



Value-Added Module (VAM)

PingFederate 2FA VAM Deployment Guide

Copyright Information

©2020. SecureAuth[®] is a registered trademark of SecureAuth Corporation. SecureAuth's Identity Platform software, appliances, and other products and solutions are copyrighted products of SecureAuth Corporation.

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.....	3
System information.....	4
Configuration.....	4
Set up the environment	5
Create a password credential validator	7
Create the HTML Form Adapter	12
Configure the Identity Platform realm for API	20
Create the 2FA adapter	21
Create the SecureAuth composite adapter.....	28
Create service provider (SP) connections.....	33
Configure the HTML Form Adapter Logout.....	59
Result.....	60
Test the configured SecureAuth 2FA functionality.....	60
Obtain a test URL.....	60
Test SMS, voice, and email delivery methods	62
Test the Push-to-Accept delivery method	64
Test the time-based passcode method	66
Conclusion	69
References.....	69

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.

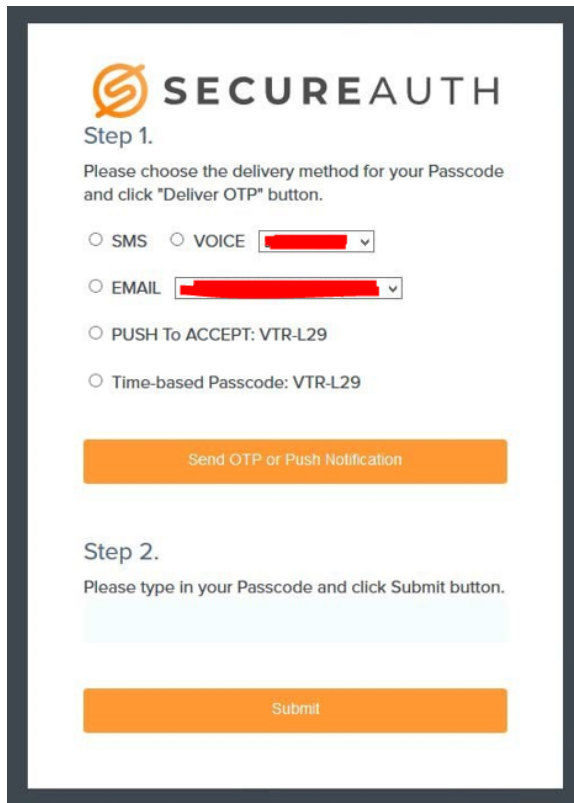
Along with standard multi-factor authentication, the VAM has additional functionality of Adaptive Authentication and Device Recognition, Push to Accept Notifications and Time-Based Passcodes (OATH). Once deployed and configured, a PingFederate server can take advantage of all the advanced security features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



The screenshot displays the SecureAuth login interface. At the top, the SecureAuth logo is visible. Below it, the text reads "Step 1. Please choose the delivery method for your Passcode and click 'Deliver OTP' button." There are four radio button options: "SMS", "VOICE" (with a dropdown menu), "EMAIL" (with a dropdown menu), "PUSH To ACCEPT: VTR-L29", and "Time-based Passcode: VTR-L29". Below these options is an orange button labeled "Send OTP or Push Notification".

Below the first section, the text reads "Step 2. Please type in your Passcode and click Submit button." There is a light blue input field for the passcode, and below it is an orange button labeled "Submit".

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

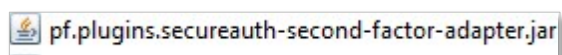
1. Set up the environment
2. Create a password credential validator
3. Create the HTML Form Adapter
4. Configure the Identity Platform for API
5. Create the SecureAuth 2FA adapter
6. Create the SecureAuth composite adapter
7. Create service provider (SP) connections
8. Configure the HTML Form Adapter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

Set up the environment

It is required to set up the PingFederate environment 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



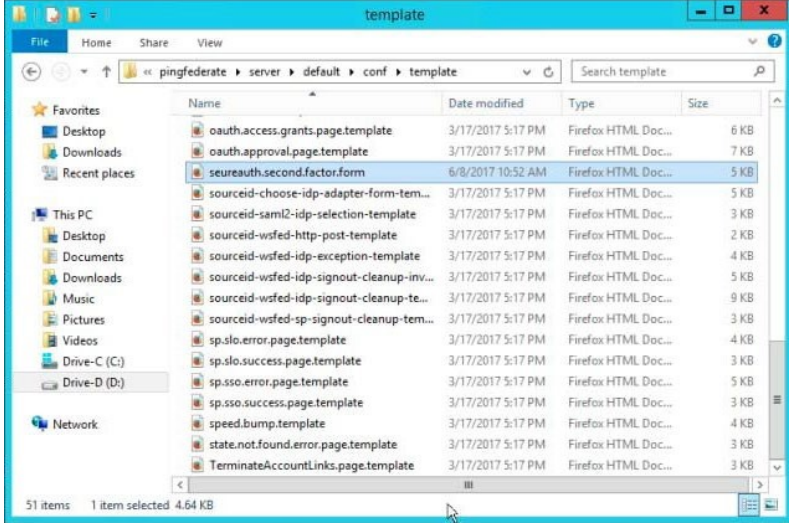
2. Copy the jar files (as shown in the image example) to the following deploy directory: ...\\pingfederate-8.3.2\\pingfederate\\server\\default\\deploy

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

- 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 
secureauth-logo.jpg	... \pingfederate\server\default\conf\template\assets\images
attribute-form-template.properties	... \pingfederate\server\default\conf\language-packs

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

```

Administrator: Command Prompt - run.bat
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 hsmypass.bat
03/17/2017  05:17 PM             893 hsmypass.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          13,920 run.properties
03/17/2017  05:17 PM          11,027 run.sh
03/17/2017  05:17 PM           975 start.ini
                27 File(s)          417,009 bytes
                3 Dir(s)    49,619,193,856 bytes free

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

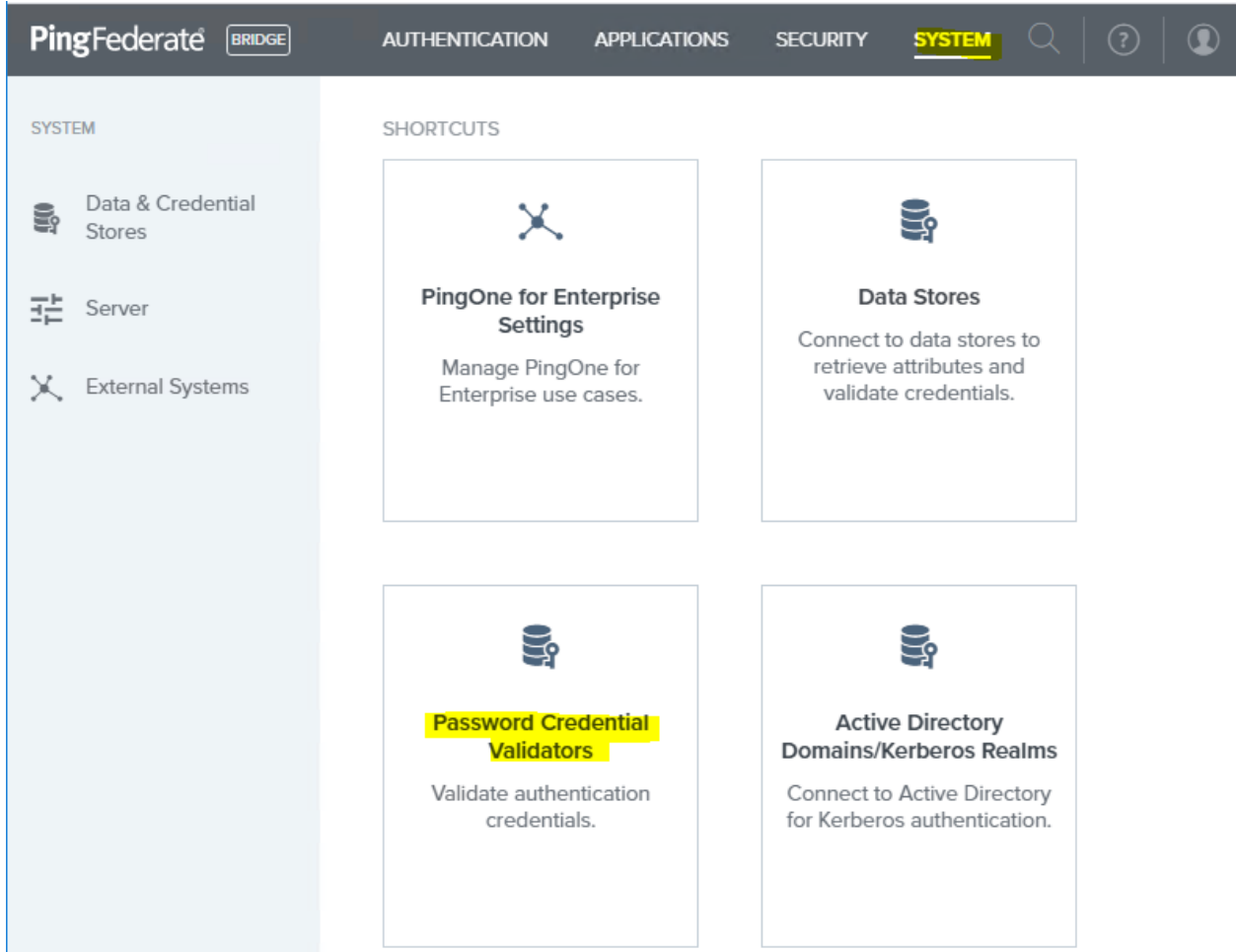
```

Create a password credential validator

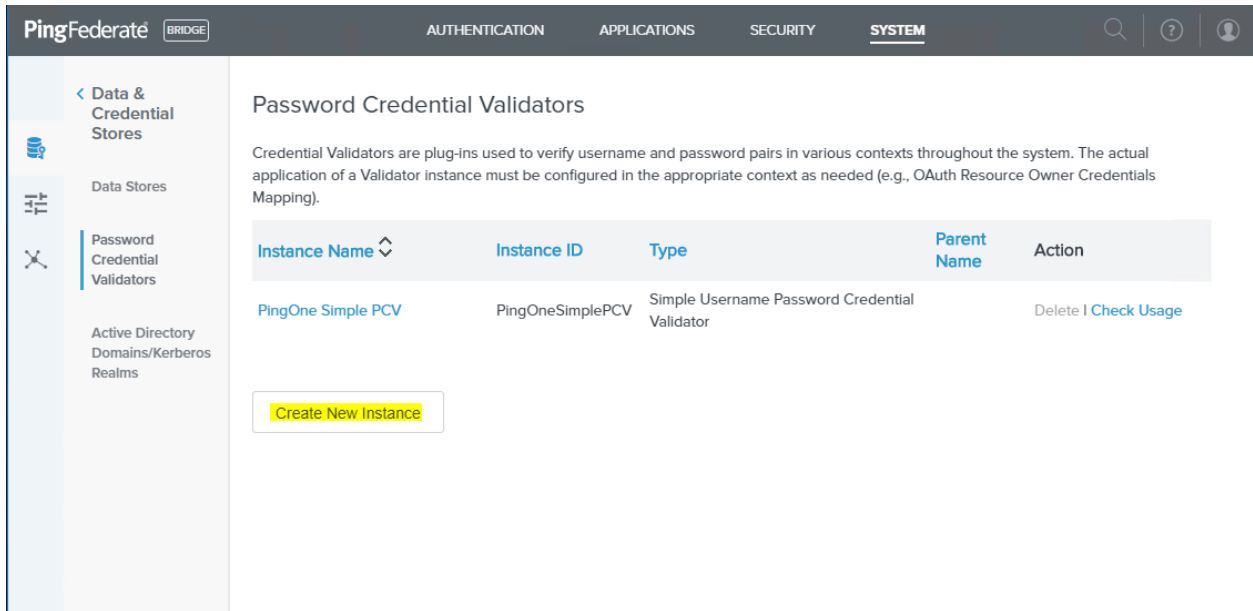
Password credential validators (PCV) allow PingFederate administrators to define a centralized location for username/password validation. This enables various PingFederate configurations to reference validator instances.

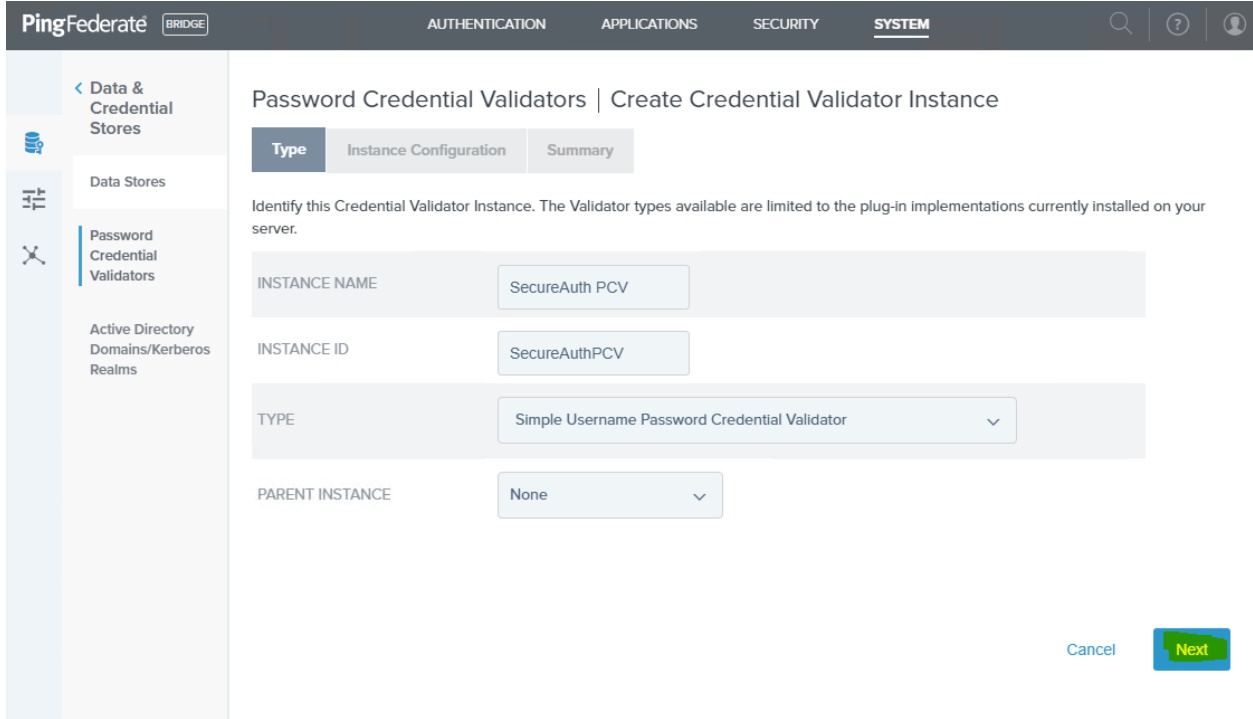
To create the password credential validator

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.

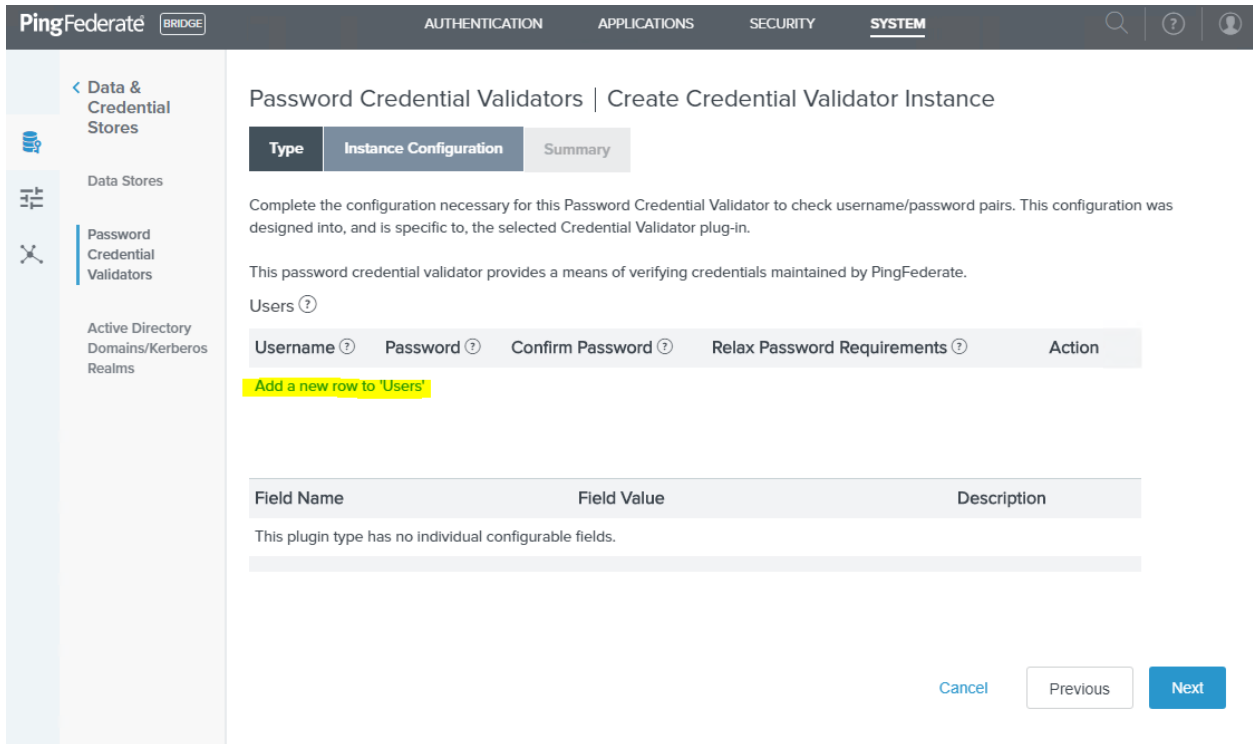


3. Click on **Create New Instance**.





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



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

PingFederate BRIDGE AUTHENTICATION APPLICATIONS SECURITY **SYSTEM**

< Data & Credential Stores

Data Stores

Password Credential Validators

Active Directory Domains/Kerberos Realms

Password Credential Validators | Create Credential Validator Instance

Type **Instance Configuration** Summary

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	*****	*****	<input type="checkbox"/>	Update Cancel

Add a new row to 'Users'

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

[Cancel](#) [Previous](#) [Next](#)

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

PingFederate BRIDGE AUTHENTICATION APPLICATIONS SECURITY SYSTEM

Data & Credential Stores

Data Stores

Password Credential Validators

Active Directory Domains/Kerberos Realms

Password Credential Validators | Create Credential Validator Instance

Type Instance Configuration Summary

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
-------	--------------------------------

Cancel Previous **Save**

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

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 Check Usage
SecureAuth PCV	SecureAuthPCV	Simple Username Password Credential Validator		Delete

Create New Instance

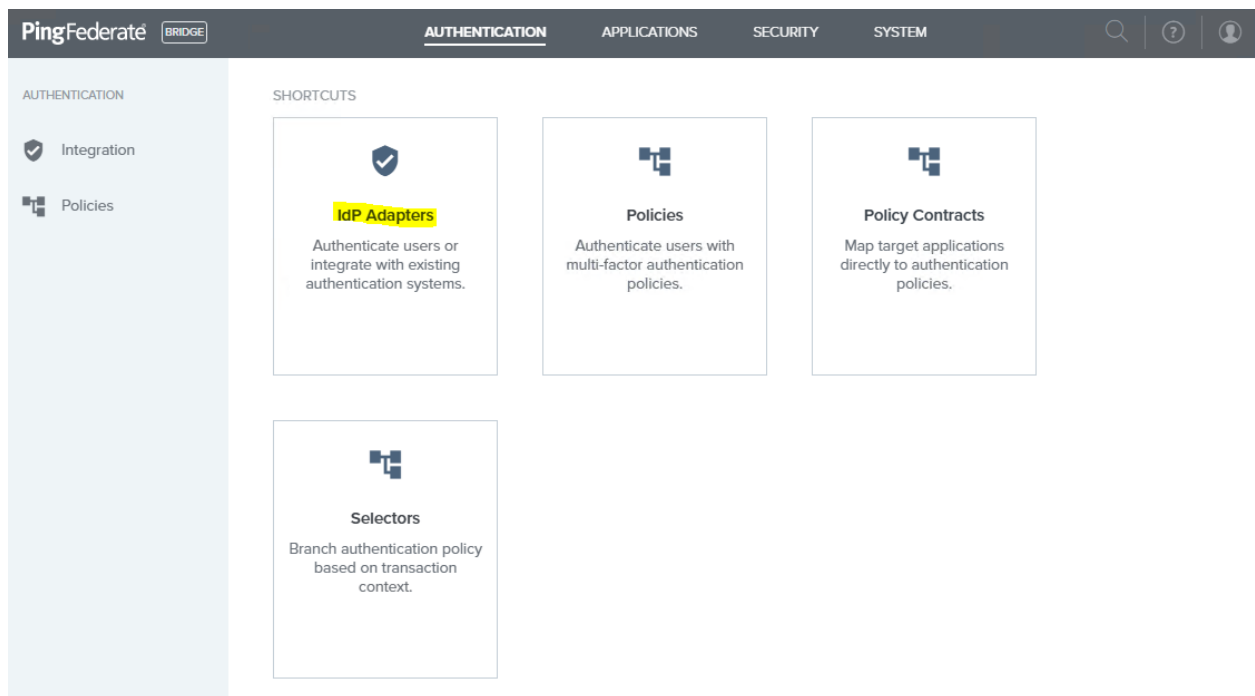
Create the HTML Form Adapter

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.

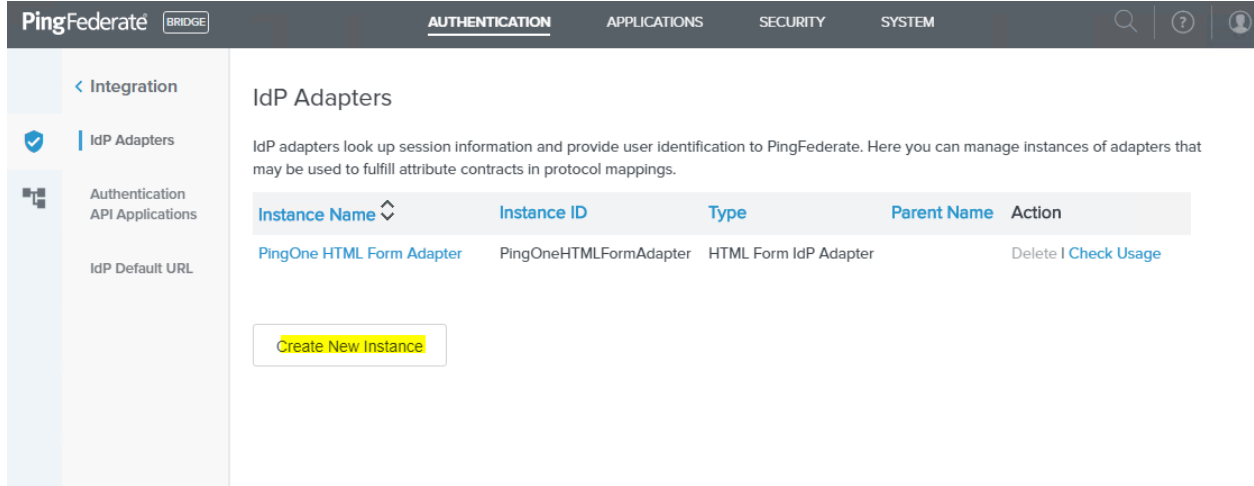
PingFederate packages an HTML Form Adapter that delegates user authentication to a configured password credential validator. This authentication mechanism validates credentials based on either an LDAP directory or a simple username validator that authenticates credentials maintained by PingFederate. 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.

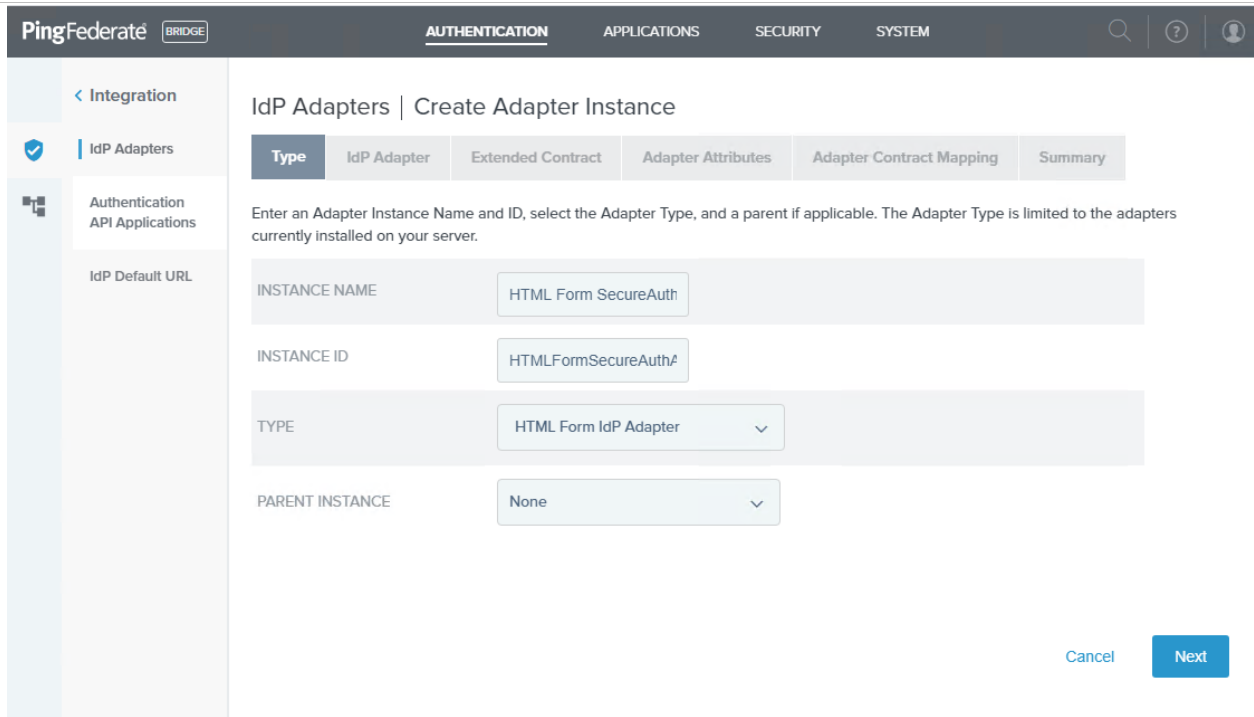


2. On the IdP Adapter Instances page, click **Create New Instance**.

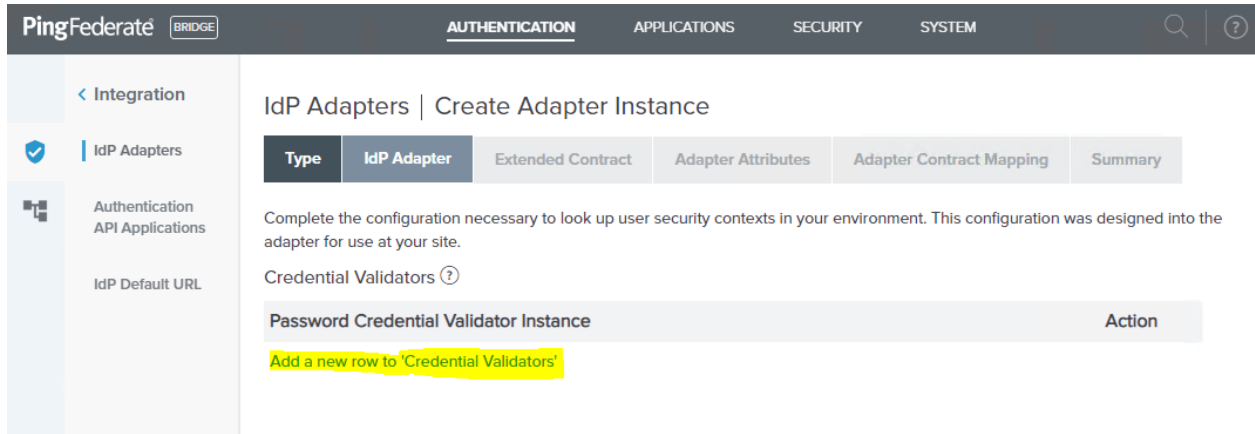


3. In the *Type* tab, set the following for the adapter instance type and click **Next**.

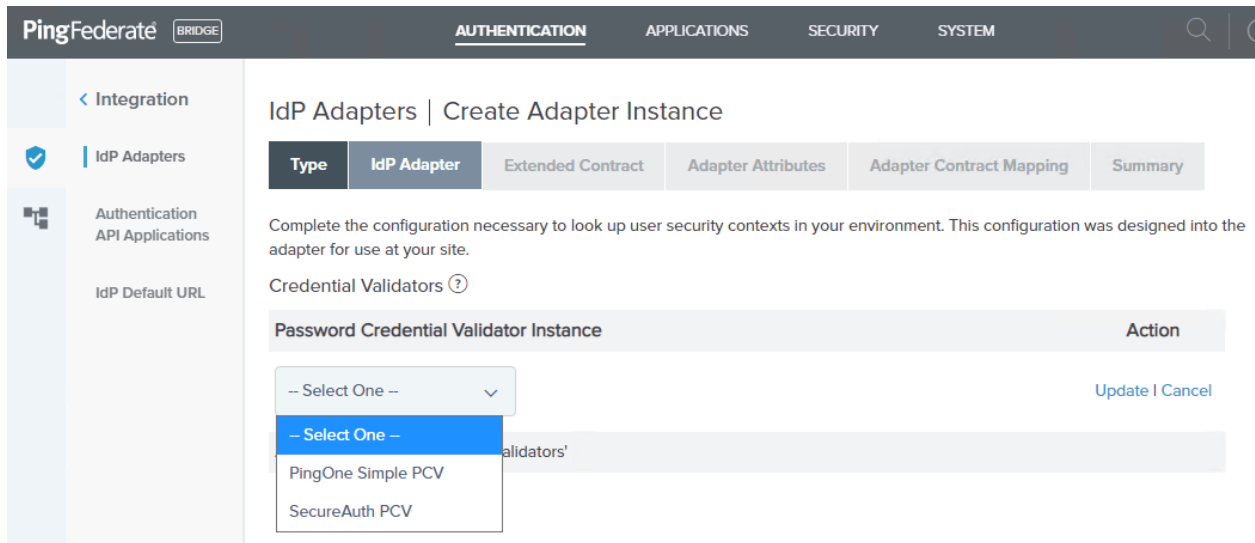
Field	Description
INSTANCE NAME	Enter the name of the instance
INSTANCE ID	Enter the ID of the instance
TYPE	Set to HTML From IdP Adapter.



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



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



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

The screenshot shows the 'Authentication' configuration page in the PingFederate Bridge console. The left sidebar contains 'Integration', 'IdP Adapters', 'Authentication API Applications', and 'IdP Default URL'. The main content area is titled 'PASSWORD RESET TYPE' and includes several configuration options:

- PASSWORD RESET TYPE:** Radio buttons for Authentication Policy, Email One-Time Link, Email One-Time Password, PingID, Text Message, and None (selected).
- PASSWORD RESET POLICY CONTRACT:** A dropdown menu with 'Select'.
- ACCOUNT UNLOCK:** A checkbox.
- LOCAL IDENTITY PROFILE:** A dropdown menu with '-- Select One --'.
- NOTIFICATION PUBLISHER:** A dropdown menu with '- SELECT -'.
- ENABLE USERNAME RECOVERY:** A checkbox.

Below these options are several management buttons: 'Manage Password Credential Validators', 'Manage SMS Provider Settings', 'Manage Local Identity Profiles', 'Manage Notification Publishers', 'Manage CAPTCHA Settings', and 'Manage Policy Contracts'. A 'Show Advanced Fields' link is also present. At the bottom right, there are 'Cancel', 'Previous', and 'Next' buttons.

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

The screenshot shows the 'IdP Adapters | Create Adapter Instance' page in the PingFederate Bridge console. The left sidebar is the same as in the previous screenshot. The main content area has a tabbed interface with the following tabs: 'Type', 'IdP Adapter', 'Extended Contract' (selected), 'Adapter Attributes', 'Adapter Contract Mapping', and 'Summary'.

Below the tabs, there is a description: "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."

The 'Extended Contract' section contains:

- Core Contract:** A text input field containing 'policy.action' and another containing 'username'.
- Extend the Contract:** A text input field.
- Action:** An 'Add' button.

At the bottom right, there are 'Cancel', 'Previous', and 'Next' buttons.

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

The screenshot shows the PingFederate Bridge console interface. The top navigation bar includes 'PingFederate BRIDGE', 'AUTHENTICATION', 'APPLICATIONS', 'SECURITY', and 'SYSTEM'. The left sidebar shows 'Integration' with sub-items 'IdP Adapters', 'Authentication API Applications', and 'IdP Default URL'. The main content area is titled 'IdP Adapters | Create Adapter Instance' and has tabs for 'Type', 'IdP Adapter', 'Extended Contract', 'Adapter Attributes' (selected), 'Adapter Contract Mapping', and 'Summary'. Below the tabs, there is a text block: '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.' Below this is a table with three columns: 'Attribute', 'Pseudonym', and 'Mask Log Values'. The table contains two rows: 'policy.action' with 'Pseudonym' and 'Mask Log Values' checkboxes unchecked, and 'username' with 'Pseudonym' checked and 'Mask Log Values' unchecked. Below the table is a checkbox labeled 'MASK ALL OGNL-EXPRESSION GENERATED LOG VALUES' which is unchecked. At the bottom right, there are three buttons: 'Cancel', 'Previous', and 'Next'.

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

The screenshot shows the PingFederate Bridge console interface, similar to the previous one. The top navigation bar and left sidebar are the same. The main content area is titled 'IdP Adapters | Create Adapter Instance' and has tabs for 'Type', 'IdP Adapter', 'Extended Contract', 'Adapter Attributes', 'Adapter Contract Mapping' (selected), and 'Summary'. Below the tabs, there is a text block: '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.' Below this text is a button labeled 'Configure Adapter Contract'. At the bottom right, there are three buttons: 'Cancel', 'Previous', and 'Next'.

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

PingFederate BRIDGE

[AUTHENTICATION](#)
[APPLICATIONS](#)
[SECURITY](#)
[SYSTEM](#)

< Integration

✓ IdP Adapters

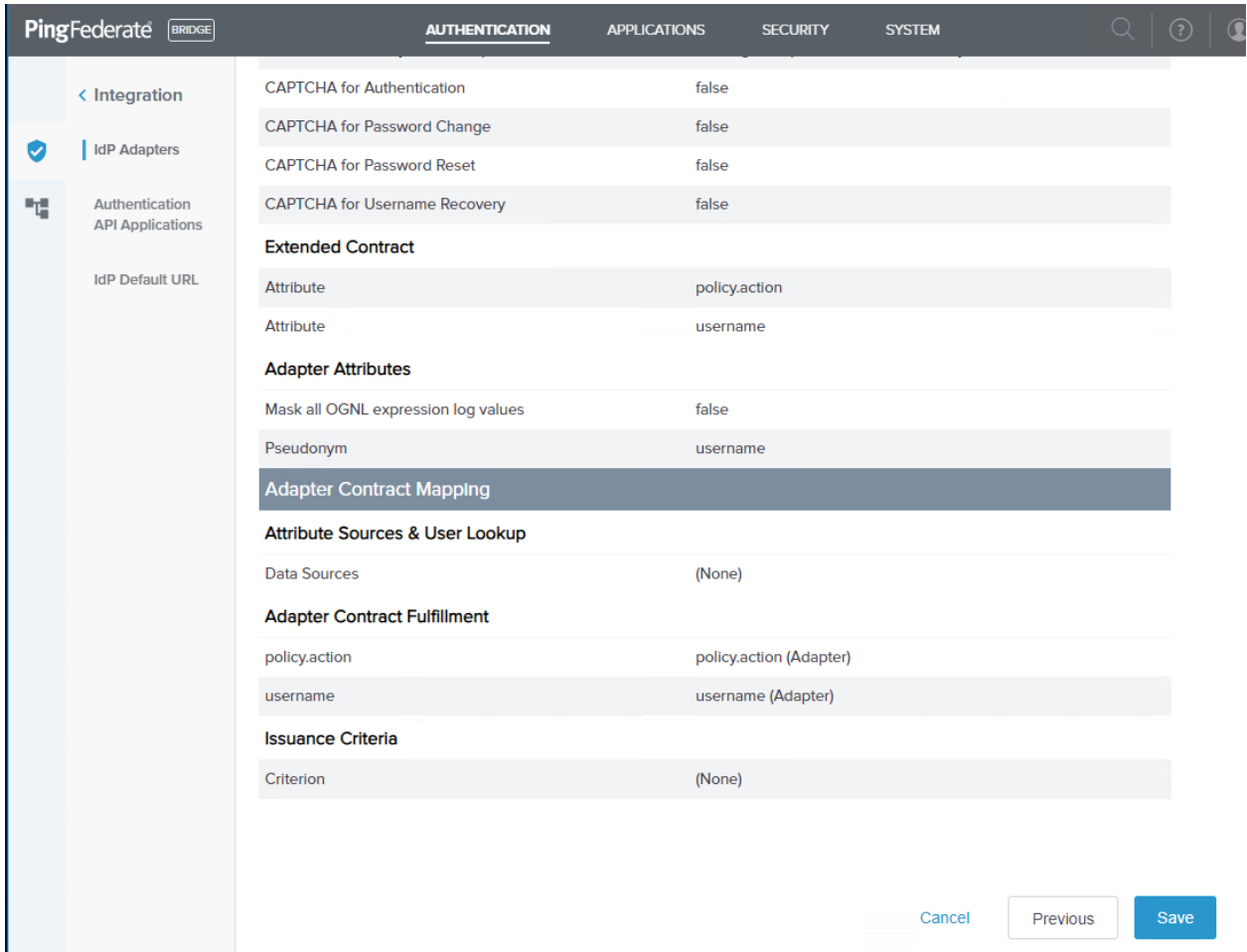
⊞ Authentication API Applications

IdP Default URL

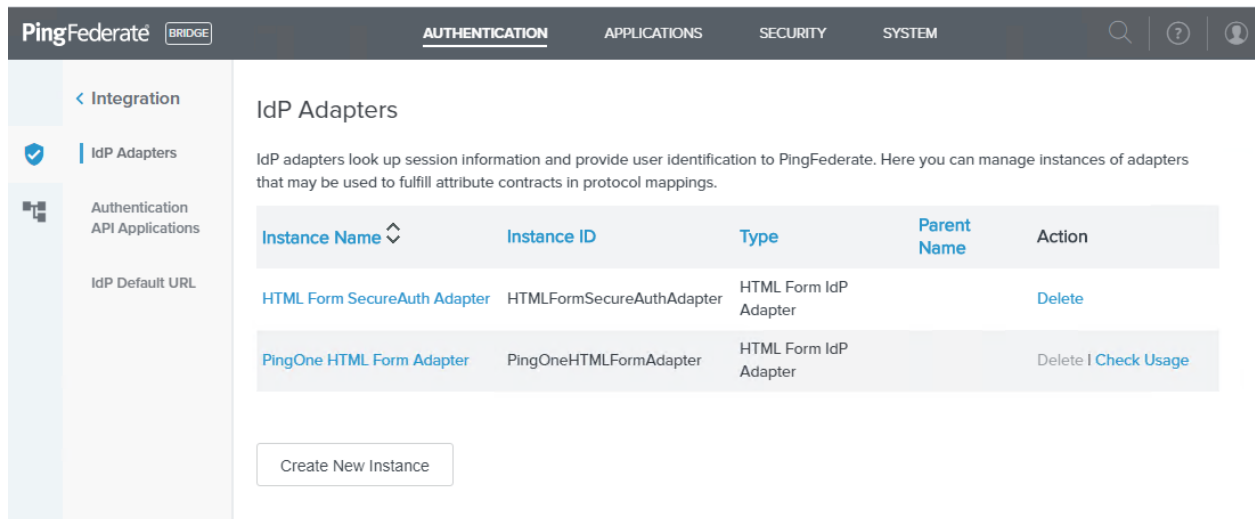
IdP Adapters | Create Adapter Instance

Type	IdP Adapter	Extended Contract	Adapter Attributes	Adapter Contract Mapping	Summary
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				

PingFederate BRIDGE		AUTHENTICATION	APPLICATIONS	SECURITY	SYSTEM
<ul style="list-style-type: none"> < Integration IdP Adapters Authentication API Applications IdP Default URL 		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	



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



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](#).

The screenshot shows the 'Membership Connection Settings' configuration page. The 'Data Store' is set to 'Active Directory (sAMAccountName)'. The 'Domain' is '@ sacustom.local', and the 'Connection String' is 'LDAP://sacustom.local/DC=sacustom,DC=local'. The 'Anonymous LookUp' is set to 'False'. The 'Service Account' is 'cd0505_svc' with the domain '@ sacustom.local'. The 'Password' is masked with dots and has a 'Hidden' checkbox checked. The 'Connection Mode' is 'Secure'. The 'Search Attribute' is 'samAccountName', and the 'searchFilter' is '(&(samAccountName=%v)(objectclass=*))'. The 'Advanced AD User Check' is 'False', 'Validate User Type' is 'Search', and 'User Group Check Type' is 'Allow Access'. The 'User Groups' field is empty, and the 'Include Nested Groups' checkbox is unchecked. The 'Groups Field' is 'memberOf'. The 'Max Invalid Password Attempts' is '10'. A 'Test Connection' button is at the bottom.

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.

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

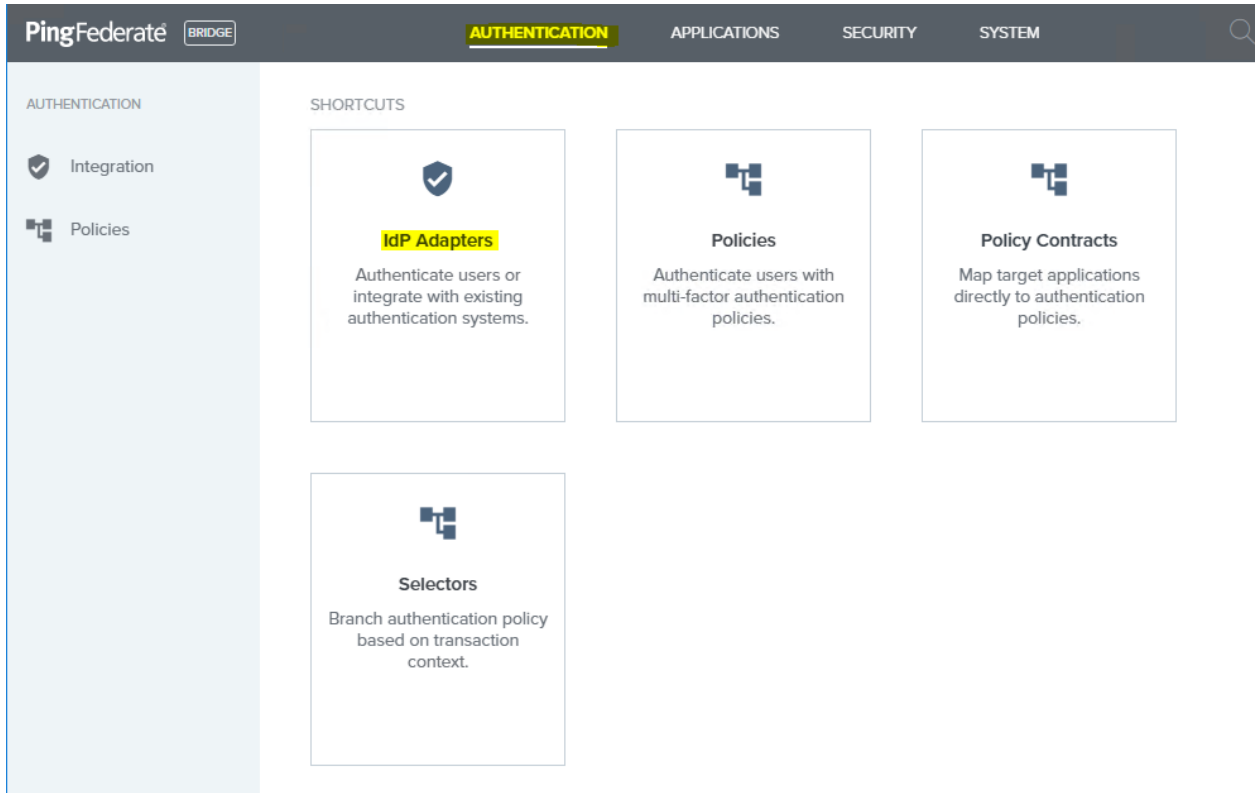
9. **Save** your changes.

For more information about API tab field settings, see [API Tab Configuration](#).

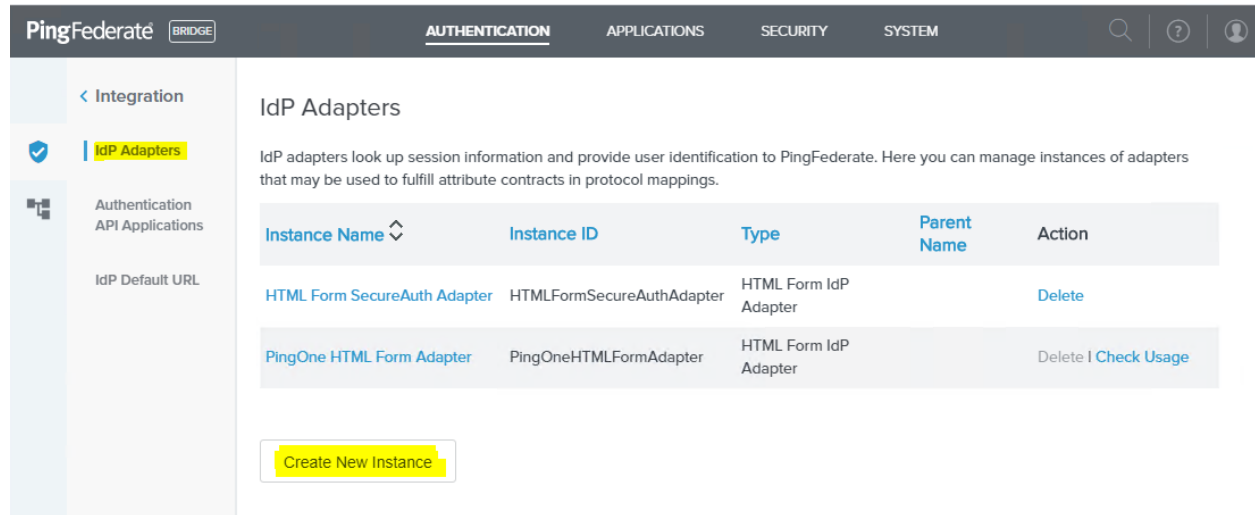
Create the 2FA adapter

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

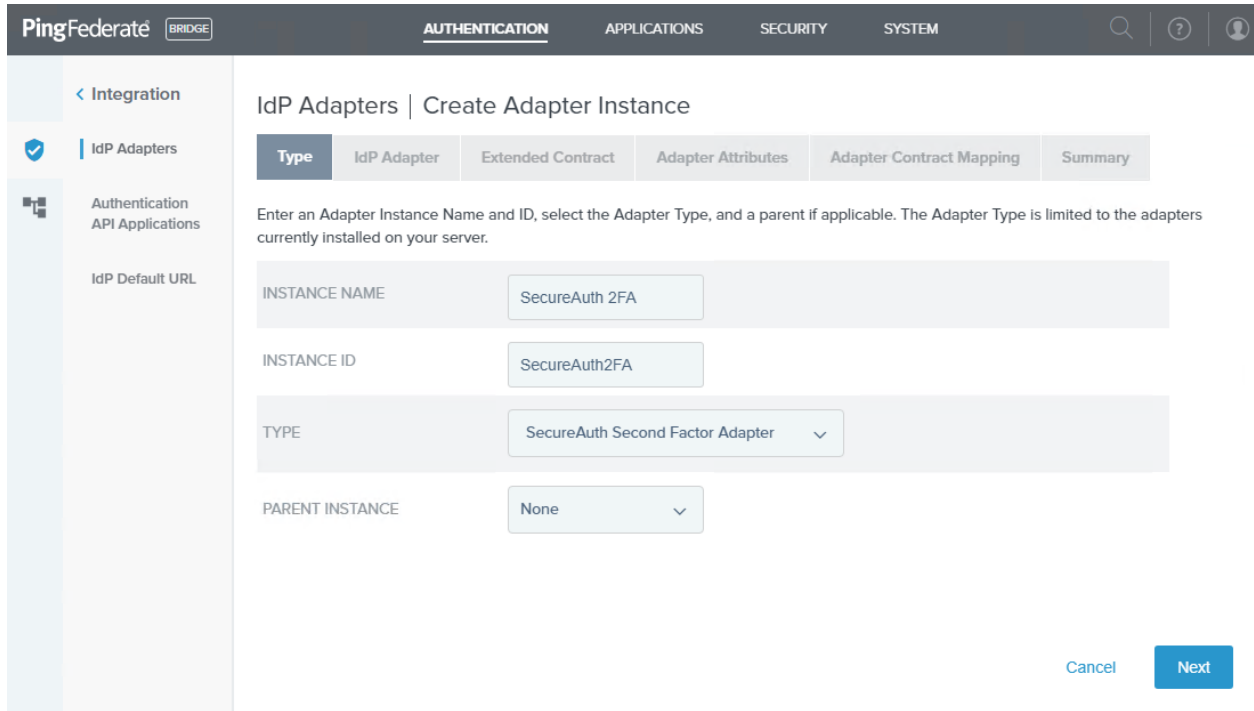
1. In PingFederate, select **AUTHENTICATION** and click the **IdP Adapters** link



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



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**.



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 .
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.

PingFederate BRIDGE AUTHENTICATION APPLICATIONS SECURITY SYSTEM

< Integration

IdP Adapters

Authentication API Applications

IdP Default URL

IdP Adapters | Create Adapter Instance

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

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

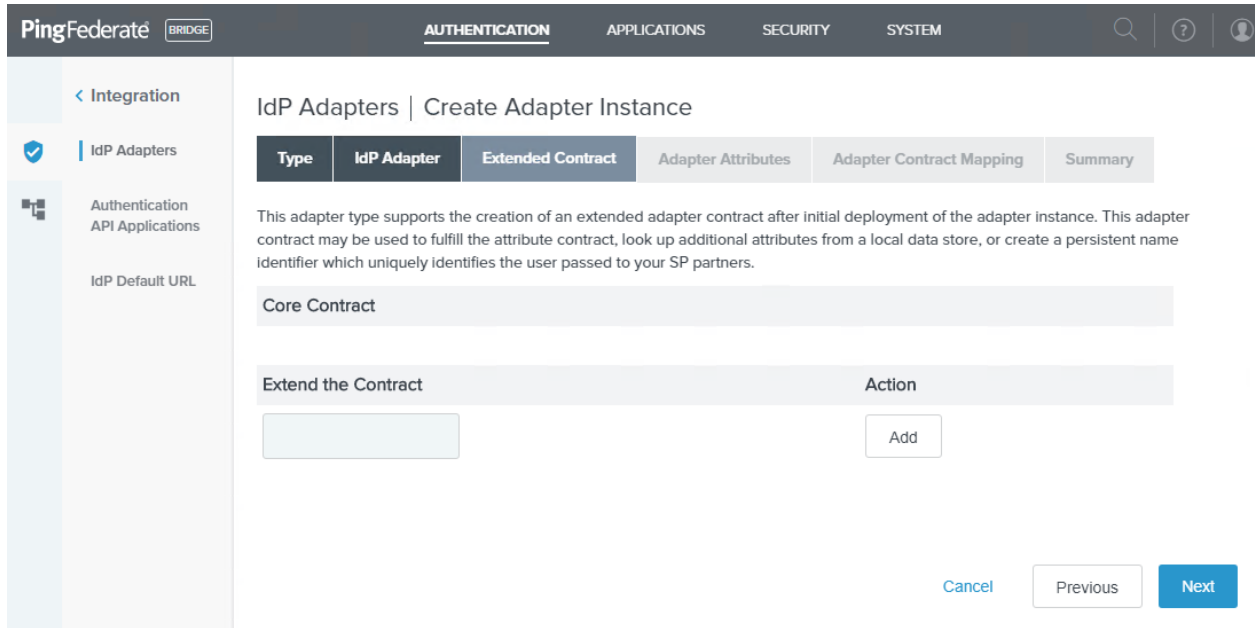
Field Name	Field Value	Description
HTML FORM TEMPLATE NAME	secureauth.second.factor.form.html	HTML template (in <pf_home>/server/default/conf/template) to render for form submission. The default value is attribute.form.template.html.
API-APP-ID	[REDACTED]	Enter the SecureAuth Realm API-App-ID to deliver 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)

The screenshot displays the configuration interface for the AUTHENTICATION tab in the PingFederate Bridge. The left sidebar shows the navigation menu with 'Integration' selected. The main content area contains a list of configuration parameters, each with an input field and a descriptive label. The parameters are:

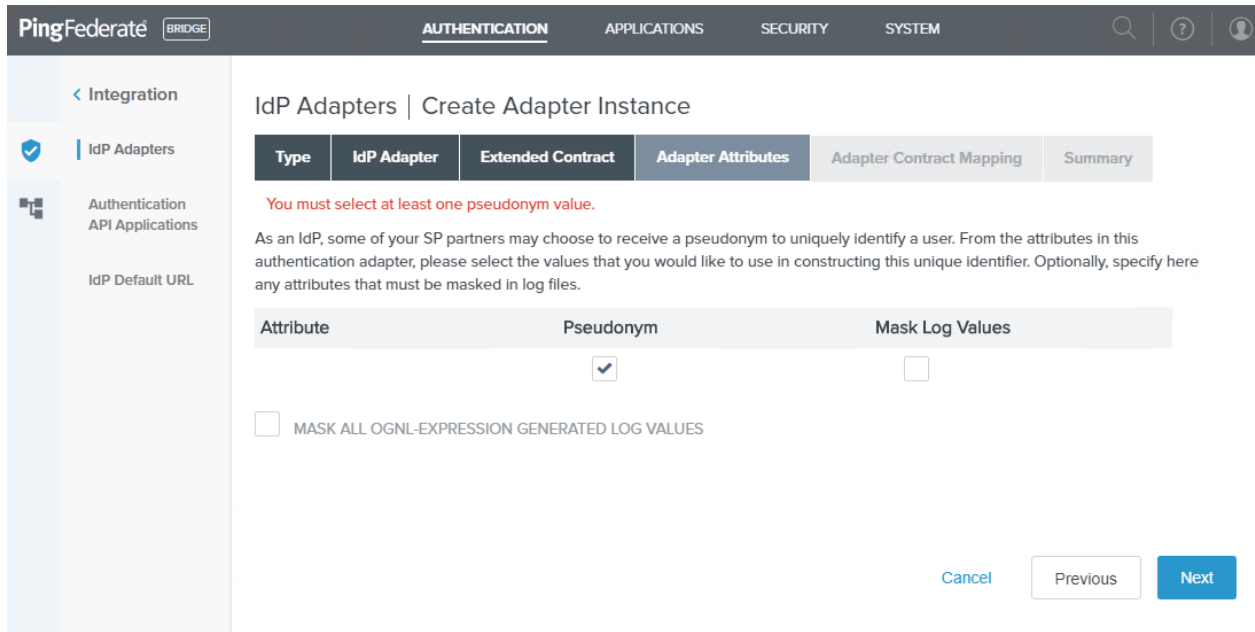
- API-APP-KEY**: Enter the SecureAuth Realm API-App-Key to deliver the OTP (Redacted)
- API-REALM**: Enter the SecureAuth Realm to deliver the OTP (Redacted)
- API-HOST**: Enter the SecureAuth Host to deliver the OTP (Redacted)
- API-PORT**: Enter the SecureAuth Realm port to deliver the OTP (443)
-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

At the bottom right of the configuration area, there are three buttons: 'Cancel', 'Previous', and 'Next'.

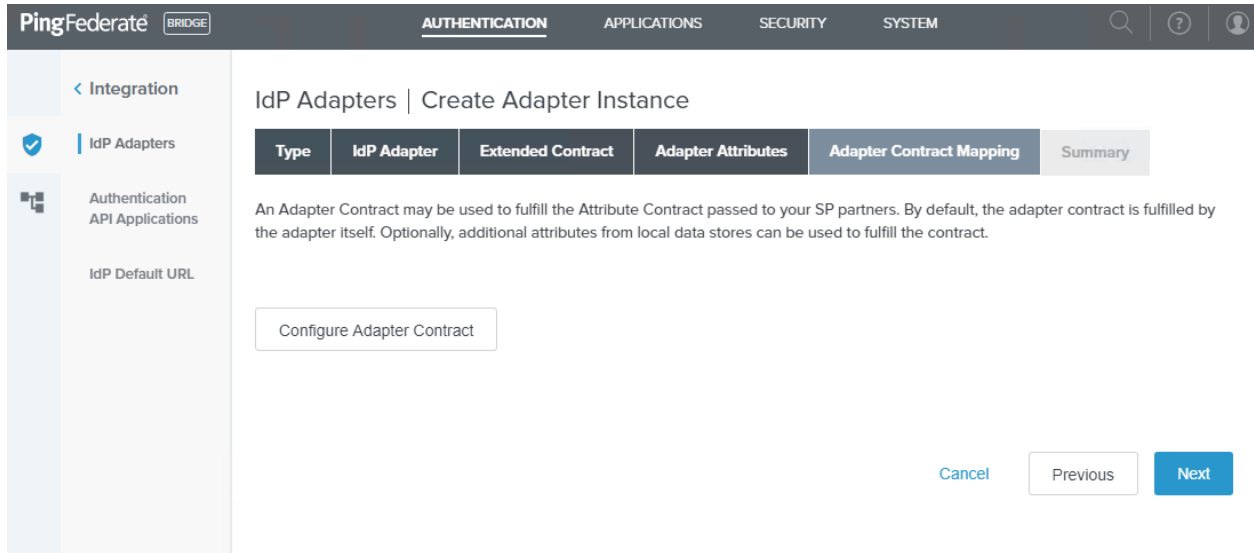
6. Click **Next**.
7. In the *Extended Contract* tab, click **Next**.



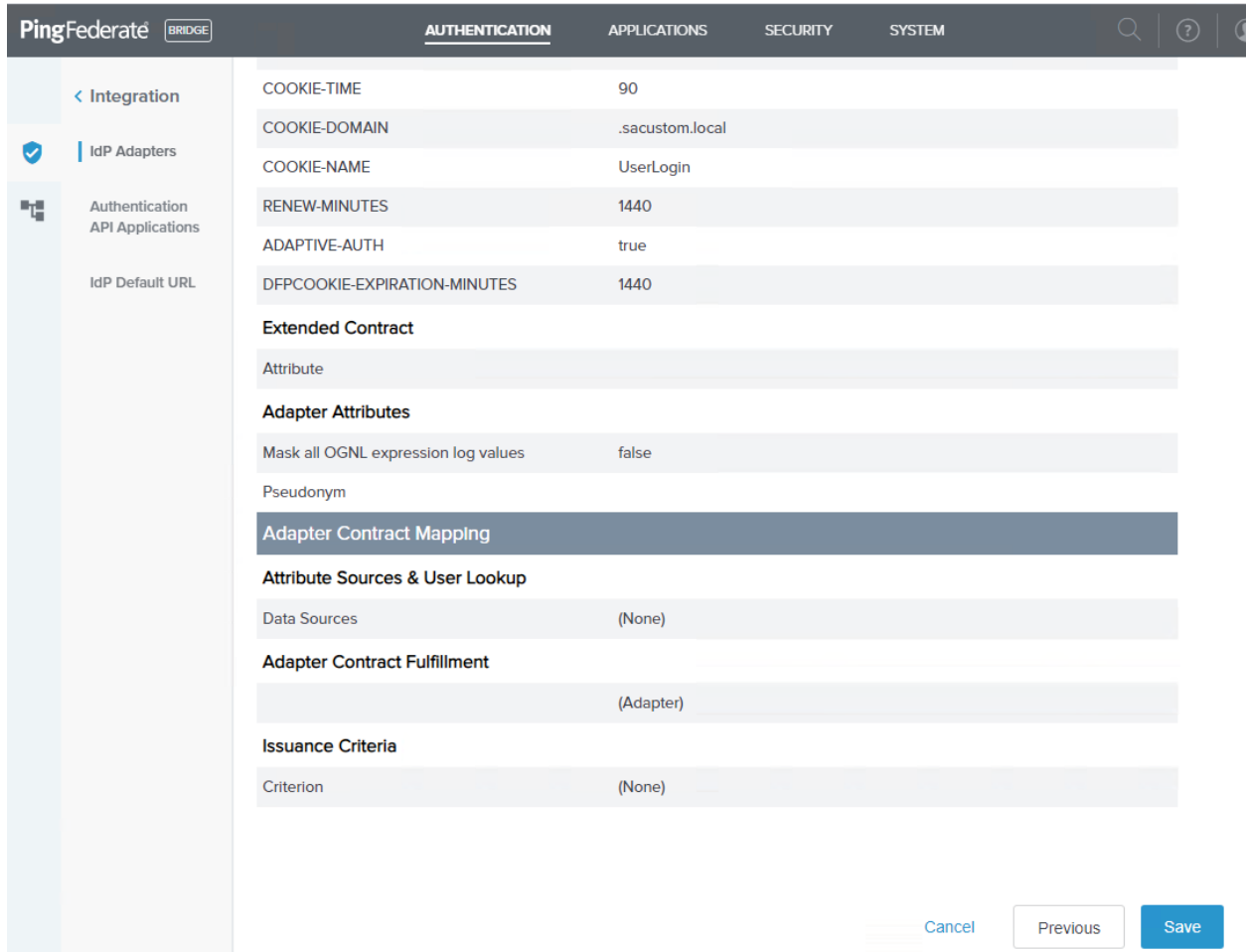
8. In the *Adapter Attributes* tab, select the **Pseudonym** check box.



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



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



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 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**.

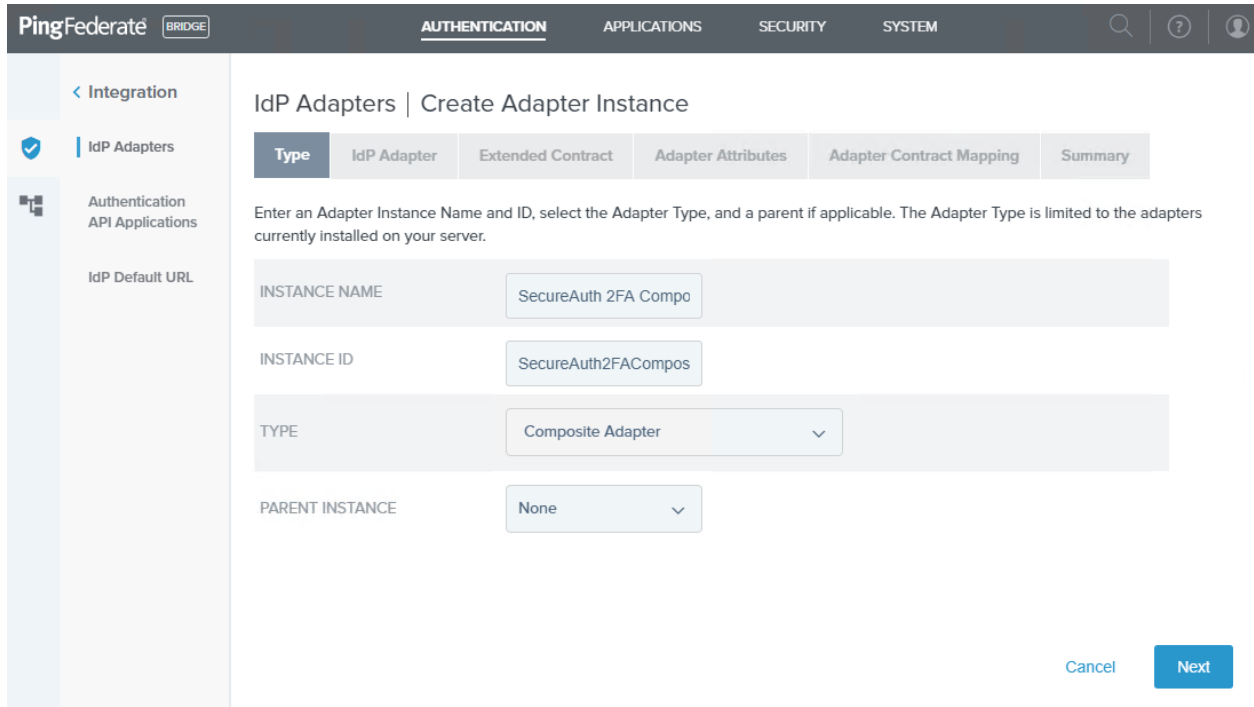
IdP Adapters

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.

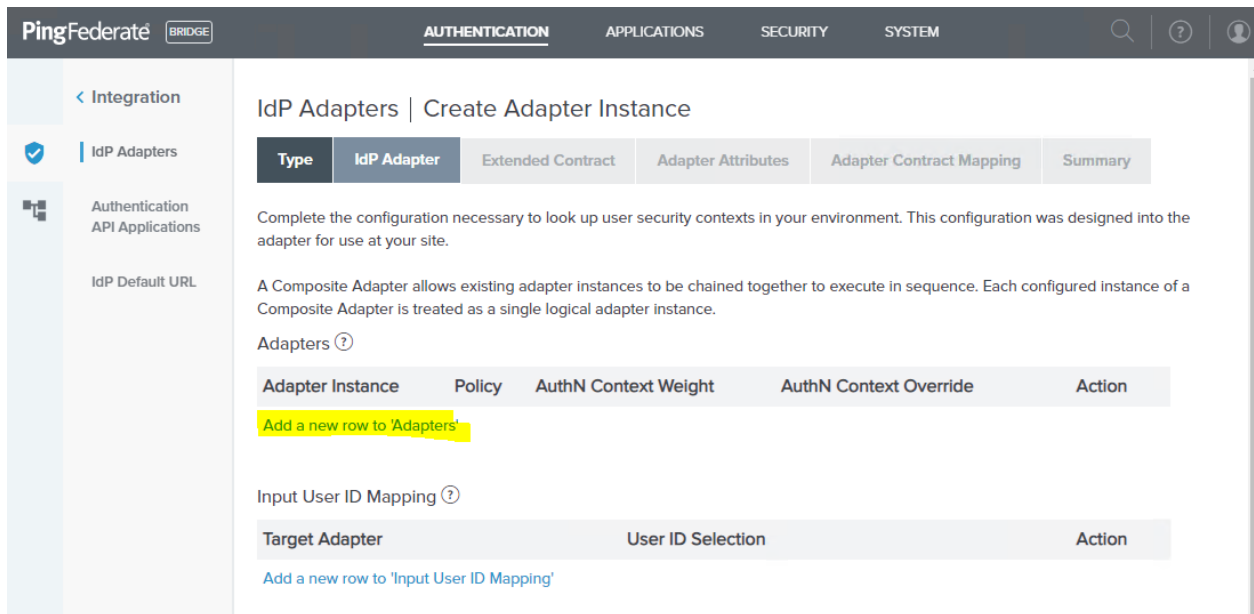
Instance Name	Instance ID	Type	Parent Name	Action
HTML Form SecureAuth Adapter	HTMLFormSecureAuthAdapter	HTML Form IdP Adapter		Delete
PingOne HTML Form Adapter	PingOneHTMLFormAdapter	HTML Form IdP Adapter		Delete Check Usage
SecureAuth 2FA	SecureAuth2FA	SecureAuth Second Factor Adapter		Delete

Create New Instance

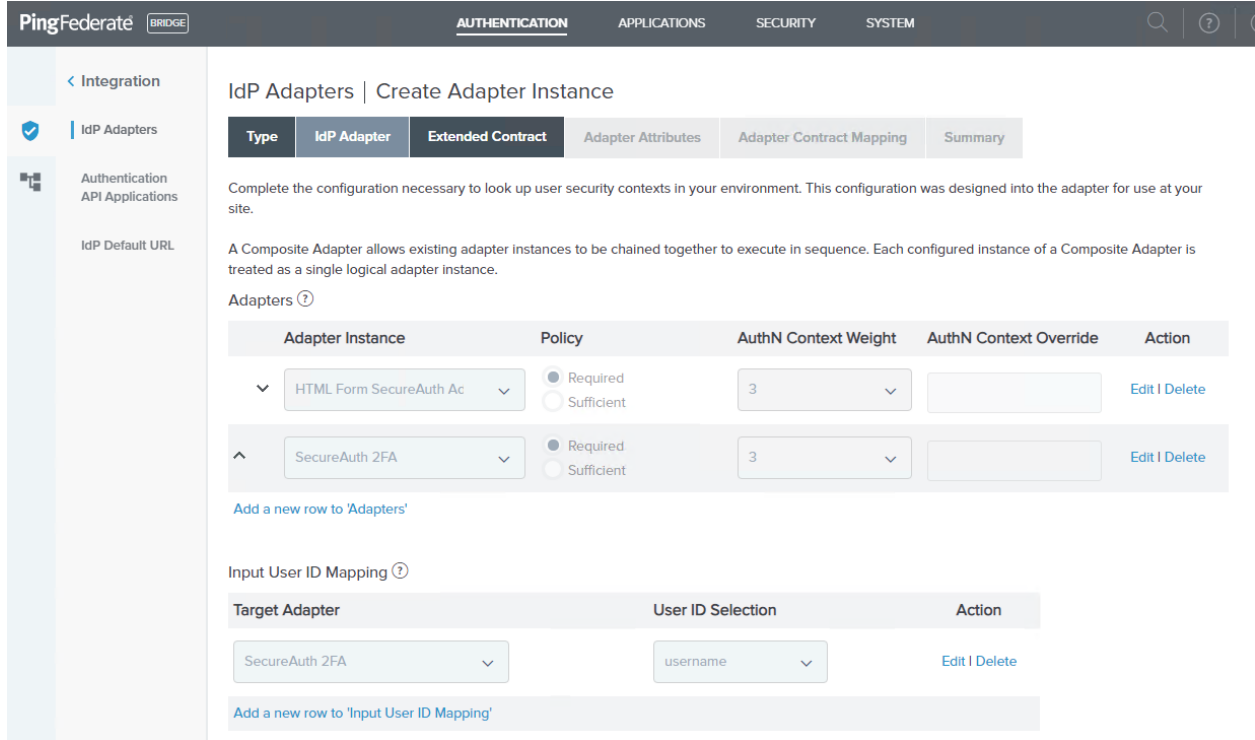
2. In the *Type* tab on the Create Adapter Instance page, set the following:
 - a. Set the **Instance Name**.
 - b. Set the **Instance ID**.
 - c. Set the **Type** to **Composite Adapter**.



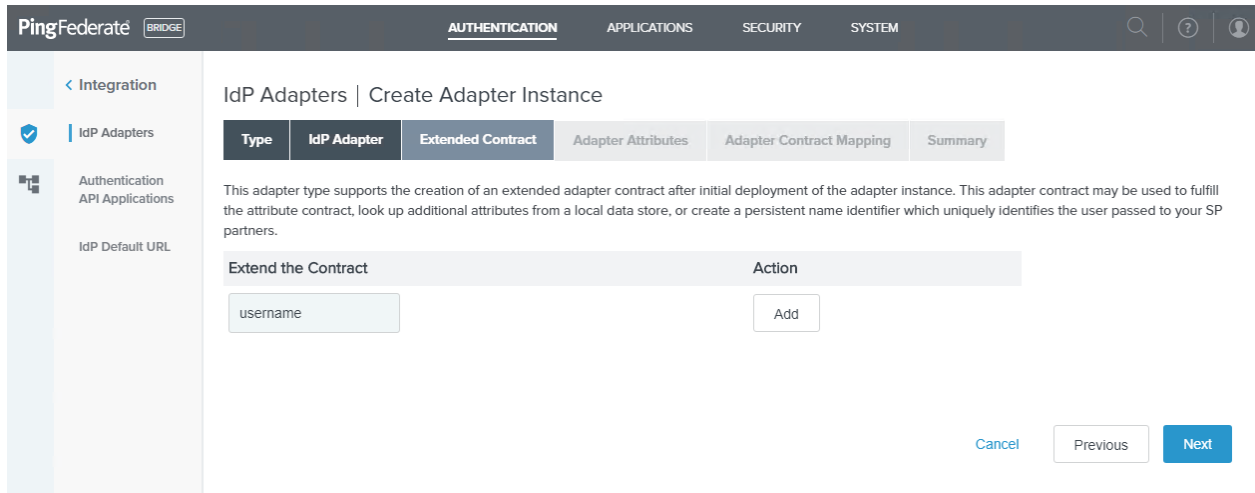
3. Click **Next**.
4. In the *IdP Adapter* tab, in the Adapters section, click the **Add a new row to 'Adapters'** link.



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.



- Verify that the order of the adapter instance is set with HTML Form IdP Adapter first, then followed by SecureAuth 2FA adapter. Click **Next**.
- In the *Extended Contract* tab, in the Extend the Contract section, add the **username** and Click **Next**.



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

The screenshot shows the PingFederate Bridge console with the 'AUTHENTICATION' tab selected. The left sidebar shows 'Integration' > 'IdP Adapters'. The main content area is titled 'IdP Adapters | Create Adapter Instance' and has a breadcrumb trail: Type > IdP Adapter > Extended Contract > **Adapter Attributes** > Adapter Contract Mapping > Summary. Below the breadcrumb, there is a text instruction: '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.' A table with three columns is shown: 'Attribute', 'Pseudonym', and 'Mask Log Values'. The 'username' row has a checked checkbox under 'Pseudonym' and an unchecked checkbox under 'Mask Log Values'. Below the table is a checkbox labeled 'MASK ALL OGNL-EXPRESSION GENERATED LOG VALUES' which is unchecked. At the bottom right, there are three buttons: 'Cancel', 'Previous', and 'Next'.

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

The screenshot shows the PingFederate Bridge console with the 'AUTHENTICATION' tab selected. The left sidebar shows 'Integration' > 'IdP Adapters'. The main content area is titled 'IdP Adapters | Create Adapter Instance' and has a breadcrumb trail: Type > IdP Adapter > Extended Contract > Adapter Attributes > **Adapter Contract Mapping** > Summary. Below the breadcrumb, there is a text instruction: '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.' A button labeled 'Configure Adapter Contract' is visible. At the bottom right, there are three buttons: 'Cancel', 'Previous', and 'Next'.

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

PingFederate BRIDGE

[AUTHENTICATION](#)
[APPLICATIONS](#)
[SECURITY](#)
[SYSTEM](#)

< Integration

| IdP Adapters

Authentication API Applications

IdP Default URL

IdP Adapters | Create Adapter Instance

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

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

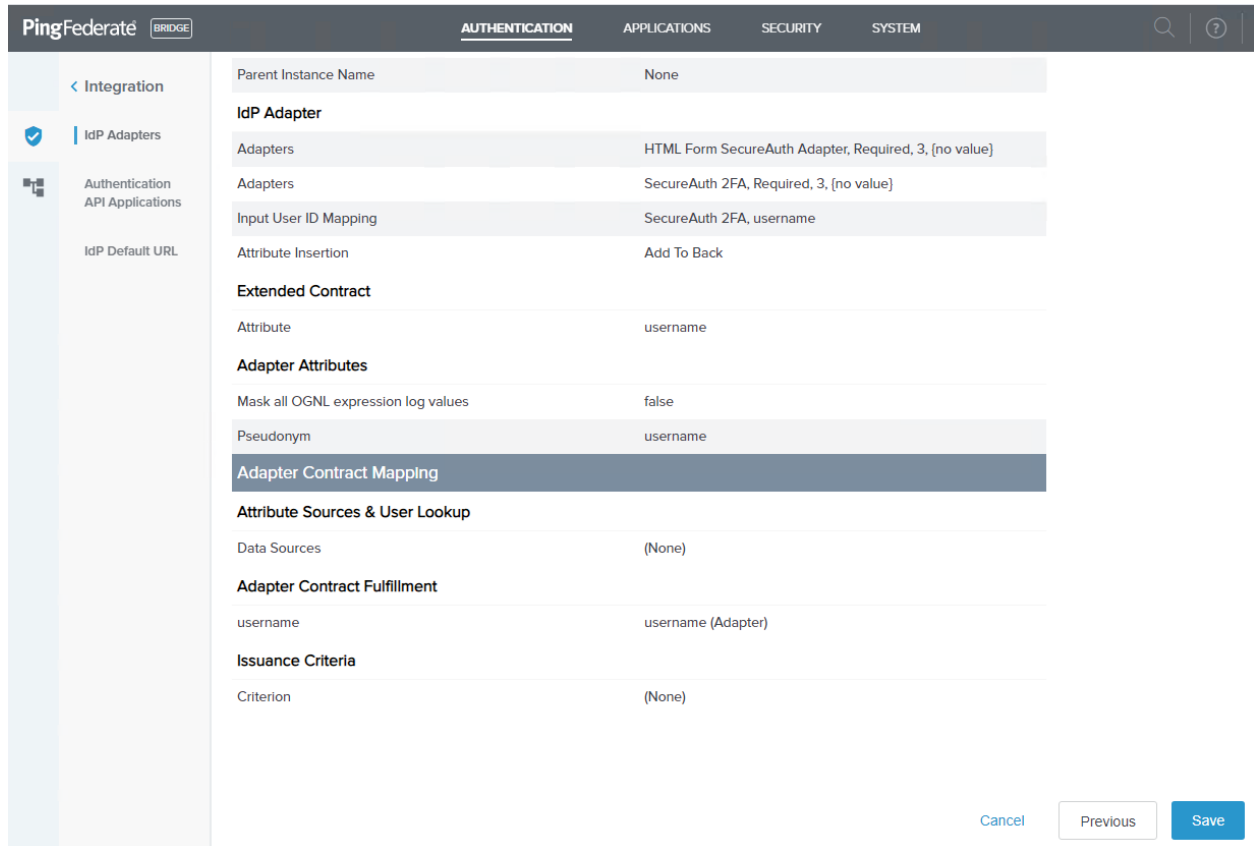
Adapters	HTML Form SecureAuth Adapter, Required, 3, [no value]
Adapters	SecureAuth 2FA, Required, 3, [no value]
Input User ID Mapping	SecureAuth 2FA, username
Attribute Insertion	Add To Back

Extended Contract

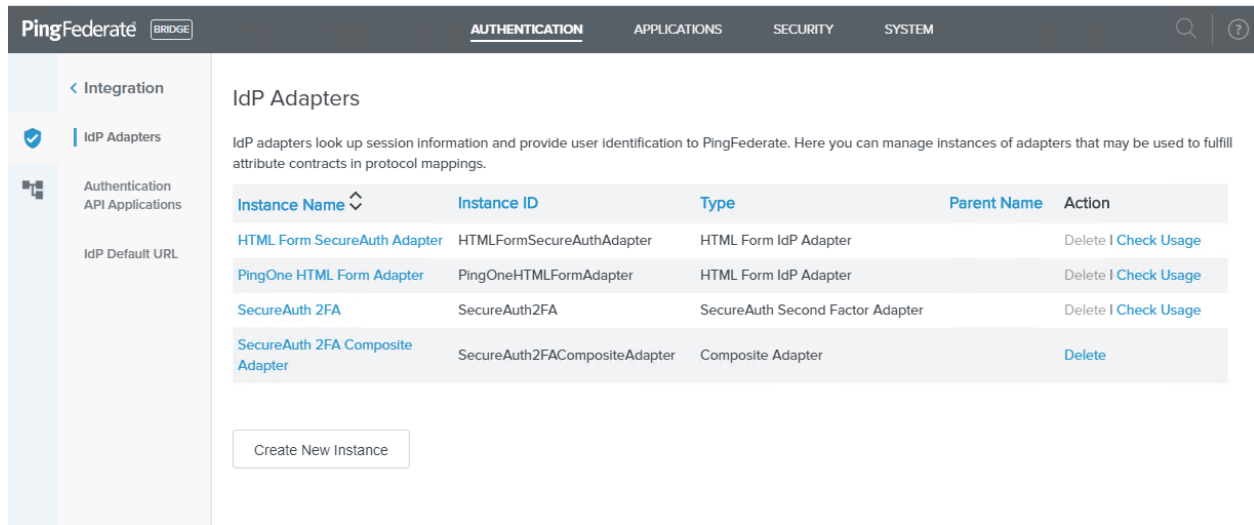
Attribute	username
-----------	----------

Adapter Attributes

Mask all OGNL expression log values	false
Pseudonym	username



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



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**.

The screenshot shows the PingFederate Bridge interface. The top navigation bar includes 'AUTHENTICATION', 'APPLICATIONS', 'SECURITY', and 'SYSTEM'. The 'APPLICATIONS' section is active, and the 'SP Connections' shortcut is highlighted. Below this, the 'SP Connections' page is shown, featuring a search bar, a table of connections, and a 'Create Connection' button.

SP Connections
Connect to partner service providers.

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

Search Clear Narrow By ▾

Connection Name ^	Connection ID	Virtual ID	Protocol	Enabled	Action
✓ PingOne	http://pingone.com/7c23048d-6b2e-42c...	urn:sam...	SAML 2.0	<input checked="" type="checkbox"/>	Select Action ▾

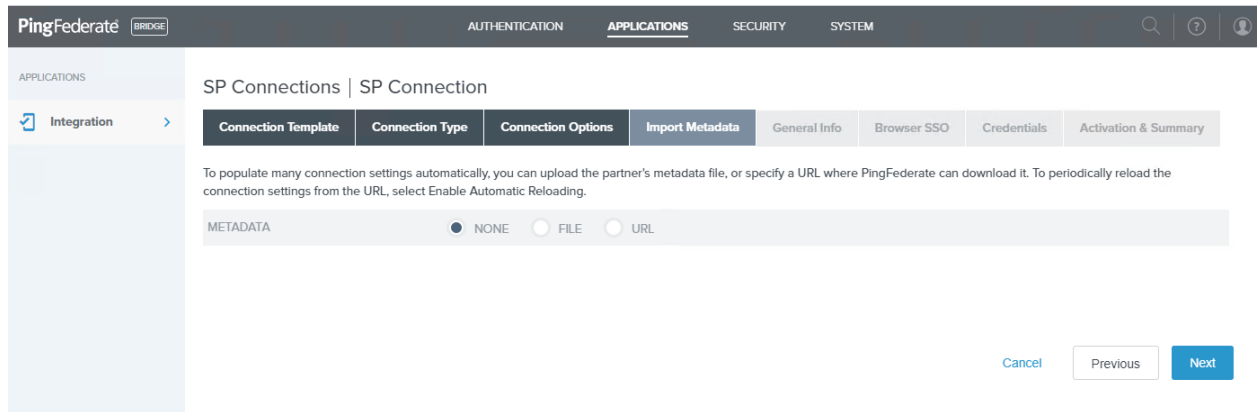
Create Connection Import Connection

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

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

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

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



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

PingFederate BRIDGE
AUTHENTICATION APPLICATIONS SECURITY SYSTEM
🔍 | ?

APPLICATIONS

🏠 Integration >

SP Connections | SP Connection

Connection Template

Connection Type

Connection Options

Import Metadata

General Info

Browser SSO

Credentials

Activation & Summary

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)

CONNECTION NAME

VIRTUAL SERVER IDS

BASE URL

COMPANY

CONTACT NAME

CONTACT NUMBER

CONTACT EMAIL

APPLICATION NAME

APPLICATION ICON URL

TRANSACTION LOGGING

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

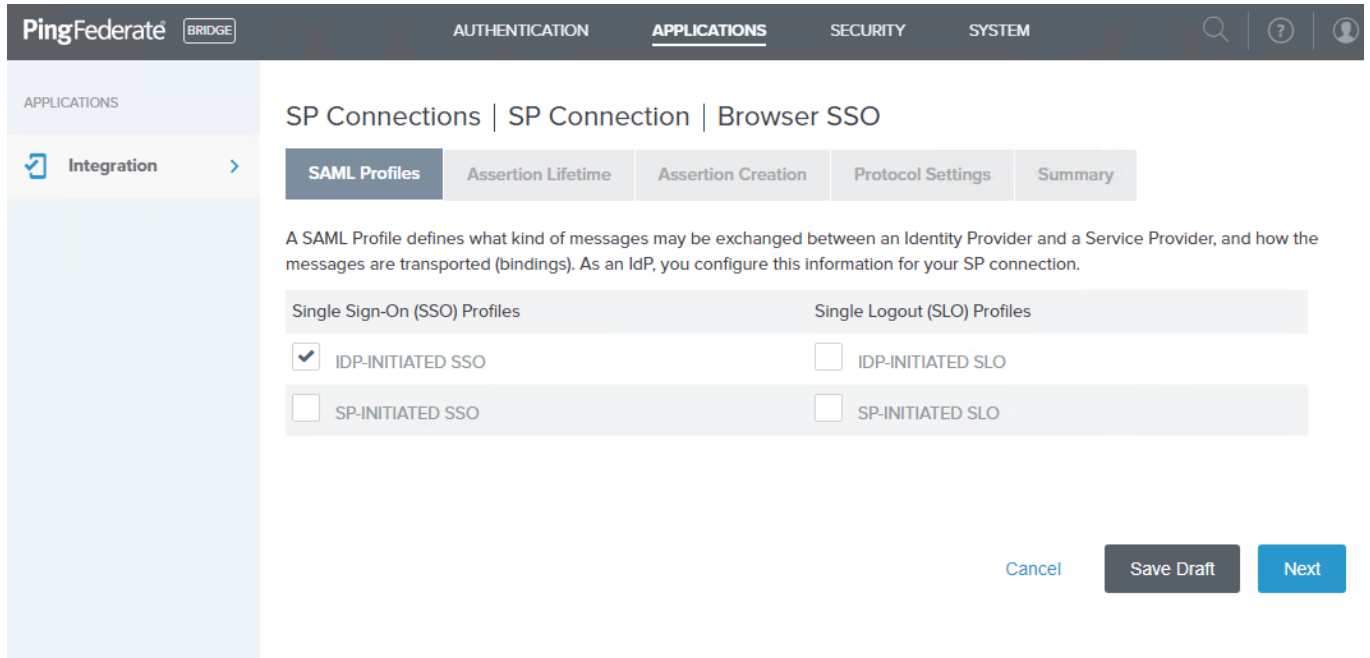
SP Connections | SP Connection

Connection Template | Connection Type | Connection Options | Import Metadata | General Info | **Browser SSO** | Credentials | Activation & Summary

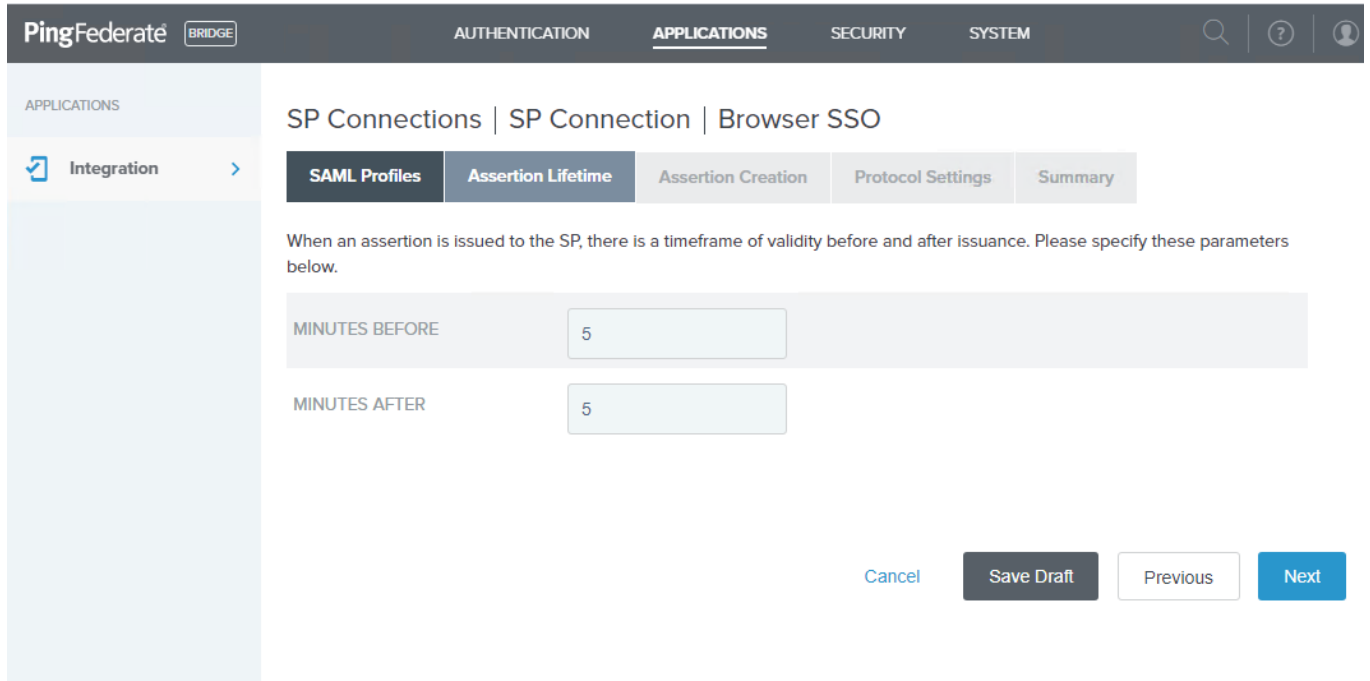
This task provides connection-endpoint and other configuration information enabling secure browser-based SSO, to resources at your partner's site. Click the button below to create or revise this configuration.

BROWSER SSO CONFIGURATION

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



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



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

The screenshot shows the PingFederate Bridge console interface. The top navigation bar includes 'PingFederate BRIDGE', 'AUTHENTICATION', 'APPLICATIONS' (selected), 'SECURITY', and 'SYSTEM'. The left sidebar shows 'APPLICATIONS' and 'Integration'. The main content area is titled 'SP Connections | SP Connection | Browser SSO' and contains several tabs: 'SAML Profiles', 'Assertion Lifetime', 'Assertion Creation' (selected), 'Protocol Settings', and 'Summary'. Below the tabs, a text block states: 'This task provides the configuration for creating SAML assertions to enable SSO access to resources at your SP partner's site.' Underneath is an 'Assertion Configuration' section with a table:

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

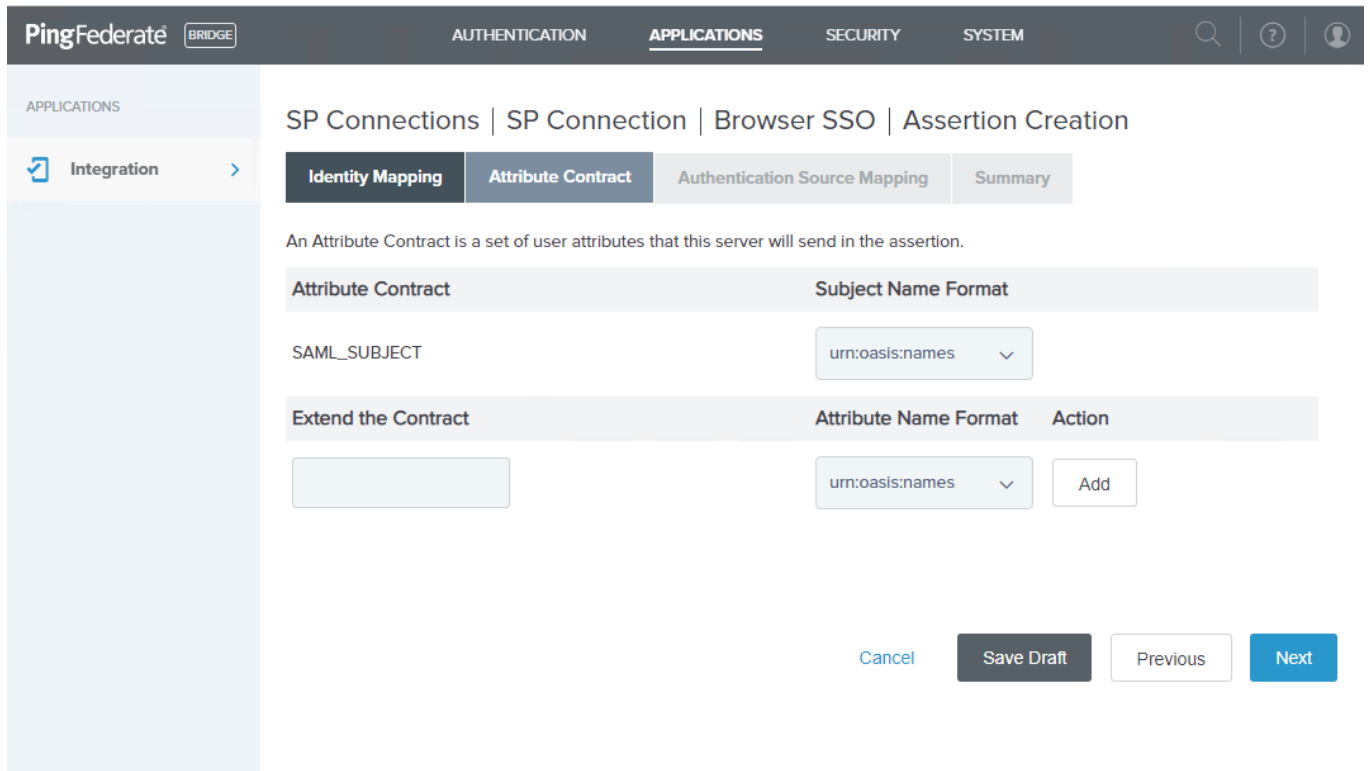
Below the table is a button labeled 'Configure Assertion Creation'. At the bottom right, there are four buttons: 'Cancel', 'Save Draft', 'Previous', and 'Next'.

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**.

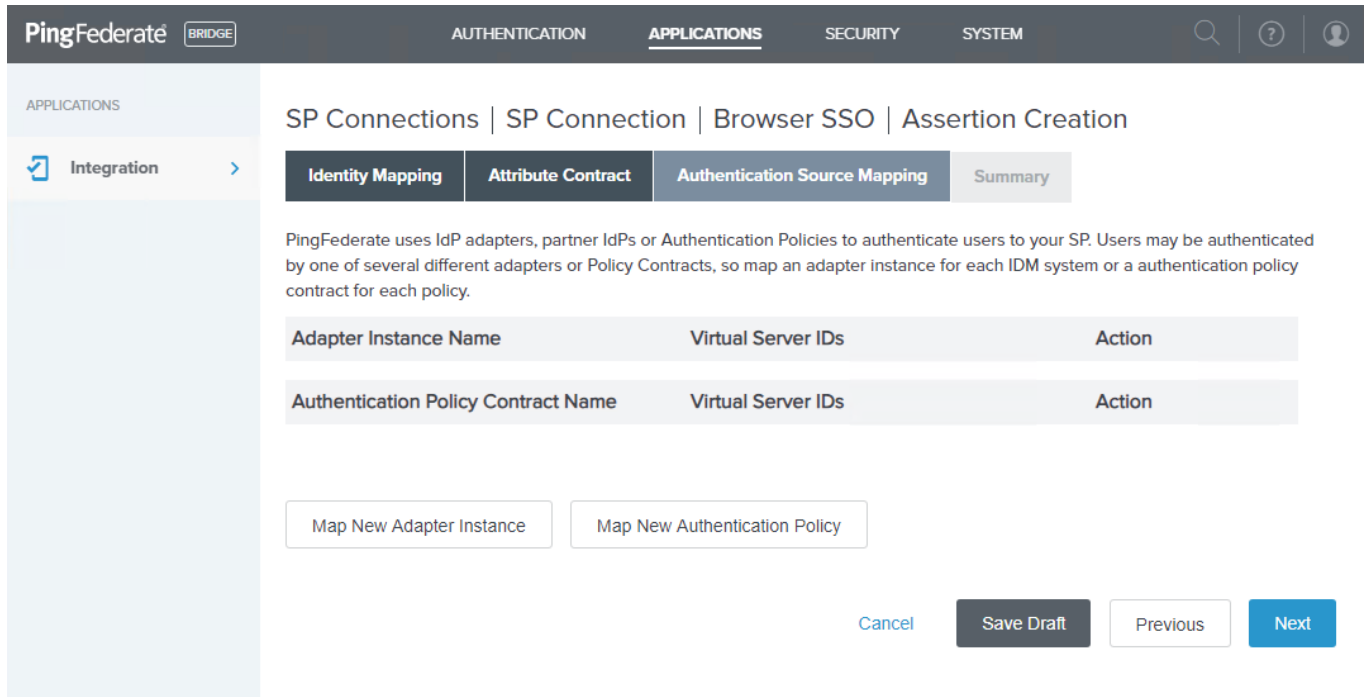
The screenshot shows the PingFederate Bridge interface. The top navigation bar includes 'PingFederate BRIDGE', 'AUTHENTICATION', 'APPLICATIONS' (selected), 'SECURITY', and 'SYSTEM'. The left sidebar shows 'APPLICATIONS' and 'Integration'. The main content area is titled 'SP Connections | SP Connection | Browser SSO | Assertion Creation' and has four tabs: 'Identity Mapping' (selected), 'Attribute Contract', 'Authentication Source Mapping', and 'Summary'. Below the tabs, a text block explains identity mapping. Three radio button options are available: 'STANDARD' (selected), 'PSEUDONYM', and 'TRANSIENT'. Each option has a checkbox for 'INCLUDE ATTRIBUTES IN ADDITION TO THE PSEUDONYM/IDENTIFIER'. At the bottom right, there are 'Cancel', 'Save Draft', and 'Next' buttons.

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**



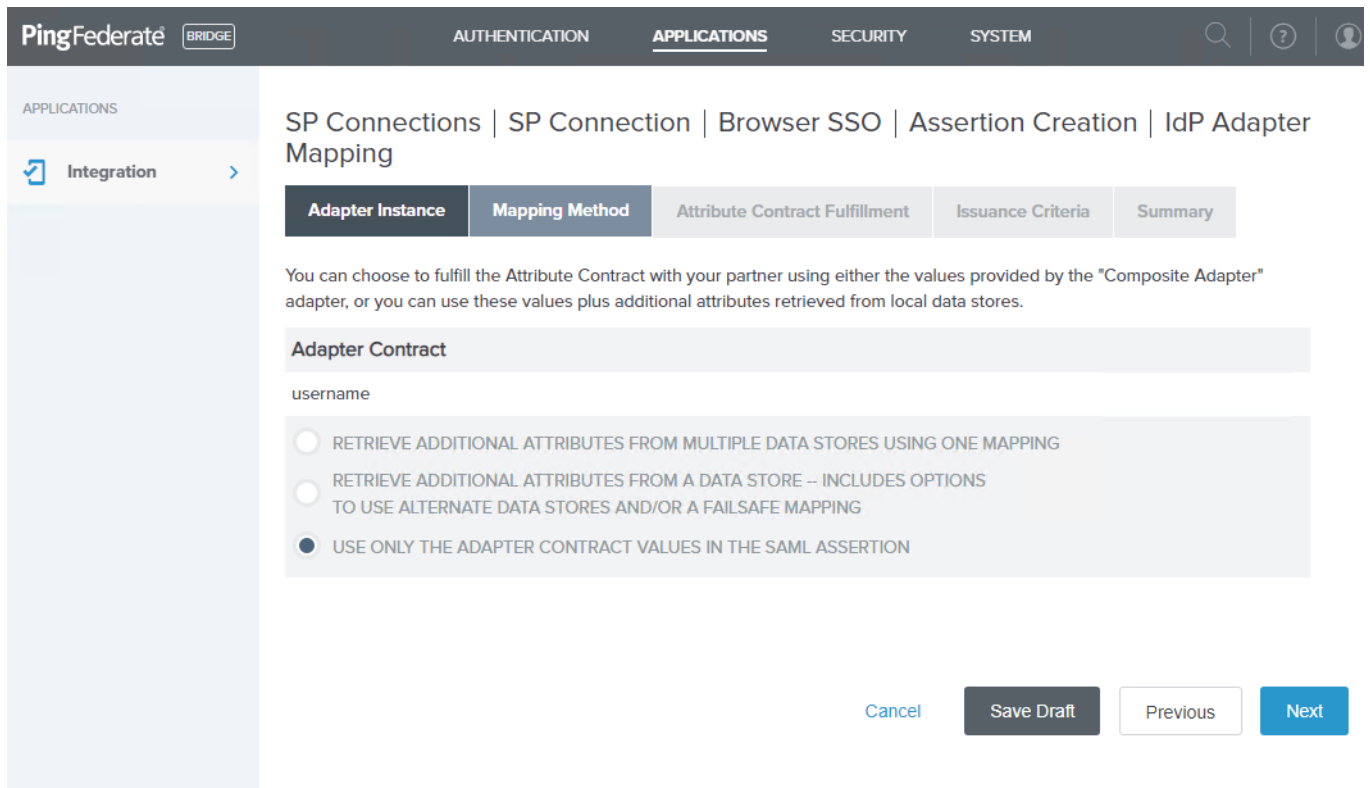
13. In the *Authentication Source Mapping* tab, click **Map New Adapter instance**.



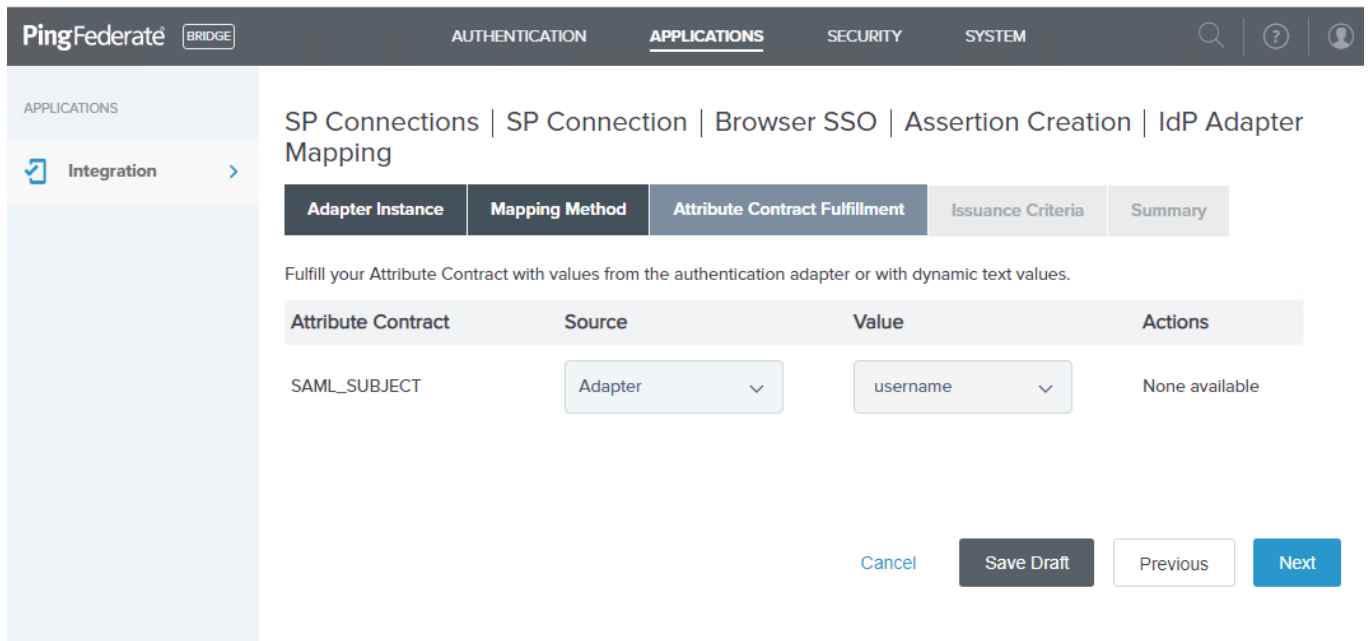
14. *Adapter Instance* tab on the SP Connection | Browser SSO | Assertion Creation | IdP Adapter Mapping page, set the **Adapter Instance** to **SecureAuth2FAComp** and click **Next**.

The screenshot shows the PingFederate Bridge console interface. The top navigation bar includes 'PingFederate BRIDGE', 'AUTHENTICATION', 'APPLICATIONS' (selected), 'SECURITY', and 'SYSTEM'. A search icon, help icon, and user profile icon are on the right. The left sidebar shows 'APPLICATIONS' and 'Integration' with a right-pointing arrow. The main content area is titled 'SP Connections | SP Connection | Browser SSO | Assertion Creation | IdP Adapter Mapping'. Below the title are five tabs: 'Adapter Instance' (active), 'Mapping Method', 'Attribute Contract Fulfillment', 'Issuance Criteria', and 'Summary'. A text block reads: '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.' Below this is a form with an 'ADAPTER INSTANCE' label and a dropdown menu showing 'SecureAuth 2FA Composite Adapter'. Underneath is the 'Adapter Contract' section with a text input field containing 'username'. A checkbox labeled 'OVERRIDE INSTANCE SETTINGS' is unchecked. A 'Manage Adapter Instances' button is located below the checkbox. At the bottom right of the form are three buttons: 'Cancel', 'Save Draft', and 'Next'.

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



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**.



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

PingFederate BRIDGE AUTHENTICATION **APPLICATIONS** SECURITY SYSTEM

APPLICATIONS

Integration >

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

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

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

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

[Show Advanced Criteria](#)

Cancel Save Draft Previous Next

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

The screenshot shows the PingFederate Bridge interface. The top navigation bar includes 'PingFederate BRIDGE' and tabs for 'AUTHENTICATION', 'APPLICATIONS', 'SECURITY', and 'SYSTEM'. The left sidebar shows 'APPLICATIONS' and 'Integration'. The main content area is titled 'SP Connections | SP Connection | Browser SSO | Assertion Creation | IdP Adapter Mapping'. Below this are tabs for 'Adapter Instance', 'Mapping Method', 'Attribute Contract Fulfillment', 'Issuance Criteria', and 'Summary'. The 'Summary' tab is active, displaying configuration details:

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

At the bottom right, there are buttons for 'Cancel', 'Save Draft', 'Previous', and 'Done'.

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

The screenshot shows the PingFederate Bridge interface. The top navigation bar includes 'PingFederate BRIDGE' and tabs for 'AUTHENTICATION', 'APPLICATIONS', 'SECURITY', and 'SYSTEM'. The left sidebar shows 'APPLICATIONS' and 'Integration'. The main content area is titled 'SP Connections | SP Connection | Browser SSO | Assertion Creation'. Below this are tabs for 'Identity Mapping', 'Attribute Contract', 'Authentication Source Mapping', and 'Summary'. The 'Authentication Source Mapping' tab is active, displaying a table of mappings:

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

Below the table are two buttons: 'Map New Adapter Instance' and 'Map New Authentication Policy'. At the bottom right, there are buttons for 'Cancel', 'Save Draft', 'Previous', and 'Next'.

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

PingFederate BRIDGE AUTHENTICATION **APPLICATIONS** SECURITY SYSTEM

APPLICATIONS

Integration >

SP Connections | SP Connection | Browser SSO | Assertion Creation

Identity Mapping | Attribute Contract | **Authentication Source Mapping** | Summary

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

Assertion Creation

Identity Mapping

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

Attribute Contract

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

Authentication Source Mapping

Adapter instance name	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**

The screenshot shows the PingFederate Bridge interface. The top navigation bar includes 'AUTHENTICATION', 'APPLICATIONS', 'SECURITY', and 'SYSTEM'. The left sidebar shows 'APPLICATIONS' and 'Integration'. The main content area is titled 'SP Connections | SP Connection | Browser SSO'. Below the title are tabs for 'SAML Profiles', 'Assertion Lifetime', 'Assertion Creation' (selected), 'Protocol Settings', and 'Summary'. A descriptive text states: 'This task provides the configuration for creating SAML assertions to enable SSO access to resources at your SP partner's site.' Below this is an 'Assertion Configuration' section with a table:

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

Below the table is a 'Configure Assertion Creation' button. At the bottom right are 'Cancel', 'Save Draft', 'Previous', and 'Next' buttons.

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

The screenshot shows the PingFederate Bridge interface. The top navigation bar includes 'AUTHENTICATION', 'APPLICATIONS', 'SECURITY', and 'SYSTEM'. The left sidebar shows 'APPLICATIONS' and 'Integration'. The main content area is titled 'SP Connections | SP Connection | Browser SSO'. Below the title are tabs for 'SAML Profiles', 'Assertion Lifetime', 'Assertion Creation', 'Protocol Settings' (selected), and 'Summary'. A descriptive text states: '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.' Below this is a 'Protocol Settings' section with a table:

Protocol Settings	
INBOUND BINDINGS	
SIGNATURE POLICY	SAML-standard
ENCRYPTION POLICY	No Encryption

Below the table is a 'Configure Protocol Settings' button. At the bottom right are 'Cancel', 'Save Draft', 'Previous', and 'Next' buttons.

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

- b. Set **Binding** to **POST**.
- c. Set the appropriate **Endpoint URL**.
- d. Click **Add**.
- e. Click **Next**.

PingFederate BRIDGE AUTHENTICATION APPLICATIONS SECURITY SYSTEM

APPLICATIONS

Integration >

SP Connections | SP Connection | Browser SSO | Protocol Settings

Assertion Consumer Service URL Signature Policy Encryption Policy Summary

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 Delete

- SELECT -

[Show Advanced Customizations](#)

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

PingFederate BRIDGE AUTHENTICATION APPLICATIONS SECURITY SYSTEM

APPLICATIONS

Integration >

SP Connections | SP Connection | Browser SSO | Protocol Settings

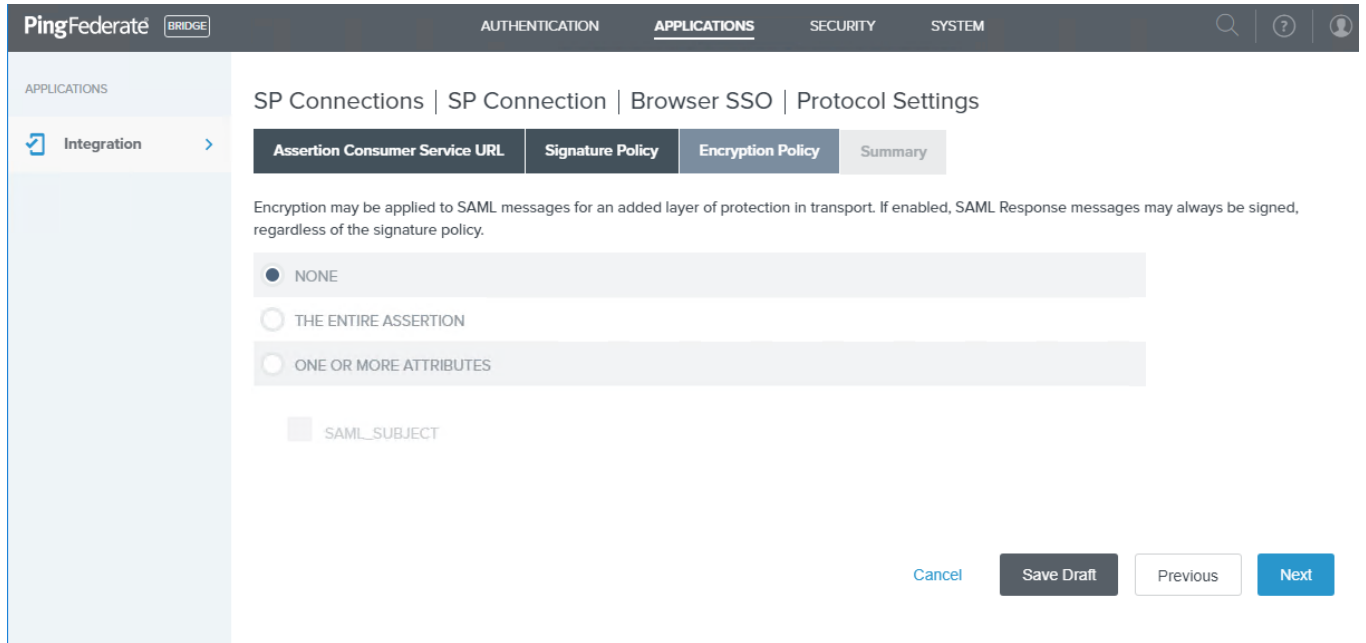
Assertion Consumer Service URL Signature Policy Encryption Policy Summary

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.

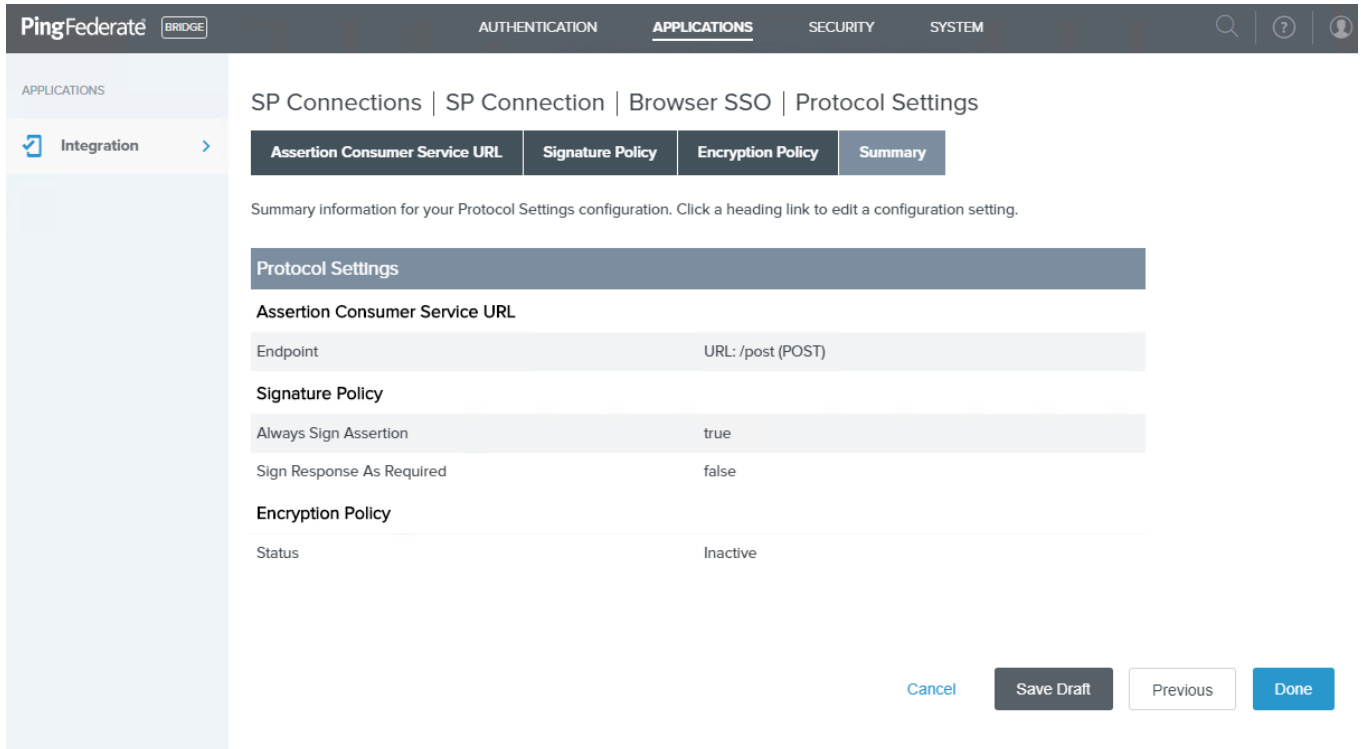
ALWAYS SIGN ASSERTION

SIGN RESPONSE AS REQUIRED

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



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



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

The screenshot shows the PingFederate Bridge console interface. The top navigation bar includes 'PingFederate BRIDGE' and tabs for 'AUTHENTICATION', 'APPLICATIONS', 'SECURITY', and 'SYSTEM'. The left sidebar shows 'APPLICATIONS' with 'Integration' selected. The main content area is titled 'SP Connections | SP Connection | Browser SSO' and features a tabbed interface with 'SAML Profiles', 'Assertion Lifetime', 'Assertion Creation', 'Protocol Settings', and 'Summary'. The 'Protocol Settings' tab is active, displaying a configuration page with the following details:

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

At the bottom of the configuration area is a 'Configure Protocol Settings' button. On the right side, there are four buttons: 'Cancel', 'Save Draft', 'Previous', and 'Next'.

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

PingFederate BRIDGE AUTHENTICATION APPLICATIONS SECURITY SYSTEM

APPLICATIONS

Integration >

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	false
SP-Initiated SLO	false

Assertion Lifetime

Valid Minutes Before	5
Valid Minutes After	5

Assertion Creation

Identity Mapping

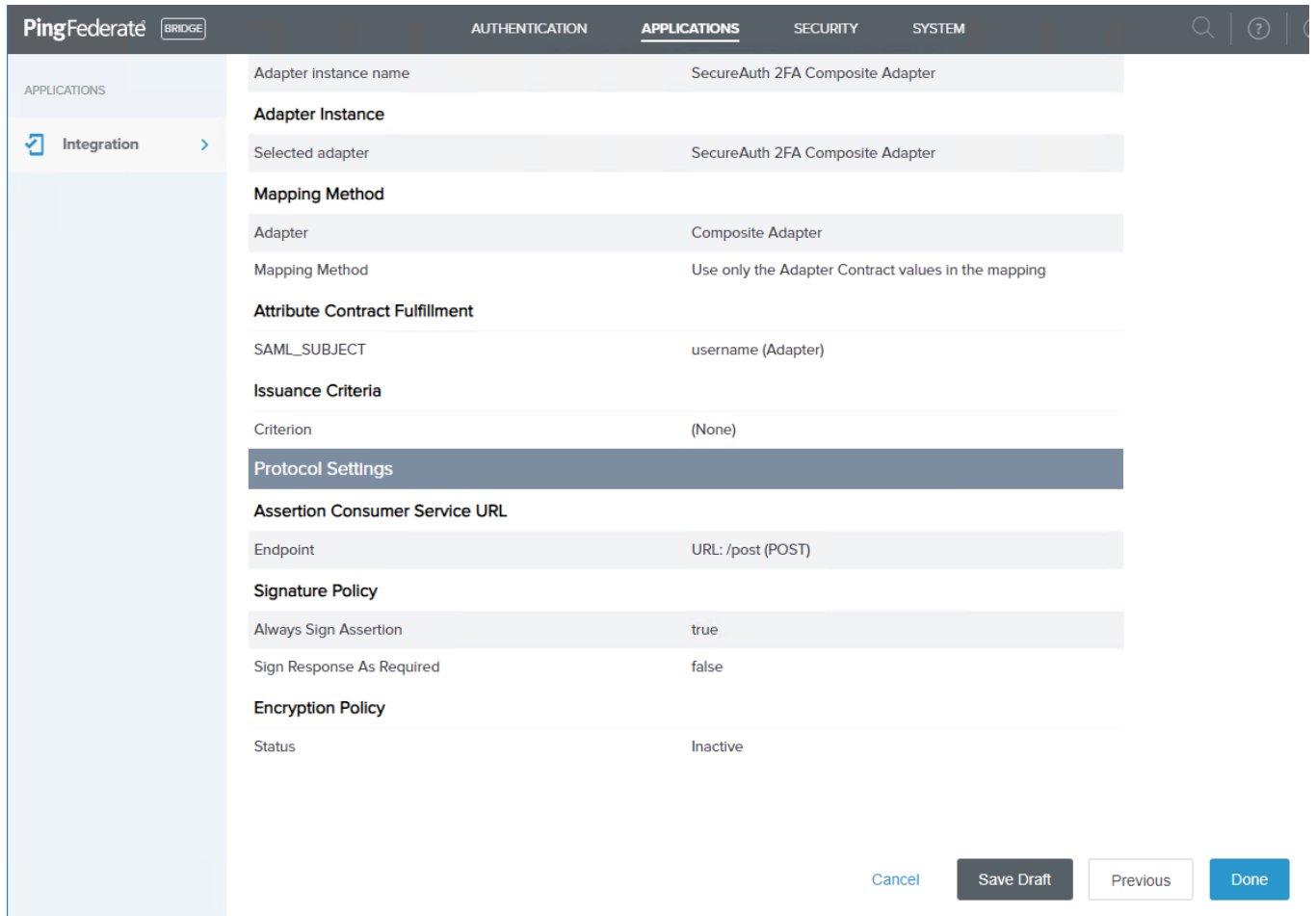
Enable Standard Identifier	true
----------------------------	------

Attribute Contract

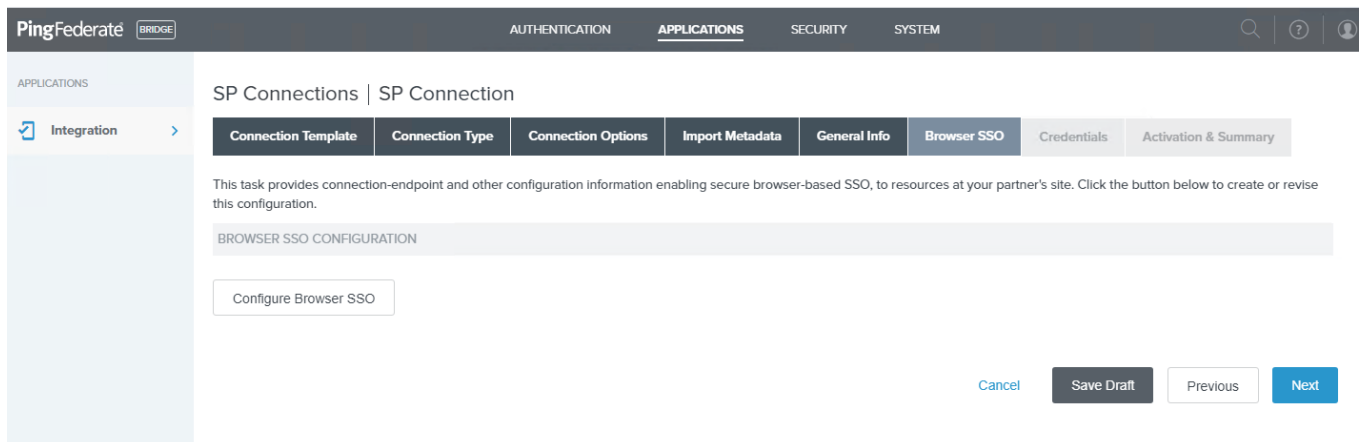
Attribute	SAML_SUBJECT
Subject Name Format	urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified

Authentication Source Mapping

Adapter instance name	SecureAuth 2FA Composite Adapter
-----------------------	----------------------------------



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



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

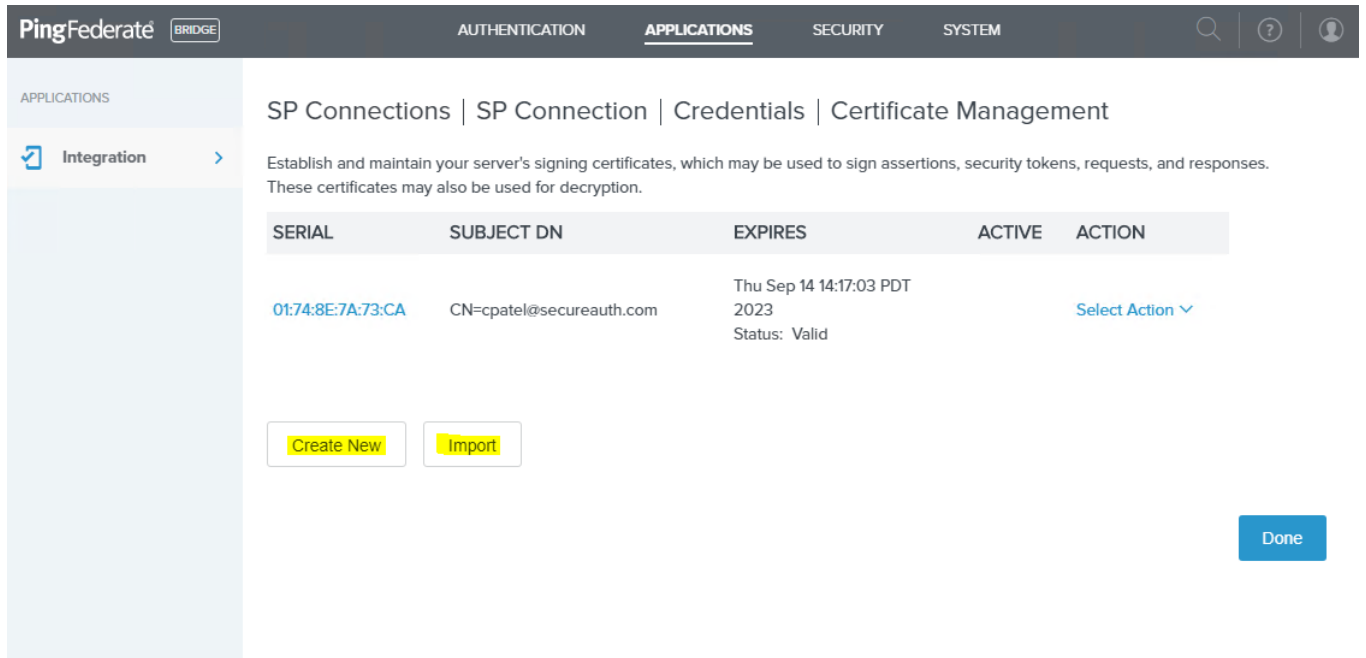
The screenshot shows the PingFederate Bridge interface. The top navigation bar includes 'PingFederate BRIDGE', 'AUTHENTICATION', 'APPLICATIONS', 'SECURITY', and 'SYSTEM'. The left sidebar shows 'APPLICATIONS' and 'Integration'. The main content area is titled 'SP Connections | SP Connection' and has several tabs: 'Connection Template', 'Connection Type', 'Connection Options', 'Import Metadata', 'General Info', 'Browser SSO', 'Credentials', and 'Activation & Summary'. The 'Credentials' tab is active. Below the tabs, there is a section for 'Credential Requirement' with 'DIGITAL SIGNATURE' set to 'Not Configured'. A yellow box highlights the 'Configure Credentials' button. At the bottom right, there are buttons for 'Cancel', 'Save Draft', 'Previous', and 'Next'.

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

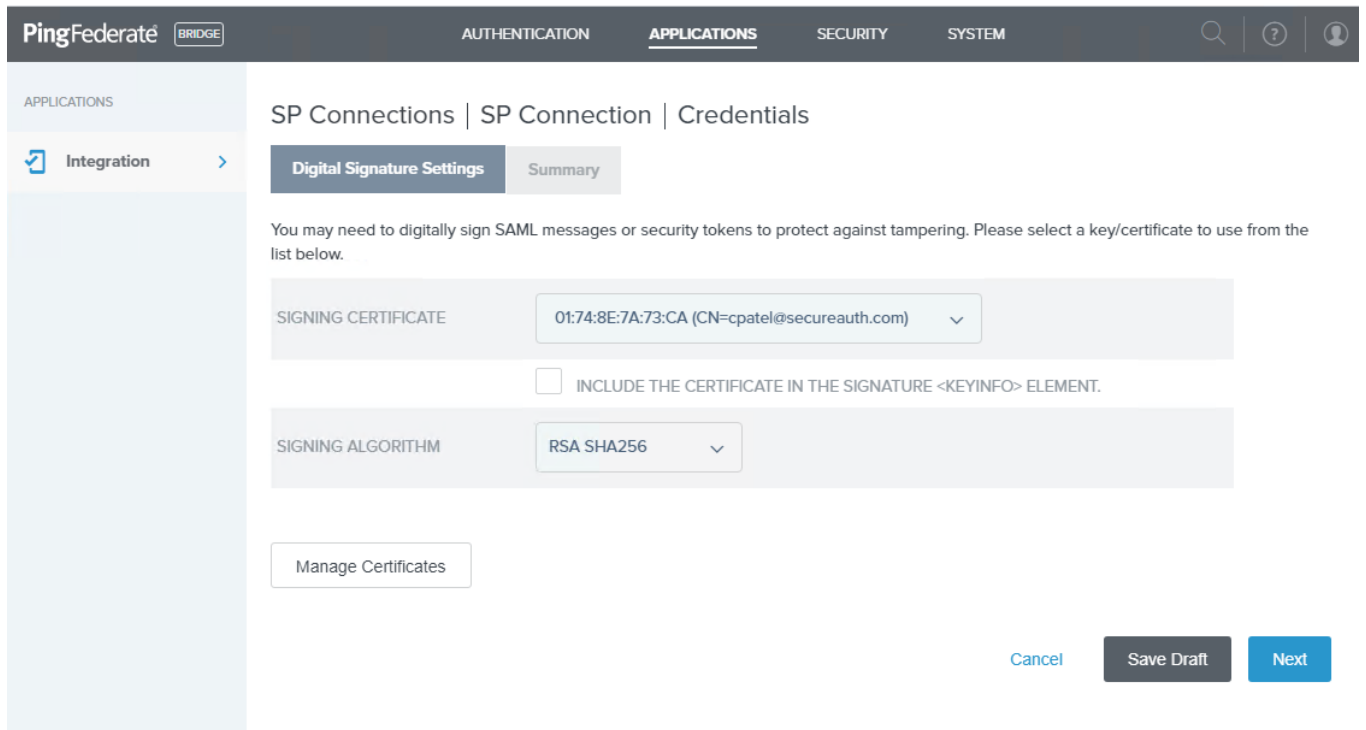
The screenshot shows the PingFederate Bridge interface. The top navigation bar includes 'PingFederate BRIDGE', 'AUTHENTICATION', 'APPLICATIONS', 'SECURITY', and 'SYSTEM'. The left sidebar shows 'APPLICATIONS' and 'Integration'. The main content area is titled 'SP Connections | SP Connection | Credentials' and has two tabs: 'Digital Signature Settings' and 'Summary'. The 'Digital Signature Settings' tab is active. Below the tabs, there is a section for '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.' A dropdown menu for 'SIGNING CERTIFICATE' is set to '- SELECT -'. Below the dropdown, there is a checkbox labeled 'INCLUDE THE CERTIFICATE IN THE SIGNATURE <KEYINFO> ELEMENT.' A yellow box highlights the 'Manage Certificates' button. At the bottom right, there are buttons for 'Cancel', 'Save Draft', and 'Next'.

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

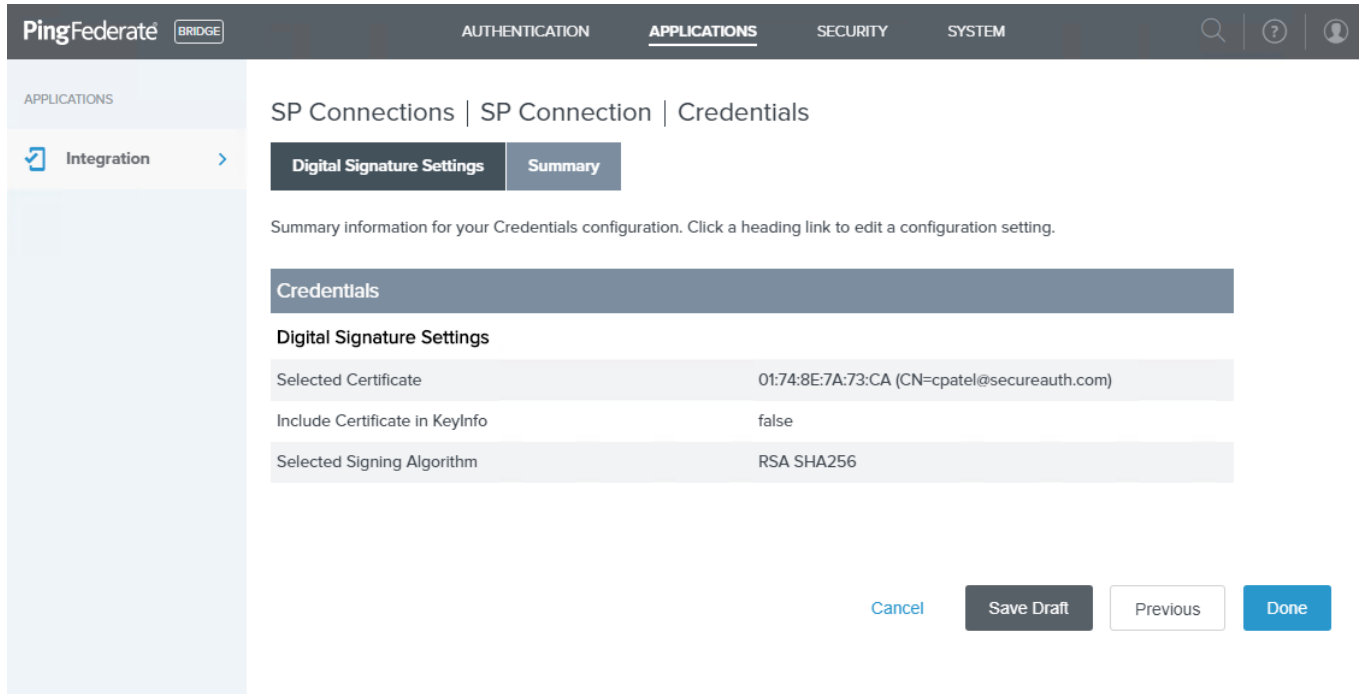
- To create an unsigned certificate, click **Create New**.
- To use an existing certificate, click **Import**.



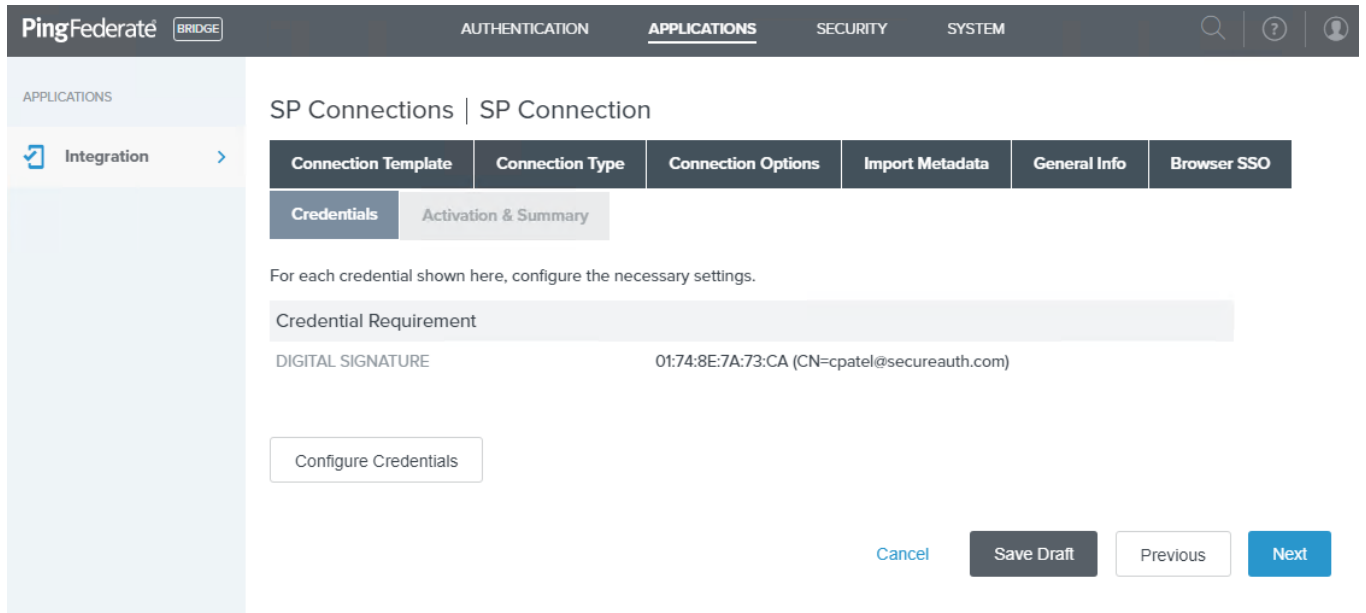
33. In the *Create Certificate* tab, enter the required values OR select existing certificate and click **Next**.



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



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



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

PingFederate BRIDGE AUTHENTICATION APPLICATIONS SECURITY SYSTEM

APPLICATIONS

Integration >

SP Connections | SP Connection

Connection Template | **Connection Type** | Connection Options | Import Metadata | General Info | Browser SSO | Credentials | Activation & Summary

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/ldap/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

Activate Windows

PingFederate BRIDGE

AUTHENTICATION APPLICATIONS SECURITY SYSTEM

APPLICATIONS

Integration >

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)

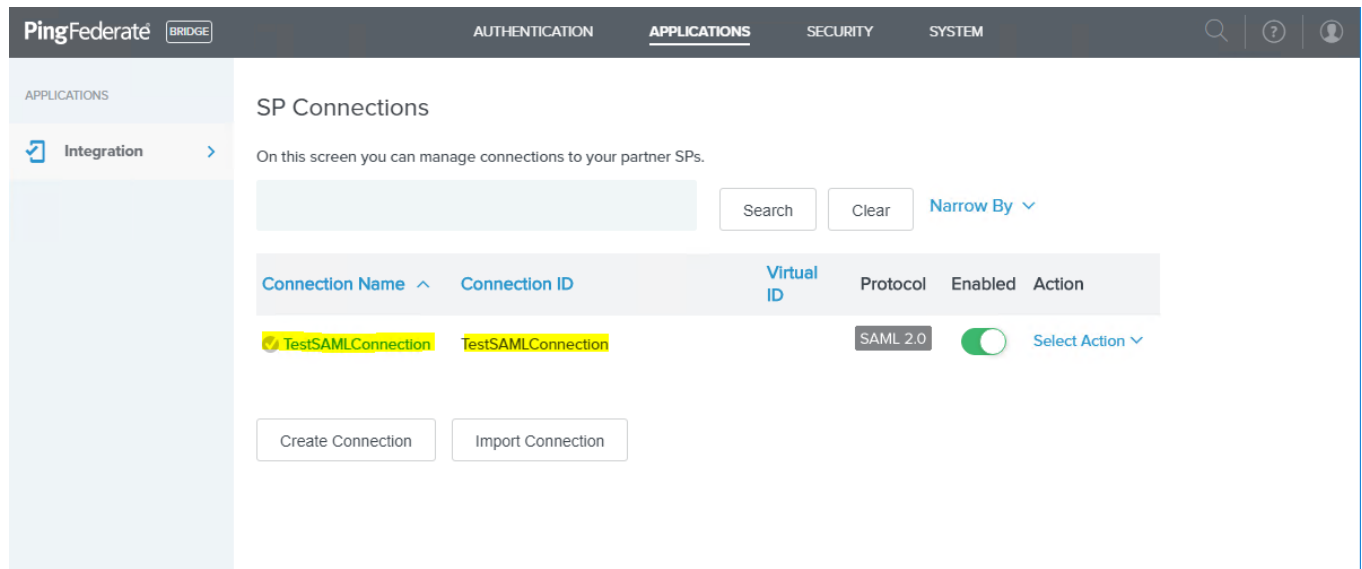
Include Certificate in KeyInfo false

Selected Signing Algorithm RSA SHA256

Cancel Previous Save

37. Click **Save**.

38. See newly created SP connection.



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	<input type="text" value="/mylogoutpath"/>
LOGOUT REDIRECT	<input type="text" value="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

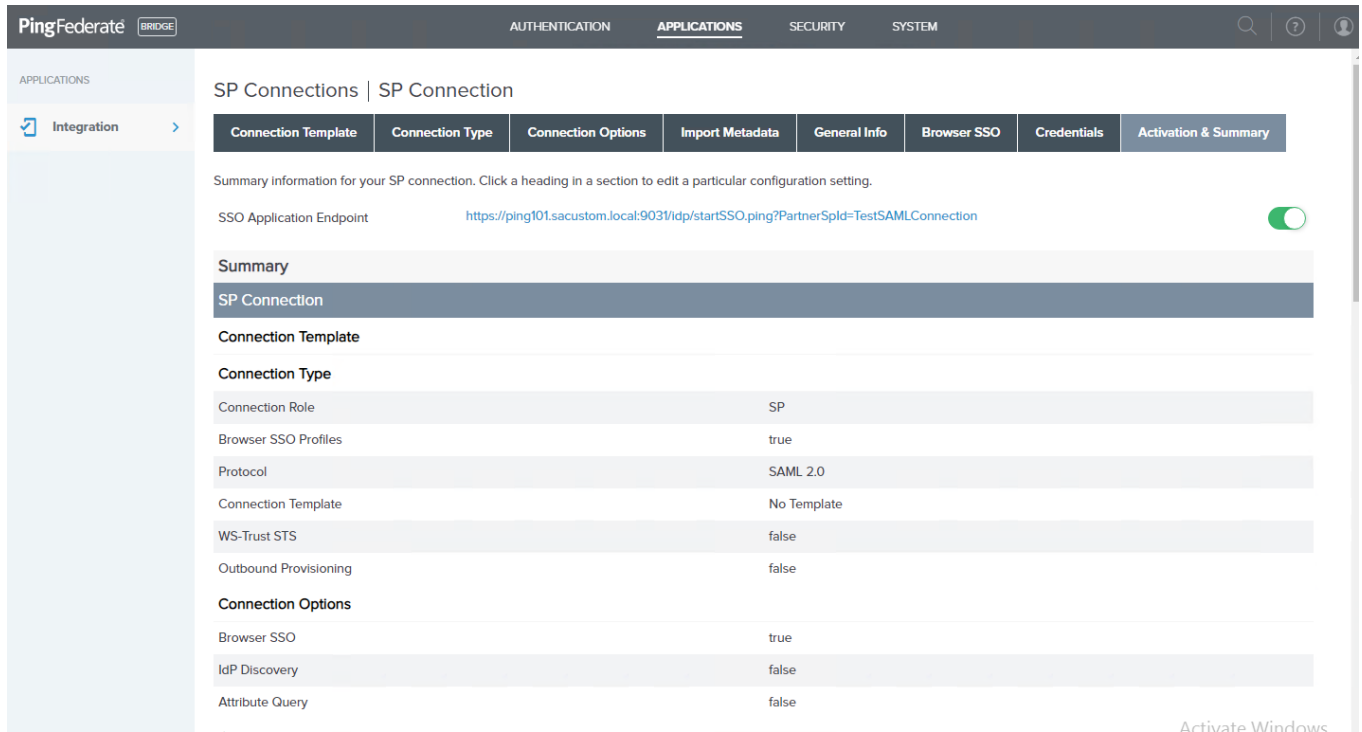
[restart login](#)

Test the configured SecureAuth 2FA functionality

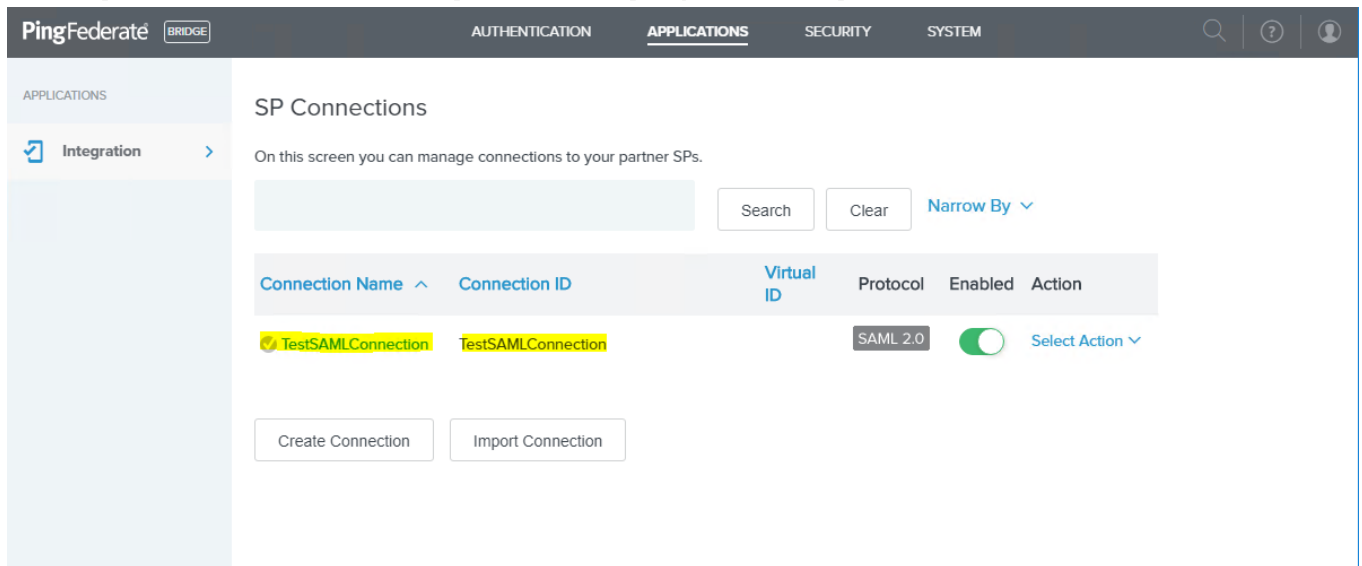
After you have set up the configurations for the SecureAuth 2FA adapter and SP connections, test the functionality.

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.



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`



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

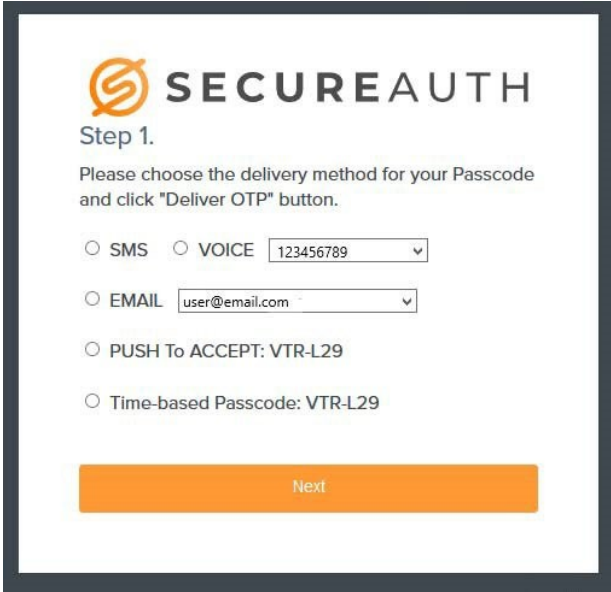
Email Field 2: One-Time Passcode via HTM

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.



SECUREAUTH

Step 1.

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

SMS VOICE 123456789

EMAIL user@email.com

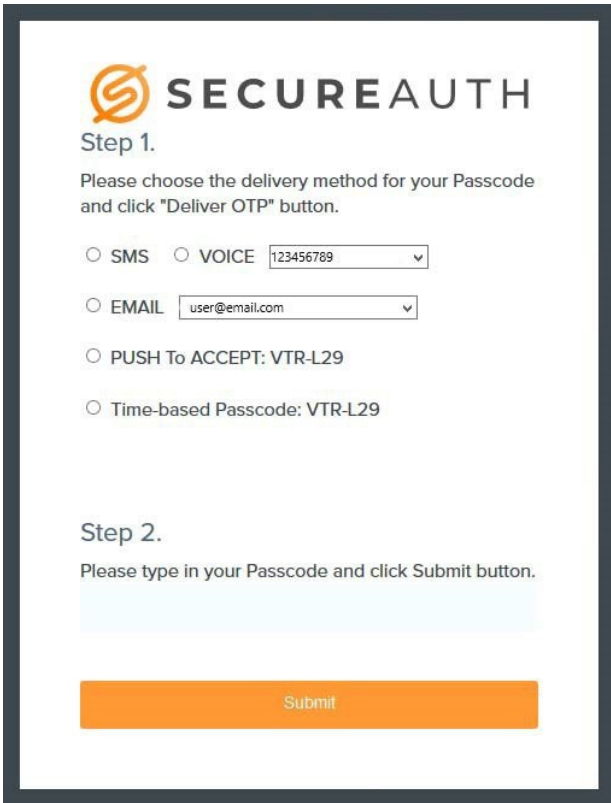
PUSH To ACCEPT: VTR-L29

Time-based Passcode: VTR-L29

Next

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.



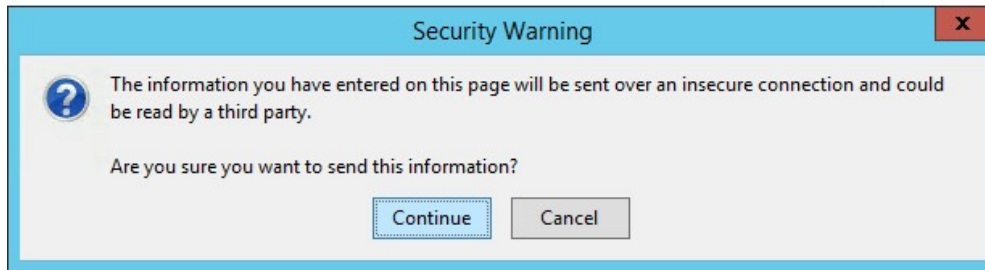
SECUREAUTH

Step 2.

Please type in your Passcode and click Submit button.

Submit

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

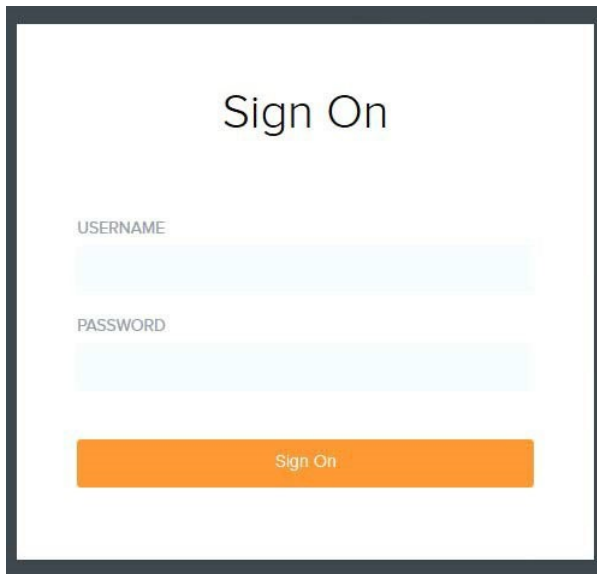


6. Repeat the test using the Voice and Email methods.

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:

A screenshot of a 'Sign On' page. The title 'Sign On' is centered at the top. Below it are two input fields: 'USERNAME' and 'PASSWORD'. The 'PASSWORD' field is masked with dots. At the bottom, there is an orange button labeled 'Sign On'.

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

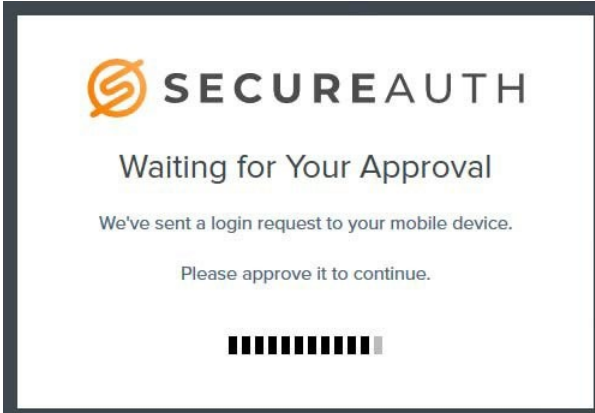
The passcode delivery method page opens, similar to the following example.



The image shows a screenshot of the SecureAuth Step 1 interface. At the top left is the SecureAuth logo, followed by the text "SECUREAUTH". Below this, it says "Step 1." and "Please choose the delivery method for your Passcode and click 'Deliver OTP' button." There are four radio button options: "SMS" (unselected), "VOICE" (unselected) with a dropdown menu showing "123456789", "EMAIL" (unselected) with a dropdown menu showing "user@email.com", and "PUSH To ACCEPT: VTR-L29" (selected). Below these is an option for "Time-based Passcode: VTR-L29" (unselected). At the bottom is an orange button labeled "Next".

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

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

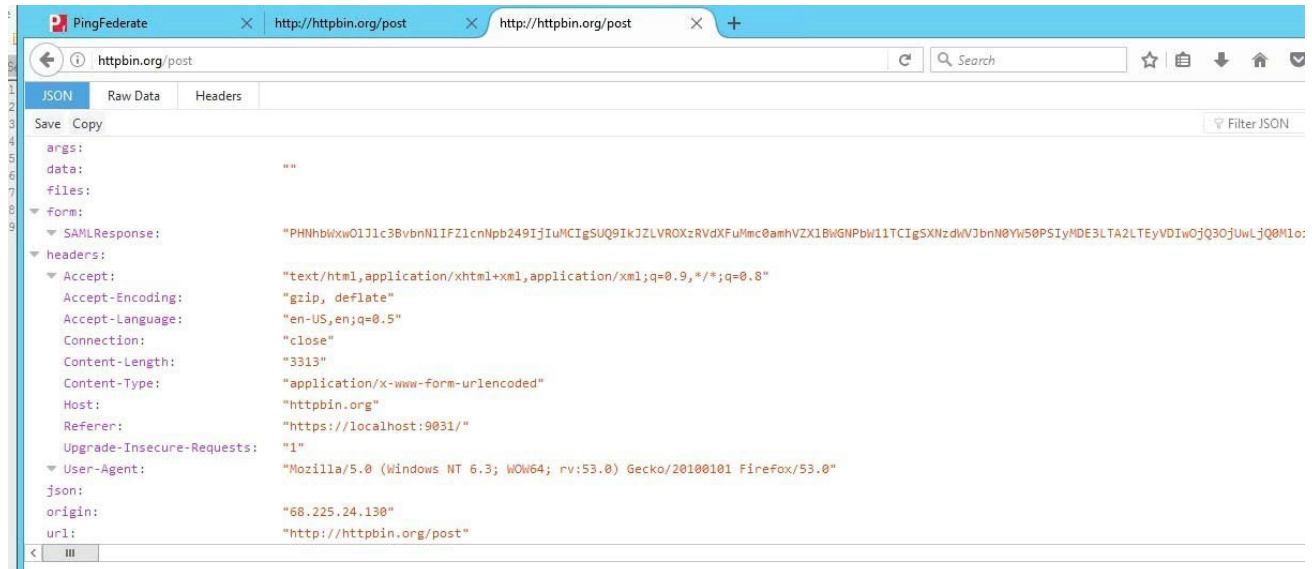


The image shows a screenshot of the SecureAuth "Waiting for Your Approval" interface. At the top left is the SecureAuth logo, followed by the text "SECUREAUTH". Below this, it says "Waiting for Your Approval" and "We've sent a login request to your mobile device." Below that, it says "Please approve it to continue." At the bottom is a progress indicator consisting of ten vertical bars of varying heights, with the last bar being the tallest.

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



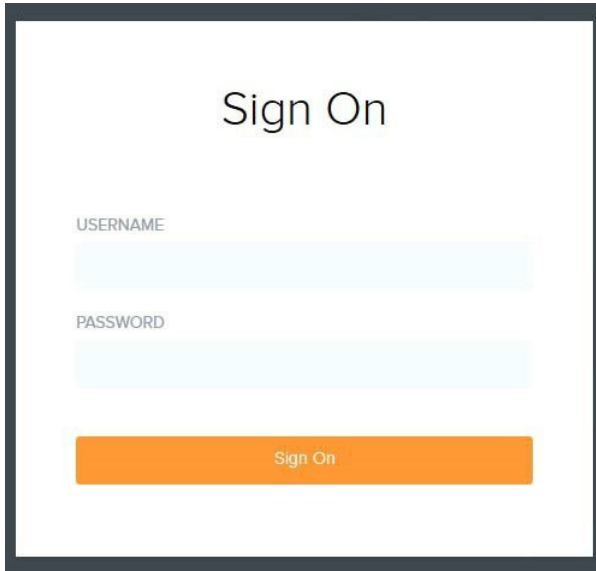
After a successful authentication, the destination page opens, similar to the following example.



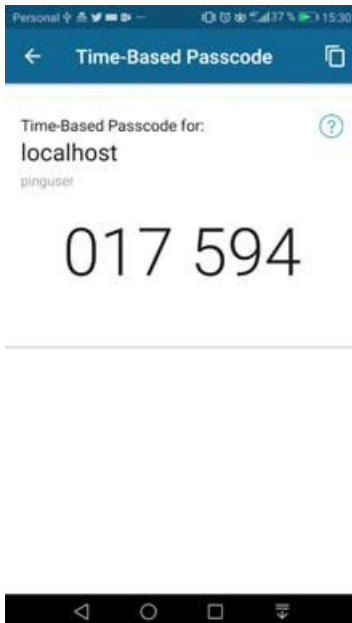
Test the time-based passcode method

1. Open a new browser tab and paste the URL that you copied in the [Obtain a test URL](#) section.

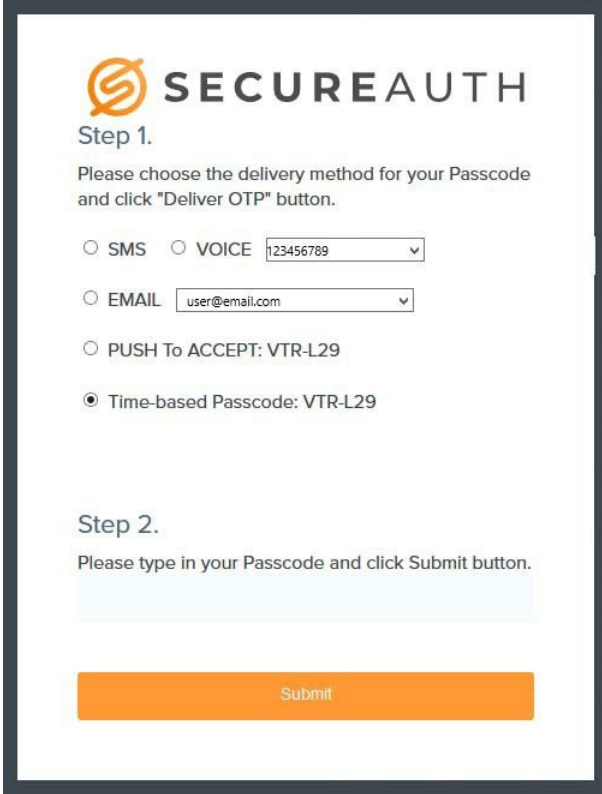
The Sign On page opens, similar to the following example:



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



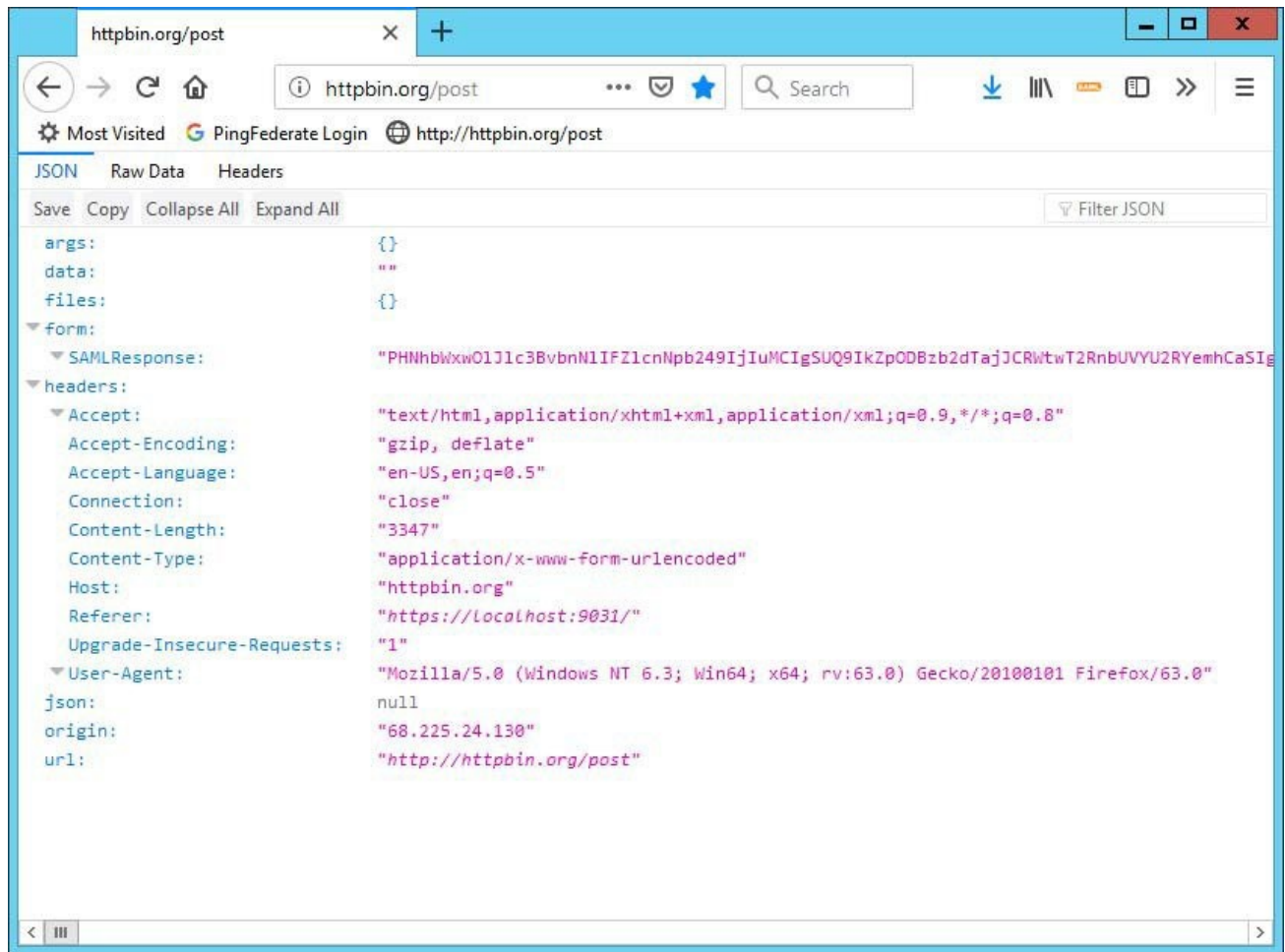
3. On your computer, select the **Time-based passcode** option as the delivery method.



The screenshot shows the SecureAuth authentication interface. At the top left is the SecureAuth logo, consisting of a stylized 'S' in a circle followed by the word 'SECUREAUTH'. Below the logo, the text 'Step 1.' is displayed. The instruction reads: 'Please choose the delivery method for your Passcode and click "Deliver OTP" button.' There are four radio button options: 'SMS', 'VOICE', 'EMAIL', and 'Time-based Passcode: VTR-L29'. The 'VOICE' option is selected, and a dropdown menu next to it shows the number '123456789'. The 'EMAIL' option is also visible with a dropdown menu showing 'user@email.com'. The 'Time-based Passcode: VTR-L29' option is selected with a filled radio button. Below this, 'Step 2.' is displayed with the instruction: 'Please type in your Passcode and click Submit button.' A light blue rectangular input field is provided for the passcode. At the bottom, there is a large orange button labeled 'Submit'.

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.



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>