1.0.jar
javax.ws.rs-api-2.0.1.jar
jersey-bundle-1.18.jar
jersey-client.jar
jersey-common-2.25.jar
jersey-container-servlet-core-2.17.jar
jersey-entity-filtering-2.25.jar
jersey-guava-2.25.jar
jersey-media-jaxb-2.17.jar
jersey-media-json-jackson-2.25.jar
json-simple-1.1.1.jar
osgi-resource-locator-1.0.1.jar
validation-api-1.1.0.Final.jar

3. Place the following files in the specified folders. If a folder does not exist for one or more files, create a new folder to accommodate these files.

File	**Folder**
secureauth.second.factor.form.html	...\pingfederate\server\default\conf\template  template « pingfederate ▸ server ▸ default ▸ conf ▸ template Name Date modified Type Size oauth.access.grants.page.template 3/17/2017 5:17 PM Firefox HTML Doc... 6 KB oauth.approval.page.template 3/17/2017 5:17 PM Firefox HTML Doc... 7 KB seureauth.second.factor.form 6/8/2017 10:52 AM Firefox HTML Doc... 5 KB sourceid-choose-idp-adapter-form-tem... 3/17/2017 5:17 PM Firefox HTML Doc... 5 KB sourceid-saml2-idp-selection-template 3/17/2017 5:17 PM Firefox HTML Doc... 3 KB sourceid-wsfed-http-post-template 3/17/2017 5:17 PM Firefox HTML Doc... 2 KB sourceid-wsfed-idp-exception-template 3/17/2017 5:17 PM Firefox HTML Doc... 4 KB sourceid-wsfed-idp-signout-cleanup-inv... 3/17/2017 5:17 PM Firefox HTML Doc... 5 KB sourceid-wsfed-idp-signout-cleanup-te... 3/17/2017 5:17 PM Firefox HTML Doc... 9 KB sourceid-wsfed-sp-signout-cleanup-tem... 3/17/2017 5:17 PM Firefox HTML Doc... 3 KB sp.slo.error.page.template 3/17/2017 5:17 PM Firefox HTML Doc... 4 KB sp.slo.success.page.template 3/17/2017 5:17 PM Firefox HTML Doc... 3 KB sp.sso.error.page.template 3/17/2017 5:17 PM Firefox HTML Doc... 5 KB sp.sso.success.page.template 3/17/2017 5:17 PM Firefox HTML Doc... 3 KB speed.bump.template 3/17/2017 5:17 PM Firefox HTML Doc... 4 KB state.not.found.error.page.template 3/17/2017 5:17 PM Firefox HTML Doc... 3 KB TerminateAccountLinks.page.template 3/17/2017 5:17 PM Firefox HTML Doc... 3 KB 51 items 1 item selected 4.64 KB File Home Share View Search template Favorites Desktop Downloads Recent places This PC Desktop Documents Downloads Music Pictures Videos Drive-C (C:) Drive-D (D:) Network
secureauth-logo.jpg	...\pingfederate\server\default\conf\template\assets\images
attribute-form-template.properties	...\pingfederate\server\default\conf\language-packs

4. Go to the ...\pingfederate-8.3.2\pingfederate\bin folder, and execute the **run.bat** command script.



```
D:\ANICOPingFed\pingfederate-8.3.2\pingfederate>cd bin

D:\ANICOPingFed\pingfederate-8.3.2\pingfederate\bin>dir
 Volume in drive D is Drive-D
 Volume Serial Number is 4E18-A1EE

 Directory of D:\ANICOPingFed\pingfederate-8.3.2\pingfederate\bin

06/07/2017  09:02 AM    <DIR>          .
06/07/2017  09:02 AM    <DIR>          ..
03/17/2017  05:17 PM             1,996 cert_auth.properties
03/17/2017  05:17 PM             1,913 configcopy.bat
03/17/2017  05:17 PM               791 configcopy.log4j2.xml
03/17/2017  05:17 PM             2,400 configcopy.sh
03/17/2017  05:17 PM    <DIR>          configcopy_templates
03/17/2017  05:17 PM             1,030 getMemAndCPUInfo.bat
03/17/2017  05:17 PM               892 hsmpass.bat
03/17/2017  05:17 PM               893 hsmpass.sh
11/18/2016  12:16 PM           142,490 jetty-start.jar
03/17/2017  05:17 PM            18,321 ldap.properties
03/17/2017  05:17 PM               952 logfilter.bat
03/17/2017  05:17 PM               715 logfilter.log4j2.xml
03/17/2017  05:17 PM               952 logfilter.sh
03/17/2017  05:17 PM             2,344 obfuscate.bat
03/17/2017  05:17 PM               364 obfuscate.log4j2.xml
03/17/2017  05:17 PM             1,883 obfuscate.sh
03/17/2017  05:23 PM           145,469 pf-consoleutils.jar
03/17/2017  05:23 PM             8,654 pf-startup.jar
05/25/2017  01:43 PM                 0 pingfederate.pid
03/17/2017  05:17 PM             1,162 provmgr.bat
03/17/2017  05:17 PM               659 provmgr.log4j2.xml
03/17/2017  05:17 PM             1,482 provmgr.sh
03/17/2017  05:17 PM             8,517 radius.properties
03/17/2017  05:17 PM             9,075 run.bat
03/17/2017  05:17 PM            38,163 run.jar
03/17/2017  05:17 PM            13,970 run.properties
03/17/2017  05:17 PM            11,027 run.sh
03/17/2017  05:17 PM               975 start.ini
              27 File(s)        417,089 bytes
               3 Dir(s)  49,619,193,856 bytes free

D:\ANICOPingFed\pingfederate-8.3.2\pingfederate\bin>run.bat
PingFederate running...
```

Create a password credential validator

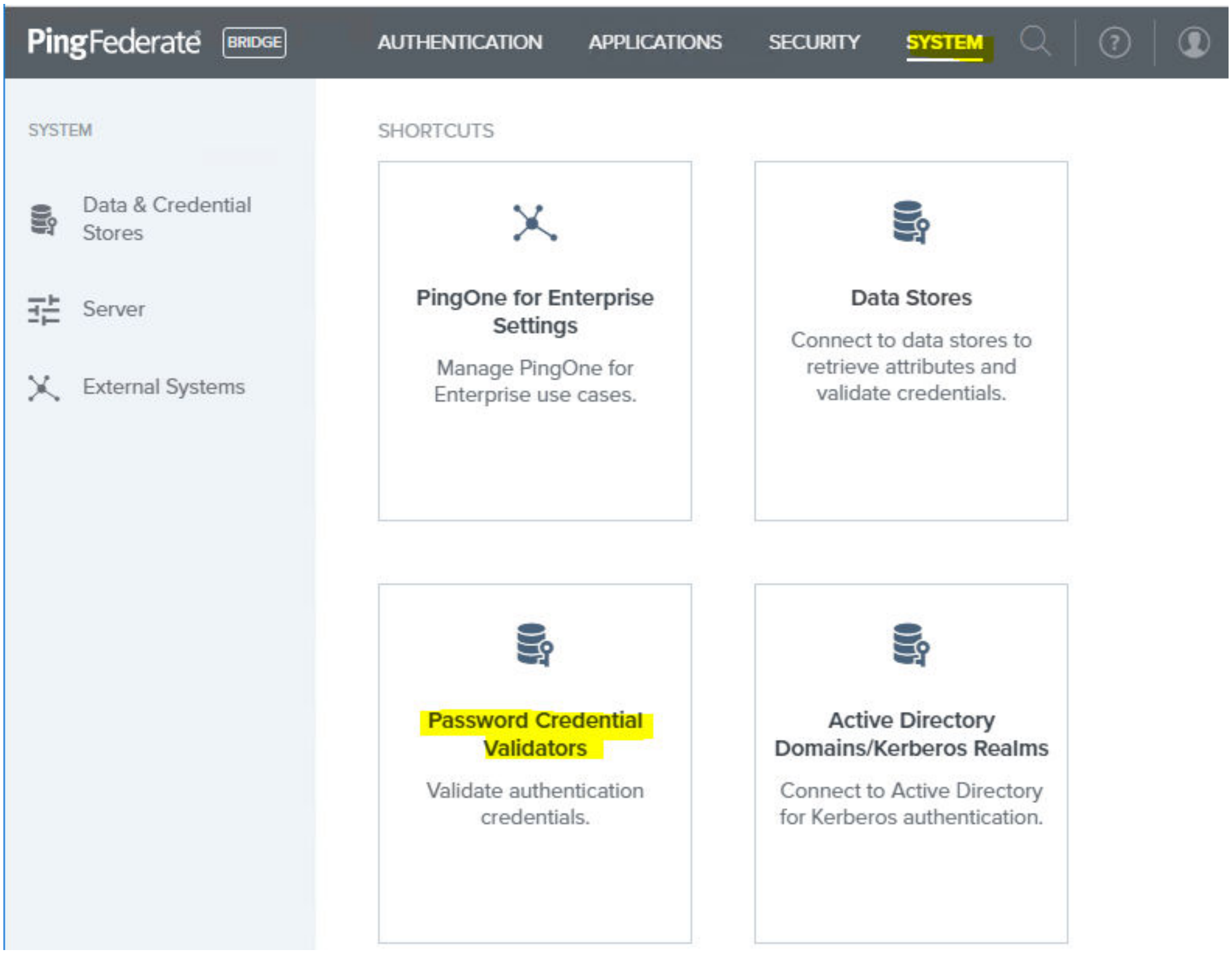
Password credential validators (PCV) allow PingFederate administrators to define a centralized location for username/password validation. This enables various PingFederate configurations to reference validator instances.

To create the password credential validator

1. Launch a web browser and enter the URL similar to the following, where <DNS_NAME> is the fully qualified domain name of the machine running the PingFederate server https://<DNS_NAME>:9999/pingfederate/app

   The PingFederate administrative console appears

2. In PingFederate, select **SYSTEM**, and then, click the **Password Credential Validators** link.



PingOne for Enterprise Settings

Manage PingOne for Enterprise use cases.

Data Stores

Connect to data stores to retrieve attributes and validate credentials.

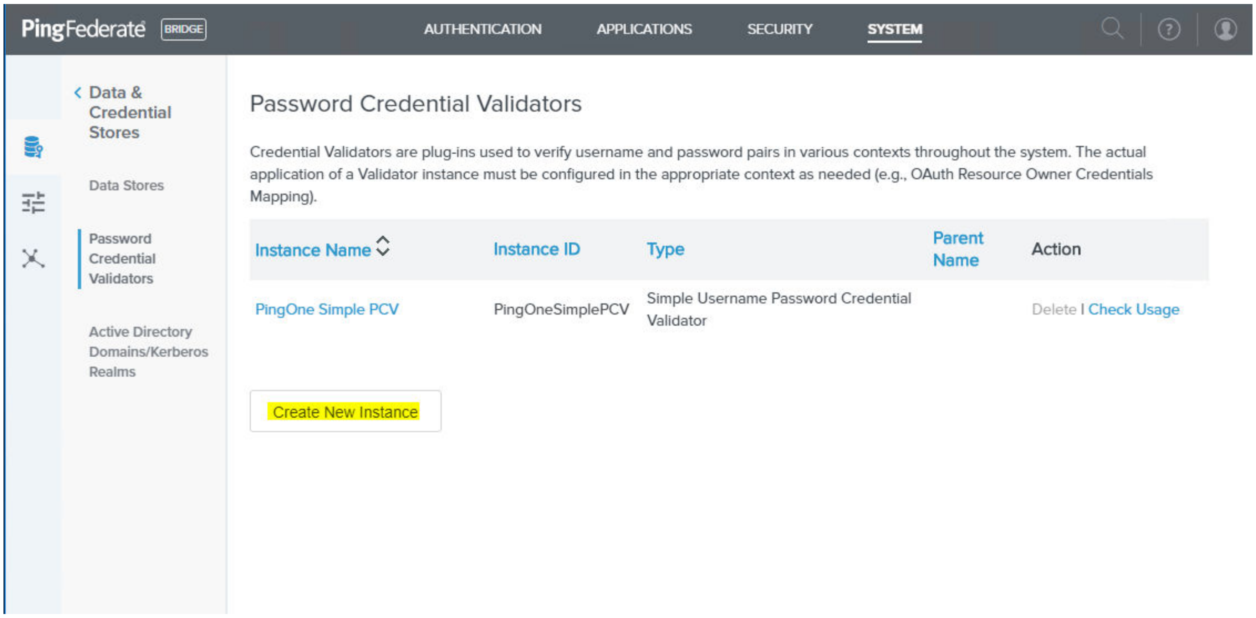
Password Credential Validators

Validate authentication credentials.

Active Directory Domains/Kerberos Realms

Connect to Active Directory for Kerberos authentication.

3. Click on **Create New Instance.**

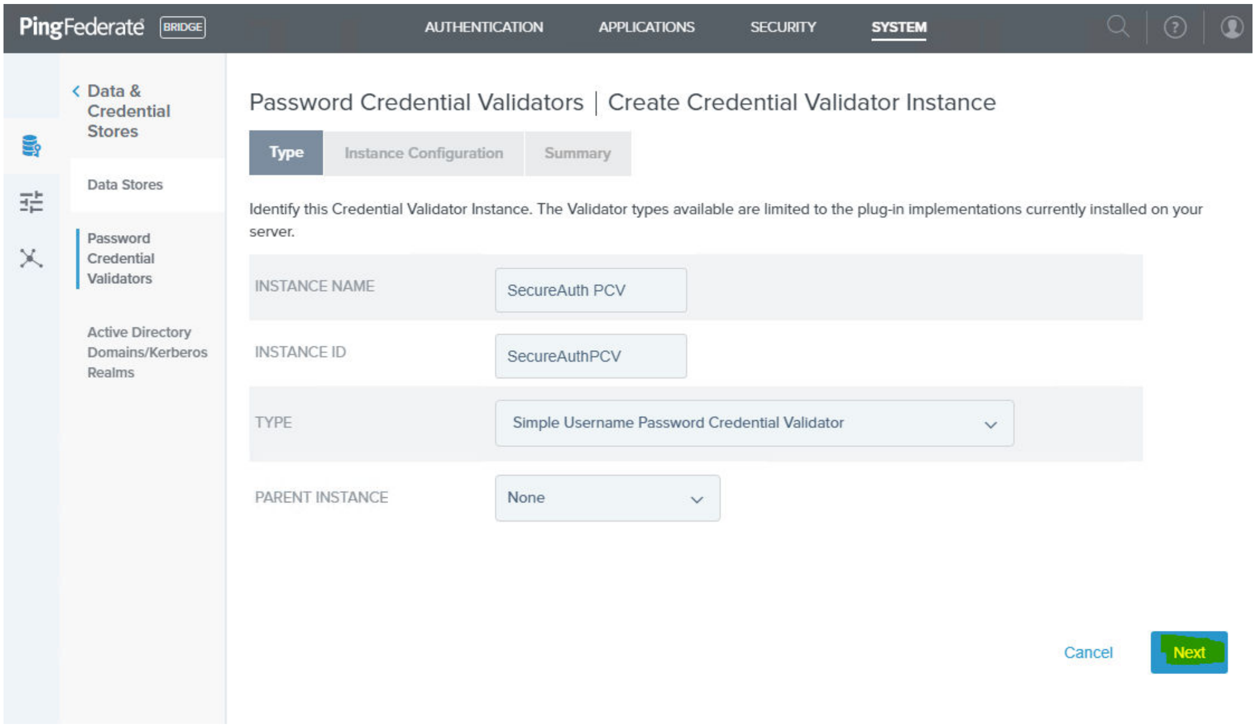

PingFederate BRIDGE
AUTHENTICATION
APPLICATIONS
SECURITY
SYSTEM
‹ Data & Credential Stores
Data Stores
Password Credential Validators
Active Directory Domains/Kerberos Realms

Password Credential Validators

Credential Validators are plug-ins used to verify username and password pairs in various contexts throughout the system. The actual application of a Validator instance must be configured in the appropriate context as needed (e.g., OAuth Resource Owner Credentials Mapping).

Instance Name	Instance ID	Type	Parent Name	Action
PingOne Simple PCV	PingOneSimplePCV	Simple Username Password Credential Validator		Delete I Check Usage

Create New Instance

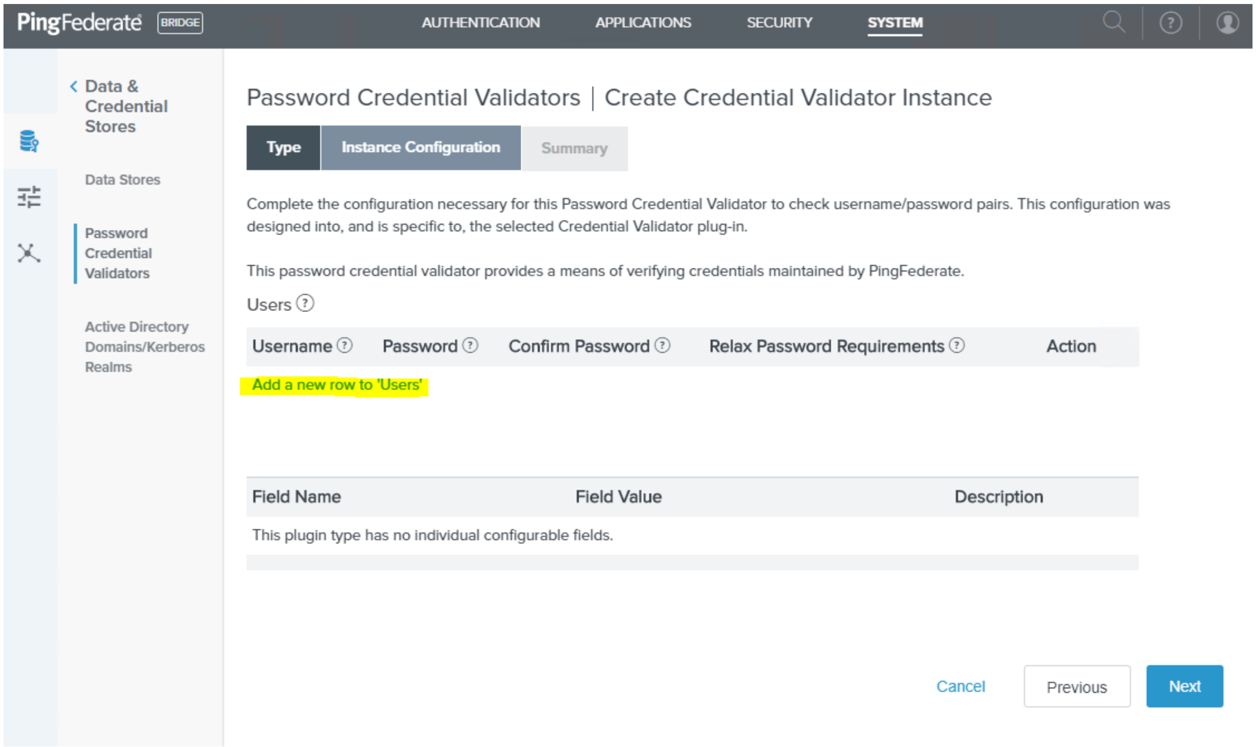


Password Credential Validators | Create Credential Validator Instance

Identify this Credential Validator Instance. The Validator types available are limited to the plug-in implementations currently installed on your server.

INSTANCE NAME	SecureAuth PCV
INSTANCE ID	SecureAuthPCV
TYPE	Simple Username Password Credential Validator
PARENT INSTANCE	None

4. In the *Instance Configuration* tab, click the **Add a new row to 'Users'** link.



Password Credential Validators | Create Credential Validator Instance

Complete the configuration necessary for this Password Credential Validator to check username/password pairs. This configuration was designed into, and is specific to, the selected Credential Validator plug-in.

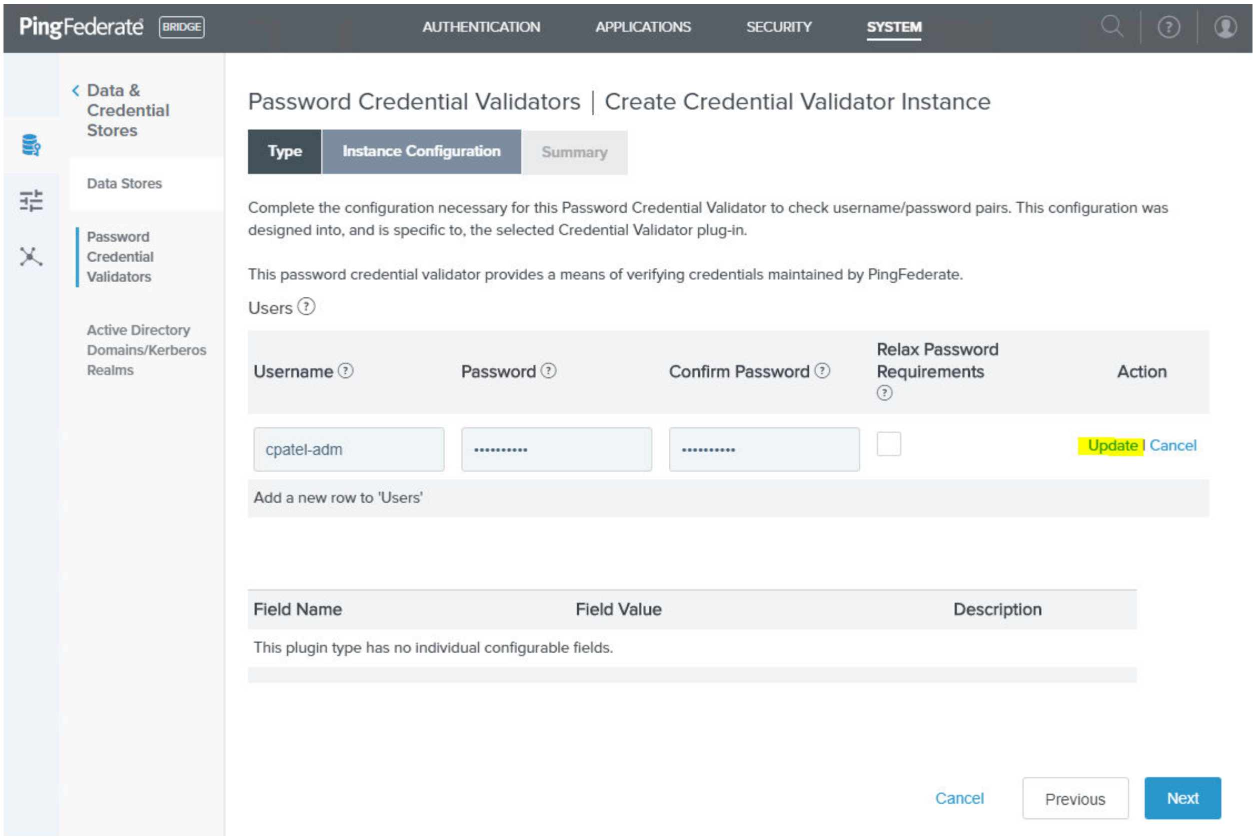
This password credential validator provides a means of verifying credentials maintained by PingFederate.

Users

Username	Password	Confirm Password	Relax Password Requirements	Action

Field Name	Field Value	Description
This plugin type has no individual configurable fields.		

5. To add a user to the list, enter the username and password and then click **Update** and then click **Next**.



Password Credential Validators | Create Credential Validator Instance

Complete the configuration necessary for this Password Credential Validator to check username/password pairs. This configuration was designed into, and is specific to, the selected Credential Validator plug-in.

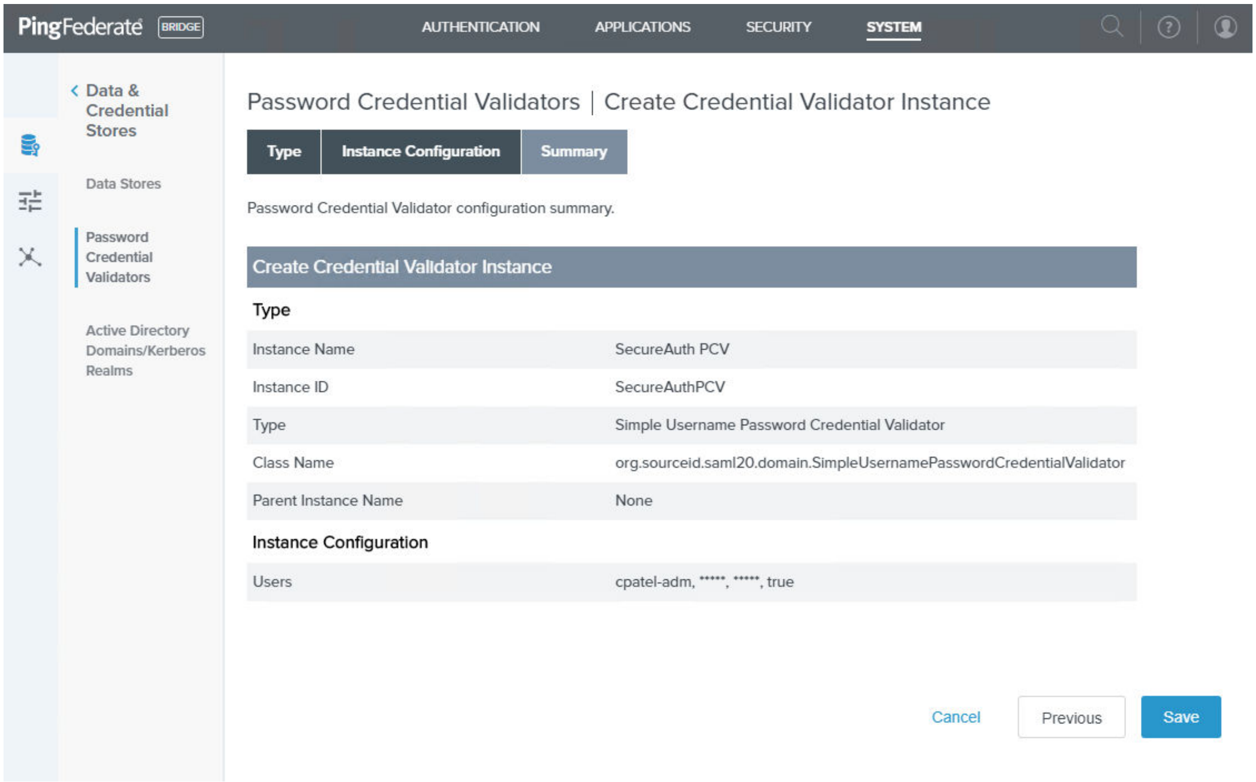
This password credential validator provides a means of verifying credentials maintained by PingFederate.

Users

Username	Password	Confirm Password	Relax Password Requirements	Action
cpatel-adm	••••••••••	••••••••••	□	Update I Cancel
Add a new row to 'Users'				

Field Name	Field Value	Description
This plugin type has no individual configurable fields.		

6. Review the *Summary* tab and then click **Save**.



Password Credential Validators | Create Credential Validator Instance

Password Credential Validator configuration summary.

Create Credential Validator Instance

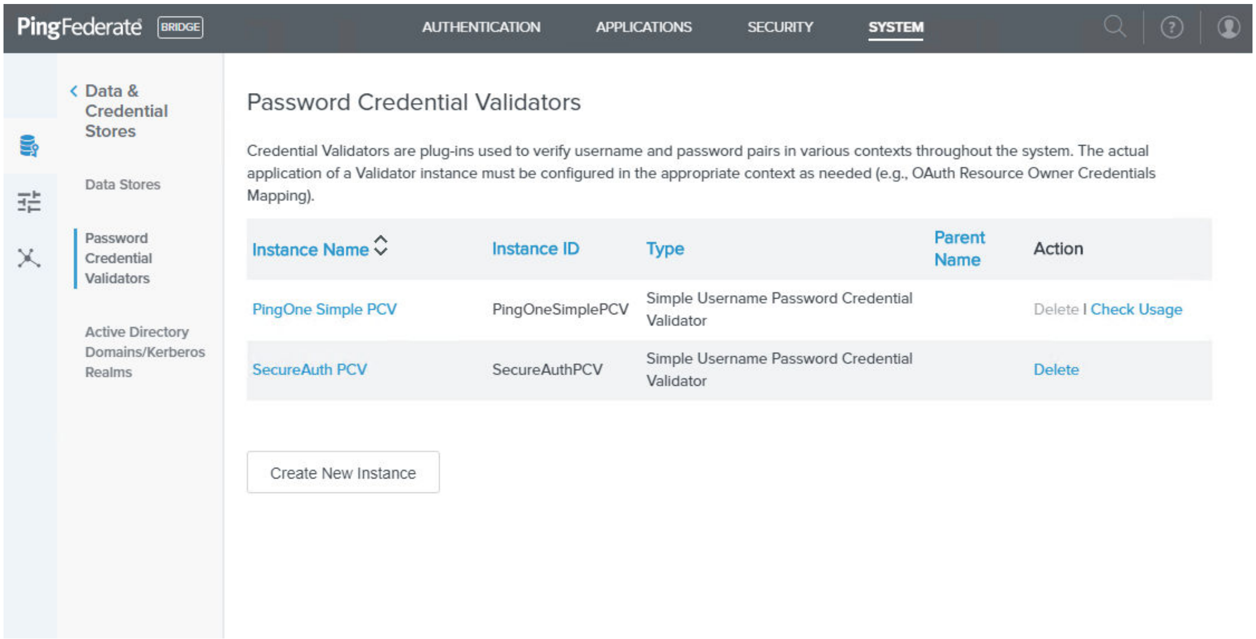
Type

Instance Name	SecureAuth PCV
Instance ID	SecureAuthPCV
Type	Simple Username Password Credential Validator
Class Name	org.sourceid.saml20.domain.SimpleUsernamePasswordCredentialValidator
Parent Instance Name	None

Instance Configuration

Users	cpatel-adm, *****, *****, true

7. On the Manage Credential Validator Instances page, you can see new created instance.


PingFederate BRIDGE
AUTHENTICATION
APPLICATIONS
SECURITY
SYSTEM
‹ Data & Credential Stores
Data Stores
Password Credential Validators
Active Directory Domains/Kerberos Realms
Create New Instance

Password Credential Validators

Credential Validators are plug-ins used to verify username and password pairs in various contexts throughout the system. The actual application of a Validator instance must be configured in the appropriate context as needed (e.g., OAuth Resource Owner Credentials Mapping).

Instance Name	Instance ID	Type	Parent Name	Action
PingOne Simple PCV	PingOneSimplePCV	Simple Username Password Credential Validator		Delete I Check Usage
SecureAuth PCV	SecureAuthPCV	Simple Username Password Credential Validator		Delete

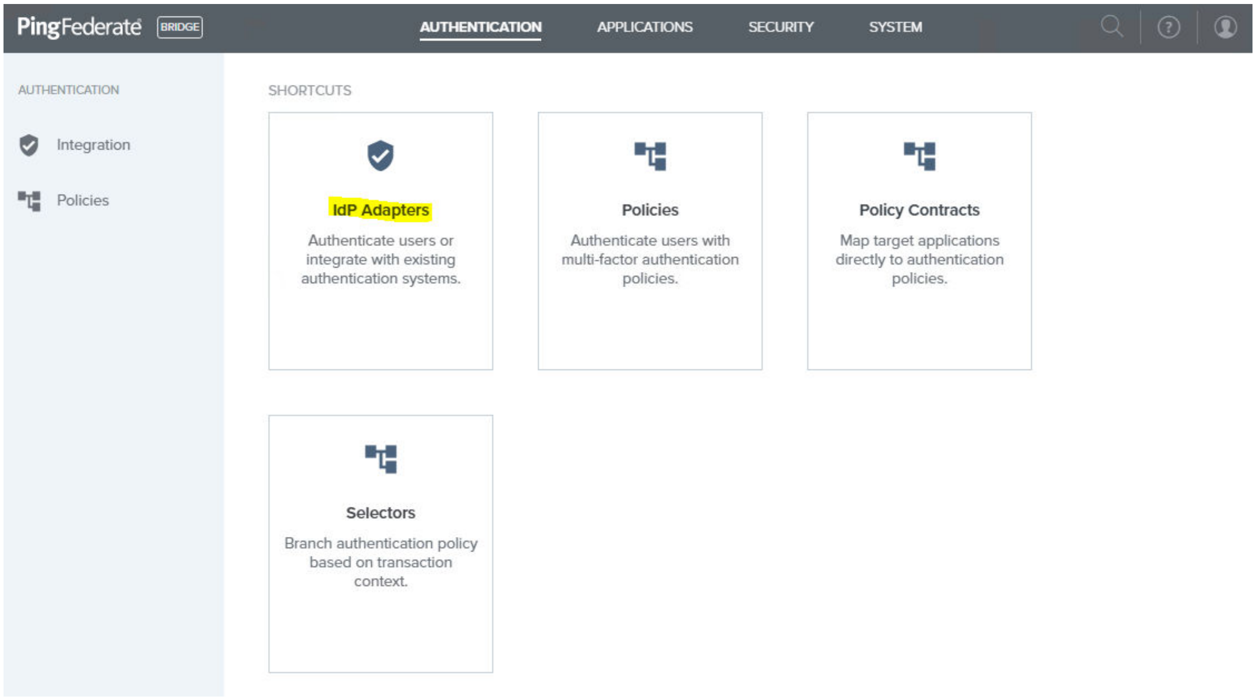
Create the HTML Form Adapter

The HTML Form Adapter enables you to customize a different login page for each configured adapter instance. You can define a logout path and page or a logout redirect page. You can also enable users to change their network passwords and customize a change-password page, or redirect users to a company-hosted password management system.

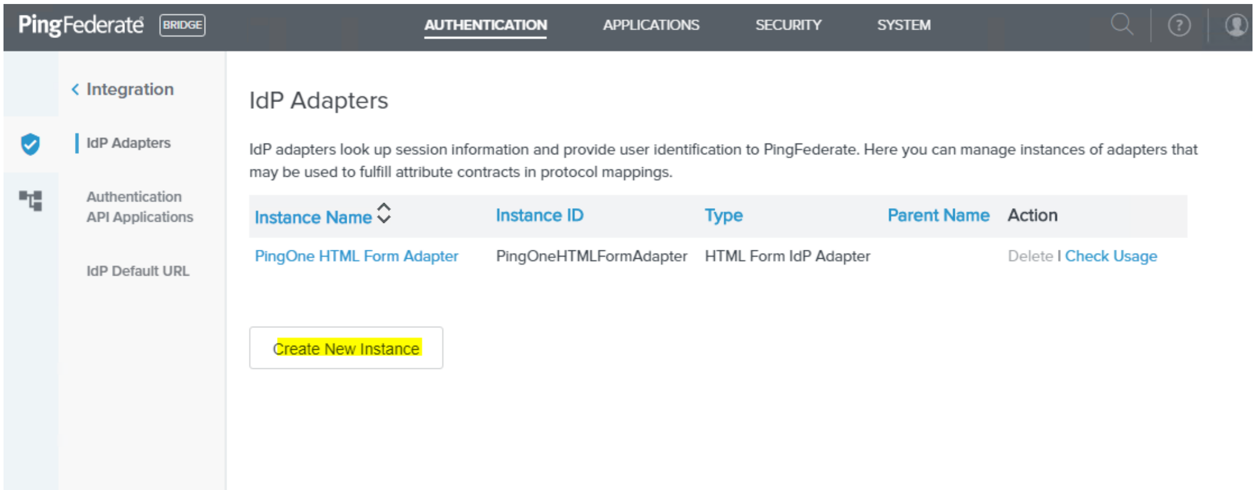
PingFederate packages an HTML Form Adapter that delegates user authentication to a configured password credential validator. This authentication mechanism validates credentials based on either an LDAP directory or a simple username validator that authenticates credentials maintained by PingFederate. If you are using the packaged adapter, you can skip this step and go to Step 4; otherwise continue with this step.

To create an HTML Form Adapter

1. In PingFederate, select **AUTHENTICATION** and click the **IdP Adapters** link.


PingFederate BRIDGE
AUTHENTICATION
APPLICATIONS
SECURITY
SYSTEM
AUTHENTICATION
Integration
Policies
SHORTCUTS
IdP Adapters
Authenticate users or integrate with existing authentication systems.
Policies
Authenticate users with multi-factor authentication policies.
Policy Contracts
Map target applications directly to authentication policies.
Selectors
Branch authentication policy based on transaction context.

2. On the IdP Adapter Instances page, click **Create New Instance**.



IdP Adapters

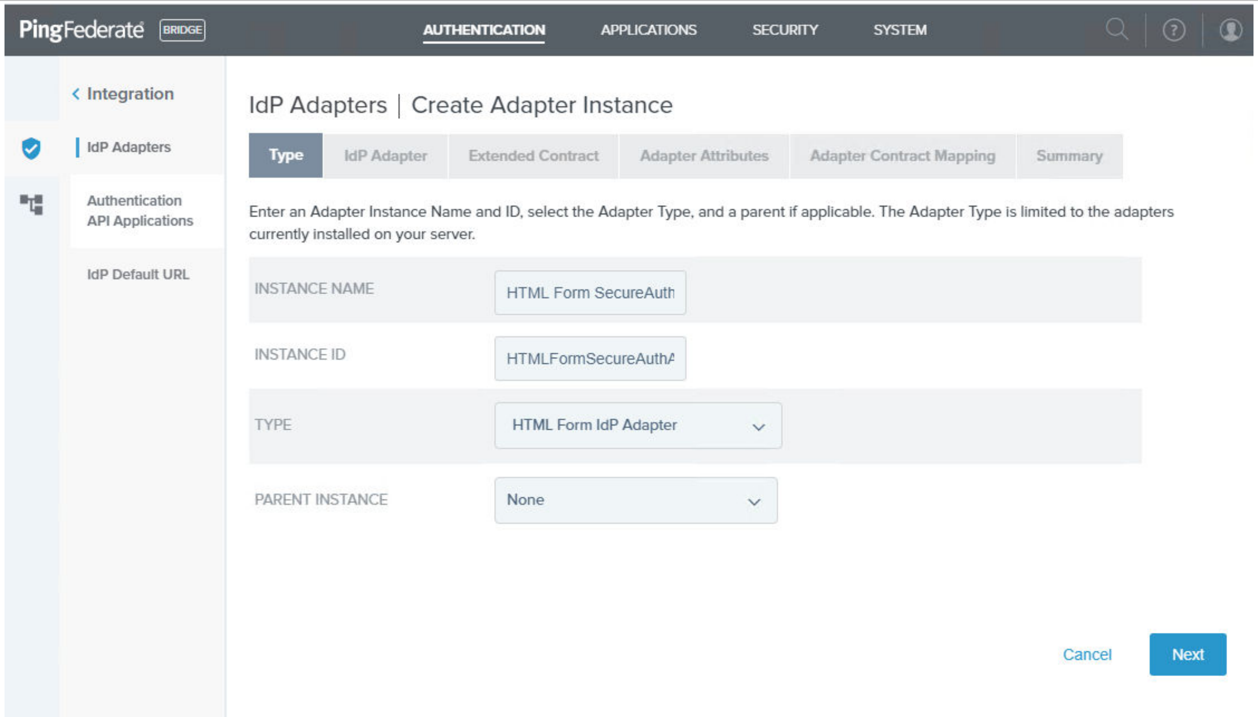
IdP adapters look up session information and provide user identification to PingFederate. Here you can manage instances of adapters that may be used to fulfill attribute contracts in protocol mappings.

Instance Name	Instance ID	Type	Parent Name	Action
PingOne HTML Form Adapter	PingOneHTMLFormAdapter	HTML Form IdP Adapter		Delete I Check Usage

Create New Instance

3. In the *Type* tab, set the following for the adapter instance type and click **Next**.

Field	**Description**
INSTANCE NAME	Enter the name of the instance
INSTANCE ID	Enter the ID of the instance
TYPE	Set to HTML From IdP Adapter.

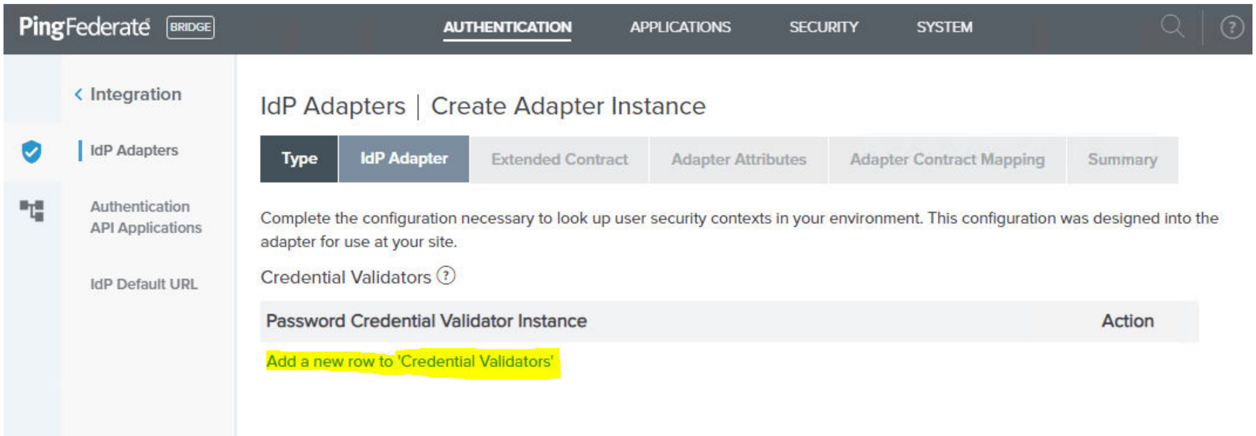


IdP Adapters | Create Adapter Instance

Enter an Adapter Instance Name and ID, select the Adapter Type, and a parent if applicable. The Adapter Type is limited to the adapters currently installed on your server.

INSTANCE NAME	HTML Form SecureAuth
INSTANCE ID	HTMLFormSecureAuthA
TYPE	HTML Form IdP Adapter
PARENT INSTANCE	None

4. In the *IdP Adapter* tab, click the **Add a new row to `Credential Validations`** link.



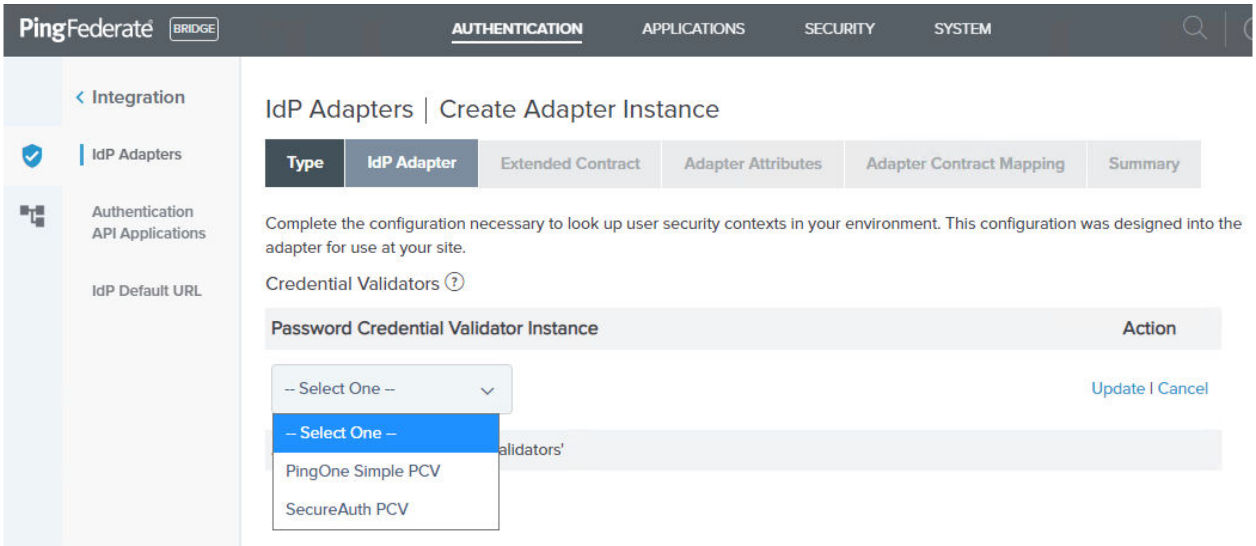
IdP Adapters | Create Adapter Instance

Complete the configuration necessary to look up user security contexts in your environment. This configuration was designed into the adapter for use at your site.

Credential Validators

Password Credential Validator Instance	Action

5. Select the password credential validator you want to use and click **Update.**



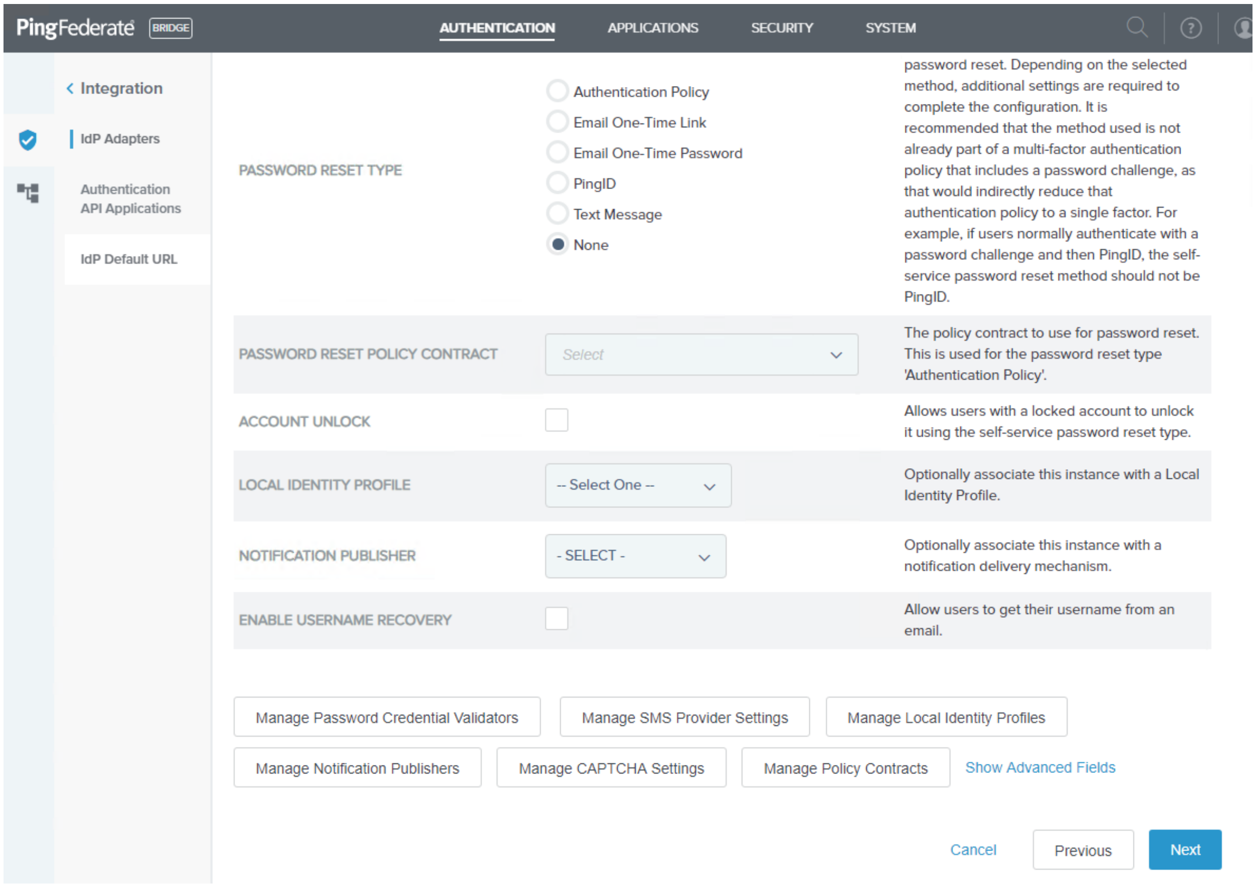
IdP Adapters | Create Adapter Instance

Complete the configuration necessary to look up user security contexts in your environment. This configuration was designed into the adapter for use at your site.

Credential Validators

Password Credential Validator Instance	Action

6. Review the summary page and click **Next**.

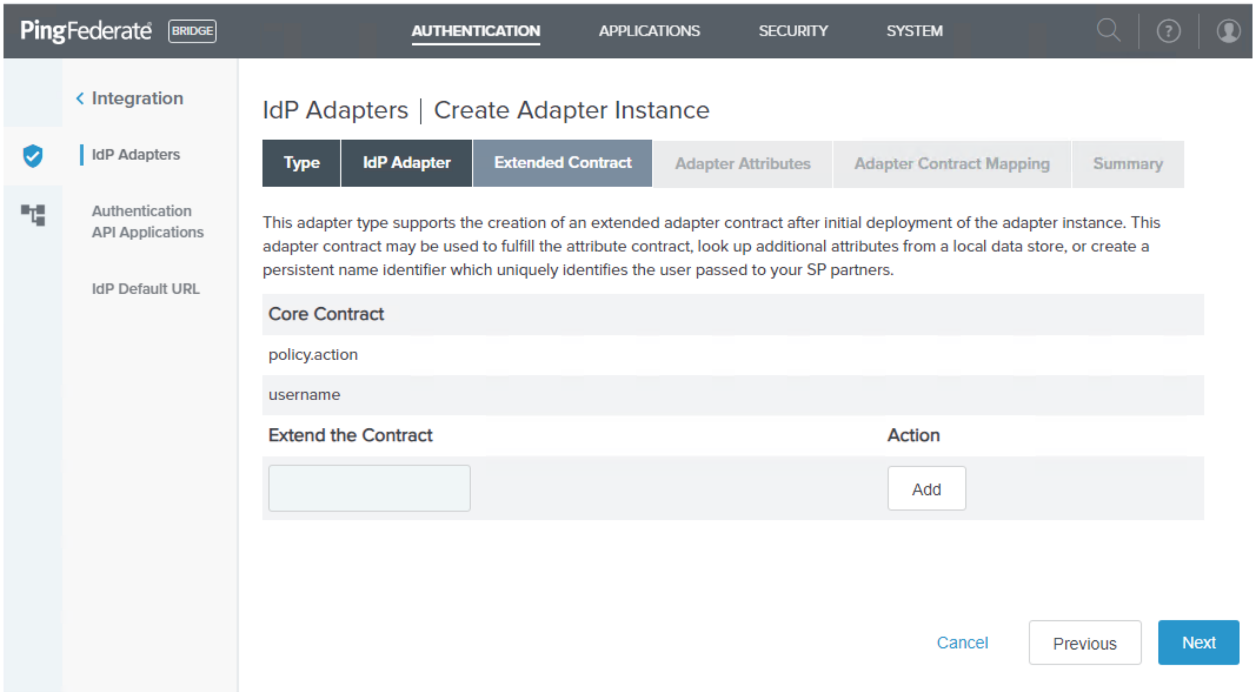


PASSWORD RESET TYPE
○ Authentication Policy
○ Email One-Time Link
○ Email One-Time Password
○ PingID
○ Text Message
● None

password reset. Depending on the selected method, additional settings are required to complete the configuration. It is recommended that the method used is not already part of a multi-factor authentication policy that includes a password challenge, as that would indirectly reduce that authentication policy to a single factor. For example, if users normally authenticate with a password challenge and then PingID, the self-service password reset method should not be PingID.

PASSWORD RESET POLICY CONTRACT	Select	The policy contract to use for password reset. This is used for the password reset type 'Authentication Policy'.
ACCOUNT UNLOCK	□	Allows users with a locked account to unlock it using the self-service password reset type.
LOCAL IDENTITY PROFILE	-- Select One --	Optionally associate this instance with a Local Identity Profile.
NOTIFICATION PUBLISHER	- SELECT -	Optionally associate this instance with a notification delivery mechanism.
ENABLE USERNAME RECOVERY	□	Allow users to get their username from an email.

7. In the *Extended Contract* tab, click **Next**.



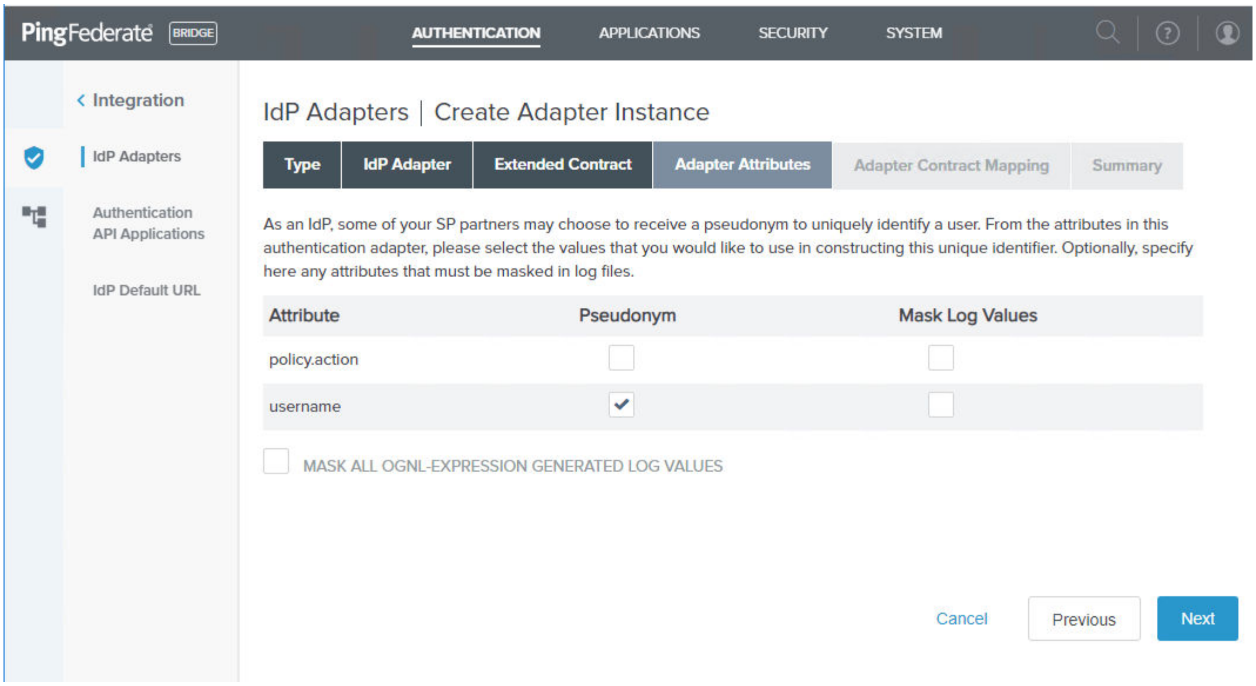
IdP Adapters | Create Adapter Instance

This adapter type supports the creation of an extended adapter contract after initial deployment of the adapter instance. This adapter contract may be used to fulfill the attribute contract, look up additional attributes from a local data store, or create a persistent name identifier which uniquely identifies the user passed to your SP partners.

Core Contract
policy.action
username

Extend the Contract	Action
	Add

8. In the *Adapter Attributes* tab, select the **Pseudonym** check box and click **Next**.



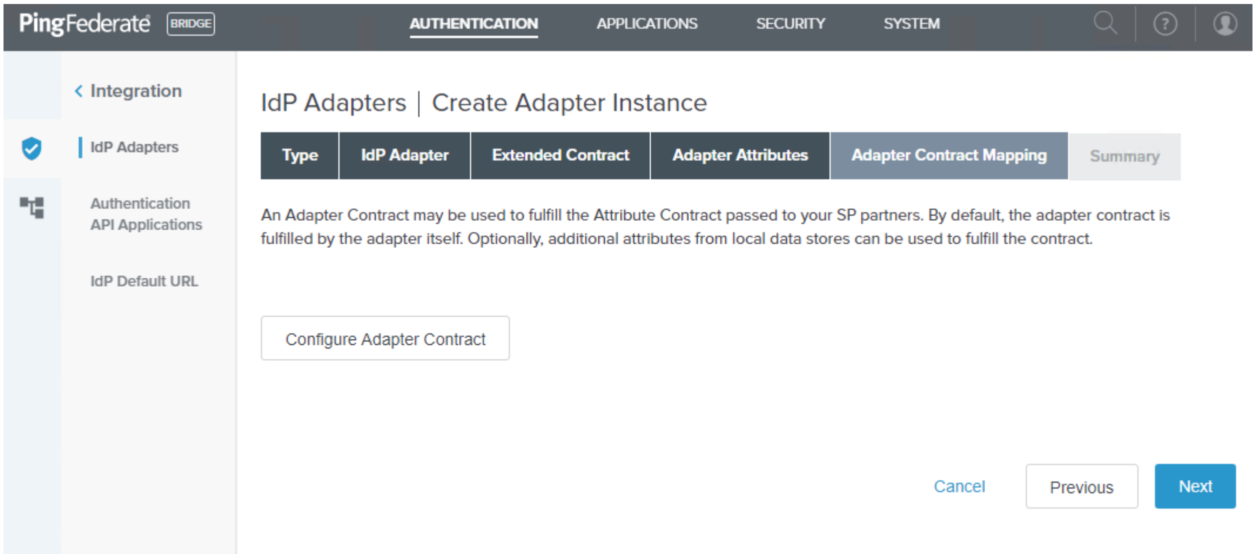
IdP Adapters | Create Adapter Instance

As an IdP, some of your SP partners may choose to receive a pseudonym to uniquely identify a user. From the attributes in this authentication adapter, please select the values that you would like to use in constructing this unique identifier. Optionally, specify here any attributes that must be masked in log files.

Attribute	Pseudonym	Mask Log Values
policy.action	□	□
username	☑	□

□ MASK ALL OGNL-EXPRESSION GENERATED LOG VALUES

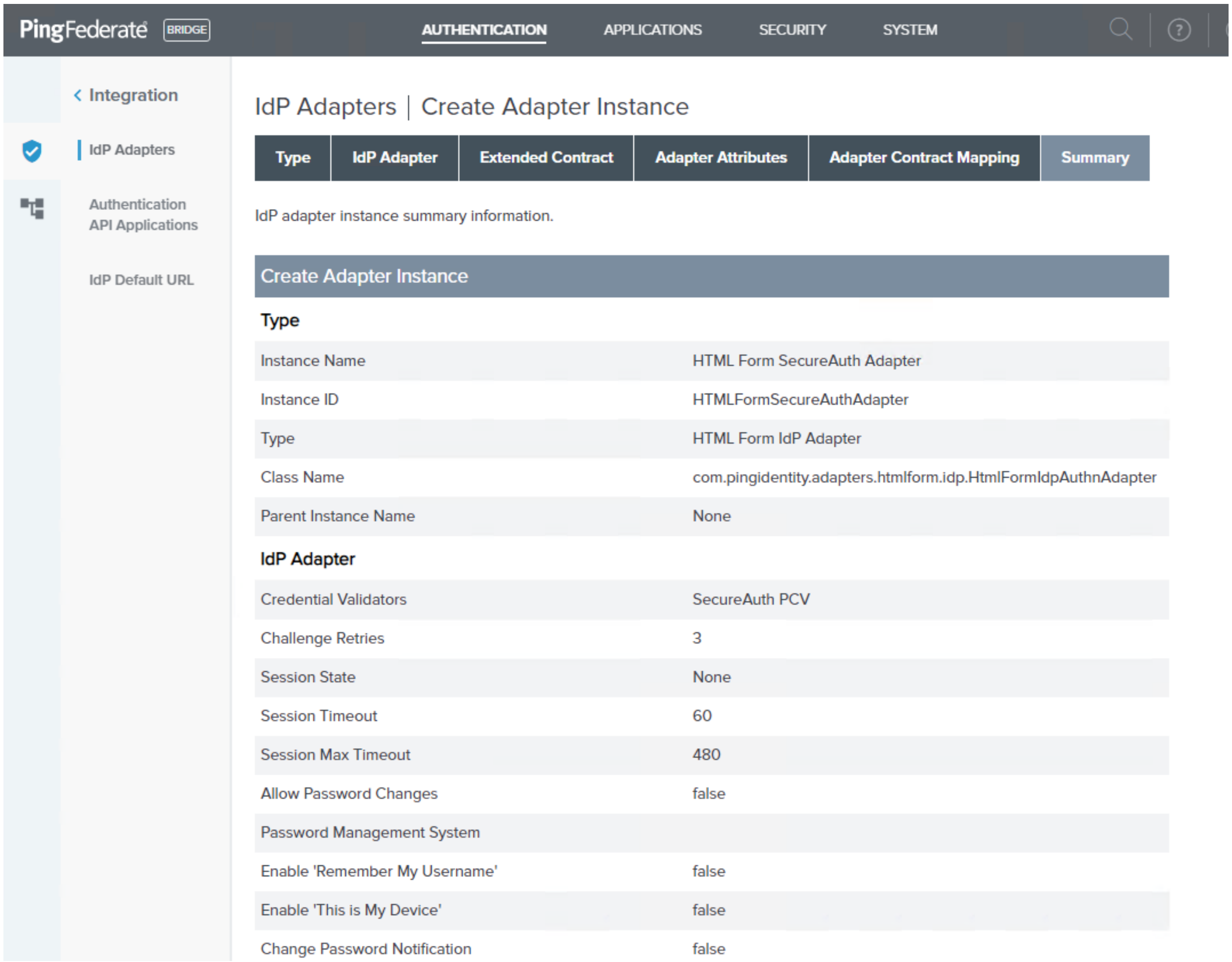
9. In the *Adapter Contract Mapping* tab, click **Next**.



IdP Adapters | Create Adapter Instance

An Adapter Contract may be used to fulfill the Attribute Contract passed to your SP partners. By default, the adapter contract is fulfilled by the adapter itself. Optionally, additional attributes from local data stores can be used to fulfill the contract.

10. Review the *Summary* tab and click **Save**.



IdP Adapters | Create Adapter Instance

IdP adapter instance summary information.

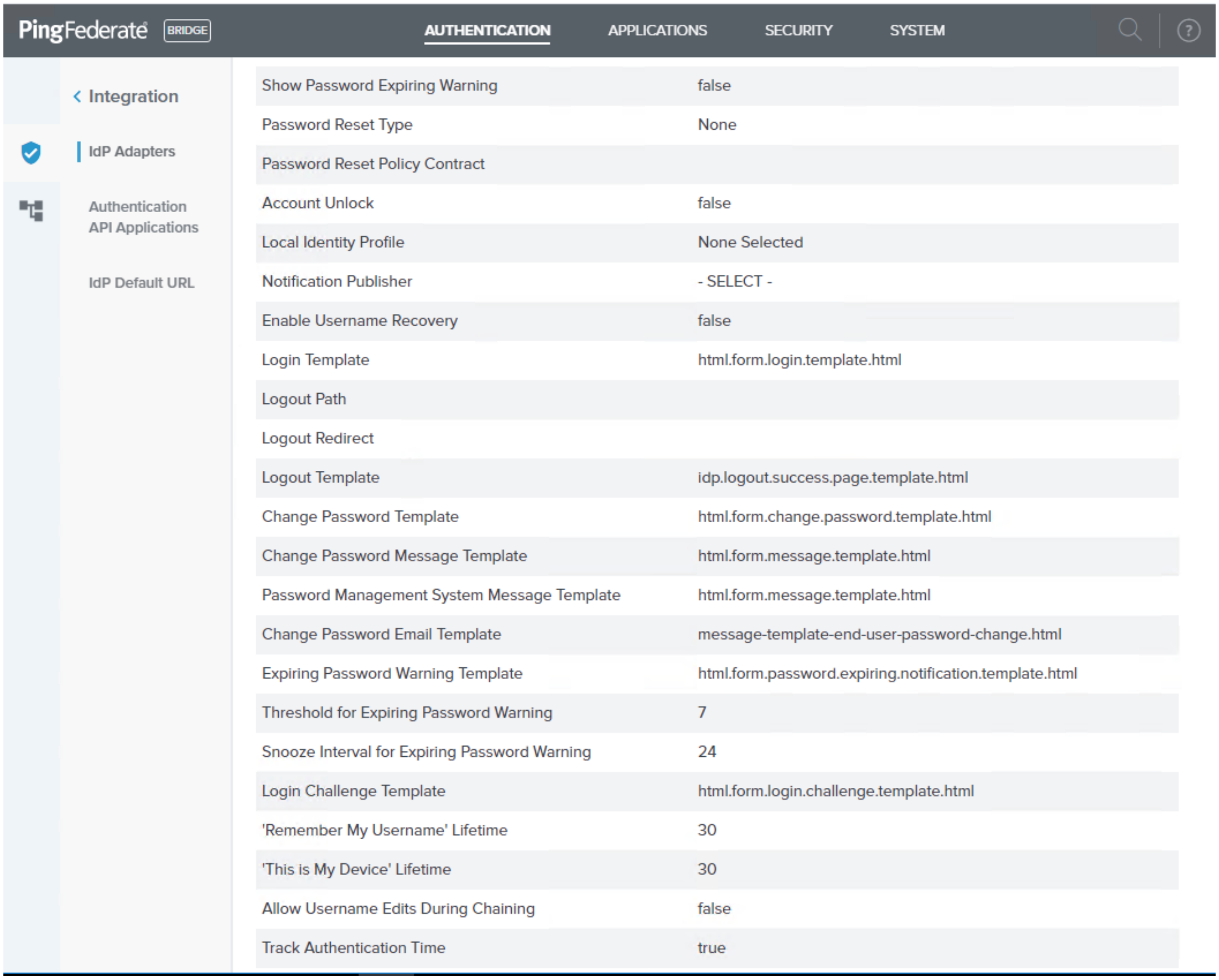
Create Adapter Instance

Type

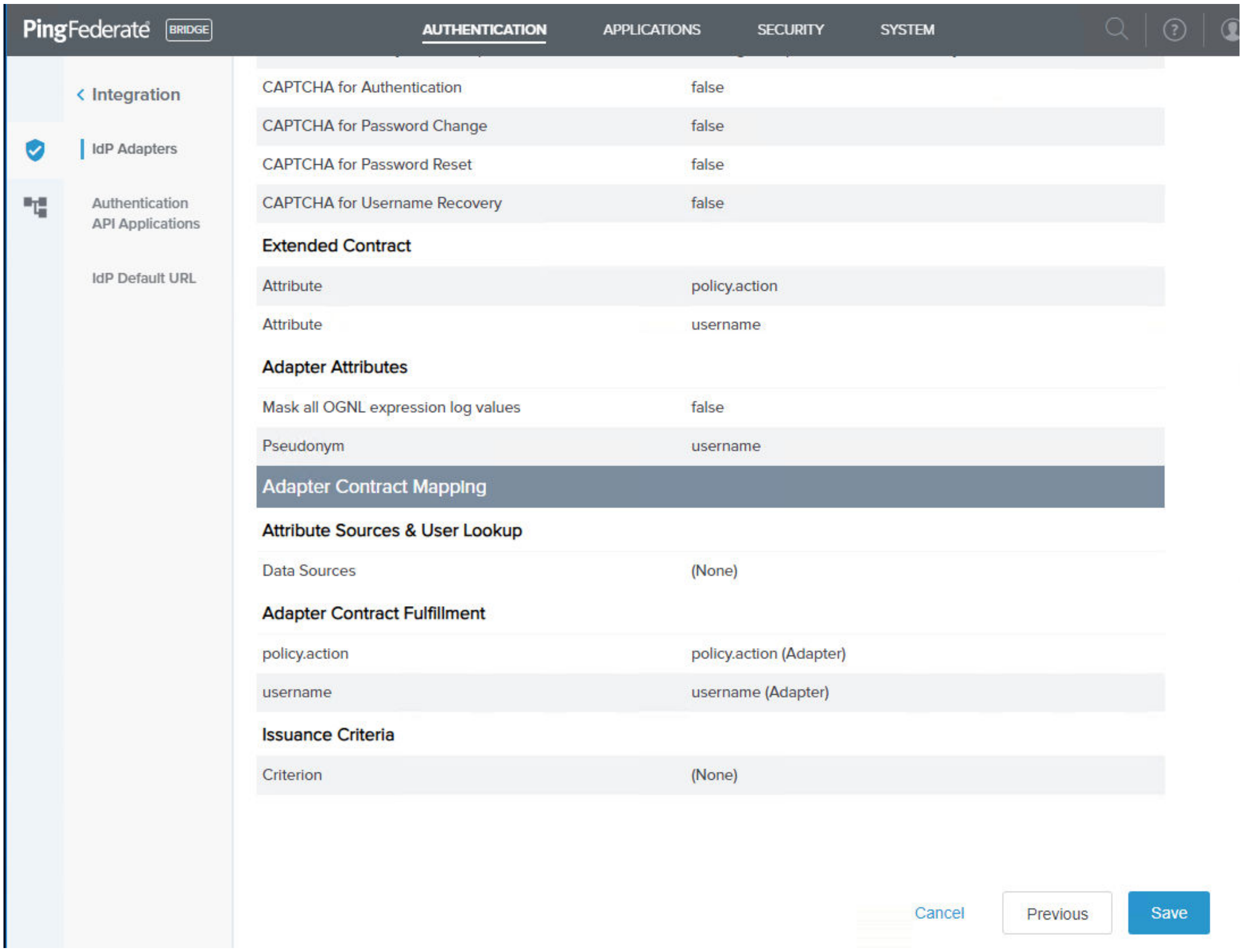
Instance Name	HTML Form SecureAuth Adapter
Instance ID	HTMLFormSecureAuthAdapter
Type	HTML Form IdP Adapter
Class Name	com.pingidentity.adapters.htmlform.idp.HtmlFormIdpAuthnAdapter
Parent Instance Name	None

IdP Adapter

Credential Validators	SecureAuth PCV
Challenge Retries	3
Session State	None
Session Timeout	60
Session Max Timeout	480
Allow Password Changes	false
Password Management System	
Enable 'Remember My Username'	false
Enable 'This is My Device'	false
Change Password Notification	false

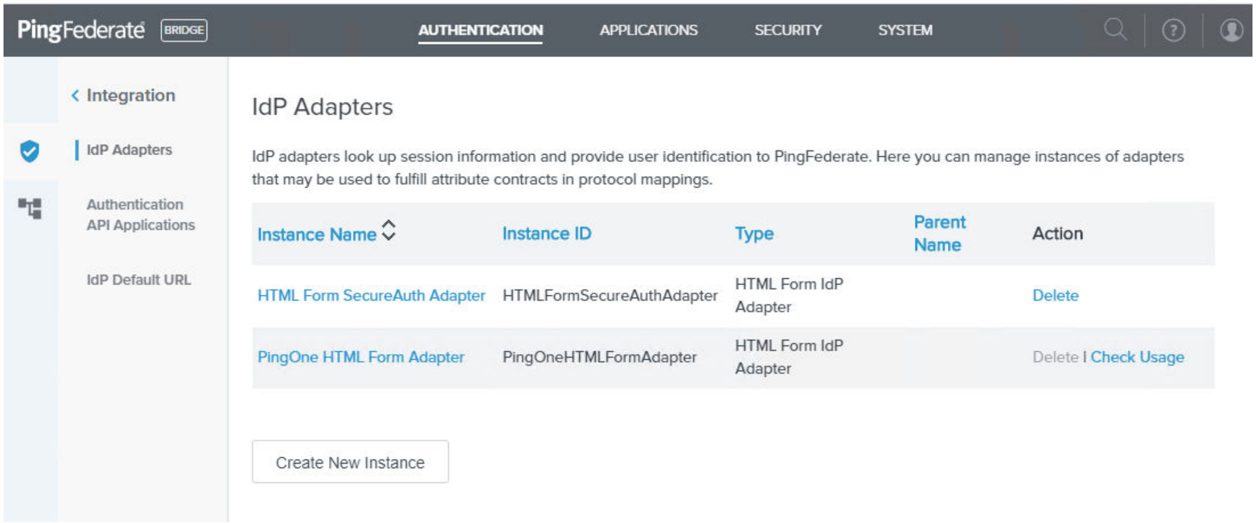


Show Password Expiring Warning	false
Password Reset Type	None
Password Reset Policy Contract	
Account Unlock	false
Local Identity Profile	None Selected
Notification Publisher	- SELECT -
Enable Username Recovery	false
Login Template	html.form.login.template.html
Logout Path	
Logout Redirect	
Logout Template	idp.logout.success.page.template.html
Change Password Template	html.form.change.password.template.html
Change Password Message Template	html.form.message.template.html
Password Management System Message Template	html.form.message.template.html
Change Password Email Template	message-template-end-user-password-change.html
Expiring Password Warning Template	html.form.password.expiring.notification.template.html
Threshold for Expiring Password Warning	7
Snooze Interval for Expiring Password Warning	24
Login Challenge Template	html.form.login.challenge.template.html
'Remember My Username' Lifetime	30
'This is My Device' Lifetime	30
Allow Username Edits During Chaining	false
Track Authentication Time	true



CAPTCHA for Authentication	false
CAPTCHA for Password Change	false
CAPTCHA for Password Reset	false
CAPTCHA for Username Recovery	false
Extended Contract	
Attribute	policy.action
Attribute	username
Adapter Attributes	
Mask all OGNL expression log values	false
Pseudonym	username
Adapter Contract Mapping	
Attribute Sources & User Lookup	
Data Sources	(None)
Adapter Contract Fulfillment	
policy.action	policy.action (Adapter)
username	username (Adapter)
Issuance Criteria	
Criterion	(None)

11. The Manage IdP Adapter Instances page shows the new HTML Form adapter instance.



IdP Adapters

IdP adapters look up session information and provide user identification to PingFederate. Here you can manage instances of adapters that may be used to fulfill attribute contracts in protocol mappings.

Instance Name	Instance ID	Type	Parent Name	Action
HTML Form SecureAuth Adapter	HTMLFormSecureAuthAdapter	HTML Form IdP Adapter		Delete
PingOne HTML Form Adapter	PingOneHTMLFormAdapter	HTML Form IdP Adapter		Delete I Check Usage

Configure the Identity Platform realm for API

If you already have an Identity Platform realm created for this purpose, skip to the next section, Create the 2FA adapter.

To create the Identity Platform realm for use with the PingFederate server

1. Install the Identity Platform appliance.

   For more information on installing an appliance, see Install the appliance.

   Use the host name/address of this appliance when configuring the PingFederate second factor (2FA) adapter (API HOST field).

2. Select or create a realm for your second factor (2FA) API.

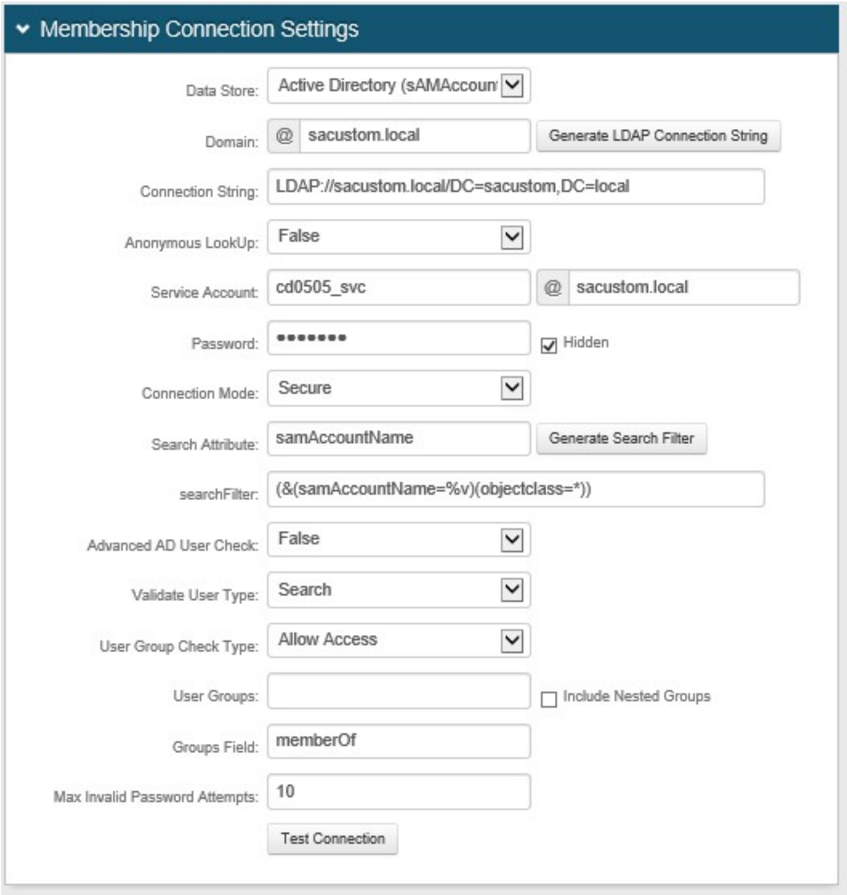
   For more information about creating a realm, see SecureAuth IdP Realm Guide.

3. Select the **Data** tab.

4. In the **Membership Connection Settings** section, set up a **Data Store** and provide the connection settings for that data store.

   The following is an example of configuration settings for an Active Directory data store.

   For more information on the configuration settings on the Data tab, see Data tab configuration.



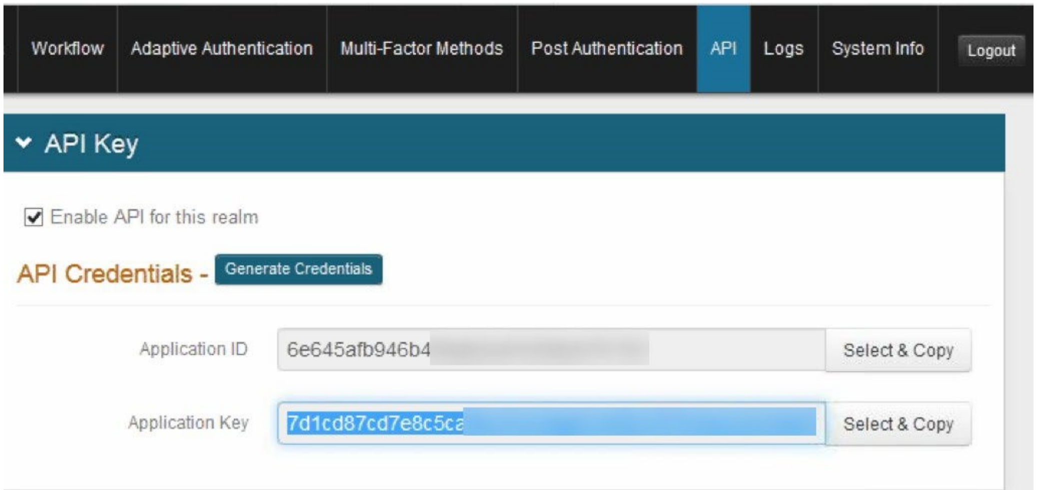
Membership Connection Settings

Data Store:	Active Directory (sAMAccoun	
Domain:	@ sacustom.local	Generate LDAP Connection String
Connection String:	LDAP://sacustom.local/DC=sacustom,DC=local	
Anonymous LookUp:	False	
Service Account:	cd0505_svc	@ sacustom.local
Password:	•••••••	☑ Hidden
Connection Mode:	Secure	
Search Attribute:	samAccountName	Generate Search Filter
searchFilter:	(&(samAccountName=%v)(objectclass=*))	
Advanced AD User Check:	False	
Validate User Type:	Search	
User Group Check Type:	Allow Access	
User Groups:		☐ Include Nested Groups
Groups Field:	memberOf	
Max Invalid Password Attempts:	10	
	Test Connection	

5. **Save** your settings.

6. Select the **API** tab.
7. In the **API Key** section, set the following:
   a. Select the **Enable API for this realm** check box.
   b. Click **Generate Credentials**.
   c. Select and copy the **Application ID** and **Application Key** to a text editor.

      You will need these values when configuring the API-App-Key and API-App-ID fields for the PingFederate 2FA adapters as explained in the Create the 2FA adapter section.



API Key

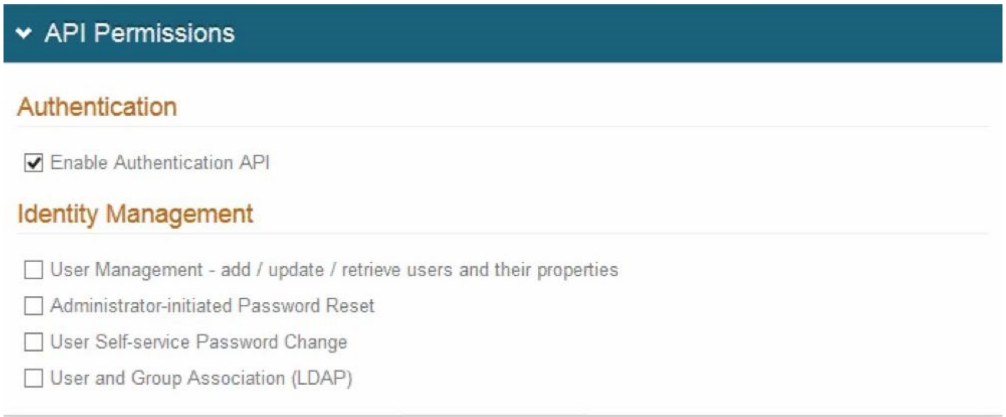
☑ Enable API for this realm

API Credentials -

Application ID 6e645afb946b4[redacted]

Application Key 7d1cd87cd7e8c5ca[redacted]

8. In the **API Permissions** section, select the **Enable Authentication API** check box.



API Permissions

Authentication

☑ Enable Authentication API

Identity Management

☐ User Management - add / update / retrieve users and their properties
☐ Administrator-initiated Password Reset
☐ User Self-service Password Change
☐ User and Group Association (LDAP)

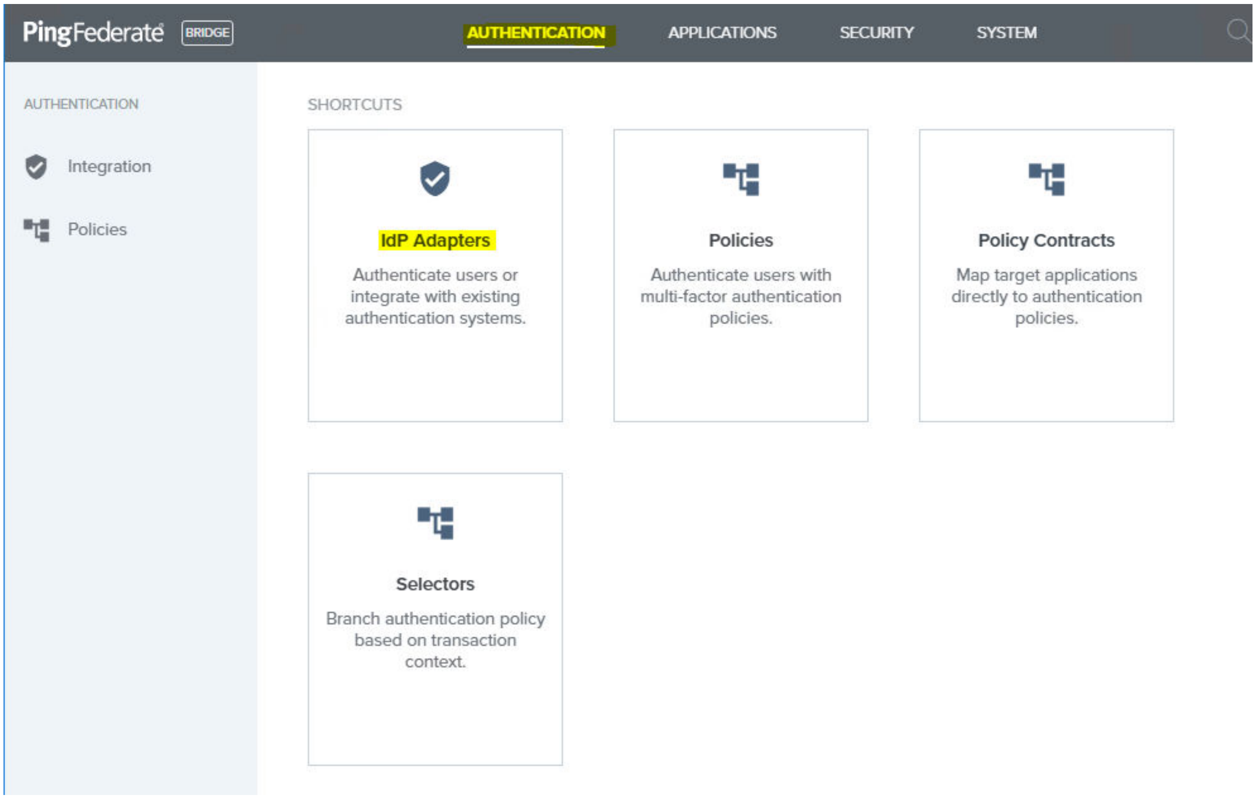
9. **Save** your changes.

   For more information about API tab field settings, see API Tab Configuration.

Create the 2FA adapter

Once you have configured a SecureAuth realm with API service, create a 2FA adapter. **To create the 2FA adapter**

1. In PingFederate, select **AUTHENTICATION** and click the **IdP Adapters** link



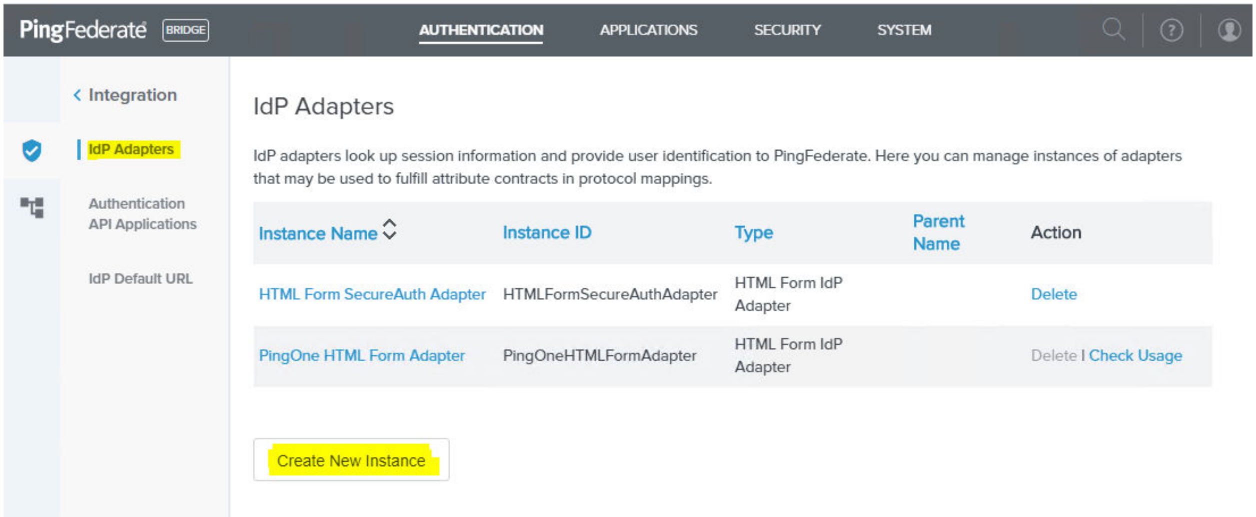
IdP Adapters
Authenticate users or integrate with existing authentication systems.

Policies
Authenticate users with multi-factor authentication policies.

Policy Contracts
Map target applications directly to authentication policies.

Selectors
Branch authentication policy based on transaction context.

2. On the IdP Adapter Instances page, click **Create New Instance**.

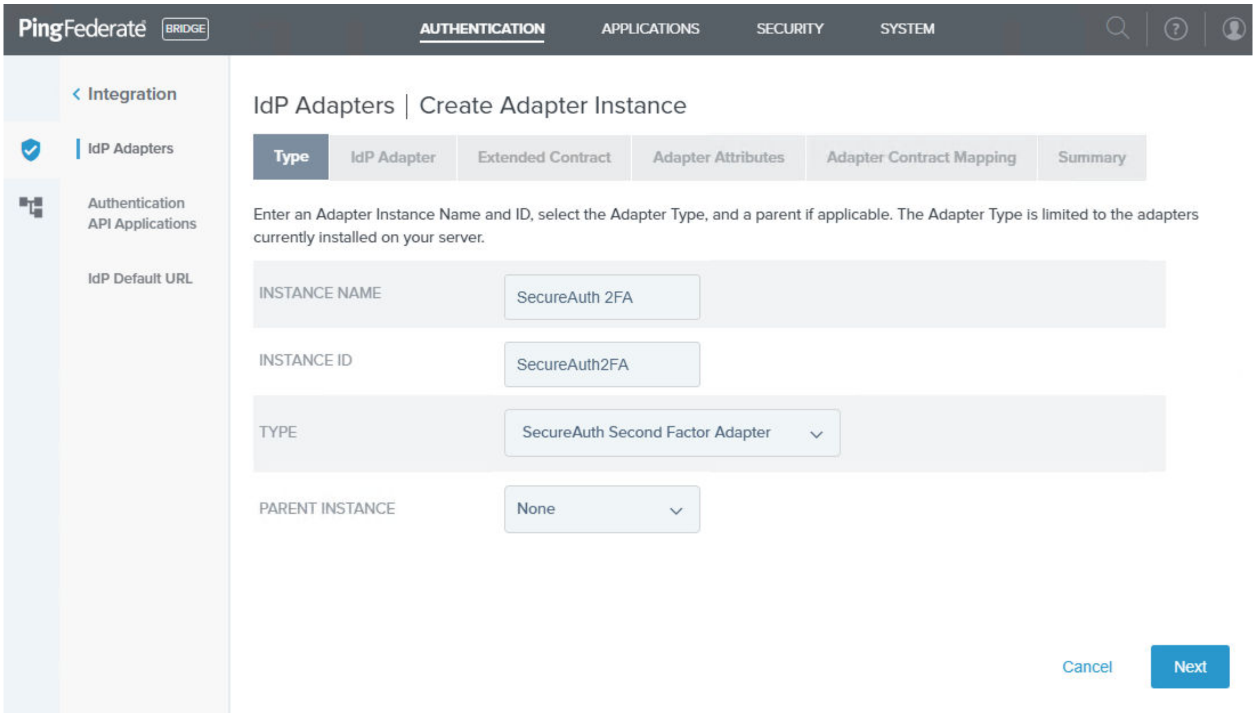


IdP Adapters

IdP adapters look up session information and provide user identification to PingFederate. Here you can manage instances of adapters that may be used to fulfill attribute contracts in protocol mappings.

Instance Name	Instance ID	Type	Parent Name	Action
HTML Form SecureAuth Adapter	HTMLFormSecureAuthAdapter	HTML Form IdP Adapter		Delete
PingOne HTML Form Adapter	PingOneHTMLFormAdapter	HTML Form IdP Adapter		Delete I Check Usage

3. In the *Type* tab for the Create Adapter Instance page, set the following:
   a. Set the **Instance Name**.
   b. Set the **Instance ID**.
   c. Set the **Type** to **SecureAuth Second Factor Adapter**.



IdP Adapters | Create Adapter Instance

Enter an Adapter Instance Name and ID, select the Adapter Type, and a parent if applicable. The Adapter Type is limited to the adapters currently installed on your server.

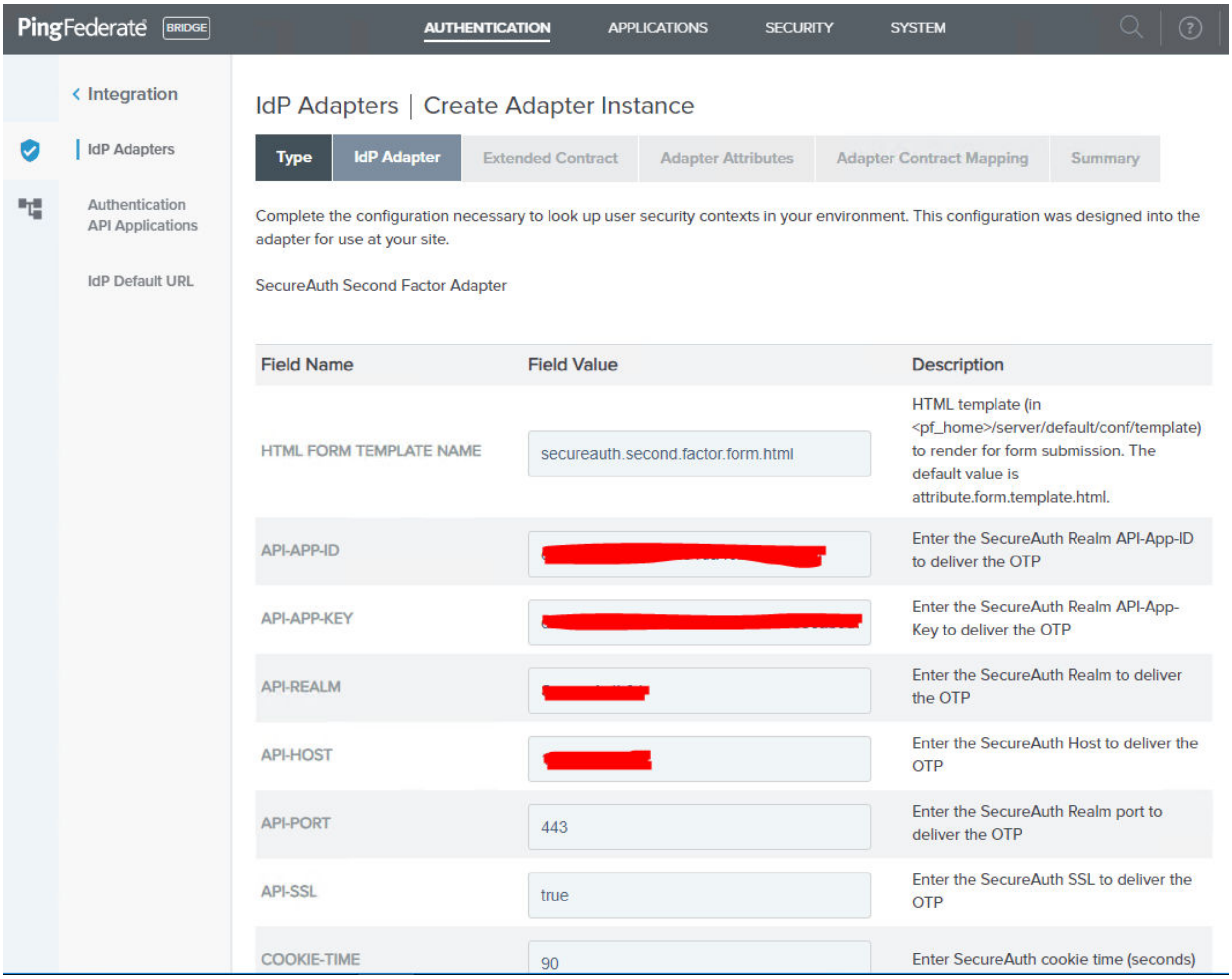
INSTANCE NAME	SecureAuth 2FA
INSTANCE ID	SecureAuth2FA
TYPE	SecureAuth Second Factor Adapter
PARENT INSTANCE	None

4. Click **Next**.

5. On the *IdP Adapter* tab, set the following:

Field	Description
HTML Form Template Name	Set to **secureauth.second.factor.form.html**.

Field	Description
API-APP-ID	Paste the Application ID API credential key copied from the Identity Platform realm. See the Configure the Identity Platform for API section.
API-APP-Key	Paste the Application Key API credential key copied from the Identity Platform realm. See the Configure the Identity Platform for API section.
API_REALM	Set to the Identity Platform realm number used for this configuration.
API-HOST	Set to the host used by the Identity Platform to deliver the OTP. .
API-PORT	Set to the API port used by the Identity Platform realm to deliver the OTP.
API-SSL	Set the SSL used by the Identity Platform to deliver the OTP.

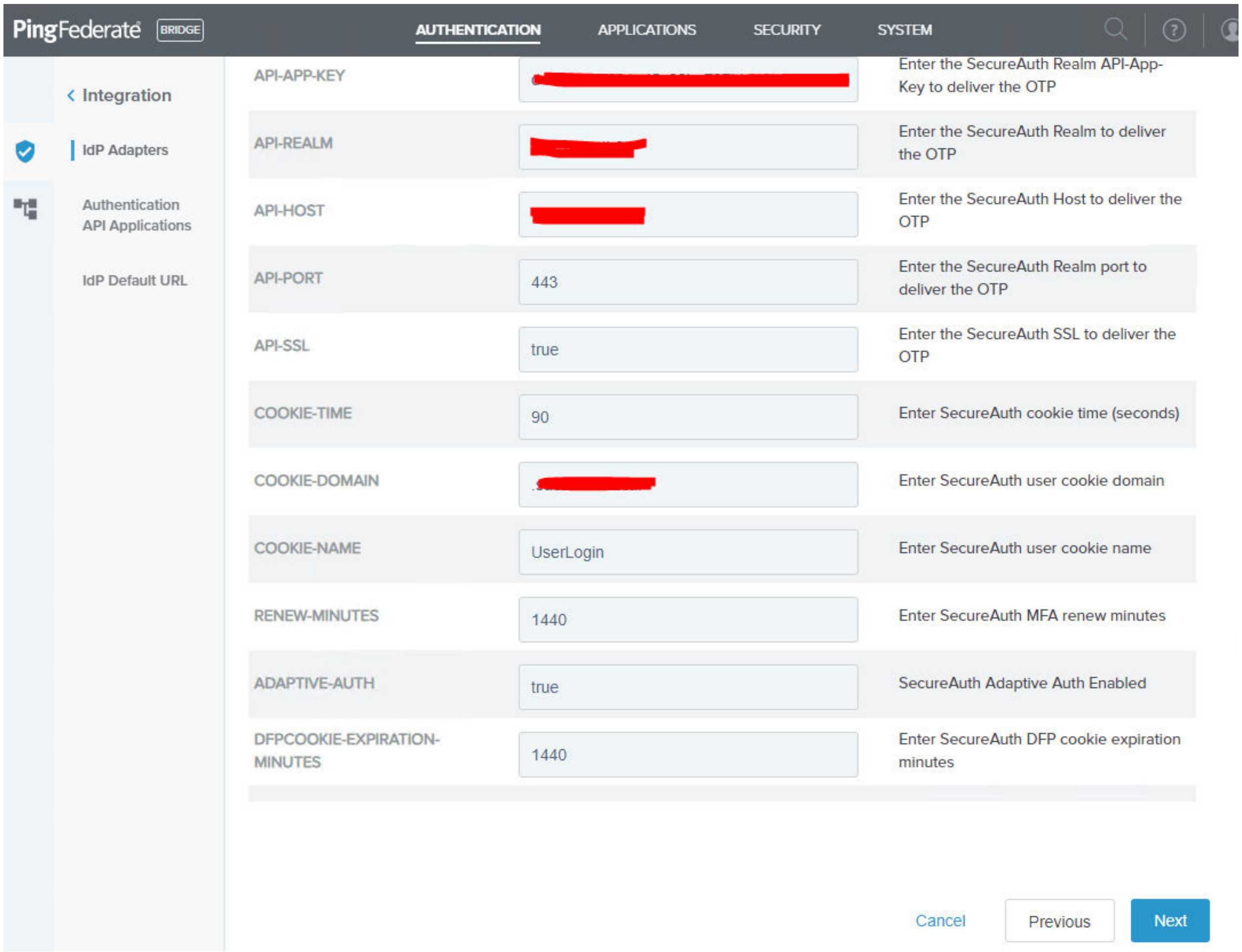


IdP Adapters | Create Adapter Instance

Complete the configuration necessary to look up user security contexts in your environment. This configuration was designed into the adapter for use at your site.

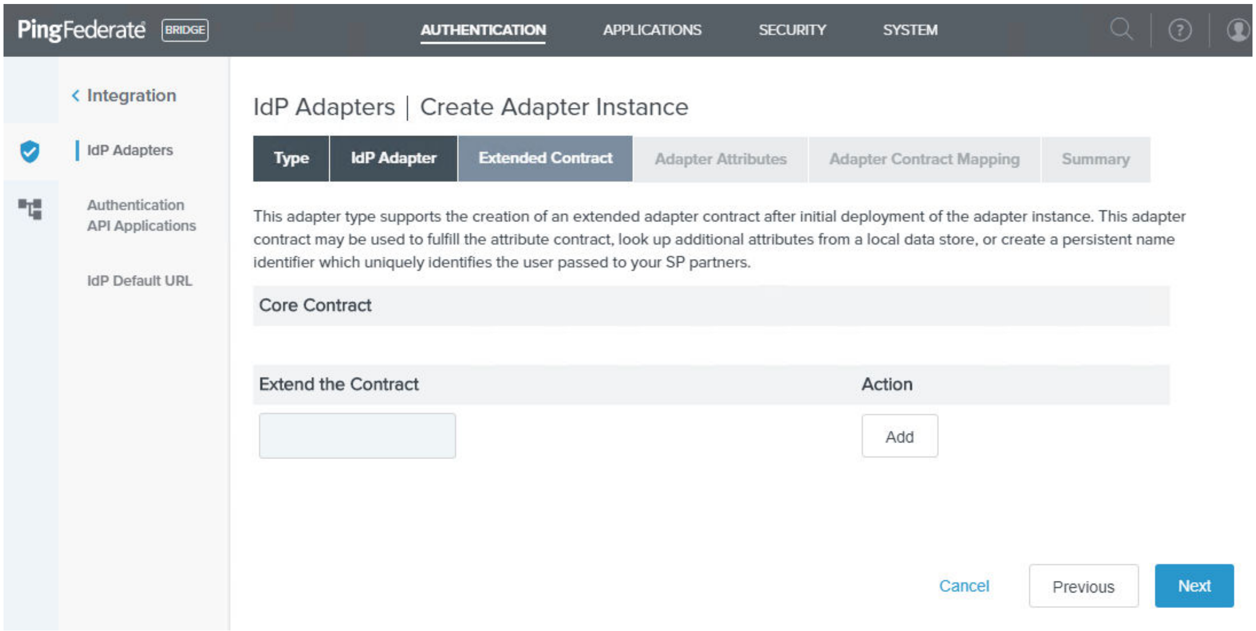
SecureAuth Second Factor Adapter

Field Name	Field Value	Description
HTML FORM TEMPLATE NAME	secureauth.second.factor.form.html	HTML template (in <pf_home>/server/default/conf/template) to render for form submission. The default value is attribute.form.template.html.
API-APP-ID	[redacted]	Enter the SecureAuth Realm API-App-ID to deliver the OTP
API-APP-KEY	[redacted]	Enter the SecureAuth Realm API-App-Key to deliver the OTP
API-REALM	[redacted]	Enter the SecureAuth Realm to deliver the OTP
API-HOST	[redacted]	Enter the SecureAuth Host to deliver the OTP
API-PORT	443	Enter the SecureAuth Realm port to deliver the OTP
API-SSL	true	Enter the SecureAuth SSL to deliver the OTP
COOKIE-TIME	90	Enter SecureAuth cookie time (seconds)



API-APP-KEY	[redacted]	Enter the SecureAuth Realm API-App-Key to deliver the OTP
API-REALM	[redacted]	Enter the SecureAuth Realm to deliver the OTP
API-HOST	[redacted]	Enter the SecureAuth Host to deliver the OTP
API-PORT	443	Enter the SecureAuth Realm port to deliver the OTP
API-SSL	true	Enter the SecureAuth SSL to deliver the OTP
COOKIE-TIME	90	Enter SecureAuth cookie time (seconds)
COOKIE-DOMAIN	[redacted]	Enter SecureAuth user cookie domain
COOKIE-NAME	UserLogin	Enter SecureAuth user cookie name
RENEW-MINUTES	1440	Enter SecureAuth MFA renew minutes
ADAPTIVE-AUTH	true	SecureAuth Adaptive Auth Enabled
DFPCOOKIE-EXPIRATION-MINUTES	1440	Enter SecureAuth DFP cookie expiration minutes

6. Click **Next**.
7. In the *Extended Contract* tab, click **Next**.



IdP Adapters | Create Adapter Instance

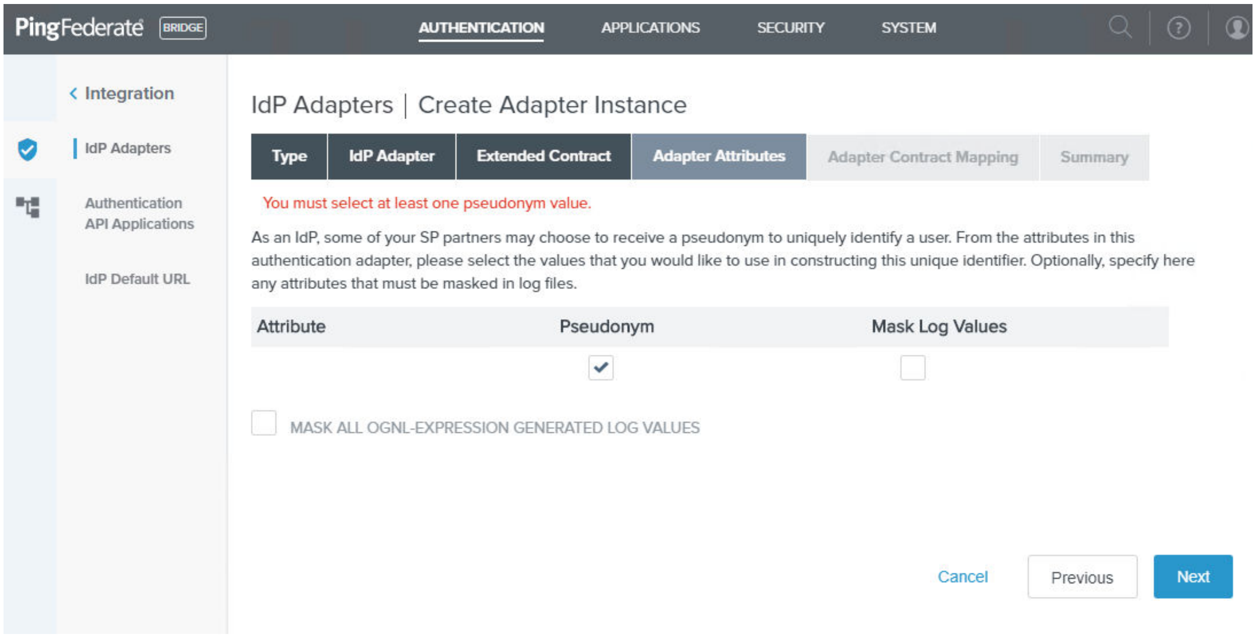
Type | IdP Adapter | Extended Contract | Adapter Attributes | Adapter Contract Mapping | Summary

This adapter type supports the creation of an extended adapter contract after initial deployment of the adapter instance. This adapter contract may be used to fulfill the attribute contract, look up additional attributes from a local data store, or create a persistent name identifier which uniquely identifies the user passed to your SP partners.

Core Contract

Extend the Contract	Action
	Add

8. In the *Adapter Attributes* tab, select the **Pseudonym** check box.



IdP Adapters | Create Adapter Instance

Type | IdP Adapter | Extended Contract | Adapter Attributes | Adapter Contract Mapping | Summary

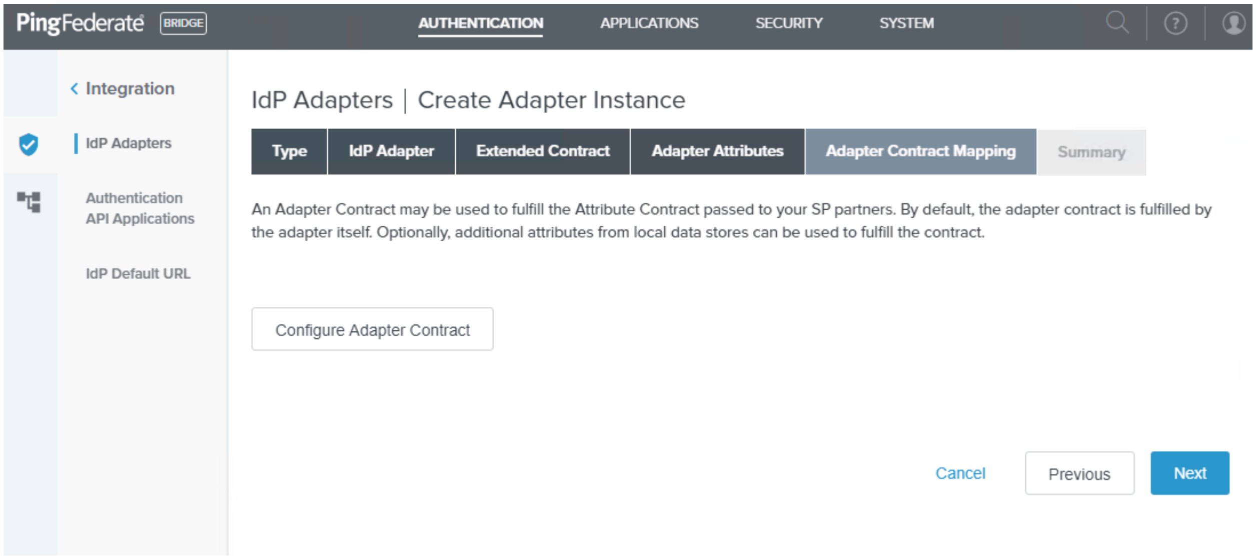
You must select at least one pseudonym value.

As an IdP, some of your SP partners may choose to receive a pseudonym to uniquely identify a user. From the attributes in this authentication adapter, please select the values that you would like to use in constructing this unique identifier. Optionally, specify here any attributes that must be masked in log files.

Attribute	Pseudonym	Mask Log Values
	☑	☐

☐ MASK ALL OGNL-EXPRESSION GENERATED LOG VALUES

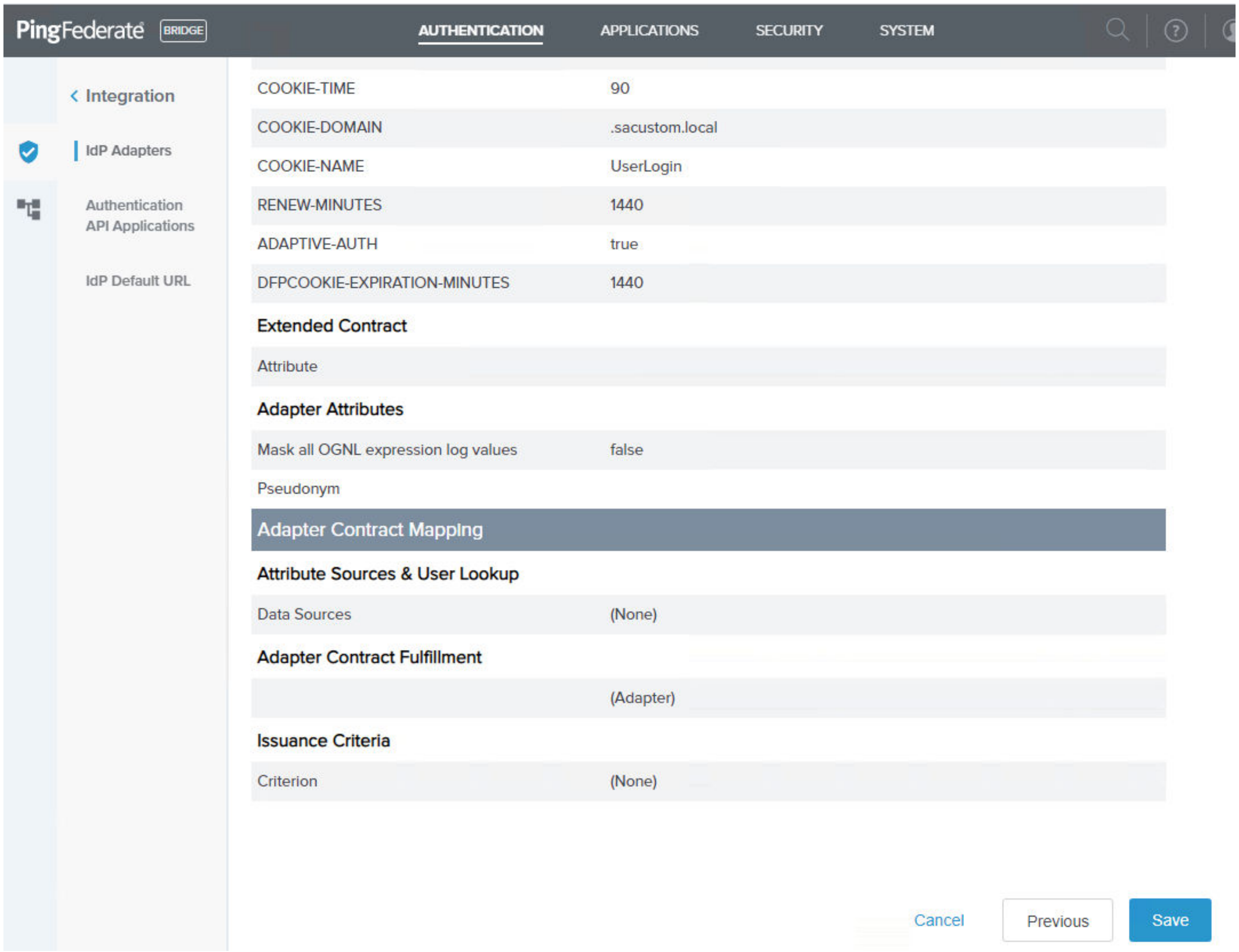
9. In the *Adapter Contract Mapping* tab, click **Next**.



IdP Adapters | Create Adapter Instance

An Adapter Contract may be used to fulfill the Attribute Contract passed to your SP partners. By default, the adapter contract is fulfilled by the adapter itself. Optionally, additional attributes from local data stores can be used to fulfill the contract.

10. Review the summary page and click **Save**.



COOKIE-TIME	90
COOKIE-DOMAIN	.sacustom.local
COOKIE-NAME	UserLogin
RENEW-MINUTES	1440
ADAPTIVE-AUTH	true
DFPCOOKIE-EXPIRATION-MINUTES	1440

Extended Contract

Attribute

Adapter Attributes

Mask all OGNL expression log values	false
Pseudonym	

Adapter Contract Mapping

Attribute Sources & User Lookup

Data Sources	(None)

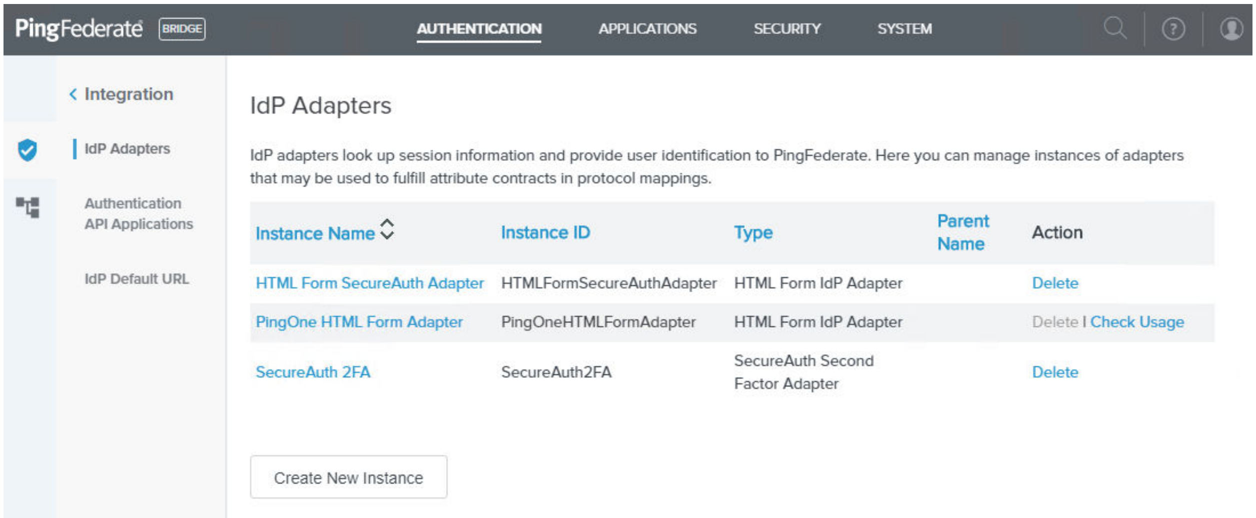
Adapter Contract Fulfillment

	(Adapter)

Issuance Criteria

Criterion	(None)

11. See the SecureAuth 2FA adapter instance in the list.



IdP Adapters

IdP adapters look up session information and provide user identification to PingFederate. Here you can manage instances of adapters that may be used to fulfill attribute contracts in protocol mappings.

Instance Name	Instance ID	Type	Parent Name	Action
HTML Form SecureAuth Adapter	HTMLFormSecureAuthAdapter	HTML Form IdP Adapter		Delete
PingOne HTML Form Adapter	PingOneHTMLFormAdapter	HTML Form IdP Adapter		Delete I Check Usage
SecureAuth 2FA	SecureAuth2FA	SecureAuth Second Factor Adapter		Delete

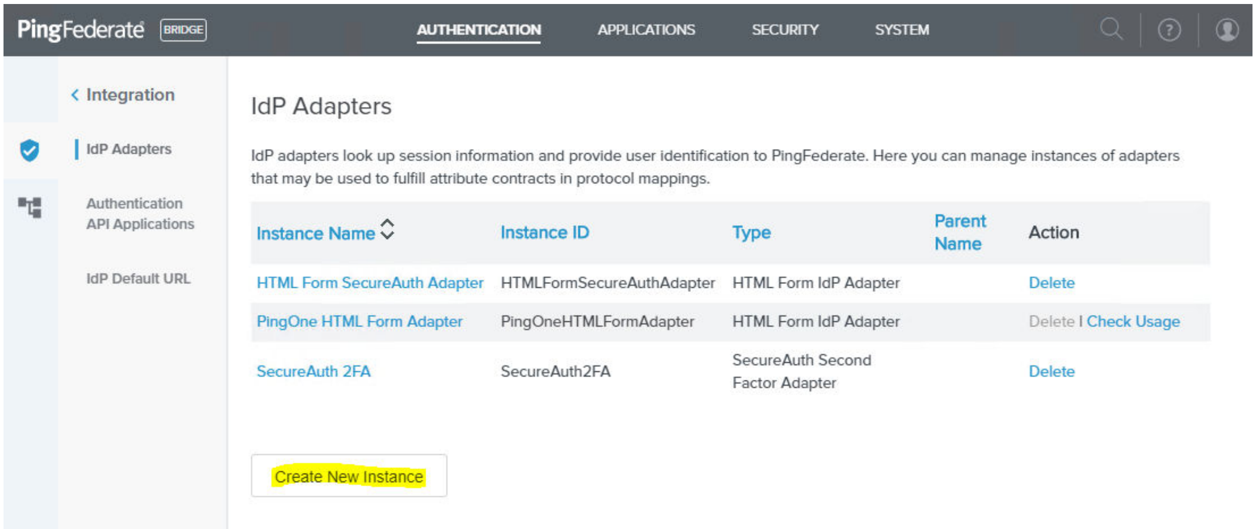
Create New Instance

Create the SecureAuth composite adapter

For the Identity Platform to communicate with the PingFederate server, you must set up a SecureAuth composite adapter.

To create the SecureAuth composite adapter

1. On the IdP Adapter Instances page, click **Create New Instance**.



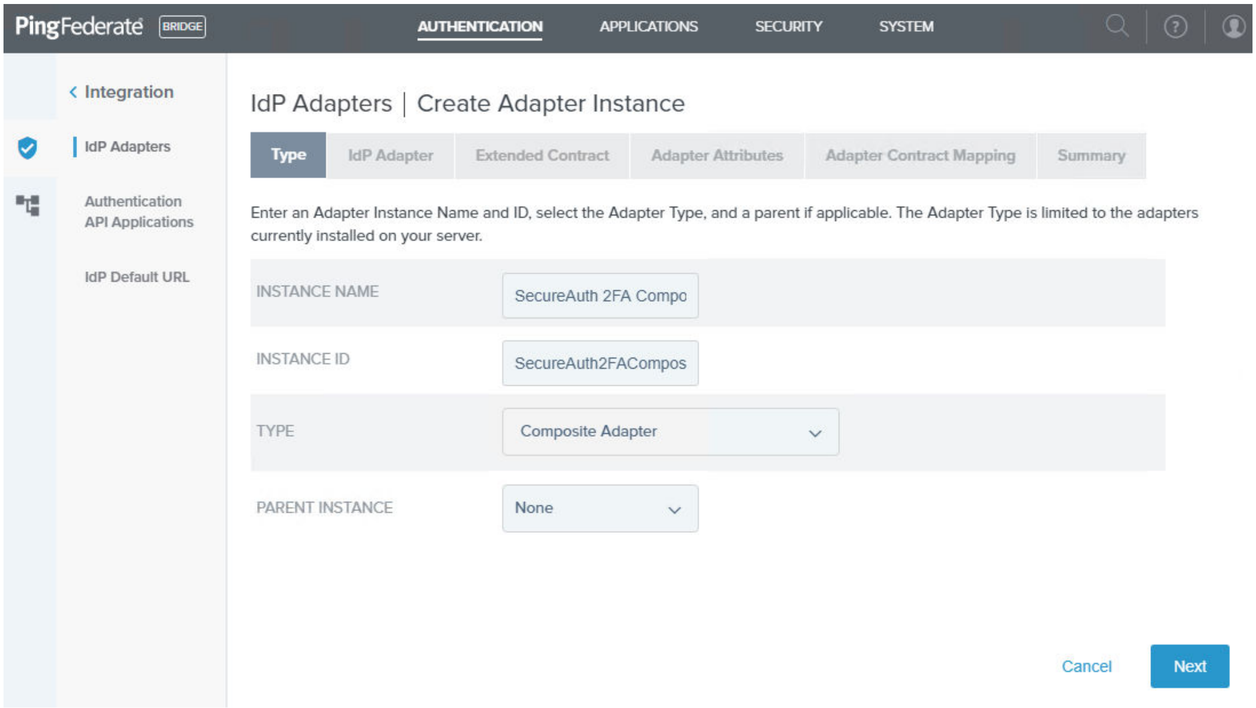
IdP Adapters

IdP adapters look up session information and provide user identification to PingFederate. Here you can manage instances of adapters that may be used to fulfill attribute contracts in protocol mappings.

Instance Name	Instance ID	Type	Parent Name	Action
HTML Form SecureAuth Adapter	HTMLFormSecureAuthAdapter	HTML Form IdP Adapter		Delete
PingOne HTML Form Adapter	PingOneHTMLFormAdapter	HTML Form IdP Adapter		Delete I Check Usage
SecureAuth 2FA	SecureAuth2FA	SecureAuth Second Factor Adapter		Delete

Create New Instance

2. In the *Type* tab on the Create Adapter Instance page, set the following:
   a. Set the **Instance Name**.
   b. Set the **Instance ID**.
   c. Set the **Type** to **Composite Adapter**.

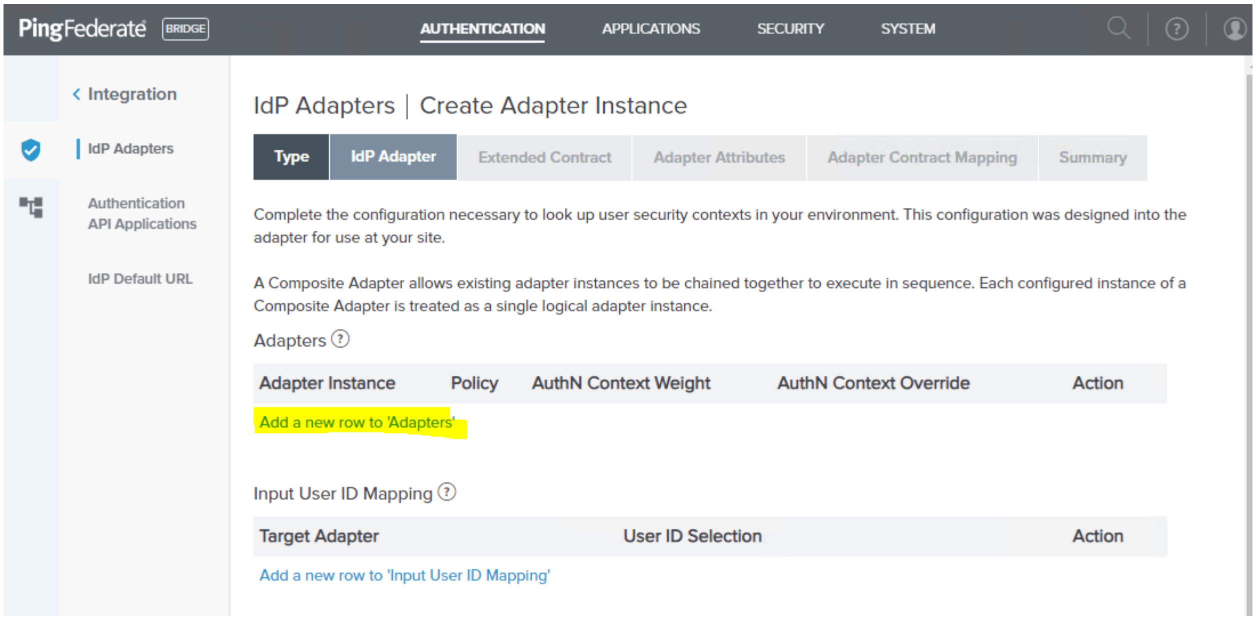


IdP Adapters | Create Adapter Instance

Enter an Adapter Instance Name and ID, select the Adapter Type, and a parent if applicable. The Adapter Type is limited to the adapters currently installed on your server.

INSTANCE NAME	SecureAuth 2FA Compo
INSTANCE ID	SecureAuth2FACompos
TYPE	Composite Adapter
PARENT INSTANCE	None

3. Click **Next**.
4. In the *IdP Adapter* tab, in the Adapters section, click the **Add a new row to ‘Adapters’** link.



IdP Adapters | Create Adapter Instance

Complete the configuration necessary to look up user security contexts in your environment. This configuration was designed into the adapter for use at your site.

A Composite Adapter allows existing adapter instances to be chained together to execute in sequence. Each configured instance of a Composite Adapter is treated as a single logical adapter instance.

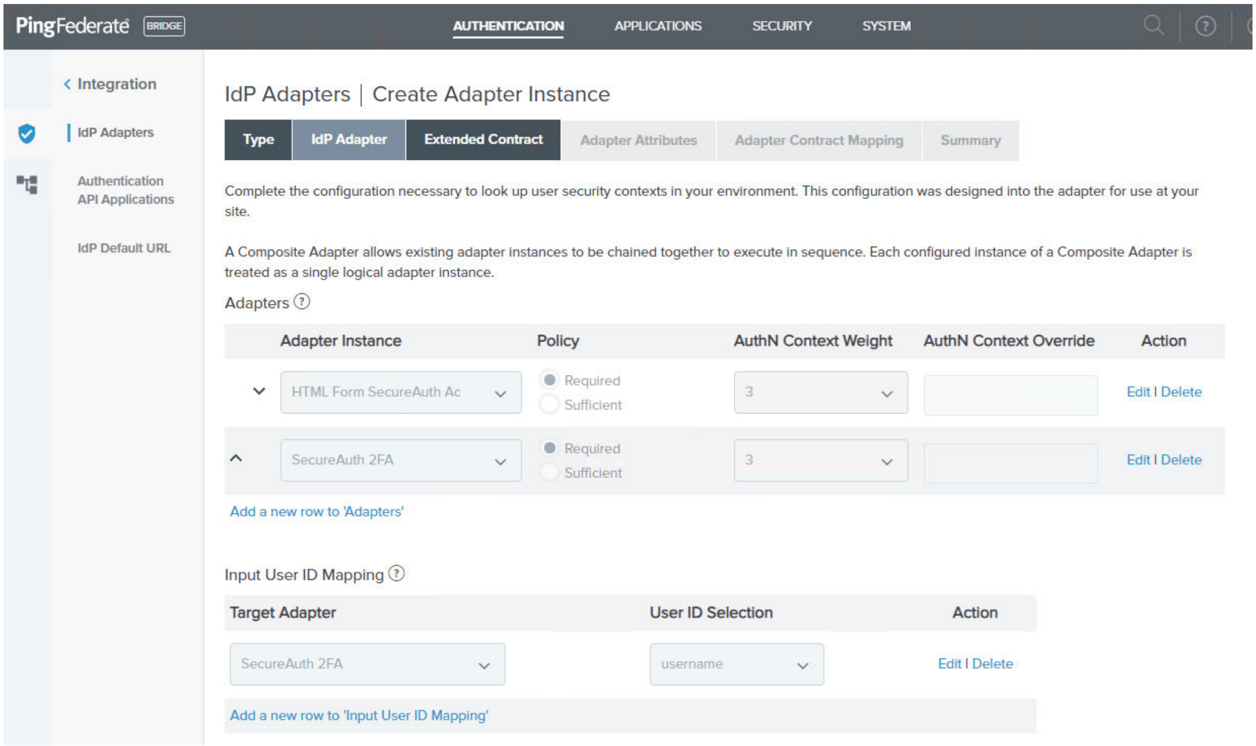
Adapters

Adapter Instance	Policy	AuthN Context Weight	AuthN Context Override	Action

Input User ID Mapping

Target Adapter	User ID Selection	Action

5. In the *IdP Adapter* tab under the Adapters section, set the following:
   a. Set Adapter Instance to **HTML Form IdP Adapter** and **SecureAuth 2FA**.
   b. Set the Target Adapter to **SecureAuth 2FA**.
   c. Set the User ID Selection to username.



IdP Adapters | Create Adapter Instance

Complete the configuration necessary to look up user security contexts in your environment. This configuration was designed into the adapter for use at your site.

A Composite Adapter allows existing adapter instances to be chained together to execute in sequence. Each configured instance of a Composite Adapter is treated as a single logical adapter instance.

Adapters

Adapter Instance	Policy	AuthN Context Weight	AuthN Context Override	Action
HTML Form SecureAuth Ac	● Required ○ Sufficient	3		Edit | Delete
SecureAuth 2FA	● Required ○ Sufficient	3		Edit | Delete

Add a new row to 'Adapters'

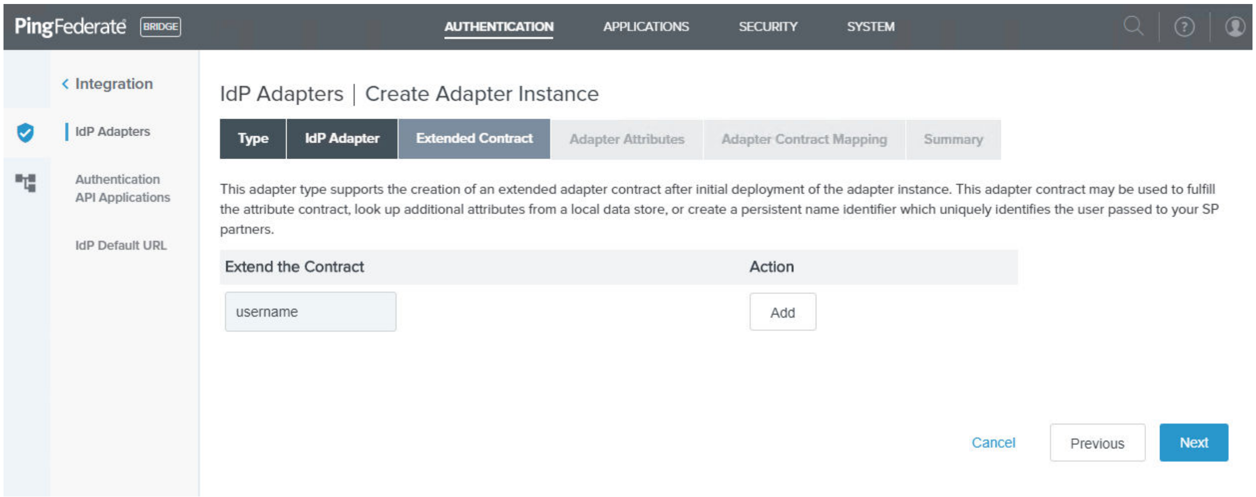
Input User ID Mapping

Target Adapter	User ID Selection	Action
SecureAuth 2FA	username	Edit | Delete

Add a new row to 'Input User ID Mapping'

6. Verify that the order of the adapter instance is set with HTML Form IdP Adapter first, then followed by SecureAuth 2FA adapter. Click **Next**.

7. In the *Extended Contract* tab, in the Extend the Contract section, add the **username** and Click **Next**.

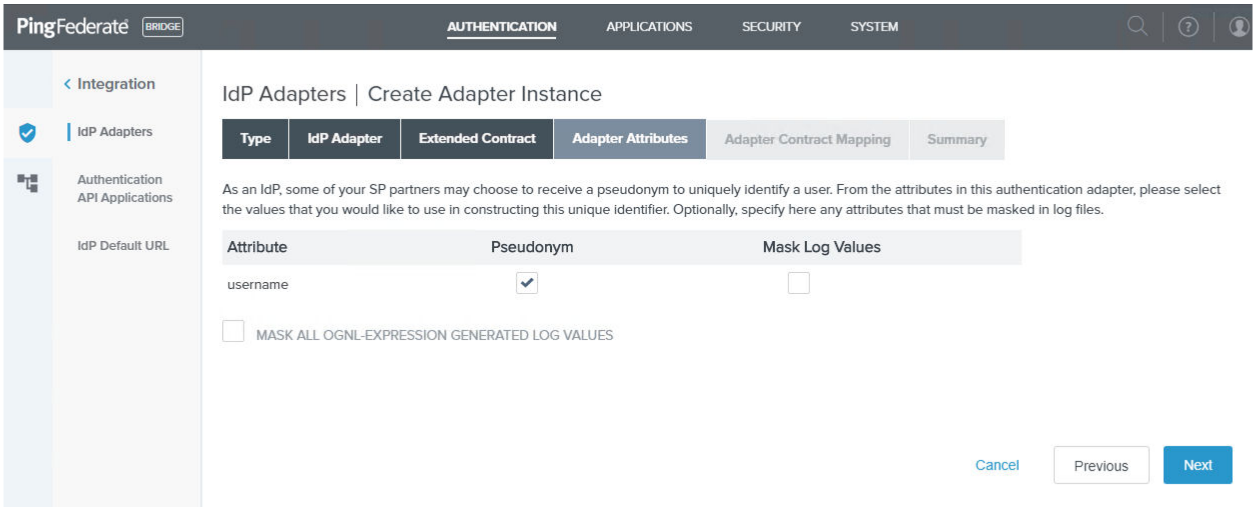


IdP Adapters | Create Adapter Instance

This adapter type supports the creation of an extended adapter contract after initial deployment of the adapter instance. This adapter contract may be used to fulfill the attribute contract, look up additional attributes from a local data store, or create a persistent name identifier which uniquely identifies the user passed to your SP partners.

Extend the Contract	Action
username	Add

8. *Adapter Attributes* tab, select the **Pseudonym** check box and click **Next**.



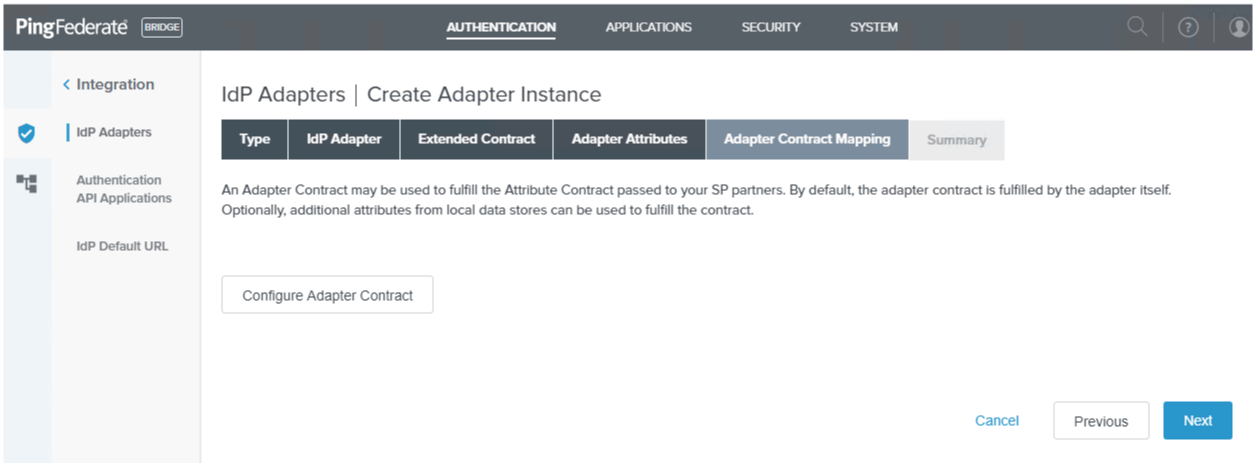
IdP Adapters | Create Adapter Instance

As an IdP, some of your SP partners may choose to receive a pseudonym to uniquely identify a user. From the attributes in this authentication adapter, please select the values that you would like to use in constructing this unique identifier. Optionally, specify here any attributes that must be masked in log files.

Attribute	Pseudonym	Mask Log Values
username	☑	□

□ MASK ALL OGNL-EXPRESSION GENERATED LOG VALUES

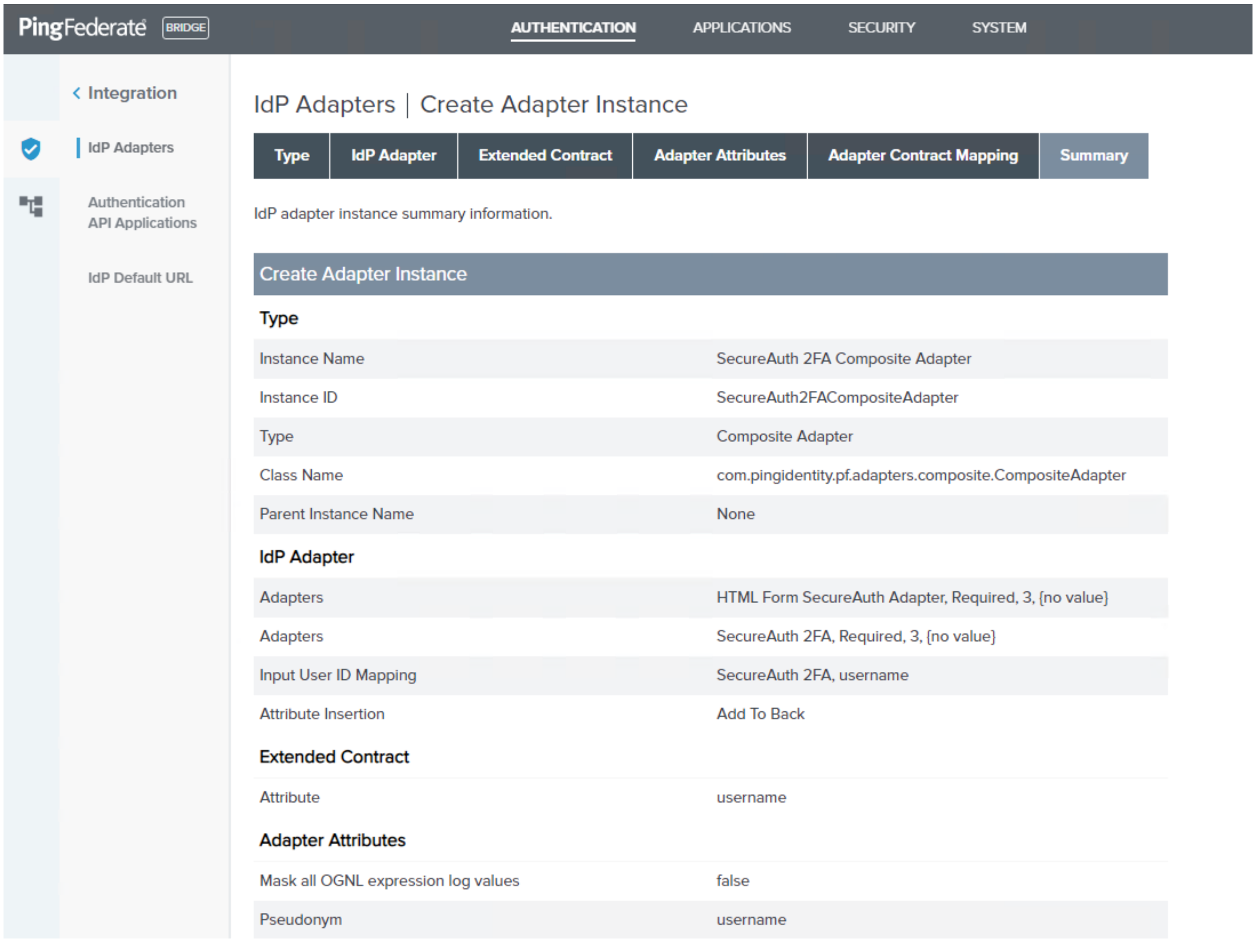
9. On Adapter Contract Mapping click **Next**



IdP Adapters | Create Adapter Instance

An Adapter Contract may be used to fulfill the Attribute Contract passed to your SP partners. By default, the adapter contract is fulfilled by the adapter itself. Optionally, additional attributes from local data stores can be used to fulfill the contract.

10. Review the summary page and click **Save**.

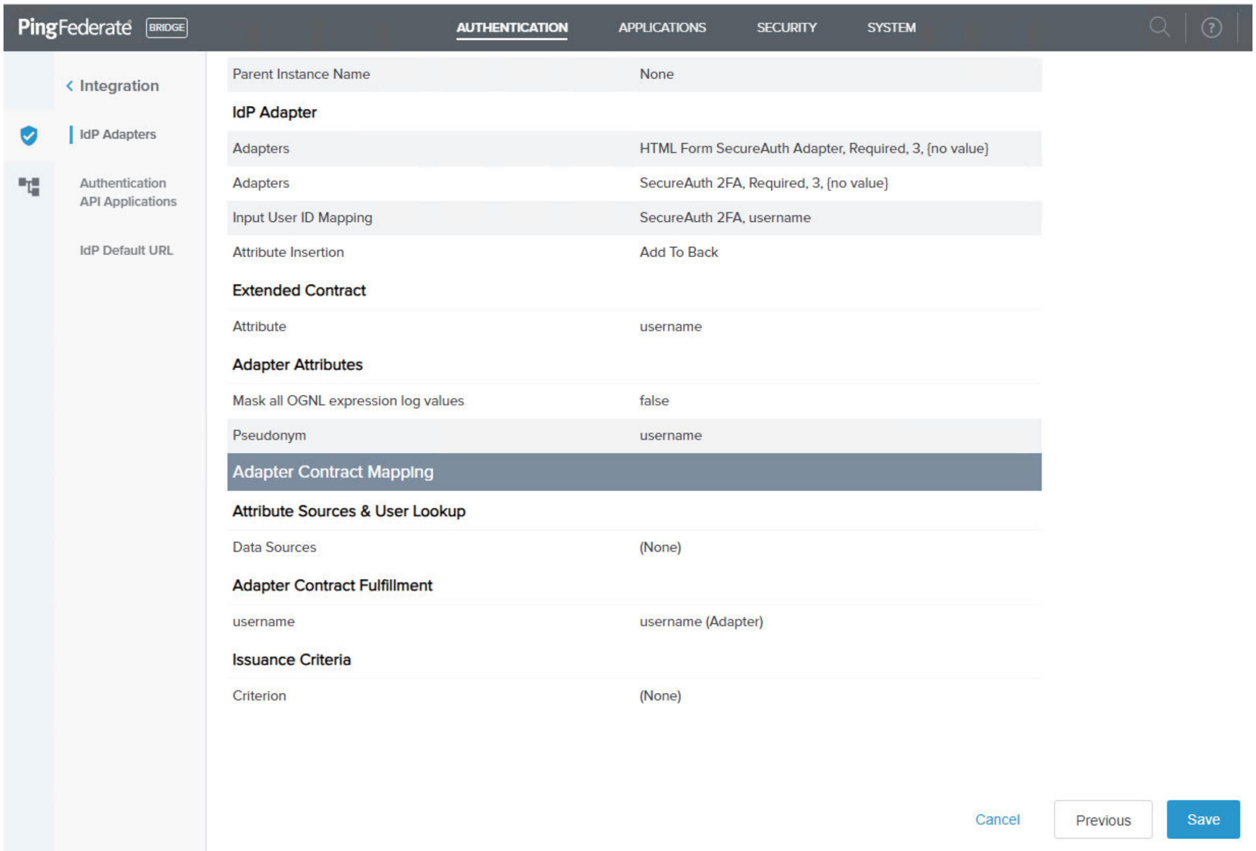


IdP Adapters | Create Adapter Instance

IdP adapter instance summary information.

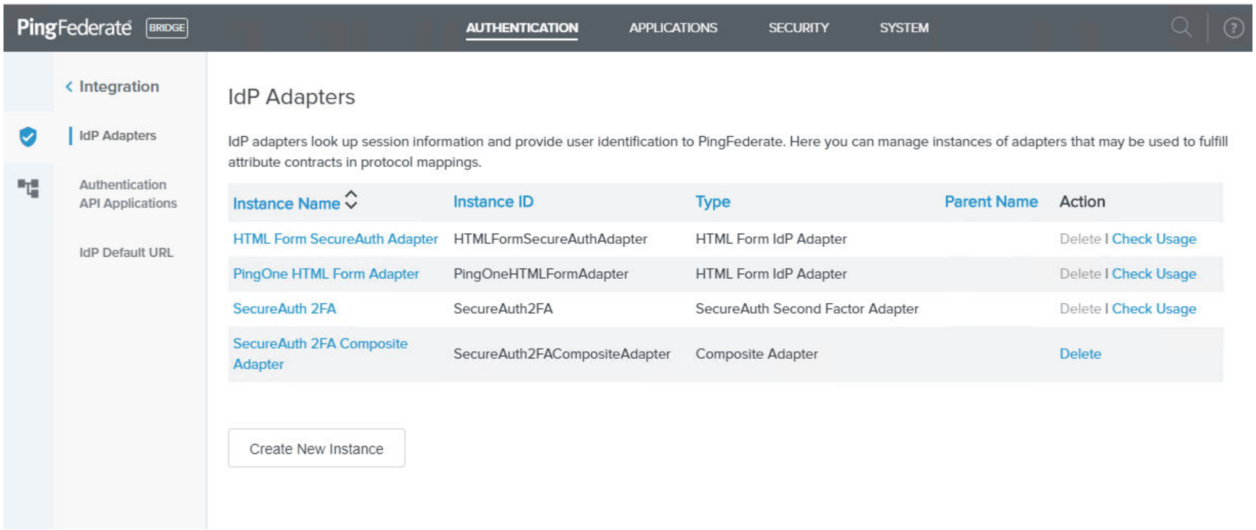
Create Adapter Instance

Type	
Instance Name	SecureAuth 2FA Composite Adapter
Instance ID	SecureAuth2FACompositeAdapter
Type	Composite Adapter
Class Name	com.pingidentity.pf.adapters.composite.CompositeAdapter
Parent Instance Name	None
IdP Adapter	
Adapters	HTML Form SecureAuth Adapter, Required, 3, {no value}
Adapters	SecureAuth 2FA, Required, 3, {no value}
Input User ID Mapping	SecureAuth 2FA, username
Attribute Insertion	Add To Back
Extended Contract	
Attribute	username
Adapter Attributes	
Mask all OGNL expression log values	false
Pseudonym	username



Parent Instance Name	None
IdP Adapter	
Adapters	HTML Form SecureAuth Adapter, Required, 3, (no value)
Adapters	SecureAuth 2FA, Required, 3, (no value)
Input User ID Mapping	SecureAuth 2FA, username
Attribute Insertion	Add To Back
Extended Contract	
Attribute	username
Adapter Attributes	
Mask all OGNL expression log values	false
Pseudonym	username
Adapter Contract Mapping	
Attribute Sources & User Lookup	
Data Sources	(None)
Adapter Contract Fulfillment	
username	username (Adapter)
Issuance Criteria	
Criterion	(None)

11. See the SecureAuth 2FA composite adapter instance in the list.



IdP Adapters

IdP adapters look up session information and provide user identification to PingFederate. Here you can manage instances of adapters that may be used to fulfill attribute contracts in protocol mappings.

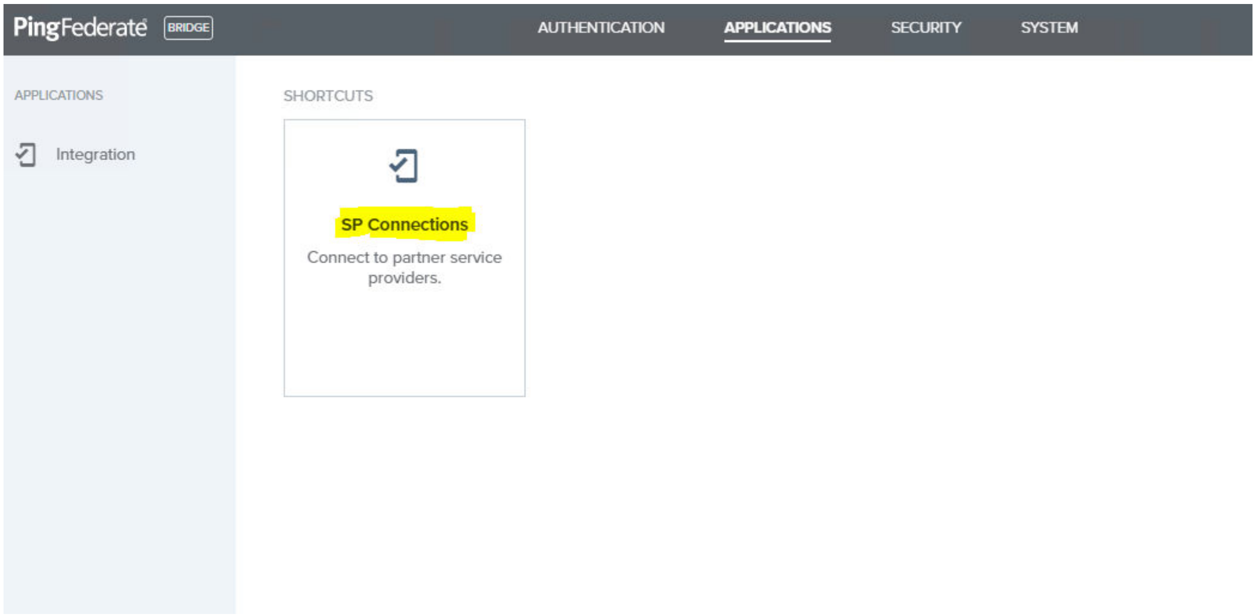
Instance Name	Instance ID	Type	Parent Name	Action
HTML Form SecureAuth Adapter	HTMLFormSecureAuthAdapter	HTML Form IdP Adapter		Delete I Check Usage
PingOne HTML Form Adapter	PingOneHTMLFormAdapter	HTML Form IdP Adapter		Delete I Check Usage
SecureAuth 2FA	SecureAuth2FA	SecureAuth Second Factor Adapter		Delete I Check Usage
SecureAuth 2FA Composite Adapter	SecureAuth2FACompositeAdapter	Composite Adapter		Delete

Create service provider (SP) connections

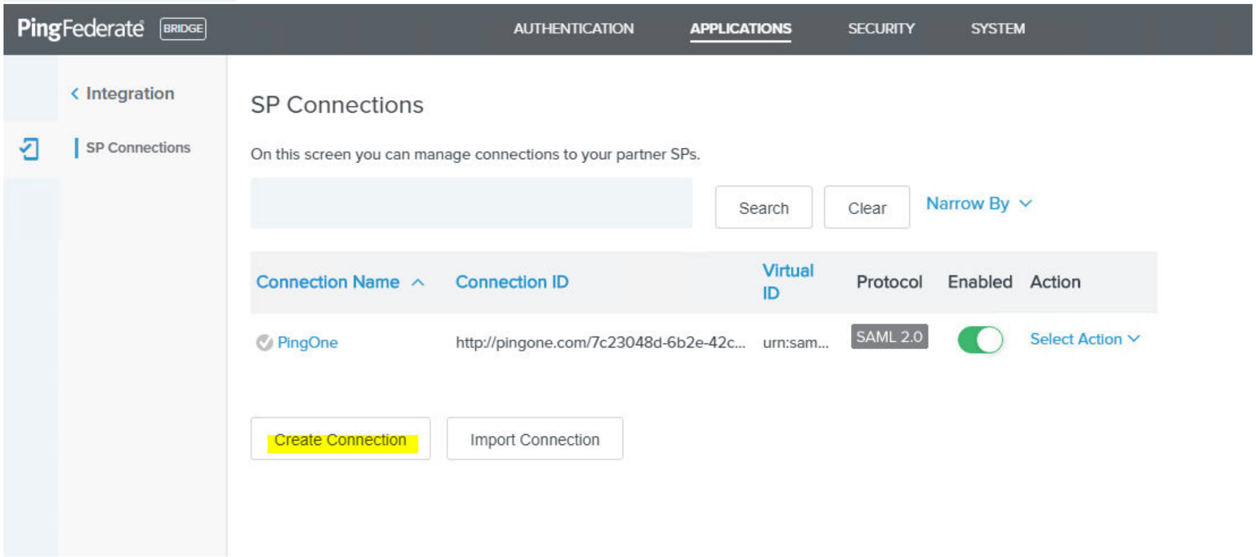
When the required composite adapter is created, the next step is to connect the existing service provider (SP) instances.

To create SP connections

1. In PingFederate, select **APPLICATIONS**, and click on **SP Connections** section and then click on **Create Connection**.



Connect to partner service providers.

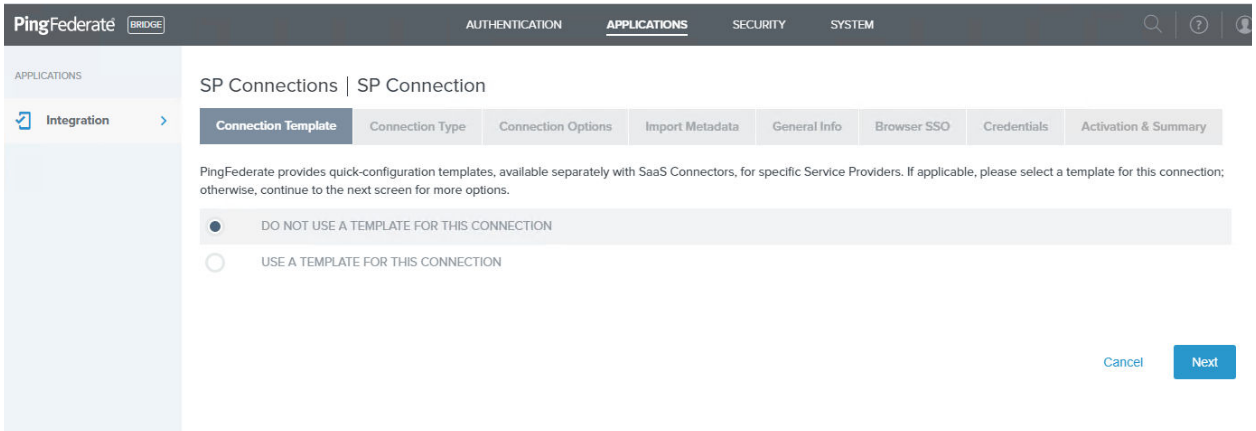


SP Connections

On this screen you can manage connections to your partner SPs.

Connection Name	Connection ID	Virtual ID	Protocol	Enabled	Action
PingOne	http://pingone.com/7c23048d-6b2e-42c...	urn:sam...	SAML 2.0	●	Select Action

2. Connection Template tab select **DO NOT USE A TEMPLATE FOR THIS CONNECTION** and then click **Next.**



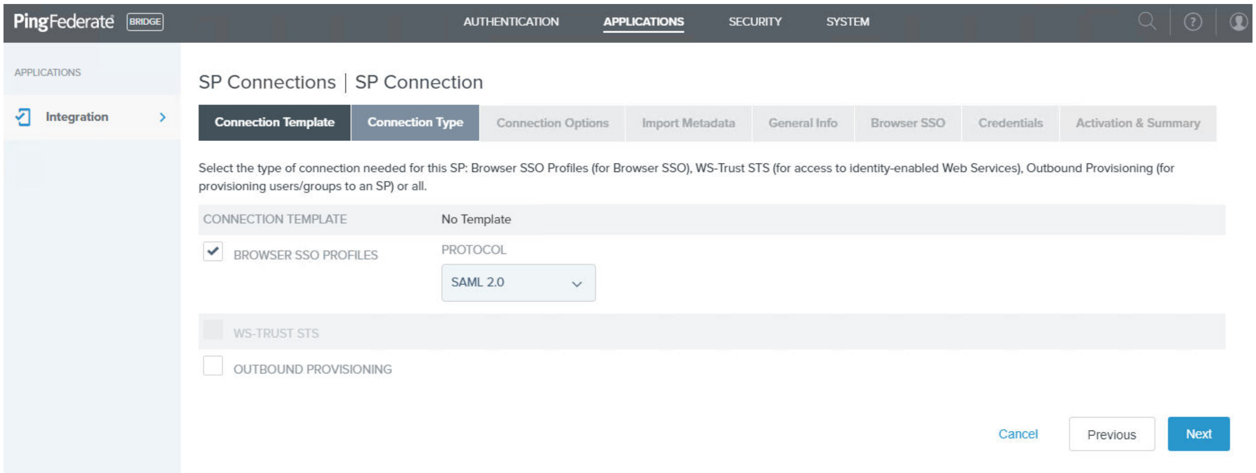
SP Connections | SP Connection

PingFederate provides quick-configuration templates, available separately with SaaS Connectors, for specific Service Providers. If applicable, please select a template for this connection; otherwise, continue to the next screen for more options.

● DO NOT USE A TEMPLATE FOR THIS CONNECTION

○ USE A TEMPLATE FOR THIS CONNECTION

2. *Connection Type* tab on the SP Connection page, select the **Browser SSO Profiles** check box and click **Next**.



SP Connections | SP Connection

Select the type of connection needed for this SP: Browser SSO Profiles (for Browser SSO), WS-Trust STS (for access to identity-enabled Web Services), Outbound Provisioning (for provisioning users/groups to an SP) or all.

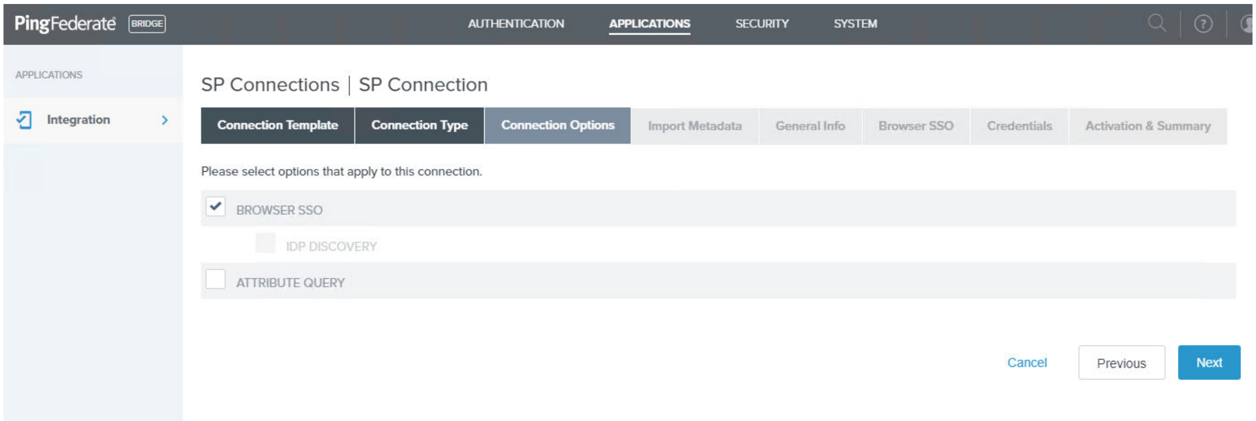
CONNECTION TEMPLATE No Template

☑ BROWSER SSO PROFILES PROTOCOL SAML 2.0

□ WS-TRUST STS

□ OUTBOUND PROVISIONING

3. In the *Connection Options* tab, select the **Browser SSO** check box and click **Next**.



SP Connections | SP Connection

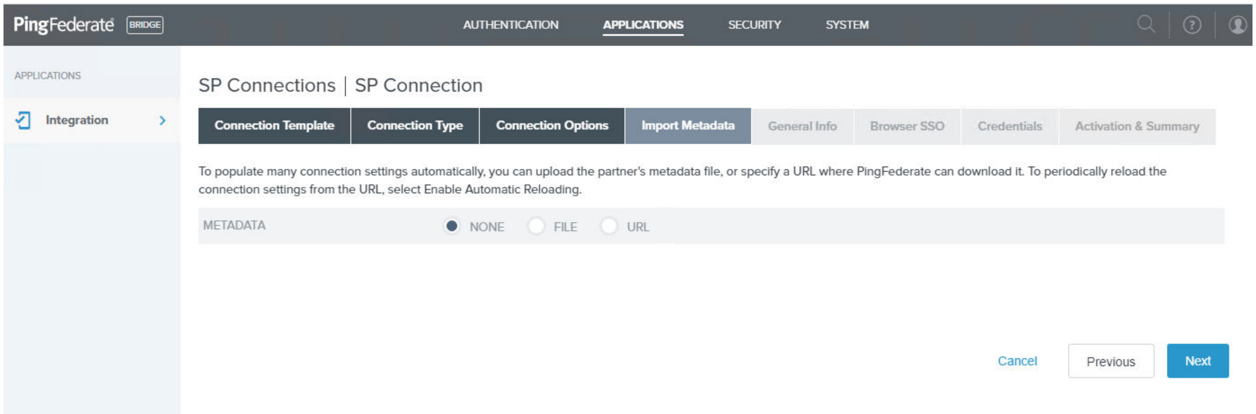
Please select options that apply to this connection.

☑ BROWSER SSO

□ IDP DISCOVERY

□ ATTRIBUTE QUERY

4. In the *Import Metadata* tab, click **Next**.



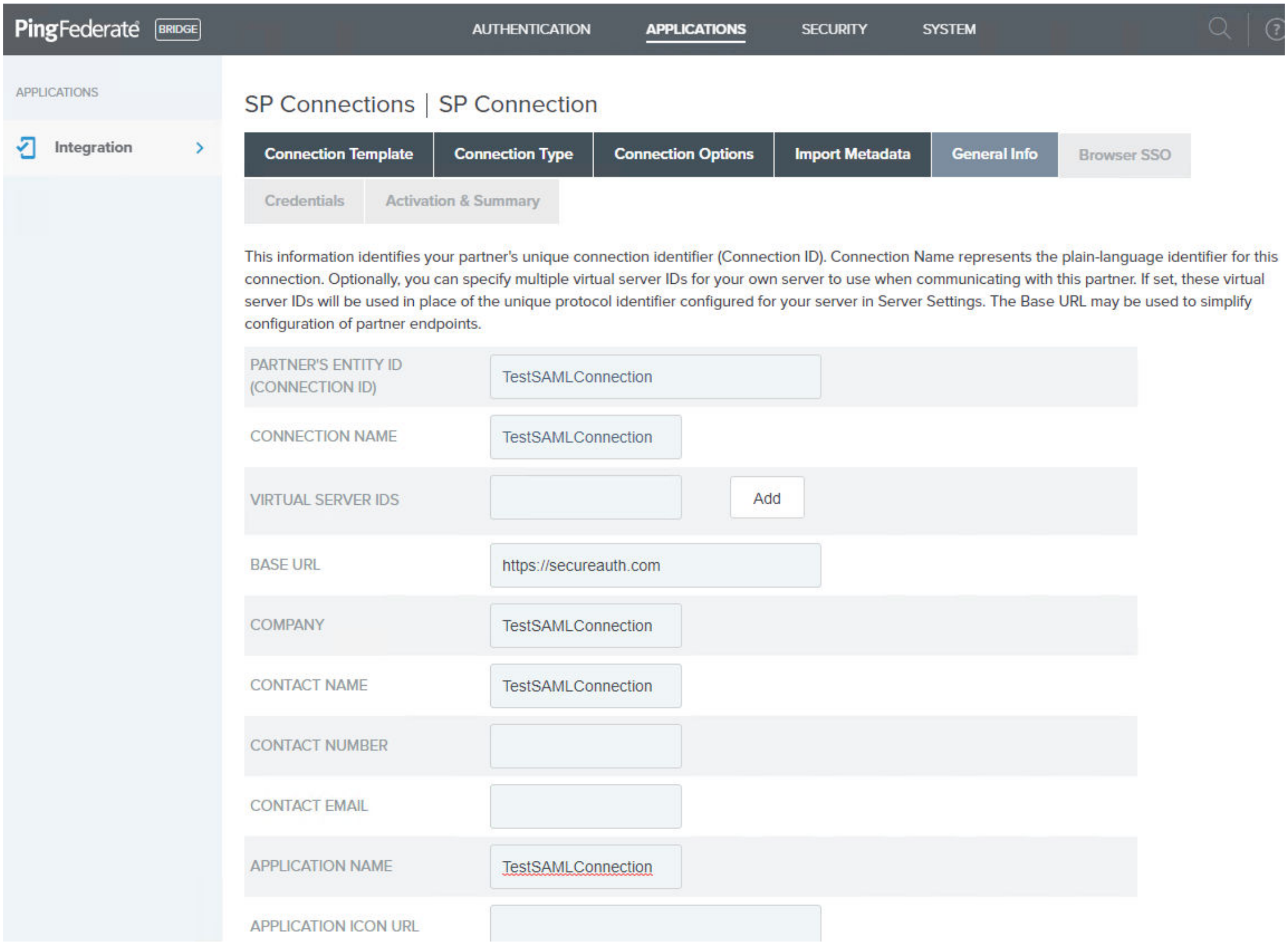
SP Connections | SP Connection

To populate many connection settings automatically, you can upload the partner's metadata file, or specify a URL where PingFederate can download it. To periodically reload the connection settings from the URL, select Enable Automatic Reloading.

METADATA ● NONE ○ FILE ○ URL

5. In the *General Info* tab, set the following:

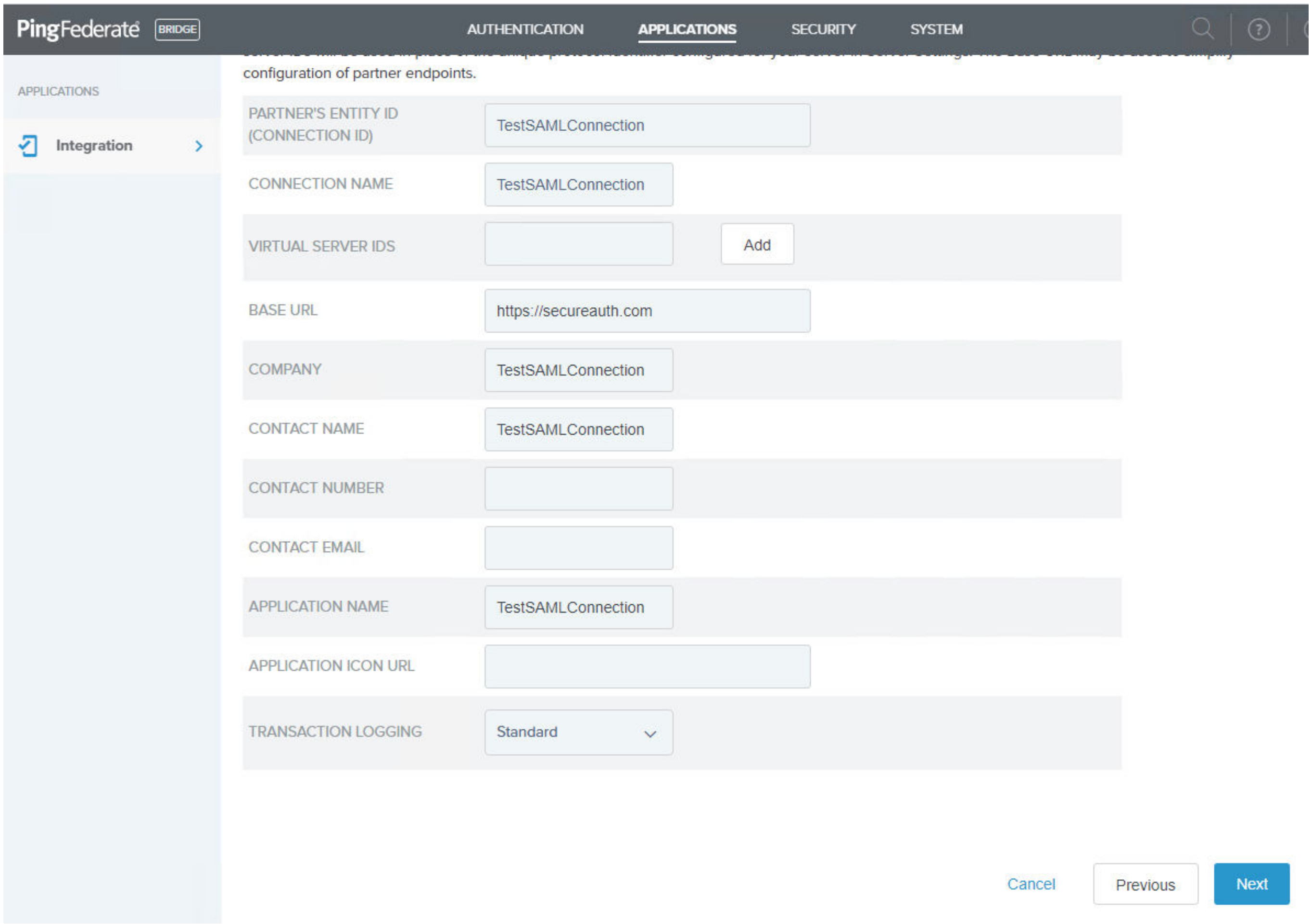
Field	**Description**
Partner's Entity ID (Connection ID)	The ID for this SP connection
Field	**Description**
Connection Name	Name of this SP connection
Base URL	Base URL for this SP connection
Company	Name of the company to which this SP connects to
Contact Name	Contact name for this SP connection
Application Name	Name of the application to which the connection accesses
Logging Mode	Set to **Standard**



SP Connections | SP Connection

This information identifies your partner's unique connection identifier (Connection ID). Connection Name represents the plain-language identifier for this connection. Optionally, you can specify multiple virtual server IDs for your own server to use when communicating with this partner. If set, these virtual server IDs will be used in place of the unique protocol identifier configured for your server in Server Settings. The Base URL may be used to simplify configuration of partner endpoints.

PARTNER'S ENTITY ID (CONNECTION ID)	TestSAMLConnection
CONNECTION NAME	TestSAMLConnection
VIRTUAL SERVER IDS	Add
BASE URL	https://secureauth.com
COMPANY	TestSAMLConnection
CONTACT NAME	TestSAMLConnection
CONTACT NUMBER	
CONTACT EMAIL	
APPLICATION NAME	TestSAMLConnection
APPLICATION ICON URL	



configuration of partner endpoints.

PARTNER'S ENTITY ID (CONNECTION ID): TestSAMLConnection

CONNECTION NAME: TestSAMLConnection

VIRTUAL SERVER IDS: Add

BASE URL: https://secureauth.com

COMPANY: TestSAMLConnection

CONTACT NAME: TestSAMLConnection

CONTACT NUMBER:

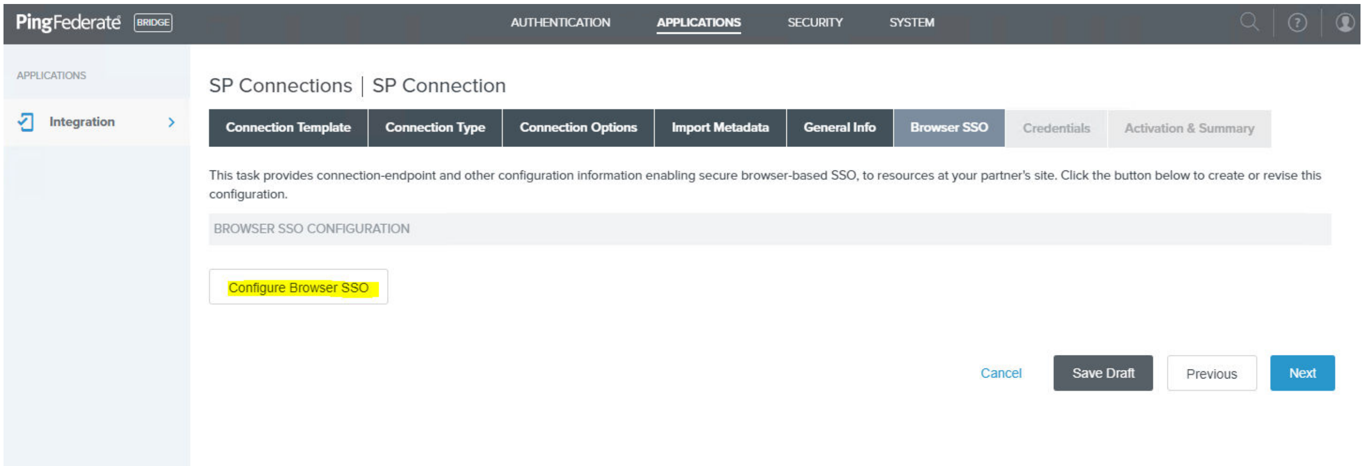
CONTACT EMAIL:

APPLICATION NAME: TestSAMLConnection

APPLICATION ICON URL:

TRANSACTION LOGGING: Standard

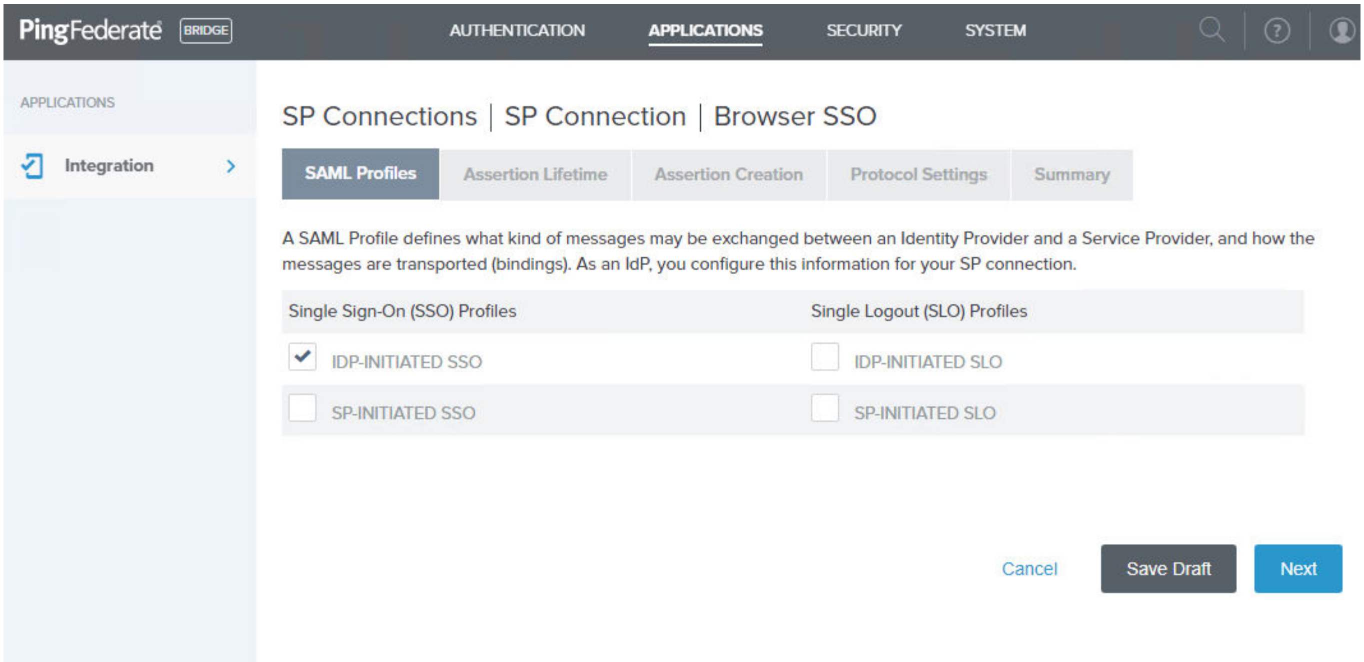
6. Click **Next**.
7. In the *Browser SSO* tab, click **Configure Browser SSO**.



This task provides connection-endpoint and other configuration information enabling secure browser-based SSO, to resources at your partner's site. Click the button below to create or revise this configuration.

BROWSER SSO CONFIGURATION

8. *SSO Profiles* tab on the SP Connection | Browser SSO page, select the **IDP-Initiated SSO** check box and click **Next**.

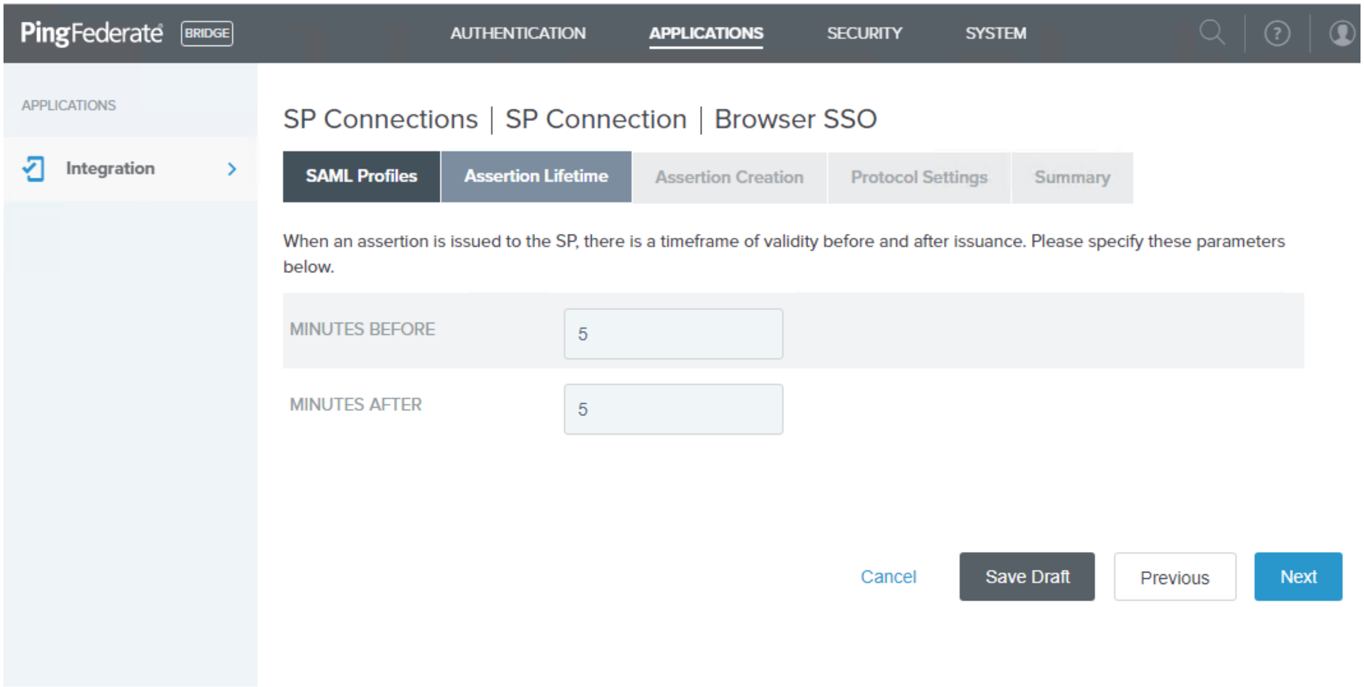


SP Connections | SP Connection | Browser SSO

A SAML Profile defines what kind of messages may be exchanged between an Identity Provider and a Service Provider, and how the messages are transported (bindings). As an IdP, you configure this information for your SP connection.

Single Sign-On (SSO) Profiles	Single Logout (SLO) Profiles
☑ IDP-INITIATED SSO	□ IDP-INITIATED SLO
□ SP-INITIATED SSO	□ SP-INITIATED SLO

9. In the *Assertion Lifetime* tab, click **Next**.



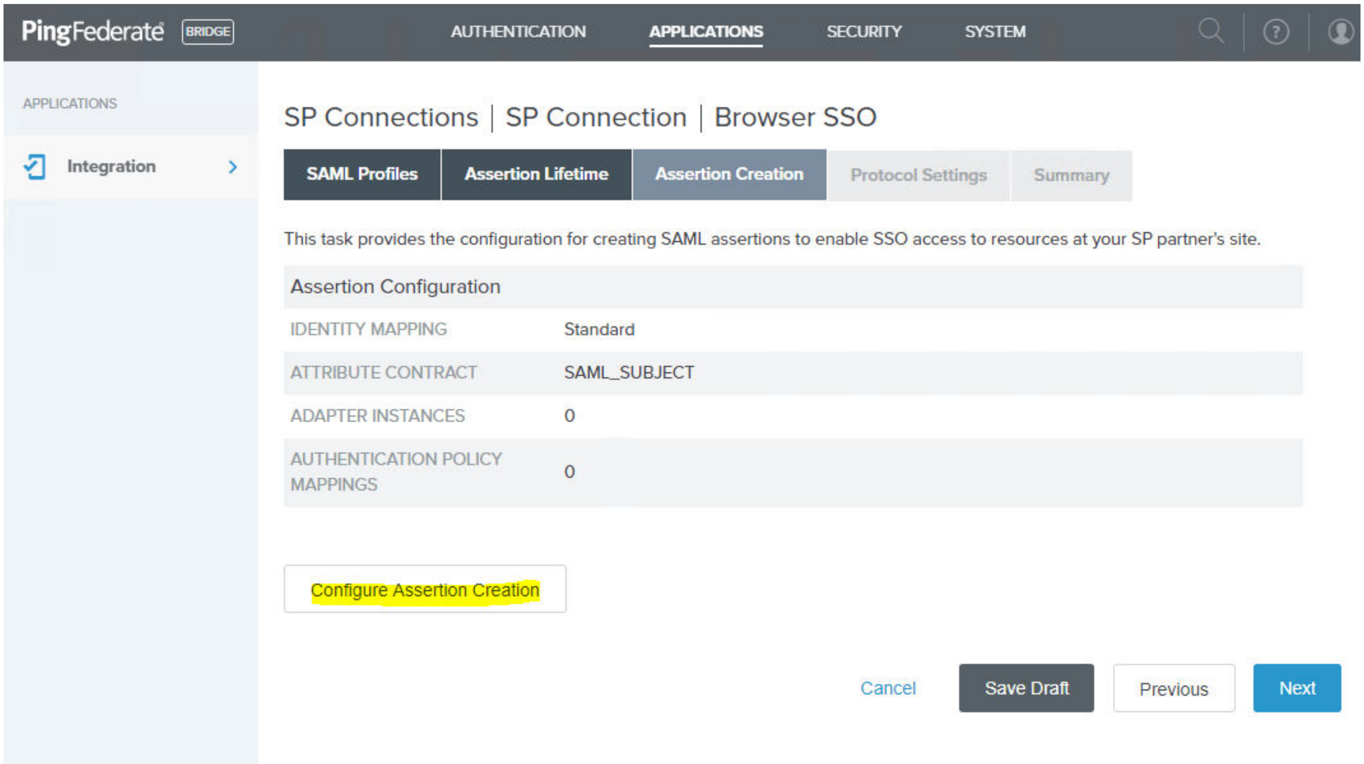
SP Connections | SP Connection | Browser SSO

When an assertion is issued to the SP, there is a timeframe of validity before and after issuance. Please specify these parameters below.

MINUTES BEFORE: 5

MINUTES AFTER: 5

10. In the *Assertion Creation* tab, click **Configure Assertion Creation**.

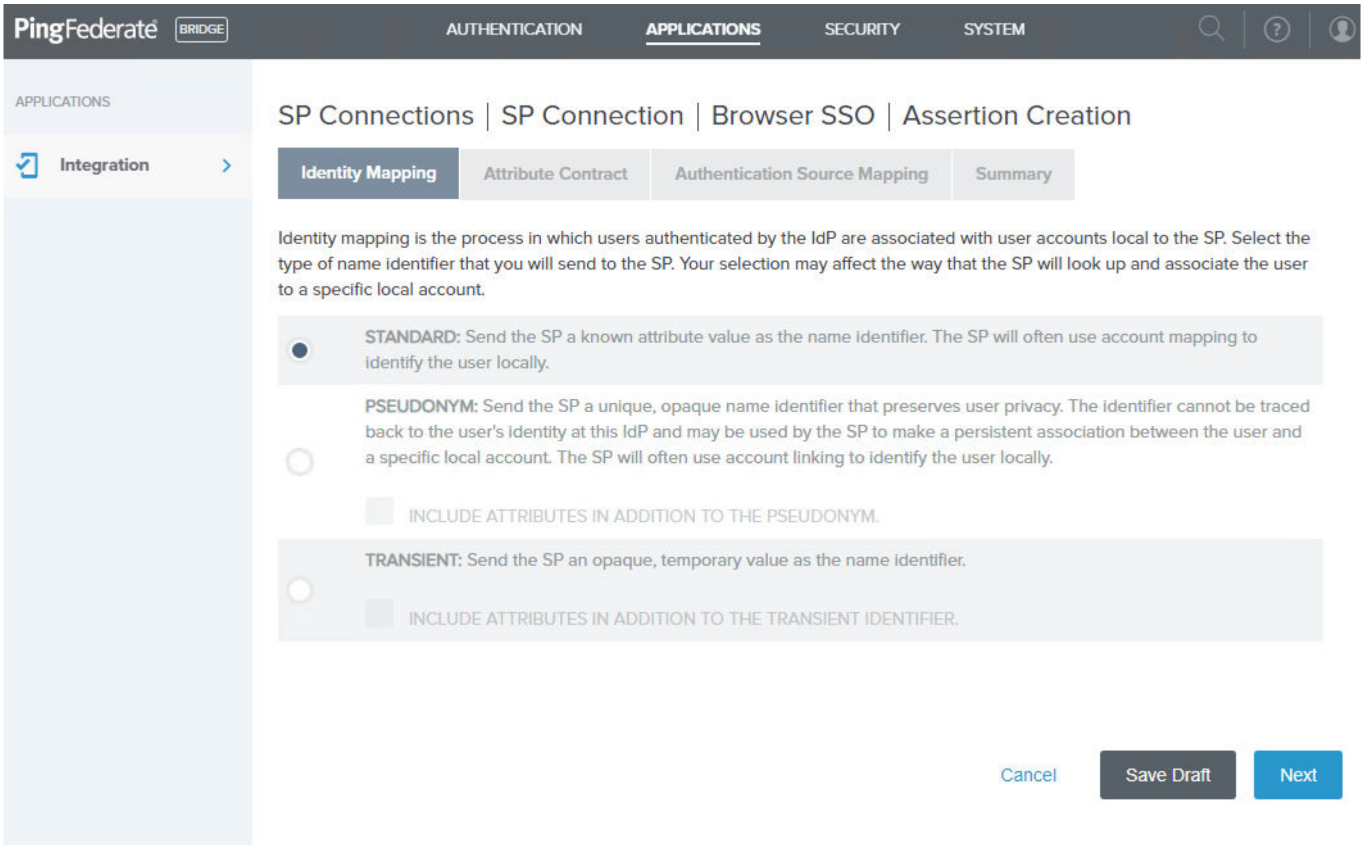


SP Connections | SP Connection | Browser SSO

This task provides the configuration for creating SAML assertions to enable SSO access to resources at your SP partner's site.

Assertion Configuration	
IDENTITY MAPPING	Standard
ATTRIBUTE CONTRACT	SAML_SUBJECT
ADAPTER INSTANCES	0
AUTHENTICATION POLICY MAPPINGS	0

11. In the *Identity Mapping* tab on the SP Connection | Browser SSO |Assertion Creation page, make sure the **Standard** option is selected and click **Next**.



SP Connections | SP Connection | Browser SSO | Assertion Creation

Identity Mapping | Attribute Contract | Authentication Source Mapping | Summary

Identity mapping is the process in which users authenticated by the IdP are associated with user accounts local to the SP. Select the type of name identifier that you will send to the SP. Your selection may affect the way that the SP will look up and associate the user to a specific local account.

● STANDARD: Send the SP a known attribute value as the name identifier. The SP will often use account mapping to identify the user locally.

○ PSEUDONYM: Send the SP a unique, opaque name identifier that preserves user privacy. The identifier cannot be traced back to the user's identity at this IdP and may be used by the SP to make a persistent association between the user and a specific local account. The SP will often use account linking to identify the user locally.

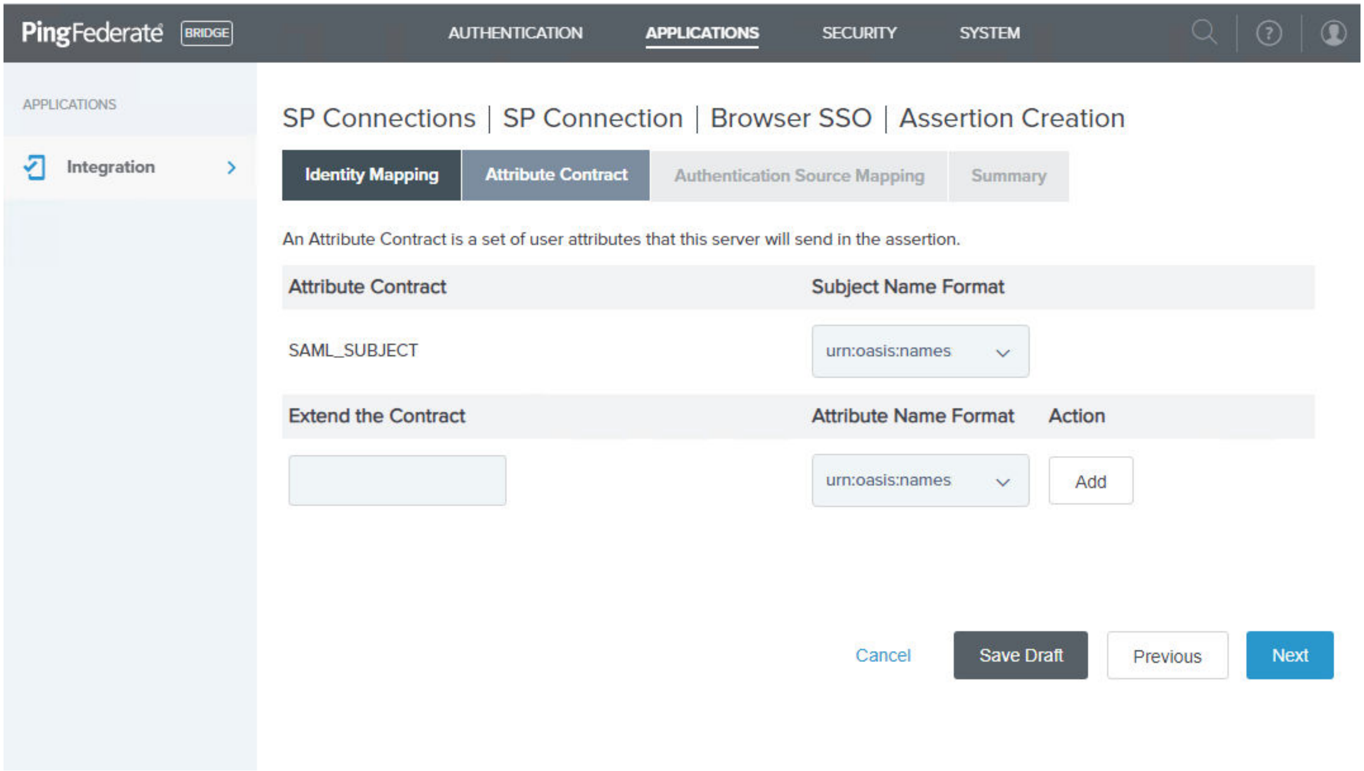
□ INCLUDE ATTRIBUTES IN ADDITION TO THE PSEUDONYM.

○ TRANSIENT: Send the SP an opaque, temporary value as the name identifier.

□ INCLUDE ATTRIBUTES IN ADDITION TO THE TRANSIENT IDENTIFIER.

12. In the *Attribute Contract* tab, in the set the SAML subject name format and click **Next**.

    For example, set to **urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified**

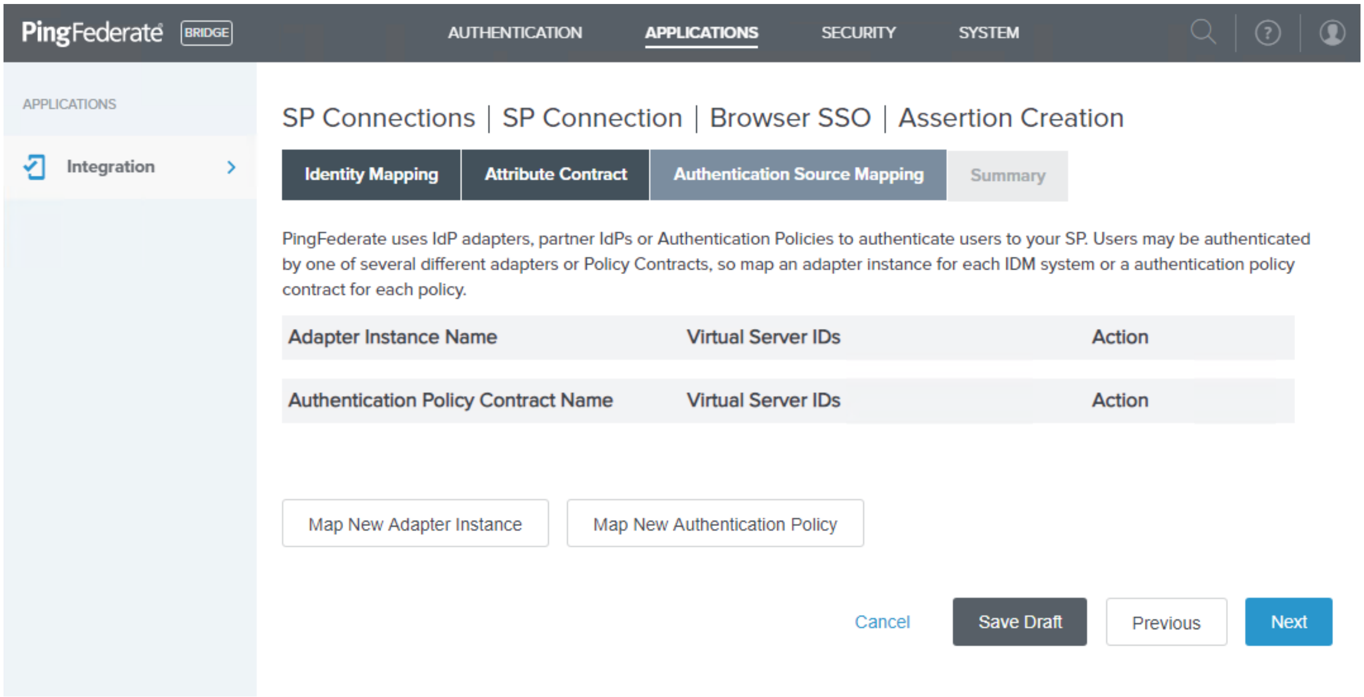


SP Connections | SP Connection | Browser SSO | Assertion Creation

An Attribute Contract is a set of user attributes that this server will send in the assertion.

Attribute Contract	Subject Name Format	
SAML_SUBJECT	urn:oasis:names	
Extend the Contract	**Attribute Name Format**	**Action**
	urn:oasis:names	Add

13. In the *Authentication Source Mapping* tab, click **Map New Adapter instance**.



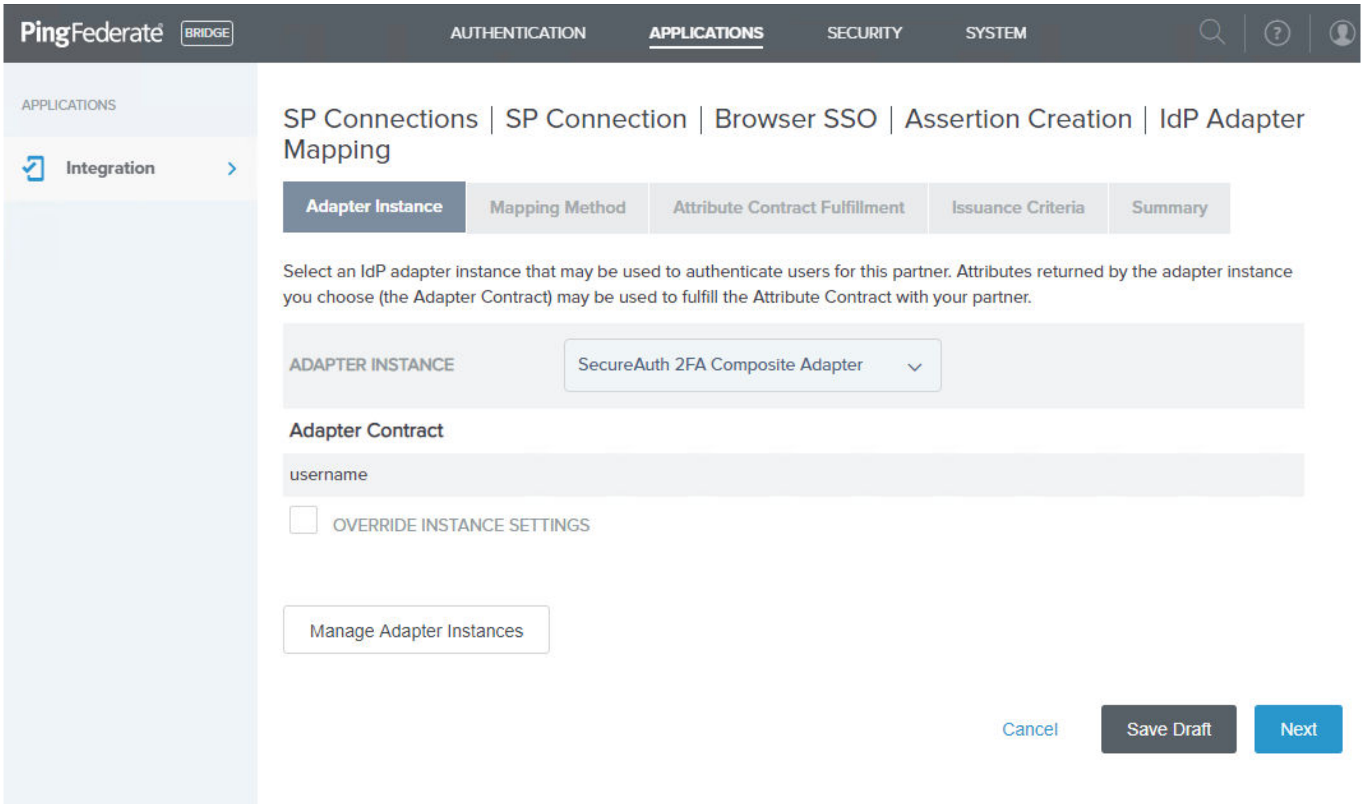
SP Connections | SP Connection | Browser SSO | Assertion Creation

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 Policy Contracts, so map an adapter instance for each IDM system or a authentication policy contract for each policy.

Adapter Instance Name	Virtual Server IDs	Action

Authentication Policy Contract Name	Virtual Server IDs	Action

14. *Adapter Instance* tab on the SP Connection | Browser SSO |Assertion Creation | IdP Adapter Mapping page, set the **Adapter Instance** to **SecureAuth2FAComp** and click **Next**.



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

Select an IdP adapter instance that may be used to authenticate users for this partner. Attributes returned by the adapter instance you choose (the Adapter Contract) may be used to fulfill the Attribute Contract with your partner.

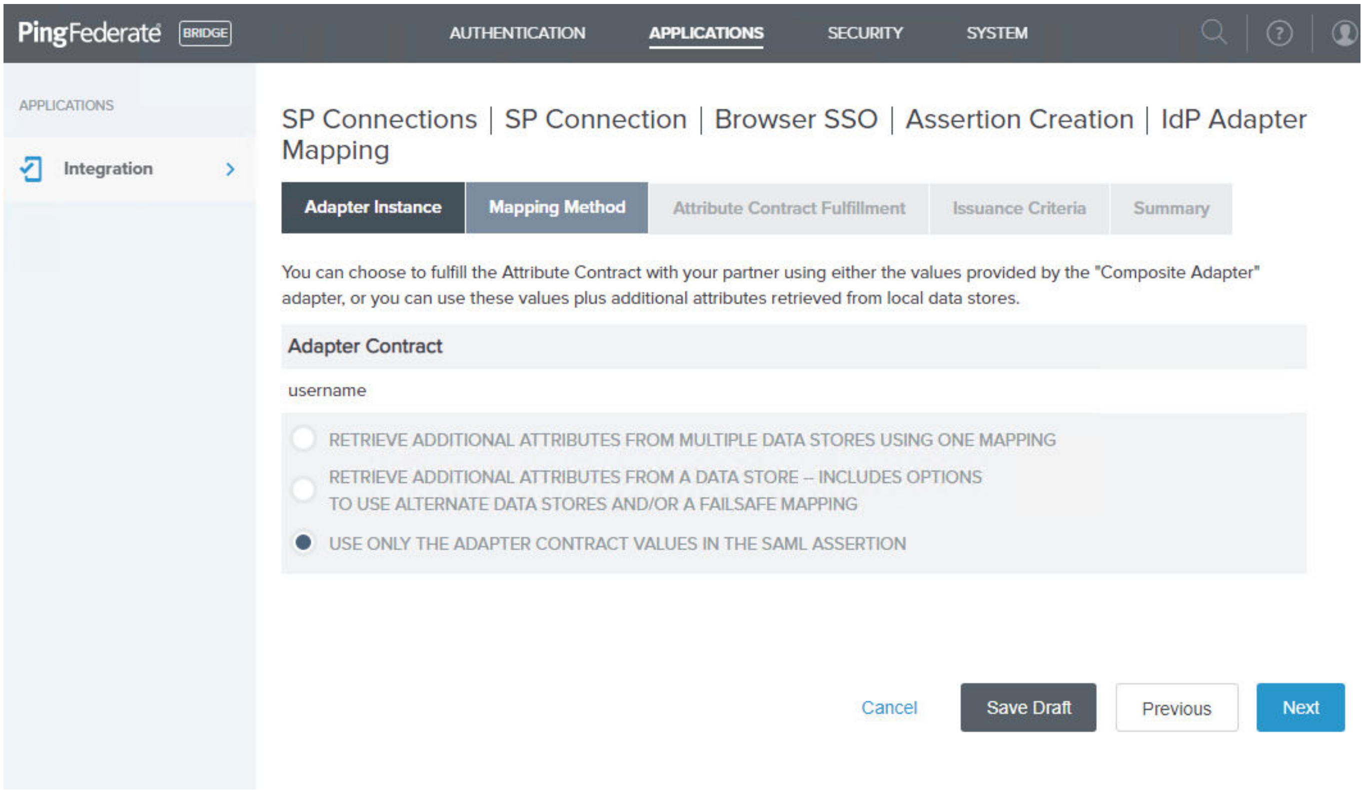
ADAPTER INSTANCE: SecureAuth 2FA Composite Adapter

Adapter Contract

username

□ OVERRIDE INSTANCE SETTINGS

15. In the *Mapping Method* tab, select the **Use only the adapter contract values in the SAML assertion** option and click **Next**.



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

You can choose to fulfill the Attribute Contract with your partner using either the values provided by the "Composite Adapter" adapter, or you can use these values plus additional attributes retrieved from local data stores.

Adapter Contract

username

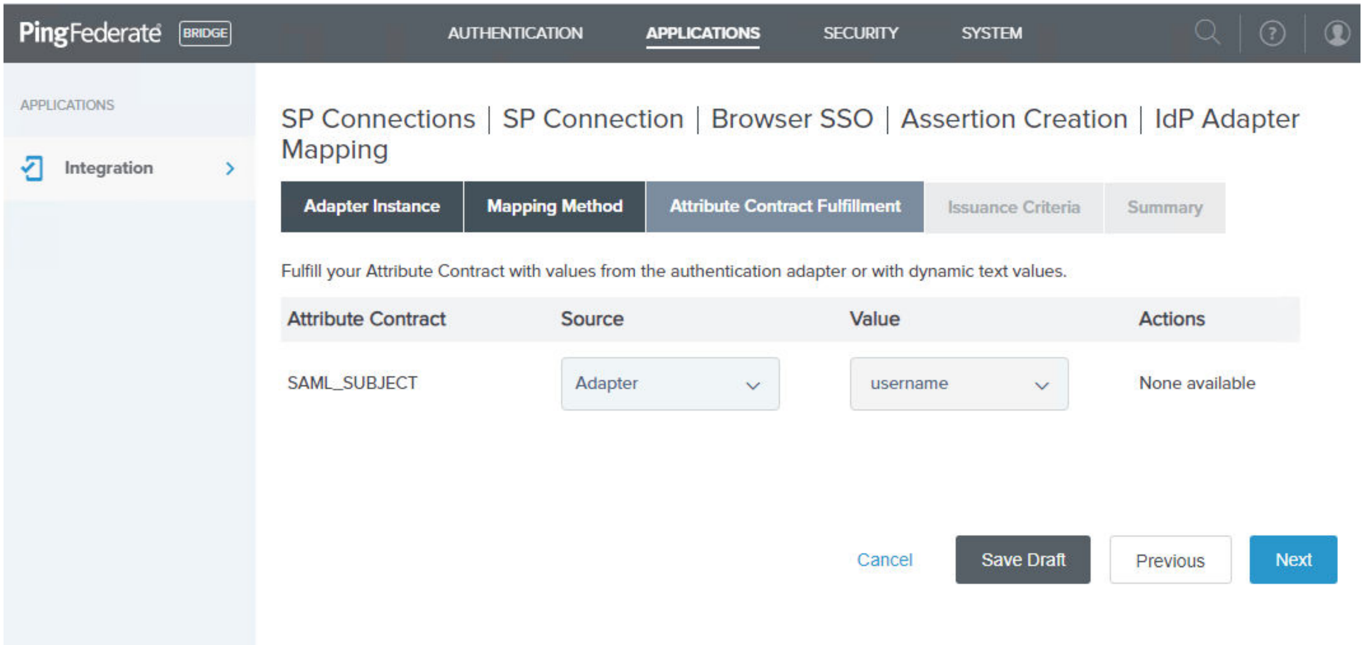
○ RETRIEVE ADDITIONAL ATTRIBUTES FROM MULTIPLE DATA STORES USING ONE MAPPING

○ RETRIEVE ADDITIONAL ATTRIBUTES FROM A DATA STORE – INCLUDES OPTIONS TO USE ALTERNATE DATA STORES AND/OR A FAILSAFE MAPPING

● USE ONLY THE ADAPTER CONTRACT VALUES IN THE SAML ASSERTION

16. In the *Attribute Contract Fulfillment* tab, set the following for the SAML_Subject attribute contract: a. Set the **Source** to **Adapter**.

    b. Set the **Value** to **username**.

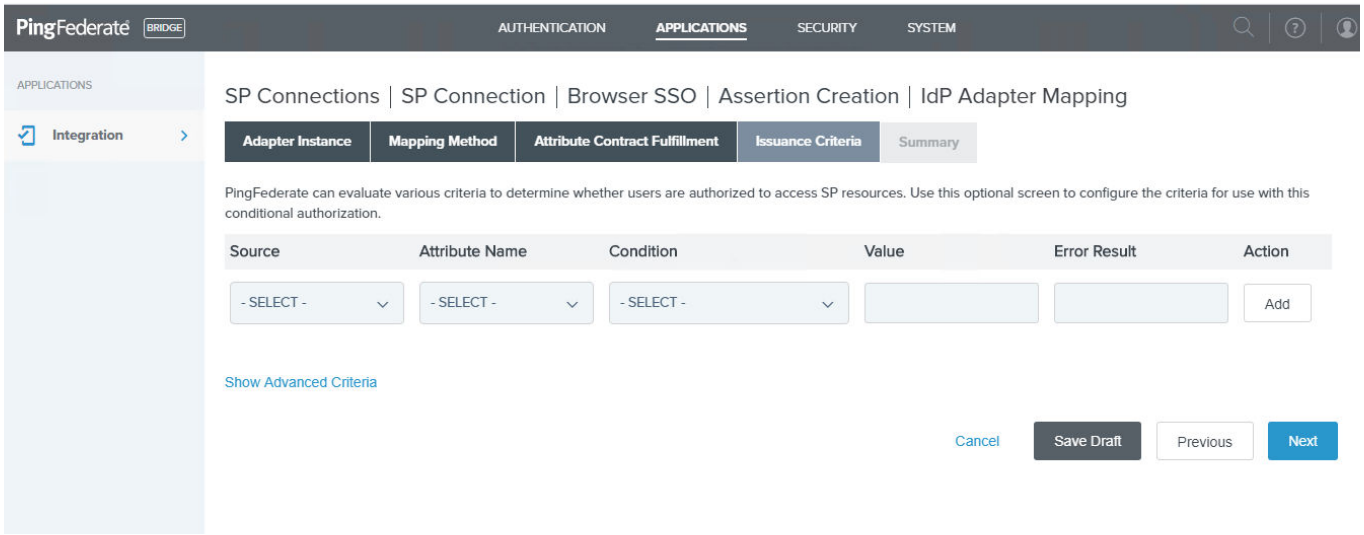


SP Connections | SP Connection | Browser SSO | Assertion Creation | IdP Adapter Mapping

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

Attribute Contract	Source	Value	Actions
SAML_SUBJECT	Adapter	username	None available

17. In the *Issuance Criteria* tab, click **Next**.

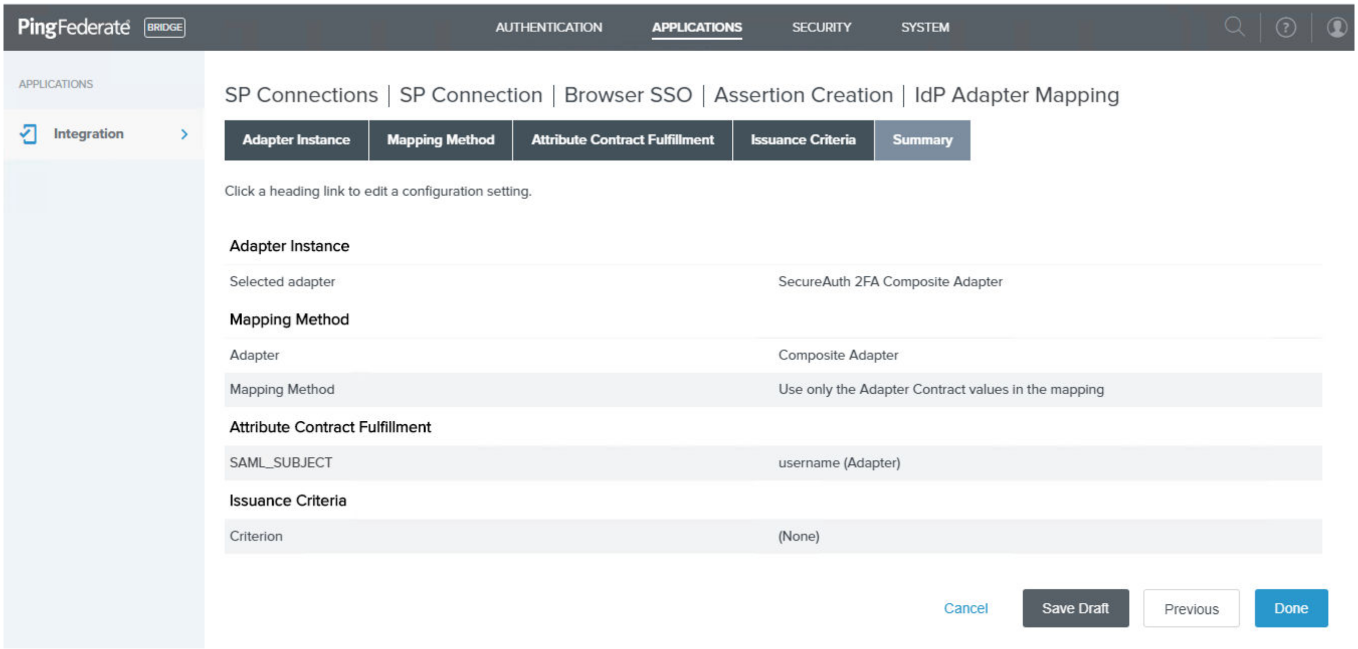


SP Connections | SP Connection | Browser SSO | Assertion Creation | IdP Adapter Mapping

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

18. Review the *Summary* tab and click **Done**.



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

Click a heading link to edit a configuration setting.

Adapter Instance

Selected adapter	SecureAuth 2FA Composite Adapter

Mapping Method

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

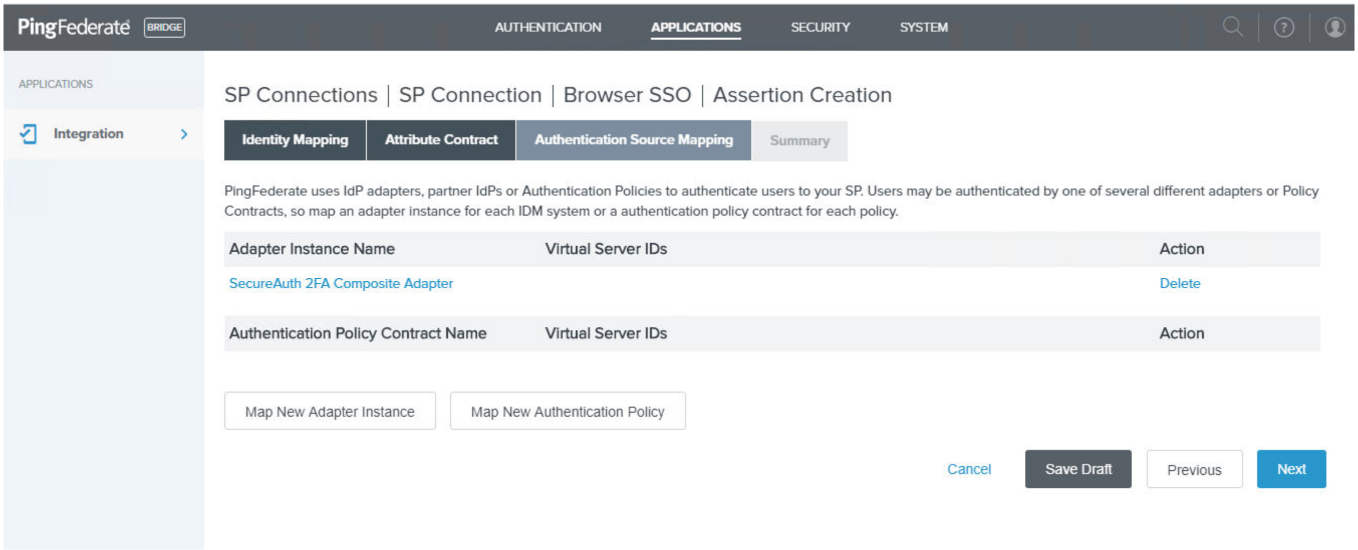
Attribute Contract Fulfillment

SAML_SUBJECT	username (Adapter)

Issuance Criteria

Criterion	(None)

19. In the *Authentication Source Mapping* tab on the SP Connection | Browser SSO |Assertion Creation page, click **Next**.



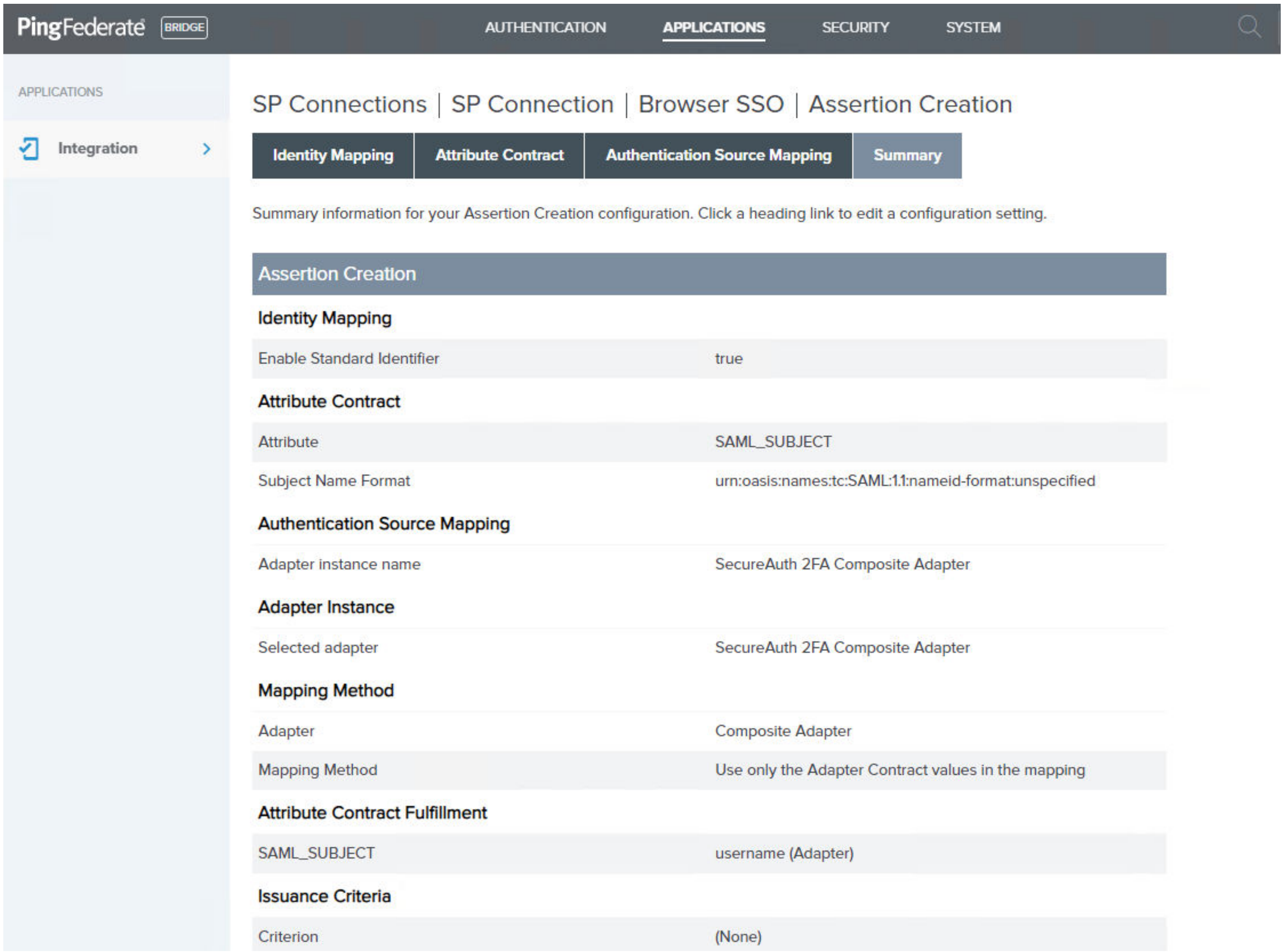
SP Connections | SP Connection | Browser SSO | Assertion Creation

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 Policy Contracts, so map an adapter instance for each IDM system or a authentication policy contract for each policy.

Adapter Instance Name	Virtual Server IDs	Action
SecureAuth 2FA Composite Adapter		Delete

Authentication Policy Contract Name	Virtual Server IDs	Action

20. Review the *Summary* tab and click **Save**.

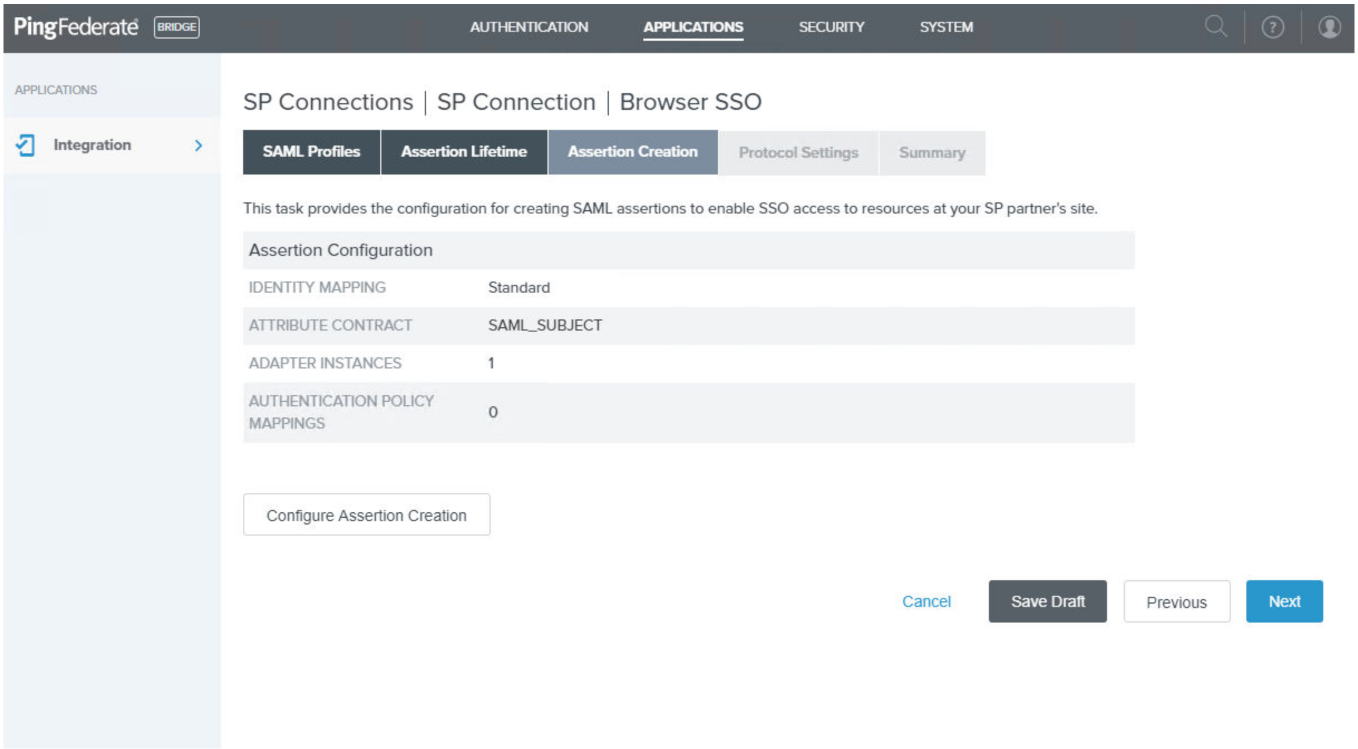


SP Connections | SP Connection | Browser SSO | Assertion Creation

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	SecureAuth 2FA Composite Adapter
Adapter Instance	
Selected adapter	SecureAuth 2FA Composite Adapter
Mapping Method	
Adapter	Composite Adapter
Mapping Method	Use only the Adapter Contract values in the mapping
Attribute Contract Fulfillment	
SAML_SUBJECT	username (Adapter)
Issuance Criteria	
Criterion	(None)

21. Assertion Creation page click **Next**



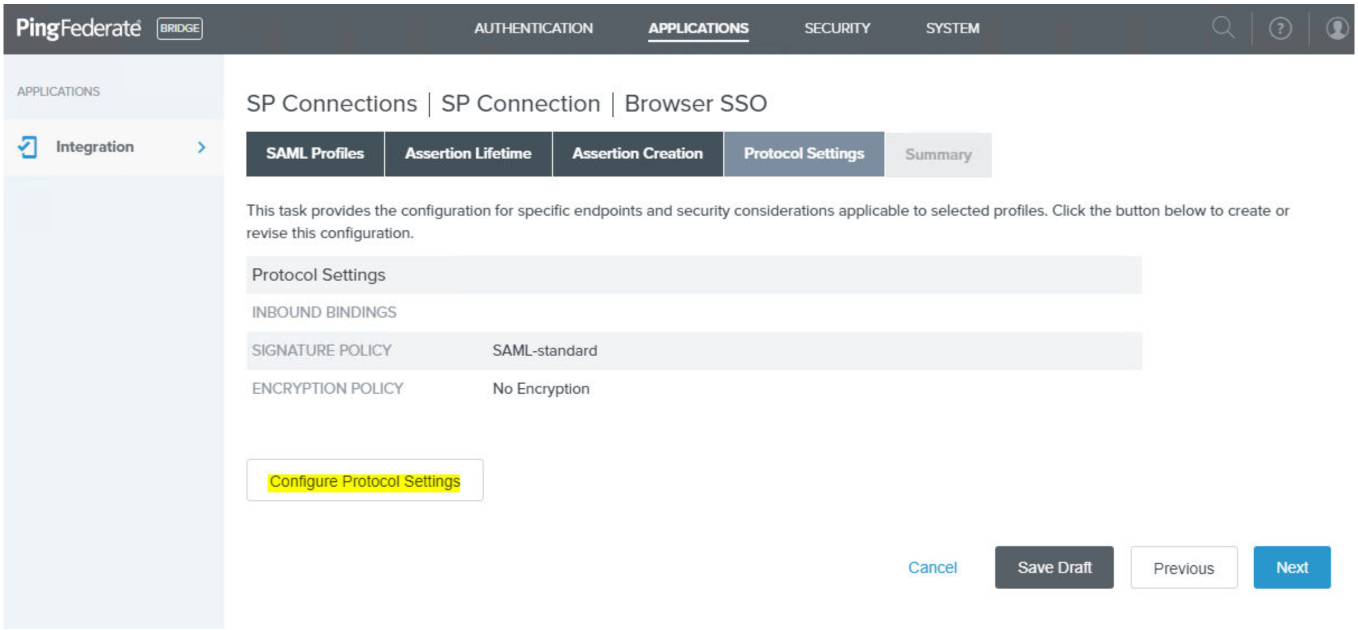
SP Connections | SP Connection | Browser SSO

This task provides the configuration for creating SAML assertions to enable SSO access to resources at your SP partner's site.

Assertion Configuration

IDENTITY MAPPING	Standard
ATTRIBUTE CONTRACT	SAML_SUBJECT
ADAPTER INSTANCES	1
AUTHENTICATION POLICY MAPPINGS	0

22. In the *Protocol Settings* tab on the SP Connection | Browser SSO page, click **Configure Protocol Settings**.



SP Connections | SP Connection | Browser SSO

This task provides the configuration for specific endpoints and security considerations applicable to selected profiles. Click the button below to create or revise this configuration.

Protocol Settings

INBOUND BINDINGS	
SIGNATURE POLICY	SAML-standard
ENCRYPTION POLICY	No Encryption

23. In the *Assertion Consumer Service URL* tab on the SP Connection | Browser SSO | Protocol Settings page, set the following:

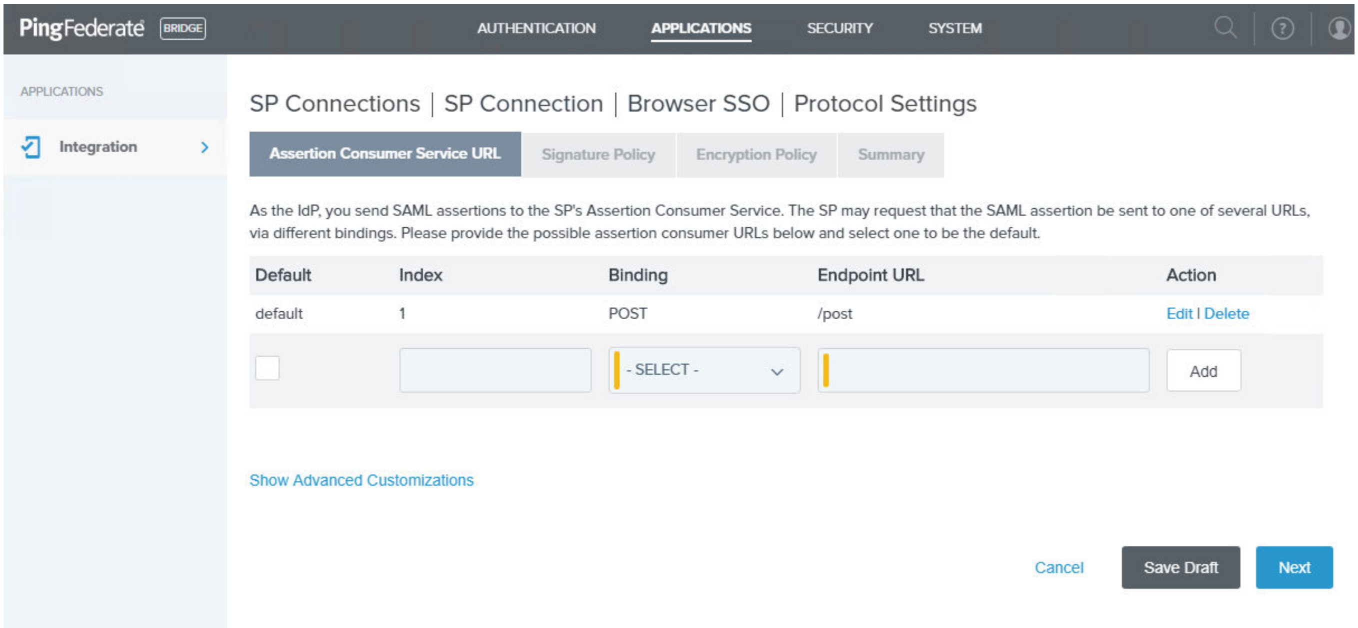
    a. Select the **Default** check box.

b. Set **Binding** to **POST**.

c. Set the appropriate **Endpoint URL**.

d. Click **Add**.

e. Click **Next**.

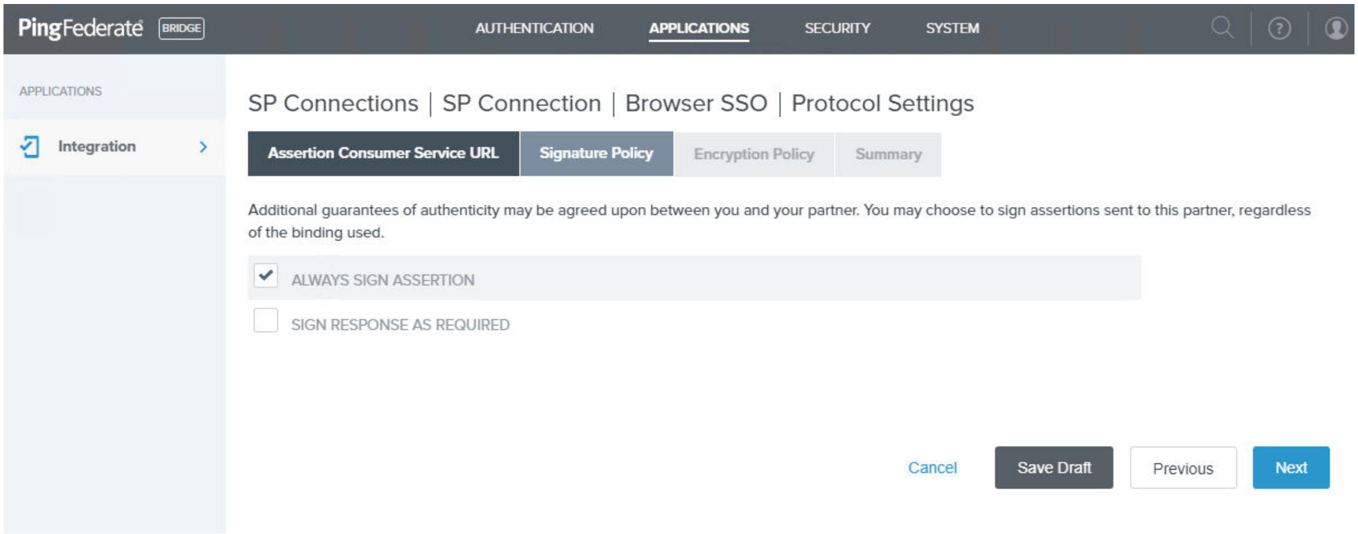


SP Connections | SP Connection | Browser SSO | Protocol Settings

As the IdP, you send SAML assertions to the SP's Assertion Consumer Service. The SP may request that the SAML assertion be sent to one of several URLs, via different bindings. Please provide the possible assertion consumer URLs below and select one to be the default.

Default	Index	Binding	Endpoint URL	Action
default	1	POST	/post	Edit I Delete
□		- SELECT -		Add

24. In the *Signature Policy* tab, select the **Always sign the SAML assertion** check box and click **Next**.



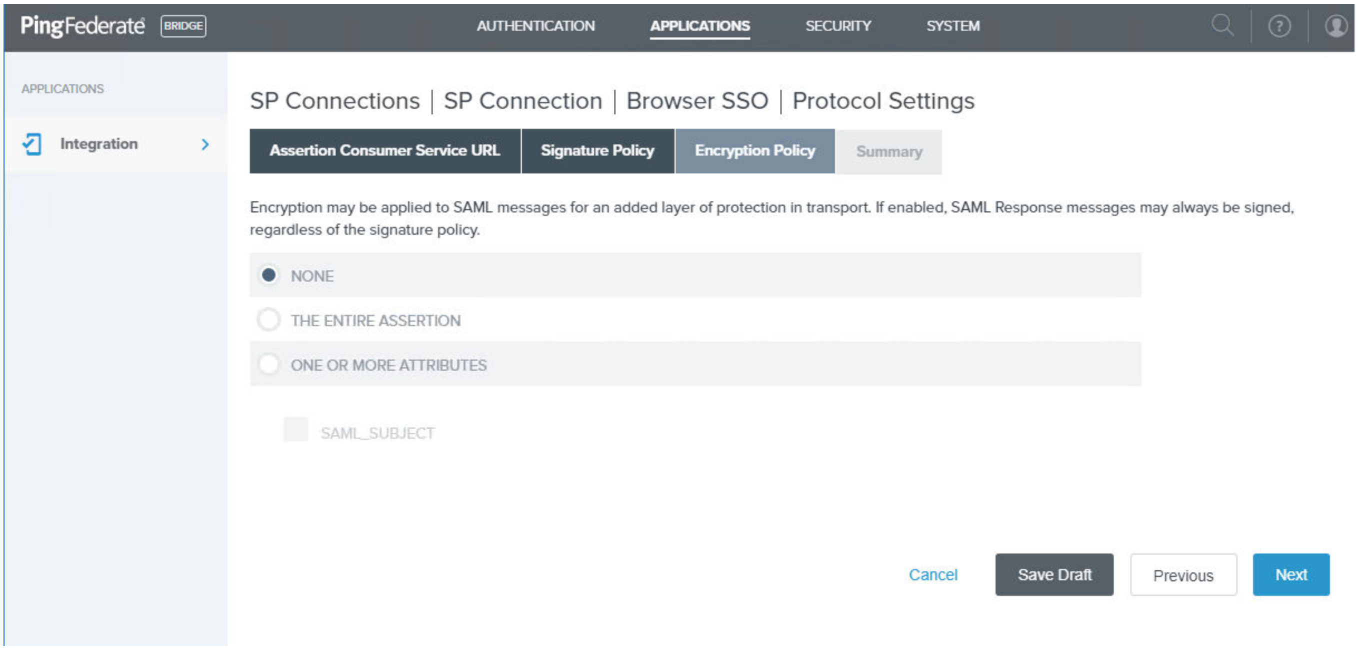
SP Connections | SP Connection | Browser SSO | Protocol Settings

Additional guarantees of authenticity may be agreed upon between you and your partner. You may choose to sign assertions sent to this partner, regardless of the binding used.

☑ ALWAYS SIGN ASSERTION

□ SIGN RESPONSE AS REQUIRED

25. In the *Encryption Policy* tab, click **Next**.



SP Connections | SP Connection | Browser SSO | Protocol Settings

Encryption may be applied to SAML messages for an added layer of protection in transport. If enabled, SAML Response messages may always be signed, regardless of the signature policy.

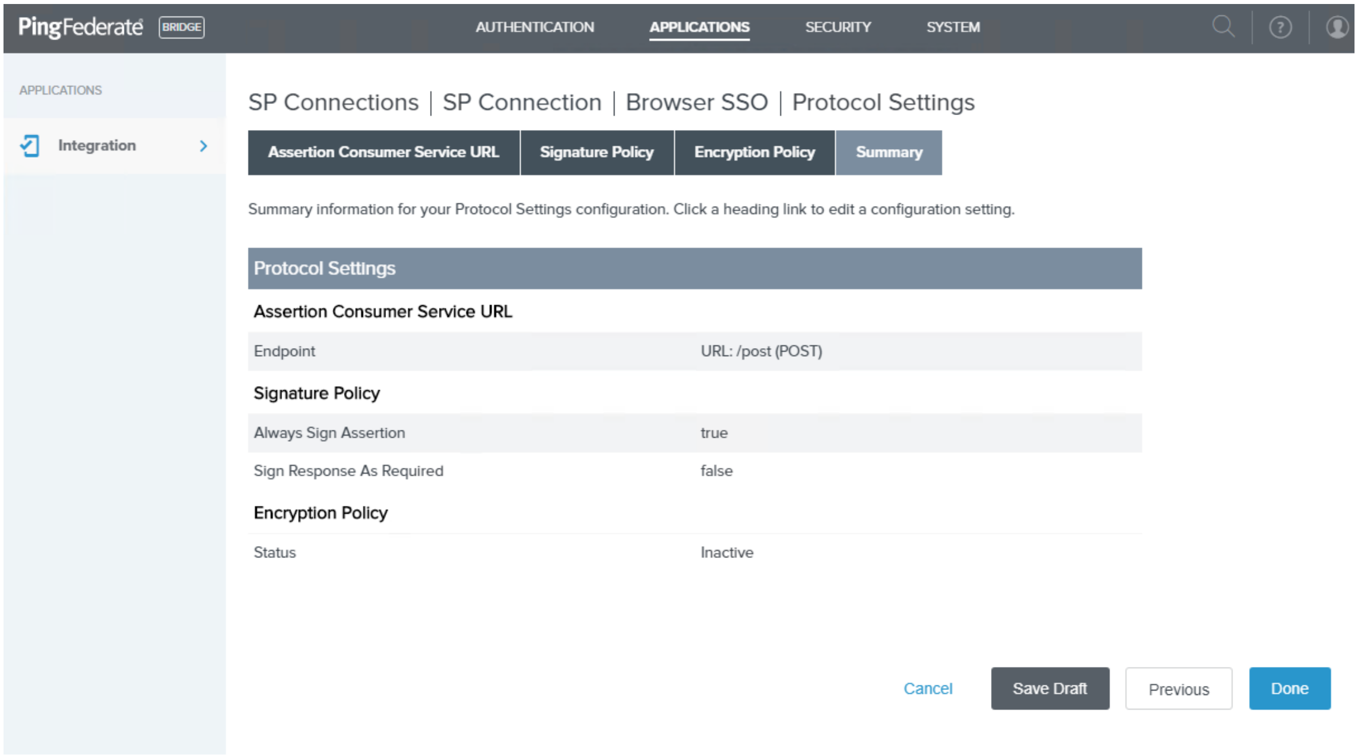
● NONE

○ THE ENTIRE ASSERTION

○ ONE OR MORE ATTRIBUTES

□ SAML_SUBJECT

26. Review the *Summary* tab and click **Done**.

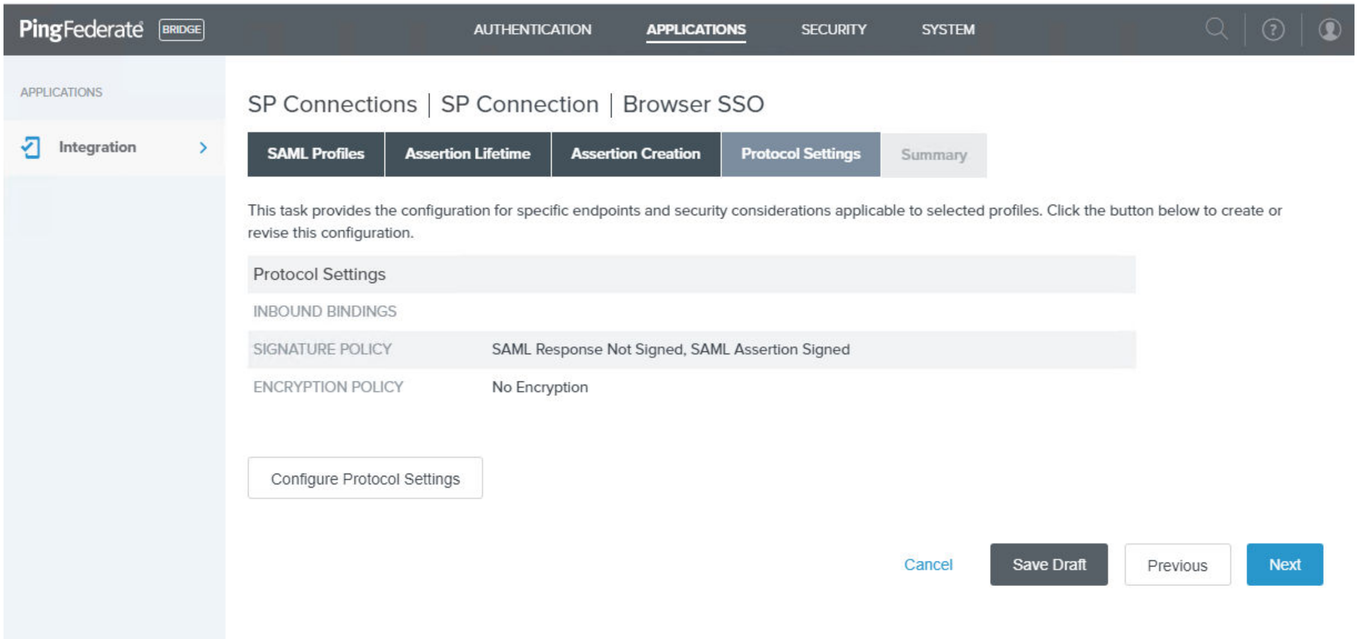


SP Connections | SP Connection | Browser SSO | Protocol Settings

Summary information for your Protocol Settings configuration. Click a heading link to edit a configuration setting.

Protocol Settings	
Assertion Consumer Service URL	
Endpoint	URL: /post (POST)
Signature Policy	
Always Sign Assertion	true
Sign Response As Required	false
Encryption Policy	
Status	Inactive

27. Review the *Summary* tab on the SP Connection | Browser SSO page, and click **Next**.

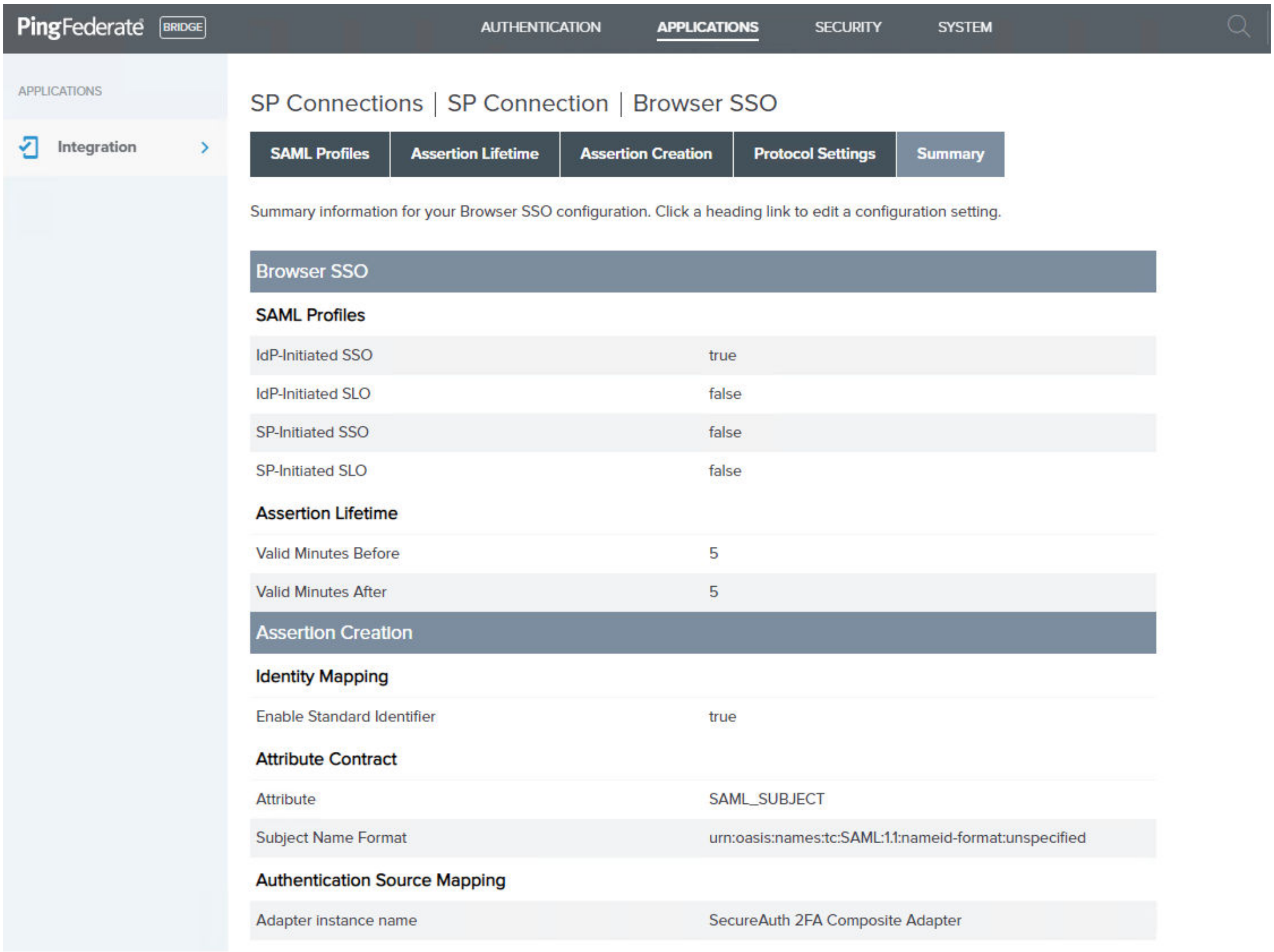


SP Connections | SP Connection | Browser SSO

This task provides the configuration for specific endpoints and security considerations applicable to selected profiles. Click the button below to create or revise this configuration.

Protocol Settings	
INBOUND BINDINGS	
SIGNATURE POLICY	SAML Response Not Signed, SAML Assertion Signed
ENCRYPTION POLICY	No Encryption

28. Review the *Summary* tab for the full Browser SSO settings and click **Done**.



SP Connections | SP Connection | Browser SSO

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	false
SP-Initiated SLO	false

Assertion Lifetime

Valid Minutes Before	5
Valid Minutes After	5

Assertion Creation

Identity Mapping

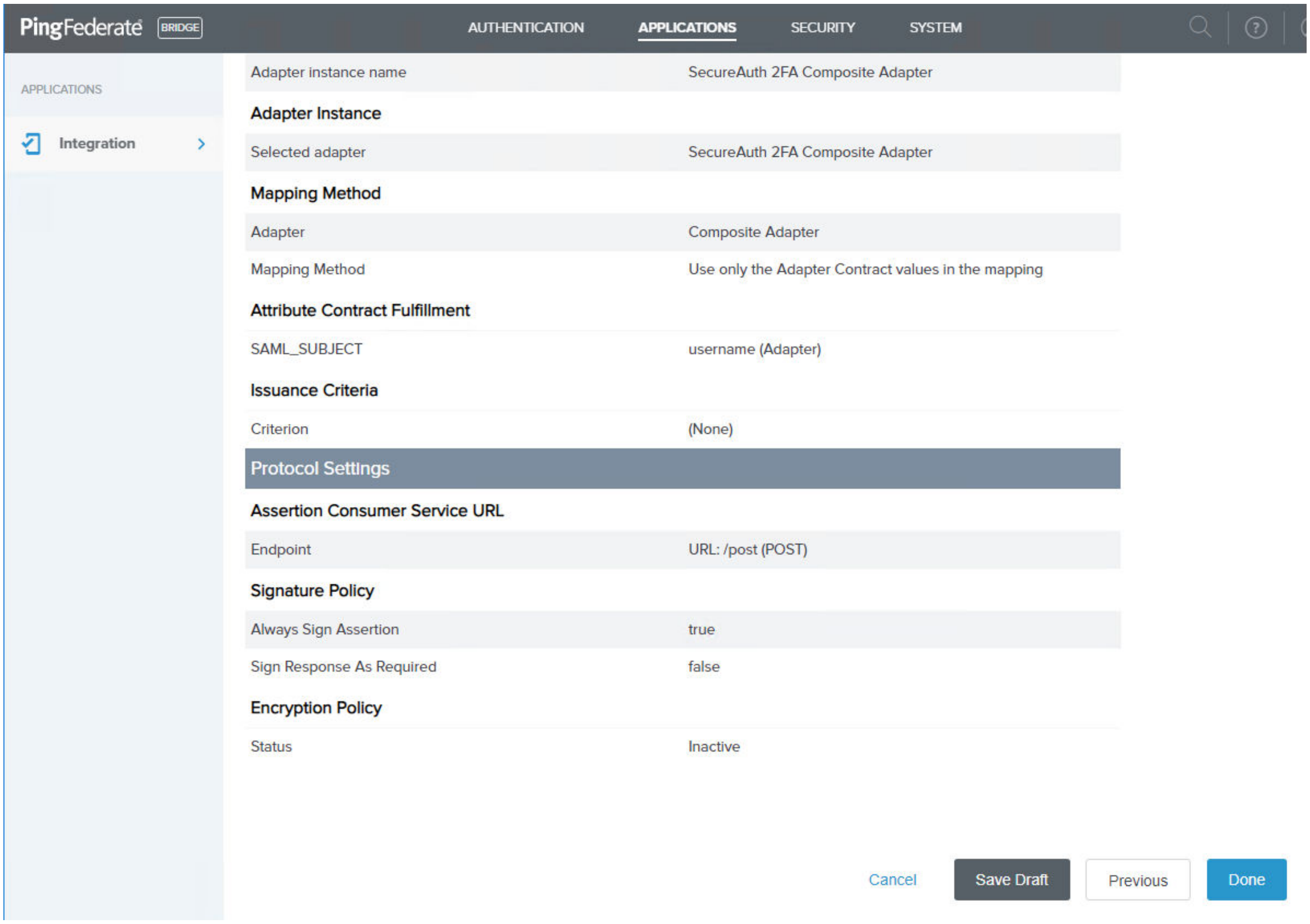
Enable Standard Identifier	true

Attribute Contract

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

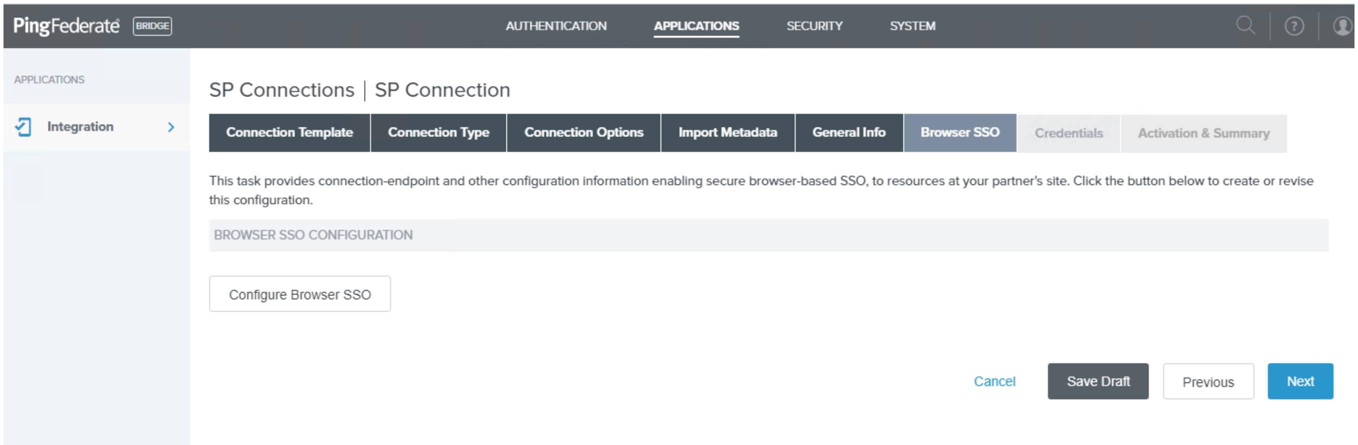
Authentication Source Mapping

Adapter instance name	SecureAuth 2FA Composite Adapter



Adapter instance name	SecureAuth 2FA Composite Adapter
Adapter Instance	
Selected adapter	SecureAuth 2FA Composite Adapter
Mapping Method	
Adapter	Composite Adapter
Mapping Method	Use only the Adapter Contract values in the mapping
Attribute Contract Fulfillment	
SAML_SUBJECT	username (Adapter)
Issuance Criteria	
Criterion	(None)
Protocol Settings	
Assertion Consumer Service URL	
Endpoint	URL: /post (POST)
Signature Policy	
Always Sign Assertion	true
Sign Response As Required	false
Encryption Policy	
Status	Inactive

29. The *Browser SSO* tab on the SP Connection page displays the new browser SSO configuration for the SP connection. Click **Next**.

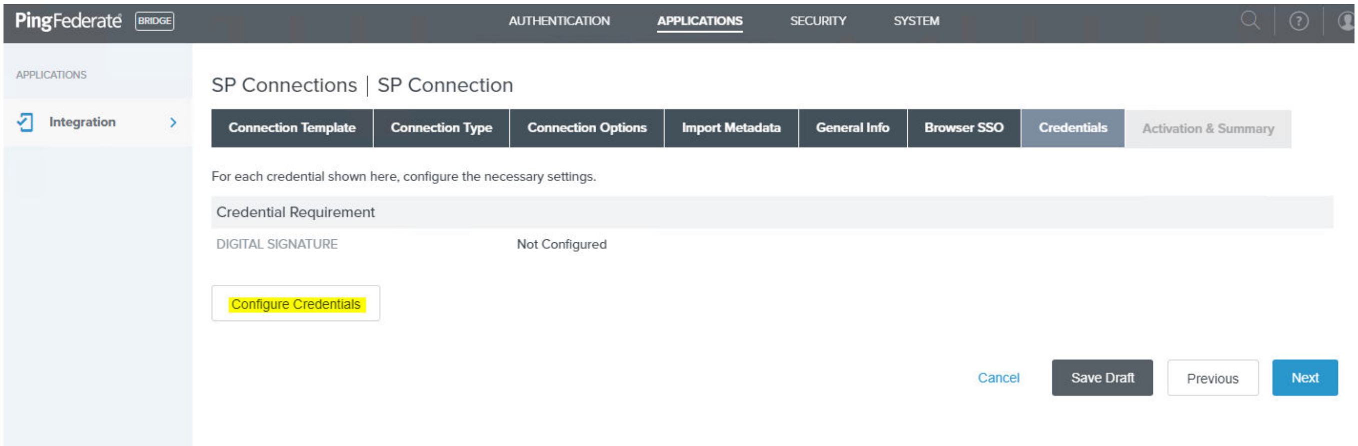


SP Connections | SP Connection

This task provides connection-endpoint and other configuration information enabling secure browser-based SSO, to resources at your partner's site. Click the button below to create or revise this configuration.

BROWSER SSO CONFIGURATION

30. In the *Credentials* tab on the SP Connection page, click **Configure Credentials**.

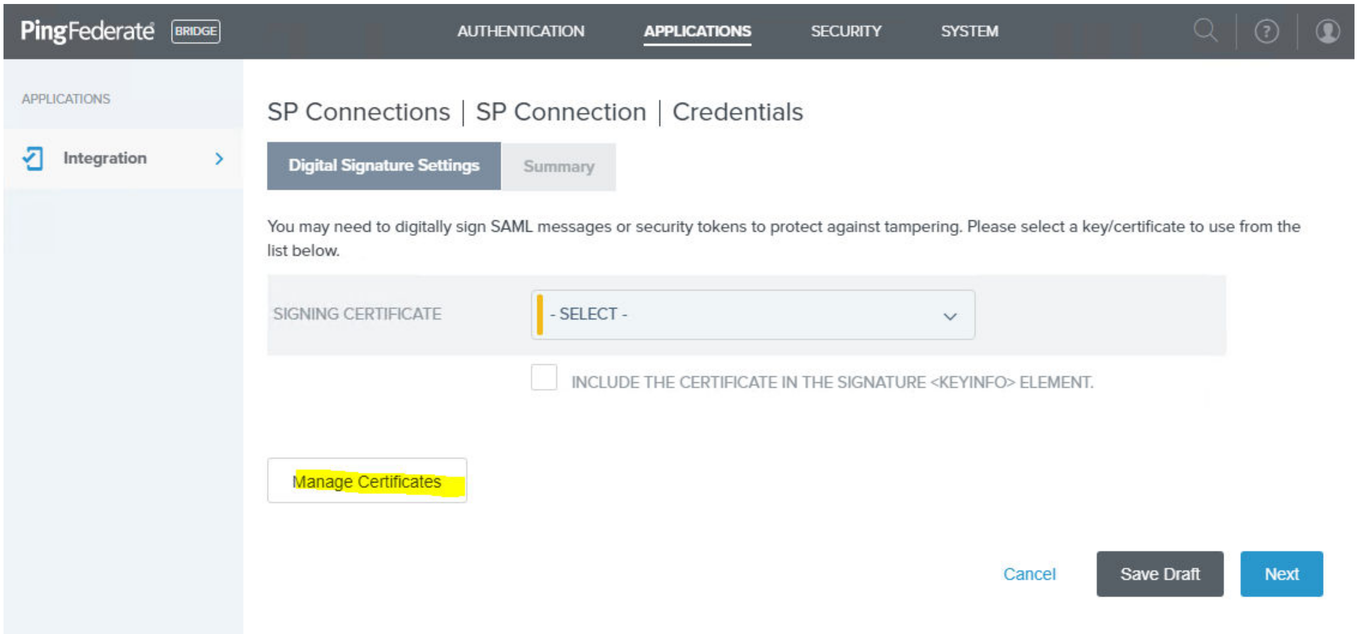


SP Connections | SP Connection

For each credential shown here, configure the necessary settings.

Credential Requirement	
DIGITAL SIGNATURE	Not Configured

31. In the *Digital Signature Settings* tab, click **Manage Certificates**.



SP Connections | SP Connection | Credentials

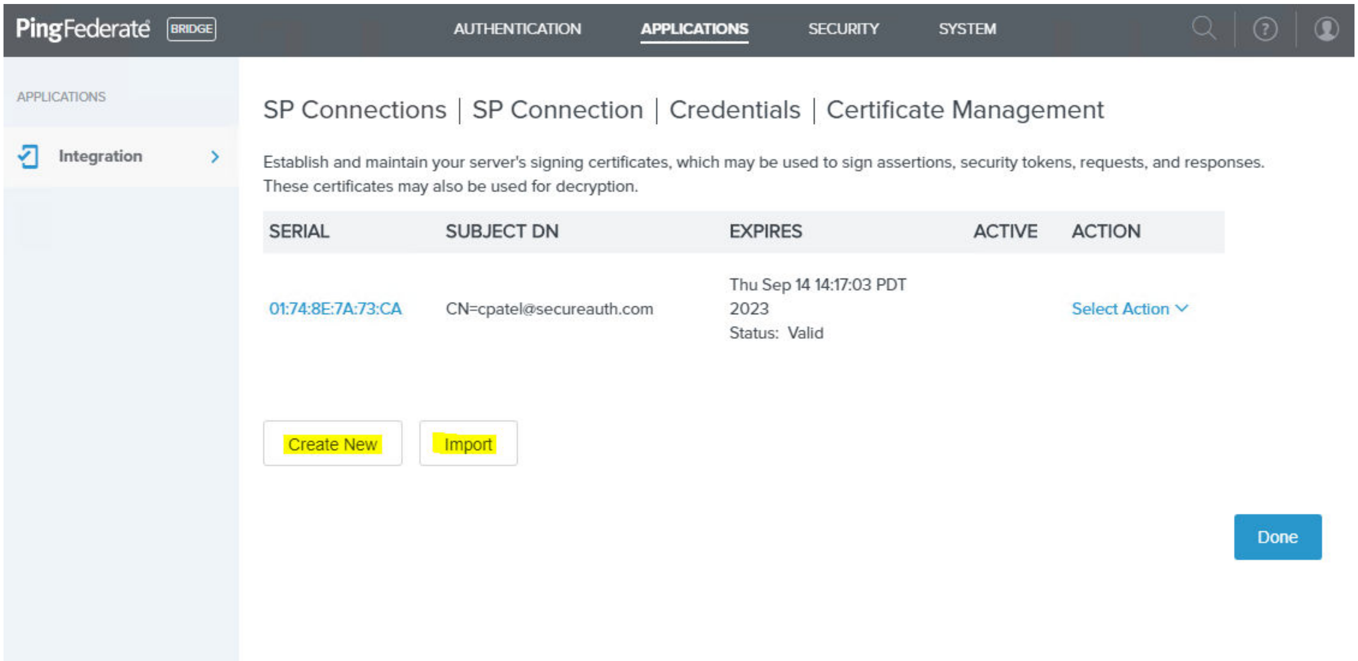
You may need to digitally sign SAML messages or security tokens to protect against tampering. Please select a key/certificate to use from the list below.

SIGNING CERTIFICATE - SELECT -

□ INCLUDE THE CERTIFICATE IN THE SIGNATURE <KEYINFO> ELEMENT.

32. In the *Manage Digital Signing Certificates* tab, do one of the following:

- To create an unsigned certificate, click **Create New**.
- To use an existing certificate, click **Import**.

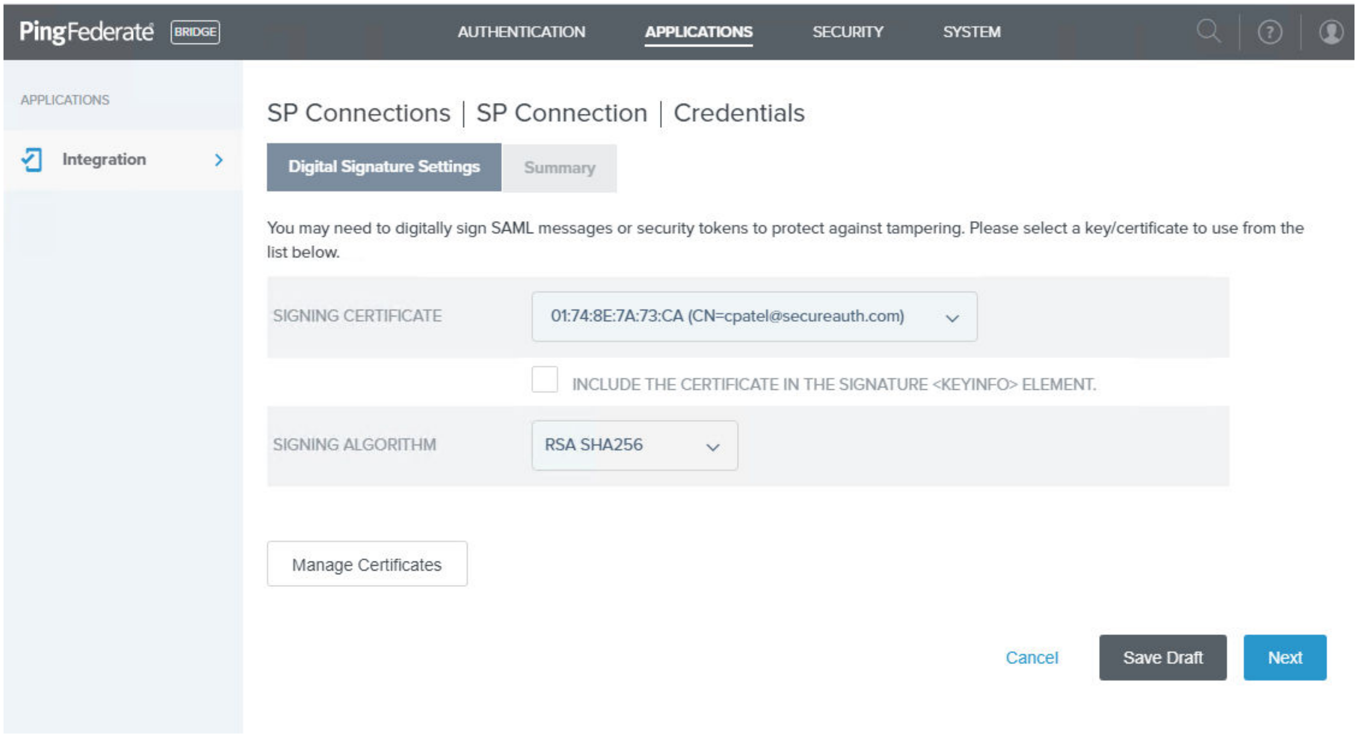


SP Connections | SP Connection | Credentials | Certificate Management

Establish and maintain your server's signing certificates, which may be used to sign assertions, security tokens, requests, and responses. These certificates may also be used for decryption.

SERIAL	SUBJECT DN	EXPIRES	ACTIVE	ACTION
01:74:8E:7A:73:CA	CN=cpatel@secureauth.com	Thu Sep 14 14:17:03 PDT 2023 Status: Valid		Select Action

33. In the *Create Certificate* tab, enter the required values OR select existing certificate and click **Next**.



SP Connections | SP Connection | Credentials

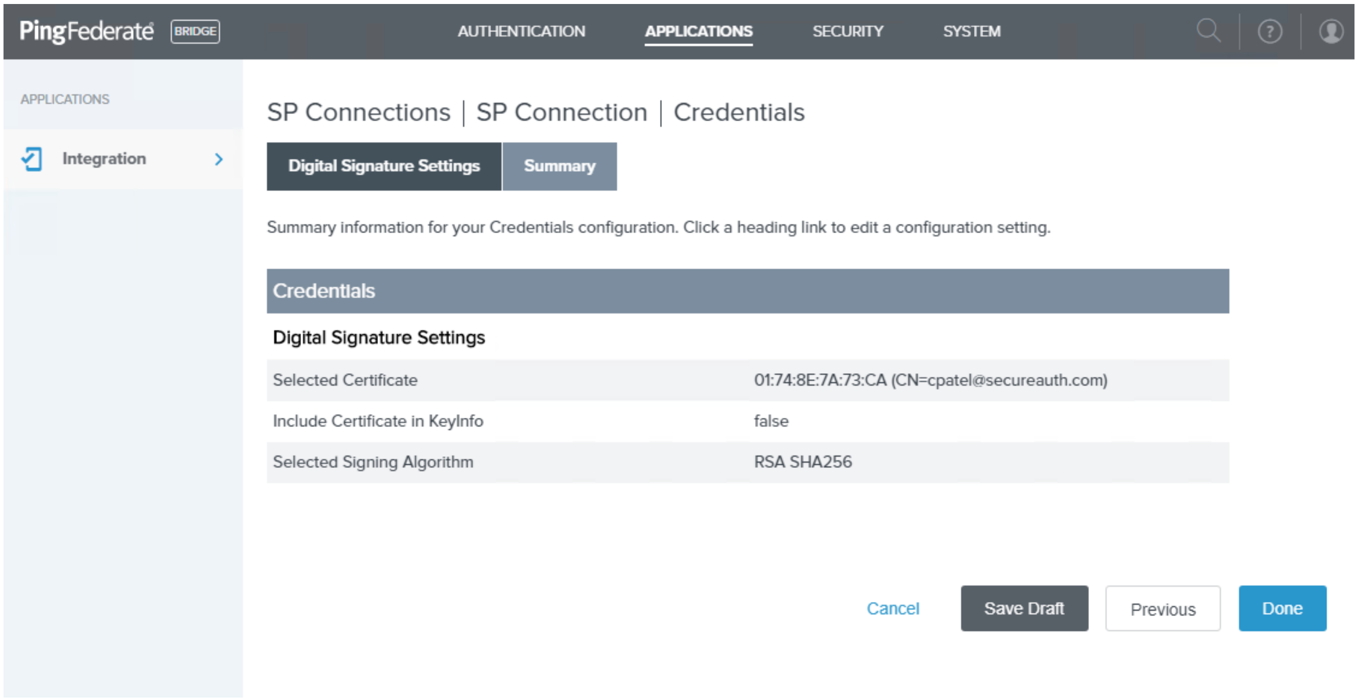
You may need to digitally sign SAML messages or security tokens to protect against tampering. Please select a key/certificate to use from the list below.

SIGNING CERTIFICATE: 01:74:8E:7A:73:CA (CN=cpatel@secureauth.com)

□ INCLUDE THE CERTIFICATE IN THE SIGNATURE <KEYINFO> ELEMENT.

SIGNING ALGORITHM: RSA SHA256

34. Review the *Summary* tab and click **Done**.



SP Connections | SP Connection | Credentials

Digital Signature Settings | Summary

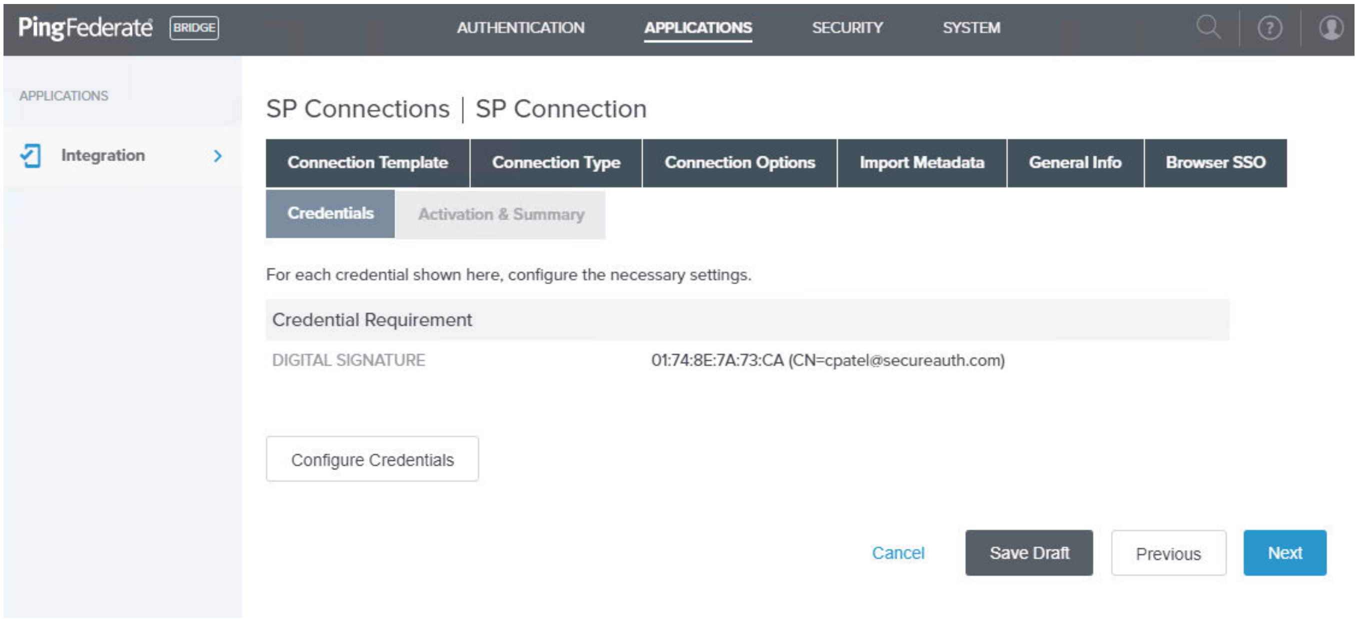
Summary information for your Credentials configuration. Click a heading link to edit a configuration setting.

Credentials

Digital Signature Settings

Selected Certificate	01:74:8E:7A:73:CA (CN=cpatel@secureauth.com)
Include Certificate in KeyInfo	false
Selected Signing Algorithm	RSA SHA256

35. In the *Credentials* tab on the SP Connection page, click **Next**.



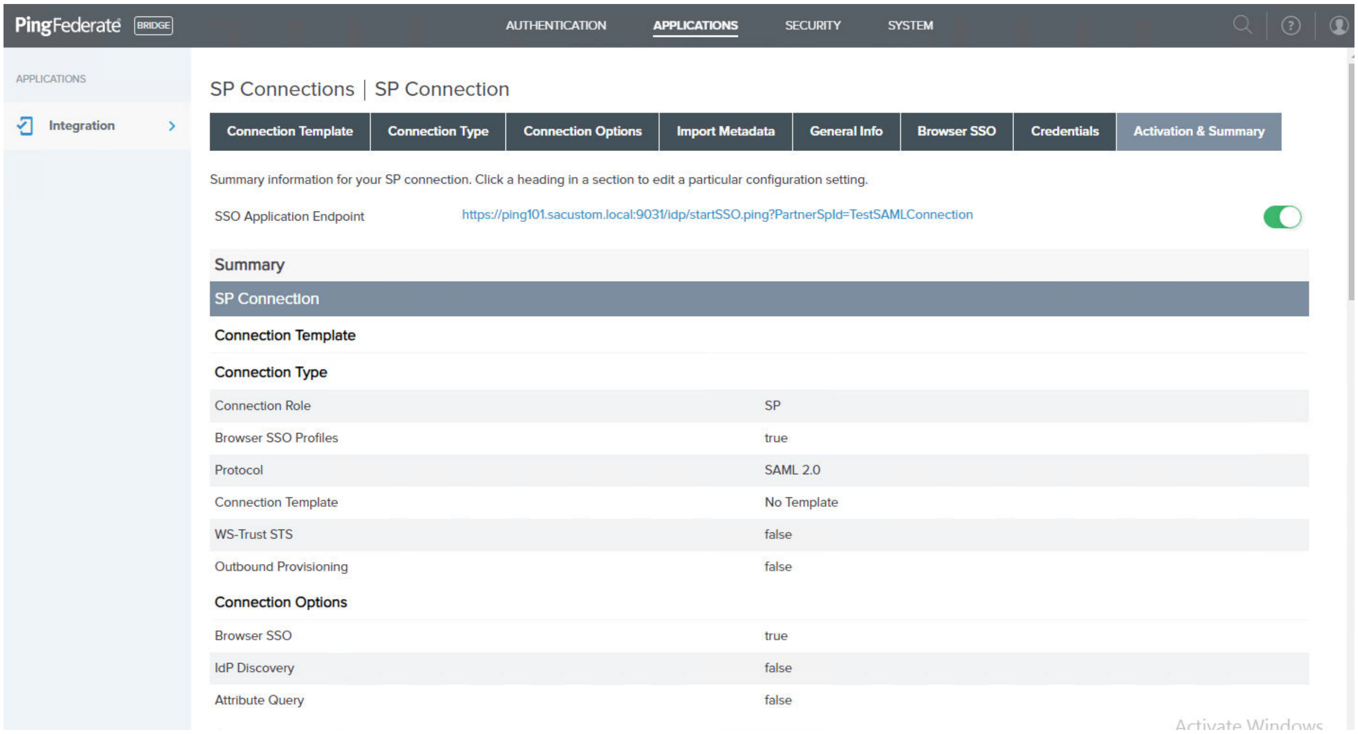
SP Connections | SP Connection

For each credential shown here, configure the necessary settings.

Credential Requirement

DIGITAL SIGNATURE	01:74:8E:7A:73:CA (CN=cpatel@secureauth.com)

36. In the *Activation & Summary* tab, set the **Connection Status** to **Active**.



SP Connections | SP Connection

Summary information for your SP connection. Click a heading in a section to edit a particular configuration setting.

SSO Application Endpoint https://ping101.sacustom.local:9031/idp/startSSO.ping?PartnerSpId=TestSAMLConnection

Summary

SP Connection

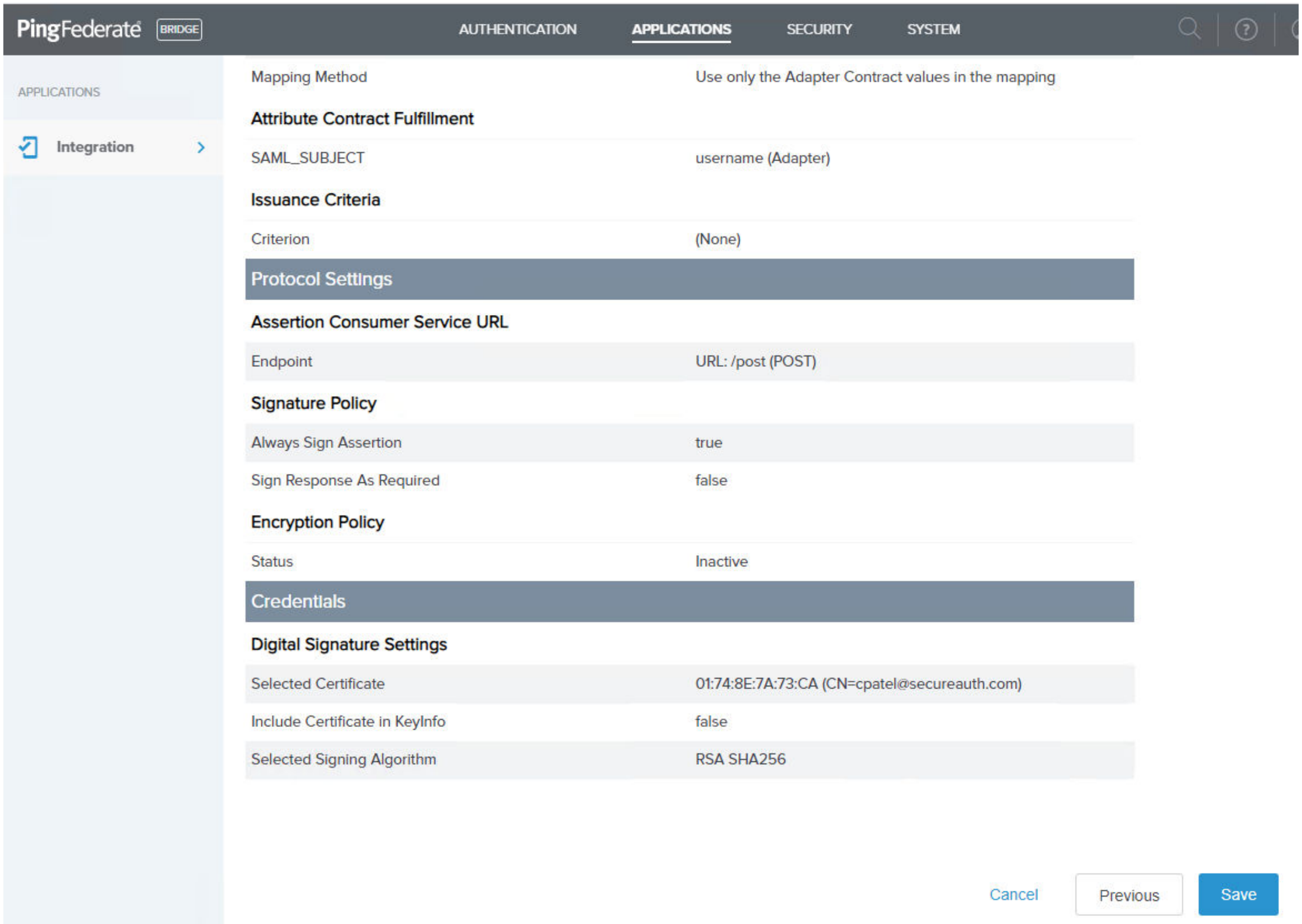
Connection Template

Connection Type

Connection Role	SP
Browser SSO Profiles	true
Protocol	SAML 2.0
Connection Template	No Template
WS-Trust STS	false
Outbound Provisioning	false

Connection Options

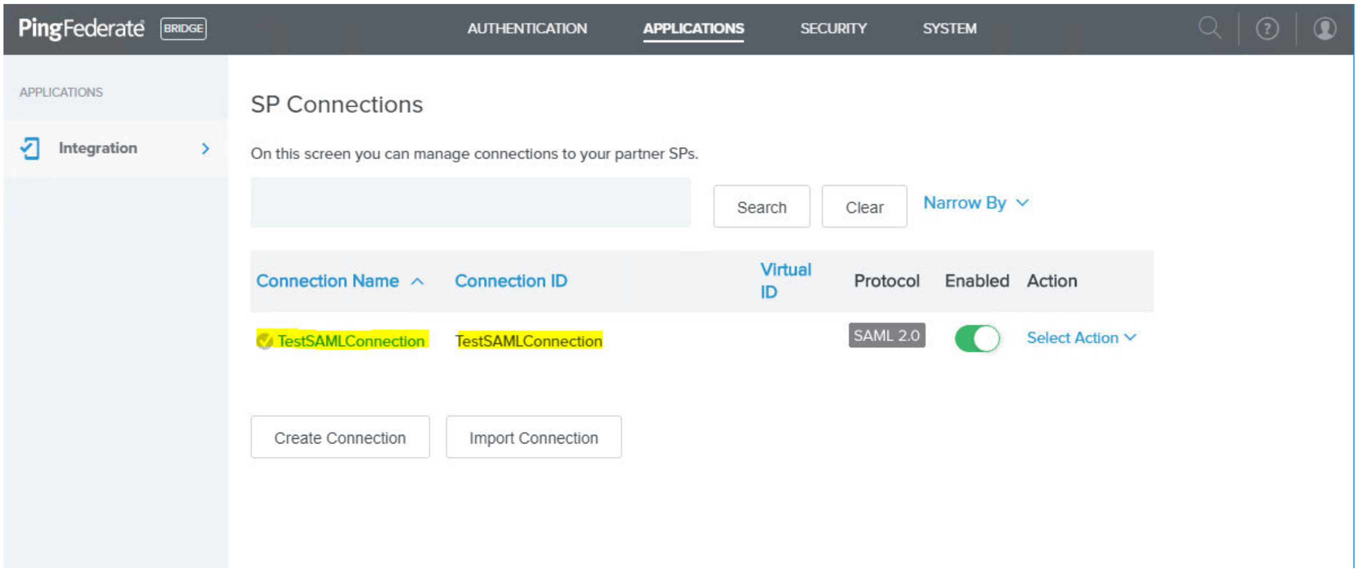
Browser SSO	true
IdP Discovery	false
Attribute Query	false



Mapping Method	Use only the Adapter Contract values in the mapping
Attribute Contract Fulfillment	
SAML_SUBJECT	username (Adapter)
Issuance Criteria	
Criterion	(None)
Protocol Settings	
Assertion Consumer Service URL	
Endpoint	URL: /post (POST)
Signature Policy	
Always Sign Assertion	true
Sign Response As Required	false
Encryption Policy	
Status	Inactive
Credentials	
Digital Signature Settings	
Selected Certificate	01:74:8E:7A:73:CA (CN=cpatel@secureauth.com)
Include Certificate in KeyInfo	false
Selected Signing Algorithm	RSA SHA256

37. Click **Save**.

38. See newly created SP connection.



SP Connections

On this screen you can manage connections to your partner SPs.

Connection Name	Connection ID	Virtual ID	Protocol	Enabled	Action
TestSAMLConnection	TestSAMLConnection		SAML 2.0	●	Select Action

Configure the HTML Form Adapter Logout

The next to last configuration step is to set up the HTML Form Adapter logout.

To configure the HTML Form Adapter logout

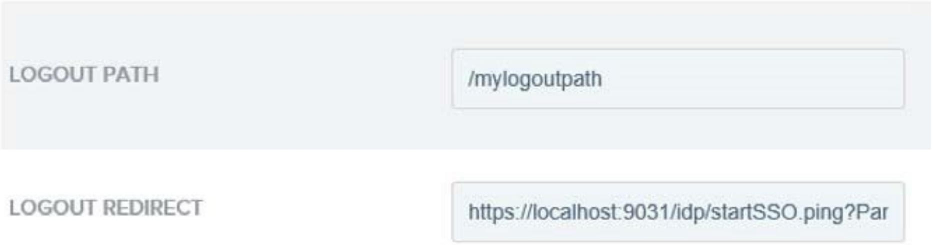
1. In PingFederate, go to **AUTHENTICATION** > **Adapters** to edit the HTML form adapter configuration.
2. In the **Logout Path** field, enter a path.

   You can enter any valid path string in this field; this value must start with a forward slash (/) character. To minimize the risk of invalid values, use an alphanumerical string.

   For example, if you enter `/mylogoutpath`, the actual logout path will be `/ext/mylogoutpath`.

   You can enter any valid path string into this field. Use alphanumerical string to minimize the risk of using an invalid value) into this field. This value must start with a / character. For example, if you enter `/mylogoutpath` into this field, the actual logout path will be `/ext/mylogoutpath`.
3. To have PingFederate redirect the user to another URL after logout, use the **Logout Redirect** field. For

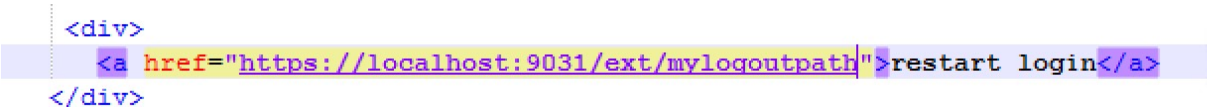
   example, use `https://myapp.example.com/loggedout.html`



LOGOUT PATH: /mylogoutpath

LOGOUT REDIRECT: https://localhost:9031/idp/startSSO.ping?Par

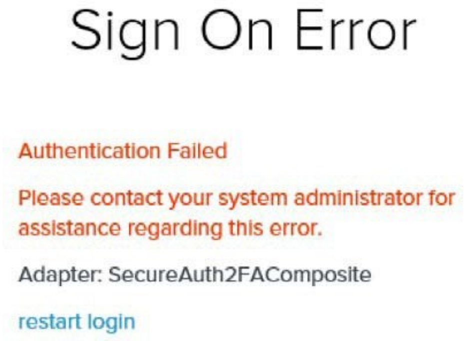
4. In the HTML script, after `\pingfederate-8.3.2\pingfederate\server\default\conf\template`, add the `restart login` link to `idp.sso.error.page.template.html`, similar to the following example:



```
 <div>
   <a href="https://localhost:9031/ext/mylogoutpath">restart login</a>
</div>
```

Result

This should result in displaying a message with a restart login link similar to the following example:



Sign On Error

Authentication Failed

Please contact your system administrator for assistance regarding this error.

Adapter: SecureAuth2FAComposite

restart login

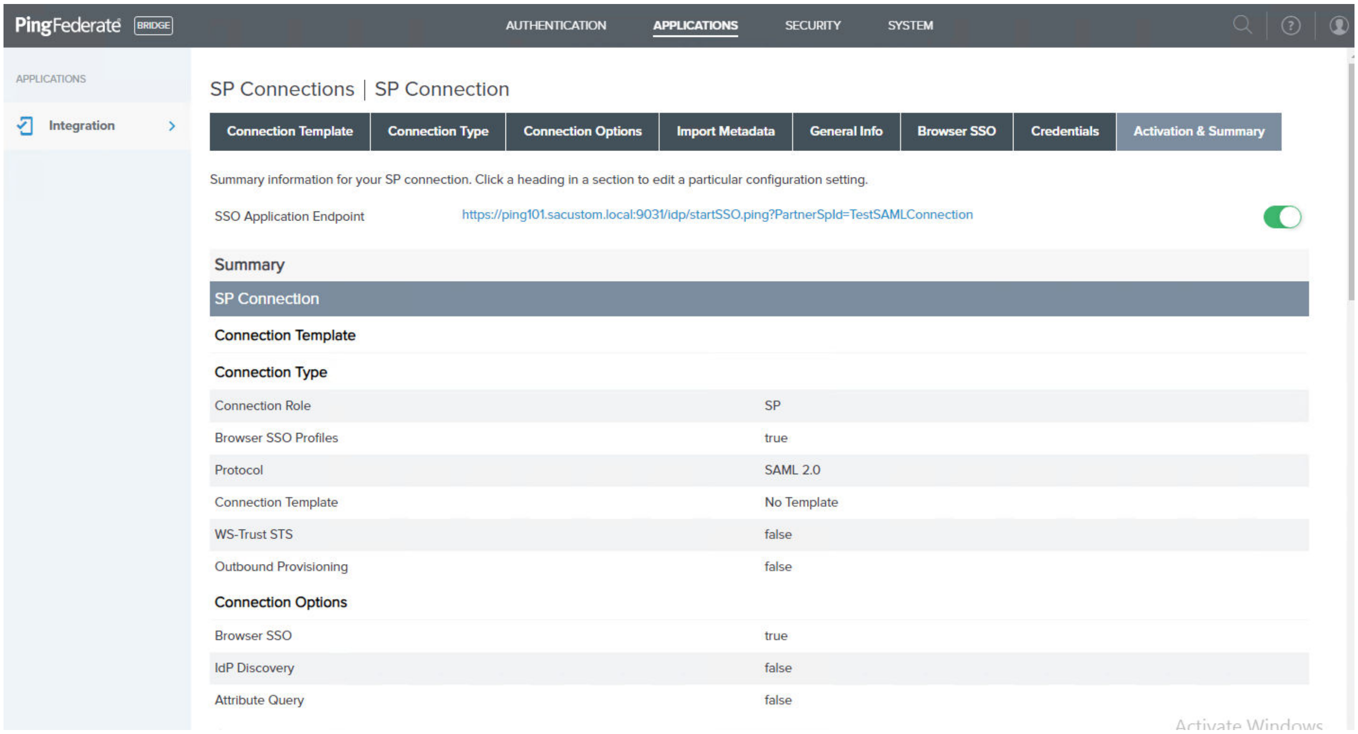
Test the configured SecureAuth 2FA functionality

After you have set up the configurations for the SecureAuth 2FA adapter and SP connections, test the functionality.

Obtain a test URL

1. To obtain a test URL, in PingFederate, select **APPLICATIONS** and click the appropriate SP connection link.

   For example, the link name is TestSAMLConnection.



SP Connections | SP Connection

Summary information for your SP connection. Click a heading in a section to edit a particular configuration setting.

SSO Application Endpoint https://ping101.sacustom.local:9031/idp/startSSO.ping?PartnerSpId=TestSAMLConnection

Summary

SP Connection

Connection Template

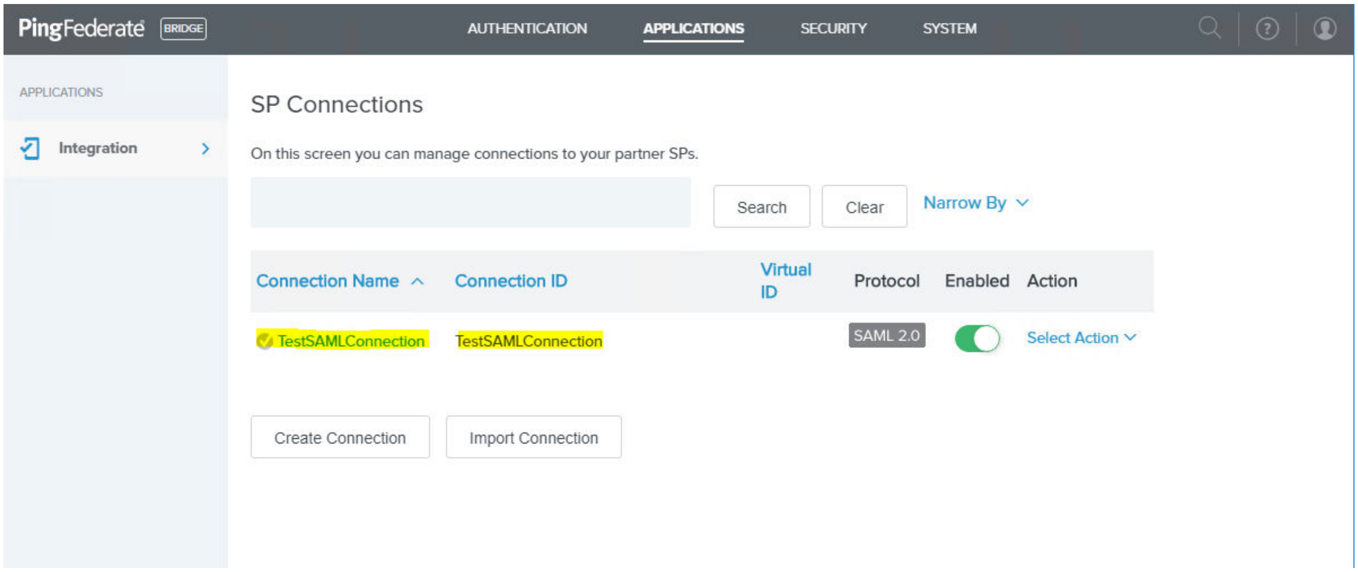
Connection Type

Connection Role	SP
Browser SSO Profiles	true
Protocol	SAML 2.0
Connection Template	No Template
WS-Trust STS	false
Outbound Provisioning	false

Connection Options

Browser SSO	true
IdP Discovery	false
Attribute Query	false

2. On the SP Connection page in the Activation & Summary tab, do the following:
   a. Make sure the Connection Status is set to **Active**.
   b. Copy the SSO Application Endpoint URL. For example, the URL is `https://localhost:9031/idp/startSSO.ping?PartnerSpId=TestSAMLConnection`



SP Connections

On this screen you can manage connections to your partner SPs.

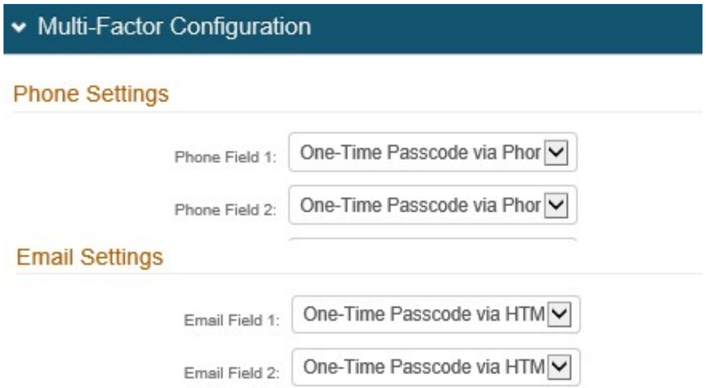
Connection Name	Connection ID	Virtual ID	Protocol	Enabled	Action
TestSAMLConnection	TestSAMLConnection		SAML 2.0	●	Select Action

3. To test the various delivery methods, see the following sections:

- Test SMS, voice, and email delivery methods
- Test the Push-to-Accept delivery method
- Test the time-based passcode method

Test SMS, voice, and email delivery methods

In the Identity Platform, you can configure the Multi-Factor Configuration tab settings to use more than one phone number and email as delivery methods to receive the passcode.



Multi-Factor Configuration

Phone Settings

Phone Field 1: One-Time Passcode via Phor

Phone Field 2: One-Time Passcode via Phor

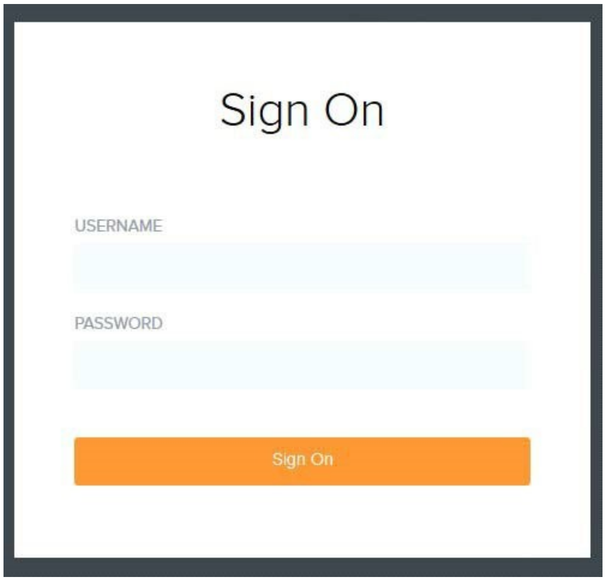
Email Settings

Email Field 1: One-Time Passcode via HTM

Email Field 2: One-Time Passcode via HTM

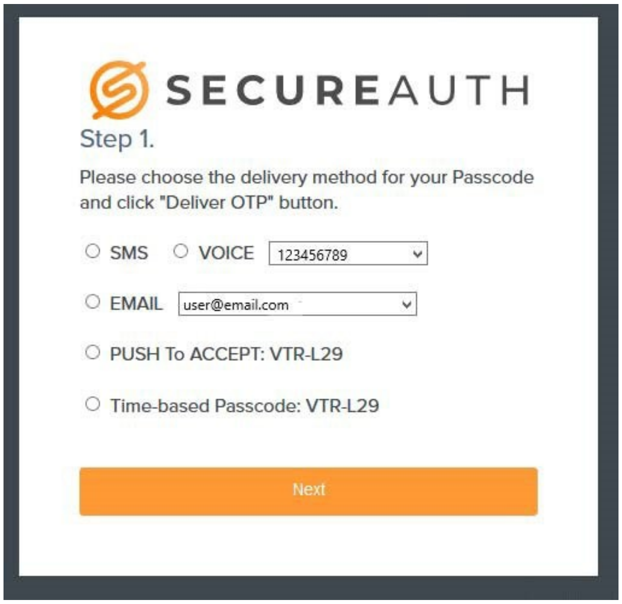
1. Open a new browser tab and paste the URL that you copied in the Obtain a test URL section.

   The Sign On page opens, similar to the following example:



2. Enter the username and password and click Sign On.

   The passcode delivery method page opens, similar to the following example.



Step 1.

Please choose the delivery method for your Passcode and click "Deliver OTP" button.

○ SMS ○ VOICE 123456789

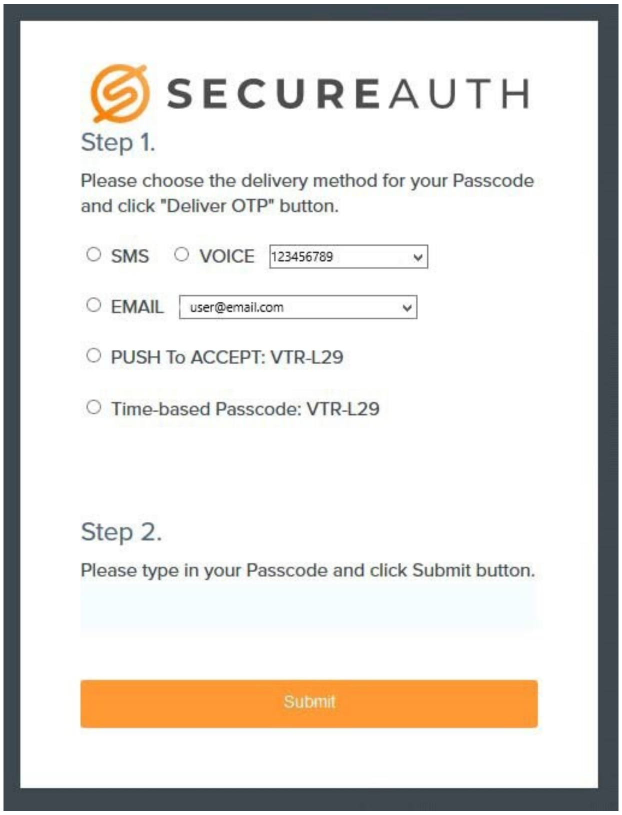
○ EMAIL user@email.com

○ PUSH To ACCEPT: VTR-L29

○ Time-based Passcode: VTR-L29

3. First, test using the SMS option.

   If the phone number associated with this account is correct, a SMS is sent with the OTP code.



Step 1.

Please choose the delivery method for your Passcode and click "Deliver OTP" button.

○ SMS ○ VOICE 123456789

○ EMAIL user@email.com

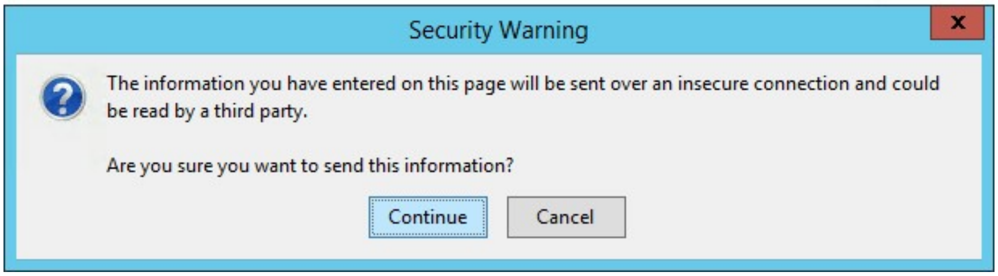
○ PUSH To ACCEPT: VTR-L29

○ Time-based Passcode: VTR-L29

Step 2.

Please type in your Passcode and click Submit button.

4. Enter the OTP code and click **Submit**.
5. If you receive a security warning similar to the following example, click **Continue**.



Security Warning

The information you have entered on this page will be sent over an insecure connection and could be read by a third party.

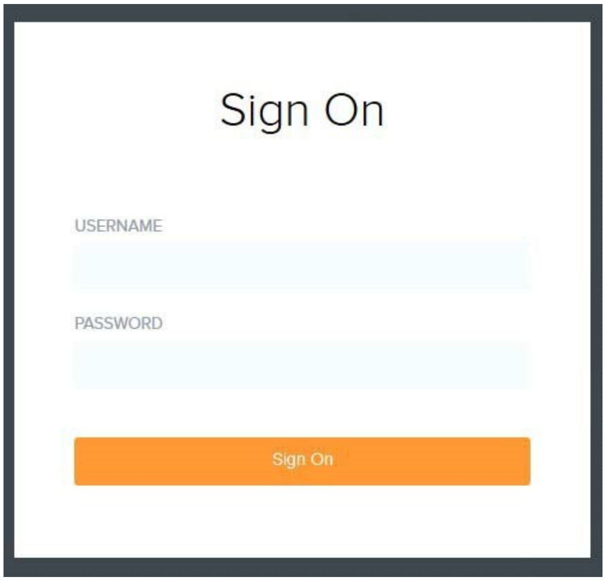
Are you sure you want to send this information?

6. Repeat the test using the Voice and Email methods.

Test the Push-to-Accept delivery method

1. Open a new browser tab and paste the URL that you copied in the Obtain a test URL section.

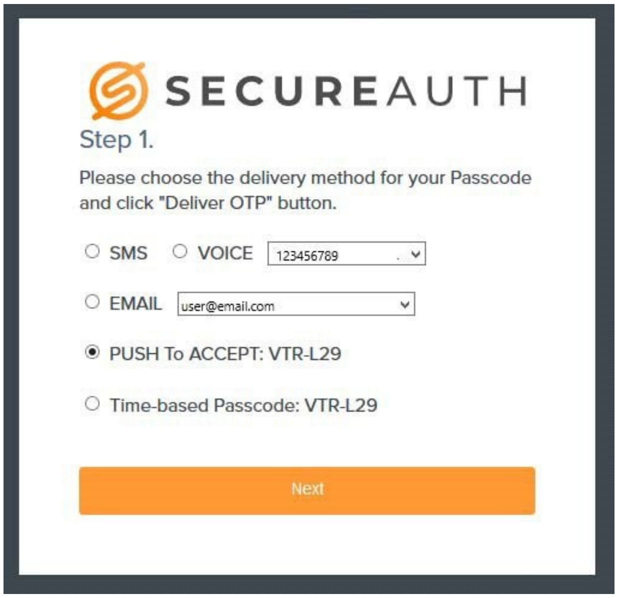
   The Sign On page opens, similar to the following example:



Sign On

2. Enter the username and password and click Sign On.

   The passcode delivery method page opens, similar to the following example.



SECUREAUTH

Step 1.

Please choose the delivery method for your Passcode and click "Deliver OTP" button.

○ SMS ○ VOICE 123456789

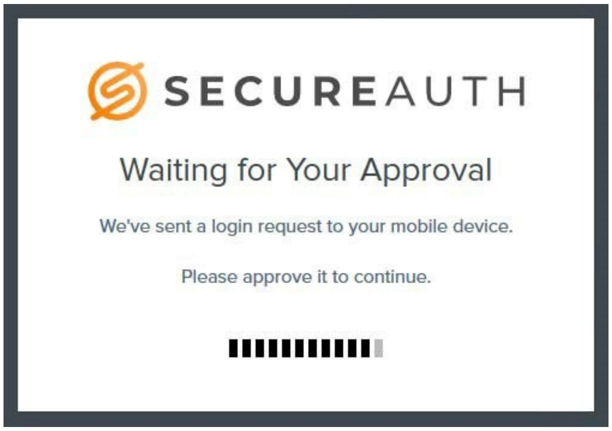
○ EMAIL user@email.com

● PUSH To ACCEPT: VTR-L29

○ Time-based Passcode: VTR-L29

3. Select the **Push to Accept** option.

   The approval request is sent to the specified user device similar to the following example.



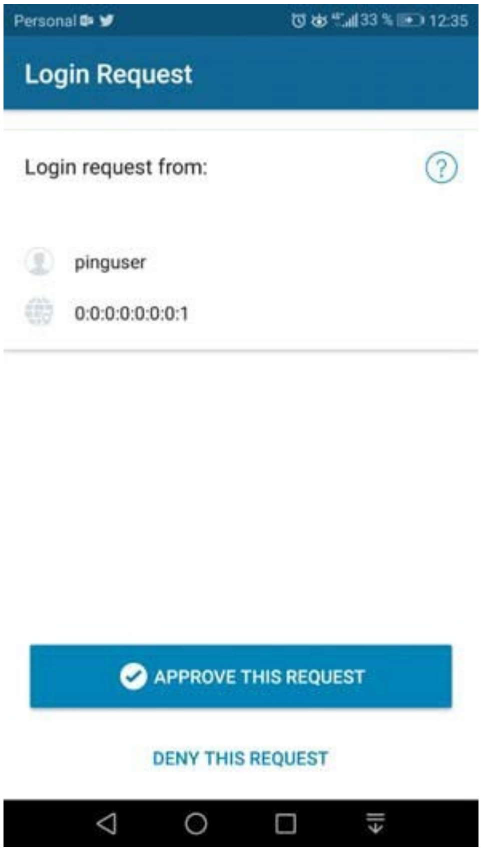
SECUREAUTH

Waiting for Your Approval

We've sent a login request to your mobile device.

Please approve it to continue.

4. When the Login Request pops up on the user device, tap **Approve this request**.



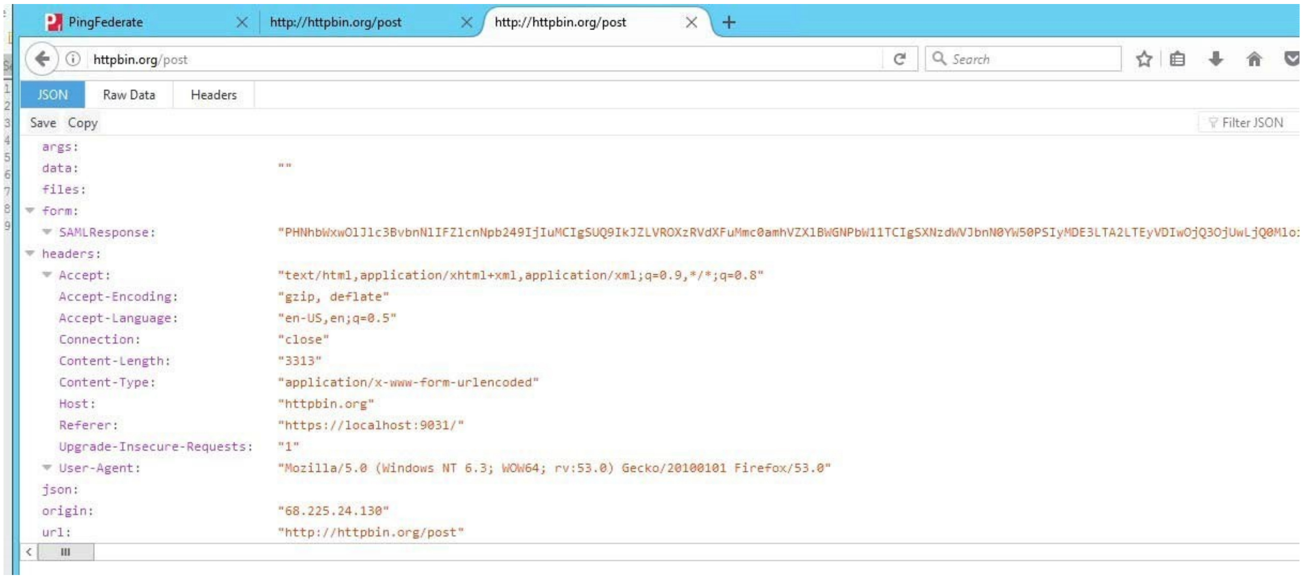
Login Request

Login request from:

pinguser

0:0:0:0:0:0:0:1

After a successful authentication, the destination page opens, similar to the following example.

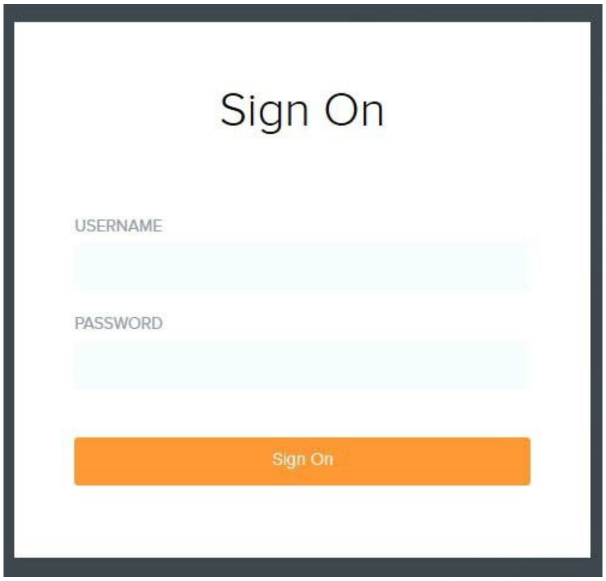


```
args:
data:                          ""
files:
▼ form:
  ▼ SAMLResponse:              "PHNhbWxwOlJlc3BvbnNlIFZlcnNpb249IjIuMCIgSUQ9IkJZLVROXzRVdXFuMmc0amhVZX1BWGNPbW11TCIgSXNzdWVJbnN0YW50PSIyMDE3LTA2LTEyVDIwOjQ3OjUwLjQ0Mlo:
▼ headers:
  ▼ Accept:                    "text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8"
    Accept-Encoding:           "gzip, deflate"
    Accept-Language:           "en-US,en;q=0.5"
    Connection:                "close"
    Content-Length:            "3313"
    Content-Type:              "application/x-www-form-urlencoded"
    Host:                      "httpbin.org"
    Referer:                   "https://localhost:9031/"
    Upgrade-Insecure-Requests: "1"
  ▼ User-Agent:                "Mozilla/5.0 (Windows NT 6.3; WOW64; rv:53.0) Gecko/20100101 Firefox/53.0"
json:
origin:                        "68.225.24.130"
url:                           "http://httpbin.org/post"
```

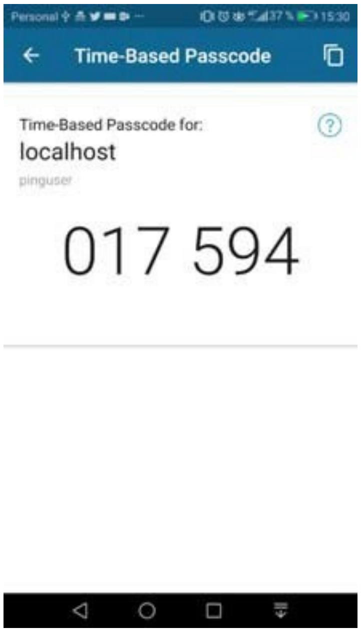
Test the time-based passcode method

1. Open a new browser tab and paste the URL that you copied in the Obtain a test URL section.

The Sign On page opens, similar to the following example:



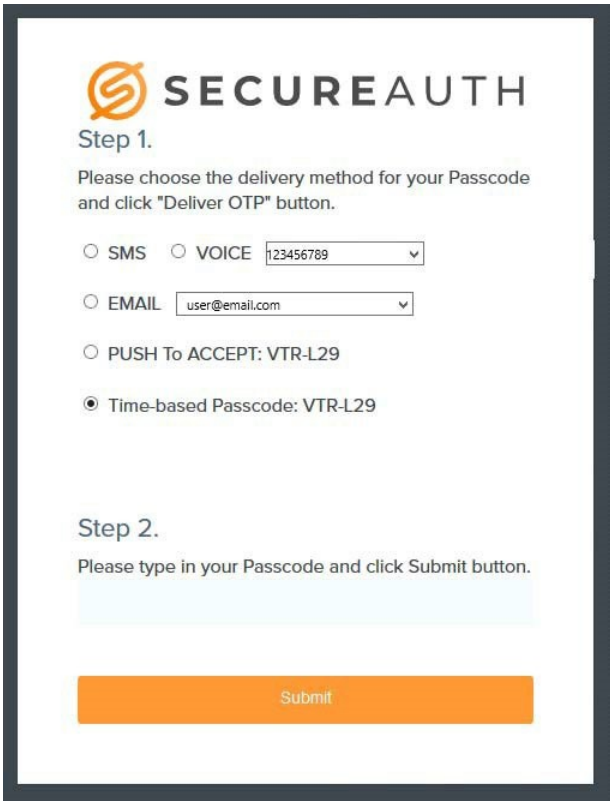
2. Open the SecureAuth Authenticate app on your mobile device and get the time-based passcode similar to the following example.



Time-Based Passcode for:
localhost
pinguser

017 594

3. On your computer, select the **Time-based passcode** option as the delivery method.



Step 1.

Please choose the delivery method for your Passcode and click "Deliver OTP" button.

○ SMS ○ VOICE 123456789

○ EMAIL user@email.com

○ PUSH To ACCEPT: VTR-L29

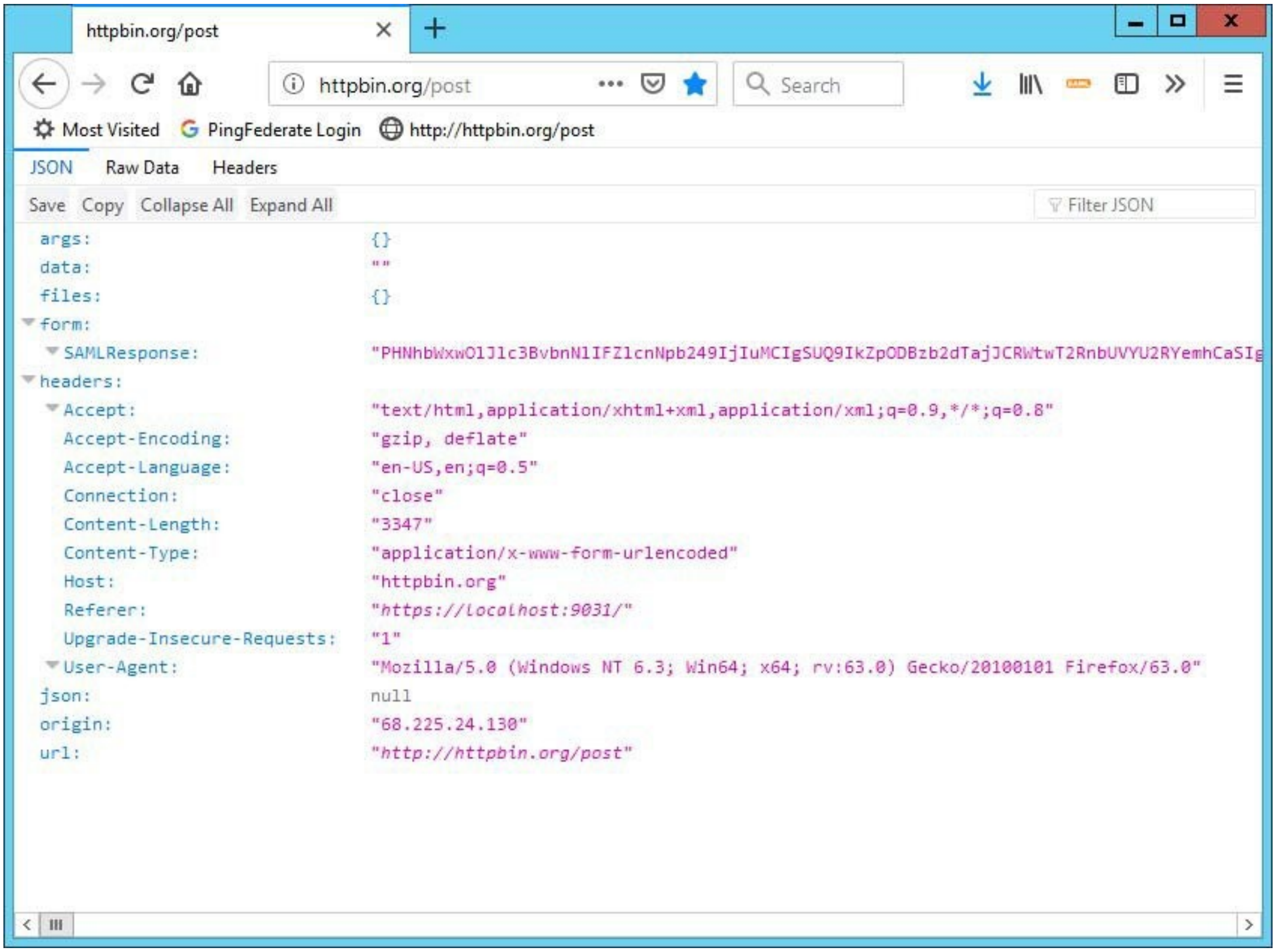
● Time-based Passcode: VTR-L29

Step 2.

Please type in your Passcode and click Submit button.

4. Enter the passcode from the SecureAuth Authenticate app and click **Submit**.

   After a successful authentication, the destination page opens, similar to the following example.



```
args:                           {}
data:                           ""
files:                          {}
form:
  SAMLResponse:                 "PHNhbWxwO1J1c3BvbnN1IFZ1cnNpb249IjIuMCIgSUQ9IkZpODBzb2dTajJCRWtwT2RnbUVYU2RYemhCaSIg
headers:
  Accept:                       "text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8"
  Accept-Encoding:              "gzip, deflate"
  Accept-Language:              "en-US,en;q=0.5"
  Connection:                   "close"
  Content-Length:               "3347"
  Content-Type:                 "application/x-www-form-urlencoded"
  Host:                         "httpbin.org"
  Referer:                      "https://localhost:9031/"
  Upgrade-Insecure-Requests:    "1"
  User-Agent:                   "Mozilla/5.0 (Windows NT 6.3; Win64; x64; rv:63.0) Gecko/20100101 Firefox/63.0"
json:                           null
origin:                         "68.225.24.130"
url:                            "http://httpbin.org/post"
```

Conclusion

Once configured and deployed, you can take advantage of using a PingFederate server for all the advanced security features to which the SecureAuth® Identity Platform can provide.

References

See the following documents to configure multi-factor authentication and adaptive authentication in the Identity Platform.

- **Adaptive Authentication tab configuration**

  9.1-9.2: https://docs.secureauth.com/x/pRmsAg

- **Device Recognition**

  19.07: https://docs.secureauth.com/x/PZUeAw 9.1-9.2:

  https://docs.secureauth.com/x/UhmsAg

Note: Both guides are identical.

- **Multi-Factor App Enrollment (URL) Realm Configuration Guide**

  19.07: https://docs.secureauth.com/x/5J0eAw

  9.3: https://docs.secureauth.com/x/sJfQAg

  9.1-9.2: https://docs.secureauth.com/x/SxKsAg
- **Multi-Factor App Enrollment (QR Code) Realm Configuration Guide**

  19.07: https://docs.secureauth.com/x/850eAw

  9.3: https://docs.secureauth.com/x/spfQAg

  9.1-9.2: https://docs.secureauth.com/x/mBisAg
- **Mobile Login Requests (Push Notifications) registration method for multi-factor authentication**

  19.07: https://docs.secureauth.com/x/KAx2Aw

  9.1-9.2: https://docs.secureauth.com/x/GBusAg
- **Time-based Passcodes (OATH) Registration Method for MFA**
  (See the configuration steps for Account Management (Help Desk) realm)

  9.1-9.2: https://docs.secureauth.com/x/4RqsAg
- **Time-based Passcodes (OATH) Registration Method for MFA**
  (See the configuration steps for Self-service Account Update realm)

  9.1-9.2: https://docs.secureauth.com/x/4RqsAg
- **SecureAuth Authenticate App for Android and iOS v5.x**

  SecureAuth Apps and Tools: https://docs.secureauth.com/x/xAVjAg