PingFederate®

PeopleSoft Integration Solution v2.4.5 (ReferenceID Adapter)

User Guide

PingFederate PeopleSoft Integration Solution (ReferenceID Adapter) User Guide
Version 2.4.5
August 2022

Ping Identity Corporation
1001 17th Street, Suite 100
Denver, CO 80202
USA

Phone: 877.898.2905 (+1 303.468.2882 outside North America)
Fax: 303.468.2909 E-mail: info@pingidentity.com
Web Site: http://www.pingidentity.com

Trademarks

Disclaimer

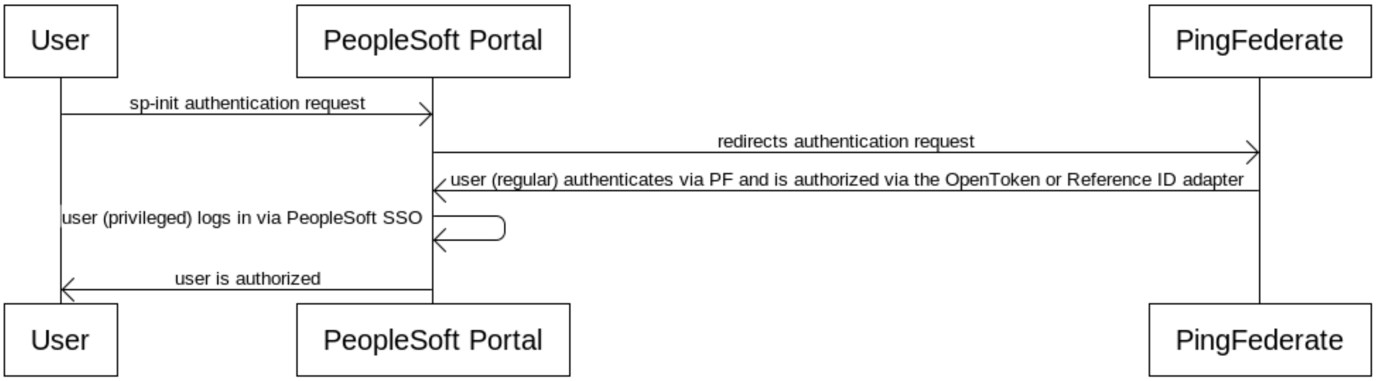
This document is proprietary and not for general publication. It may be provided ad hoc for informational purposes only, and the information herein is subject to change without notice. Ping Identity does not provide any warranties and specifically disclaims any liability in connection with this document.

Note that Ping Identity may not provide support for any sample configurations provided in this document. The variability inherent among security environments prevents full testing and support for all possible platform configurations. If you need special assistance or would like to inquire about implementation or support programs, please contact Ping Identity Global Client Services (http://support.pingidentity.com).

Contents

Purpose

The PeopleSoft Integration Solution provides a way to integrate PingFederate with the PeopleSoft application in order to provide Single Sign On (SSO) for users. The flow of this integration is SP-initiated, which starts with the user going to the PeopleSoft login page. If the user hasn't been authenticated yet, he/she would be redirected to PingFederate to initiate the SSO process. Once authenticated, the user will be authorized into the PeopleSoft application. If the user has already authenticated prior, and his/her session has not ended yet, the user will stay authenticated. Otherwise, the user will be redirected to log in again. This solution also allows the ability for privileged users, such as PeopleSoft administrators, to be able to bypass the general SSO process via PingFederate, and log into PeopleSoft directly.


User
PeopleSoft Portal
PingFederate
sp-init authentication request
redirects authentication request
user (regular) authenticates via PF and is authorized via the OpenToken or Reference ID adapter
user (privileged) logs in via PeopleSoft SSO
user is authorized
User
PeopleSoft Portal
PingFederate

Prerequisites

This document assumes that you already have the following installed and configured:

- A functional PingFederate environment with a compatible JDK installed
- A pre-configured IdP adapter (e.g., Kerberos, HTML Form IdP Adapter, etc.)
- A functional PeopleSoft environment with a compatible JDK installed

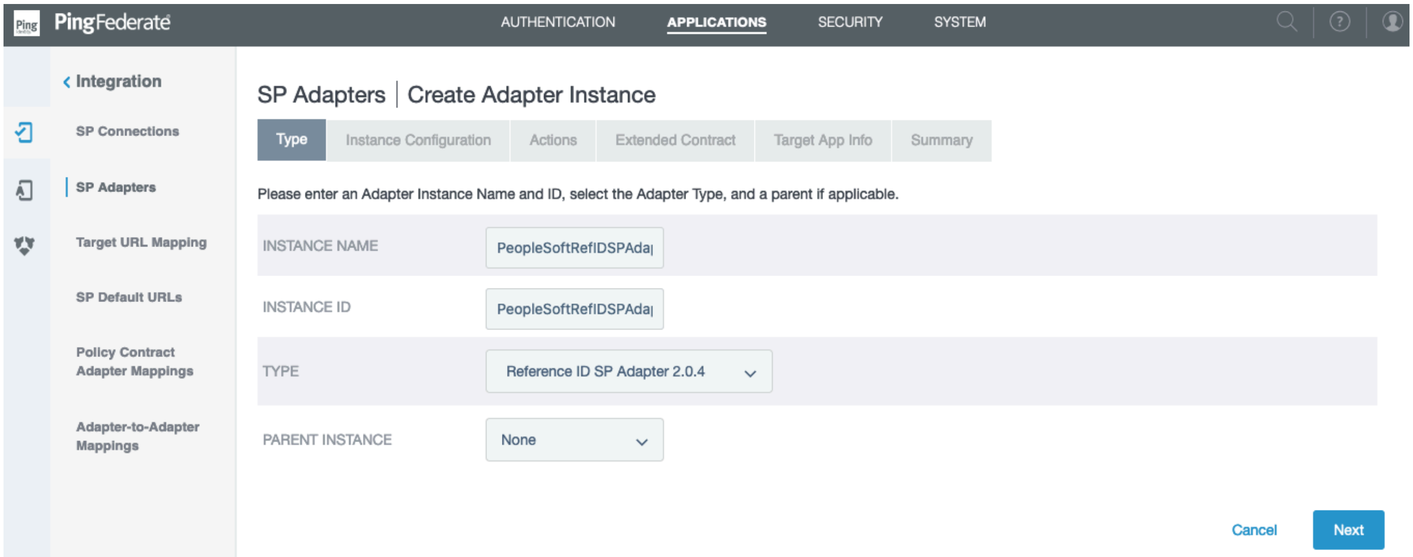
Installation & Configuration

Note: It is recommended that a PeopleSoft environment with limited users should be used for the initial installation and configuration of the solution, as downtime is needed.

PINGFEDERATE CONFIGURATION

Configuring the ReferenceID Adapter

1. Log into the PingFederate admin console and click on **Applications** >> **SP Adapters**.
2. Click **Create New Instance**.
3. Enter the **Instance Name**, **Instance ID**, select **ReferenceID Adapter X.X.X** from the **Type** dropdown, and click **Next**.

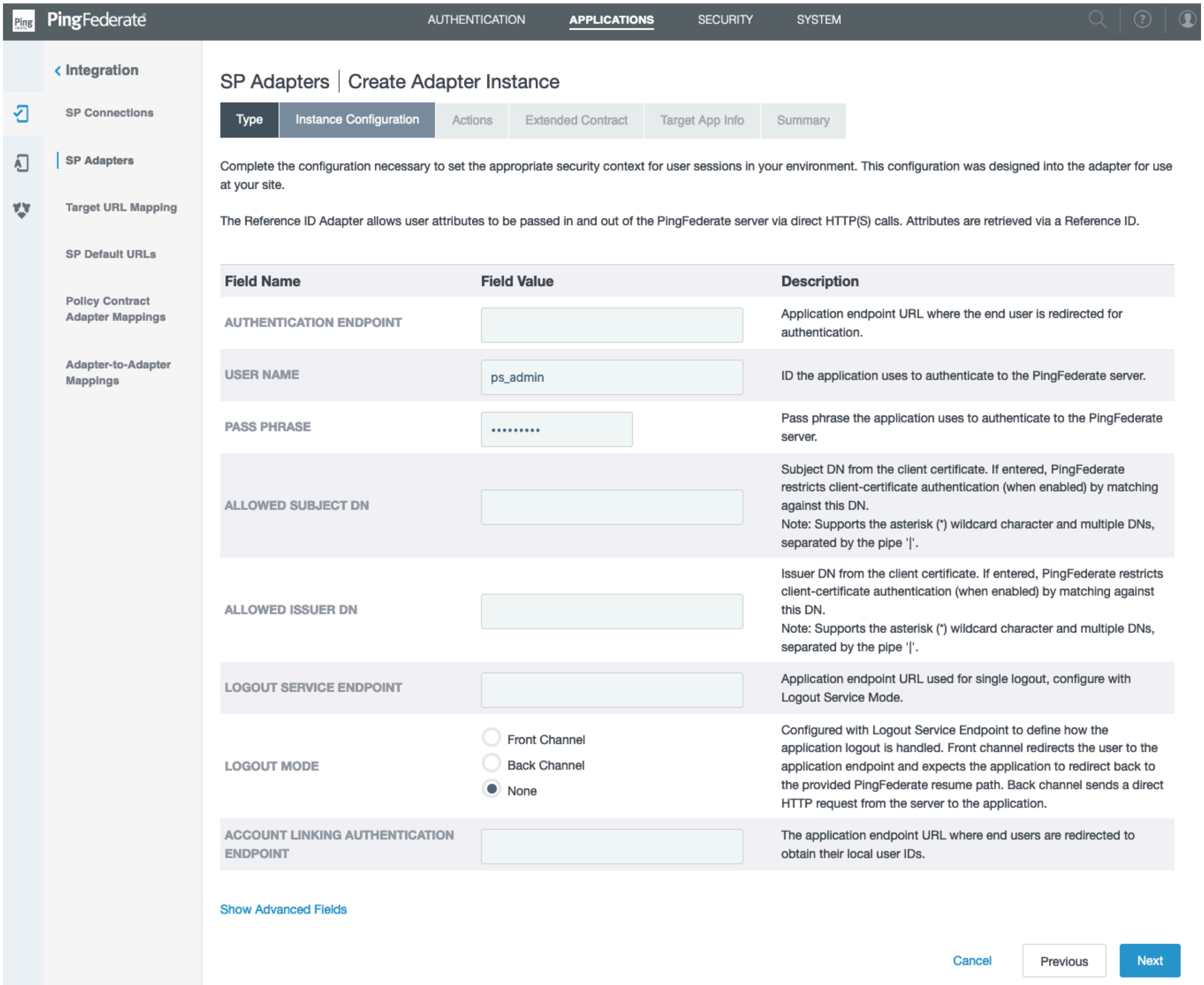


SP Adapters | Create Adapter Instance

Please enter an Adapter Instance Name and ID, select the Adapter Type, and a parent if applicable.

INSTANCE NAME	PeopleSoftRefIDSPAda
INSTANCE ID	PeopleSoftRefIDSPAda
TYPE	Reference ID SP Adapter 2.0.4
PARENT INSTANCE	None

4. Configure the following and click **Next**.
   a. User Name
   b. Pass Phrase



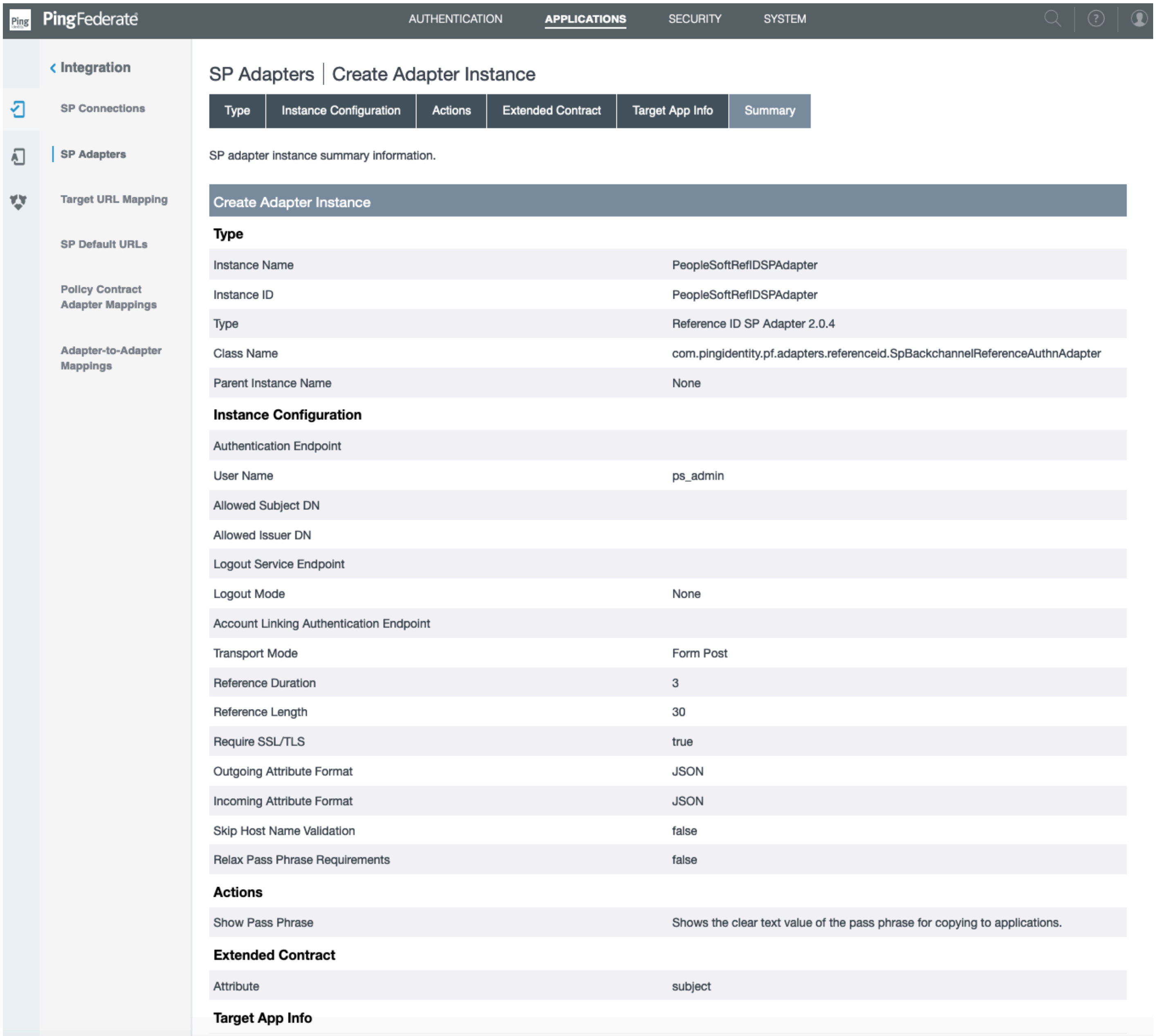
SP Adapters | Create Adapter Instance

Complete the configuration necessary to set the appropriate security context for user sessions in your environment. This configuration was designed into the adapter for use at your site.

The Reference ID Adapter allows user attributes to be passed in and out of the PingFederate server via direct HTTP(S) calls. Attributes are retrieved via a Reference ID.

Field Name	Field Value	Description
AUTHENTICATION ENDPOINT		Application endpoint URL where the end user is redirected for authentication.
USER NAME	ps_admin	ID the application uses to authenticate to the PingFederate server.
PASS PHRASE	•••••••••	Pass phrase the application uses to authenticate to the PingFederate server.
ALLOWED SUBJECT DN		Subject DN from the client certificate. If entered, PingFederate restricts client-certificate authentication (when enabled) by matching against this DN. Note: Supports the asterisk (*) wildcard character and multiple DNs, separated by the pipe '|'.
ALLOWED ISSUER DN		Issuer DN from the client certificate. If entered, PingFederate restricts client-certificate authentication (when enabled) by matching against this DN. Note: Supports the asterisk (*) wildcard character and multiple DNs, separated by the pipe '|'.
LOGOUT SERVICE ENDPOINT		Application endpoint URL used for single logout, configure with Logout Service Mode.
LOGOUT MODE	○ Front Channel ○ Back Channel ● None	Configured with Logout Service Endpoint to define how the application logout is handled. Front channel redirects the user to the application endpoint and expects the application to redirect back to the provided PingFederate resume path. Back channel sends a direct HTTP request from the server to the application.
ACCOUNT LINKING AUTHENTICATION ENDPOINT		The application endpoint URL where end users are redirected to obtain their local user IDs.

5. Click **Next**.
6. Click **Next**.
7. Click **Next**.
8. Review the **Summary**, and click **Save**.



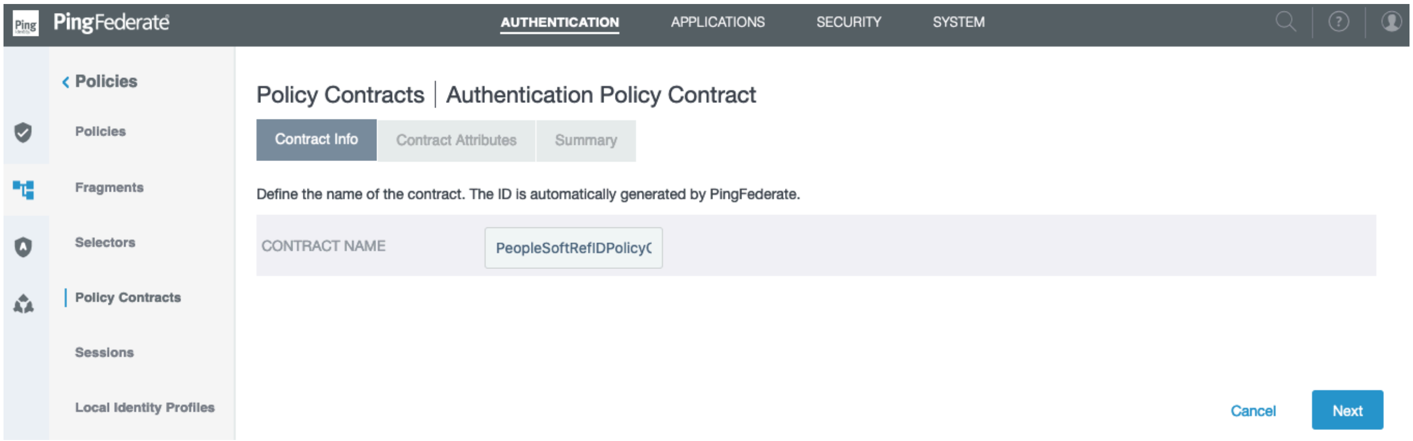
SP Adapters | Create Adapter Instance

SP adapter instance summary information.

Create Adapter Instance	
Type	
Instance Name	PeopleSoftRefIDSPAdapter
Instance ID	PeopleSoftRefIDSPAdapter
Type	Reference ID SP Adapter 2.0.4
Class Name	com.pingidentity.pf.adapters.referenceid.SpBackchannelReferenceAuthnAdapter
Parent Instance Name	None
Instance Configuration	
Authentication Endpoint	
User Name	ps_admin
Allowed Subject DN	
Allowed Issuer DN	
Logout Service Endpoint	
Logout Mode	None
Account Linking Authentication Endpoint	
Transport Mode	Form Post
Reference Duration	3
Reference Length	30
Require SSL/TLS	true
Outgoing Attribute Format	JSON
Incoming Attribute Format	JSON
Skip Host Name Validation	false
Relax Pass Phrase Requirements	false
Actions	
Show Pass Phrase	Shows the clear text value of the pass phrase for copying to applications.
Extended Contract	
Attribute	subject
Target App Info	

Configuring the Policy Contract

1. Log into the PingFederate admin console and click on **Policy Contracts** under **Authentication** >> **Policies**.
2. Click **Create New Contract**.
3. Enter the **Contract Name** and click **Next**.

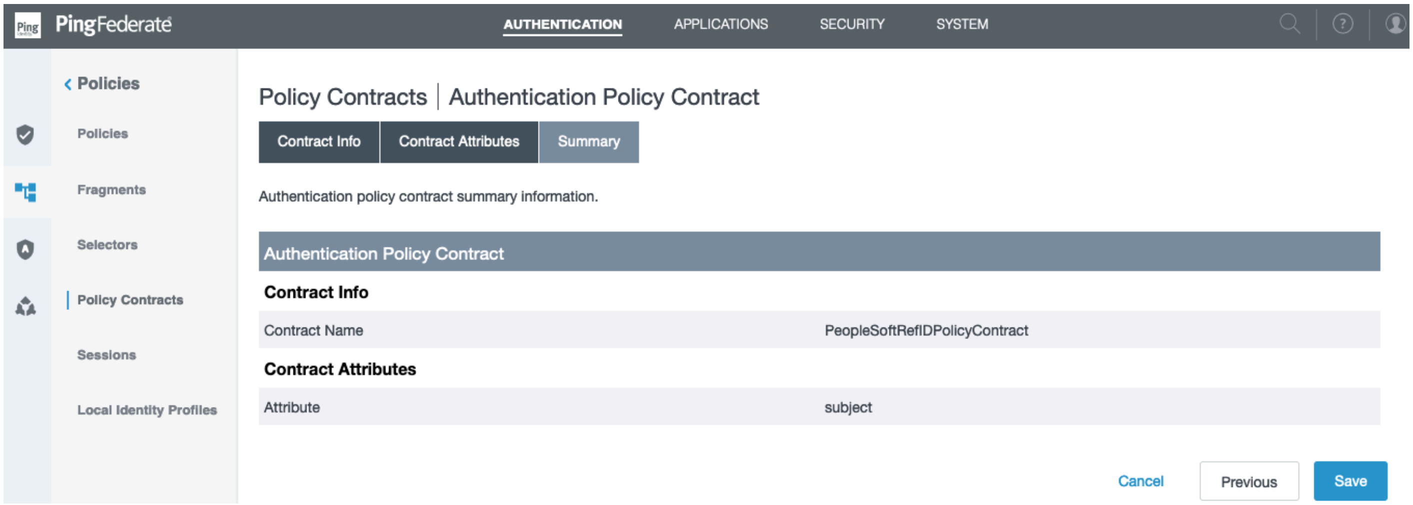


Policy Contracts | Authentication Policy Contract

Define the name of the contract. The ID is automatically generated by PingFederate.

CONTRACT NAME: PeopleSoftRefIDPolicyC

4. Click **Next**.
5. Review the **Summary** and click **Save**.



Policy Contracts | Authentication Policy Contract

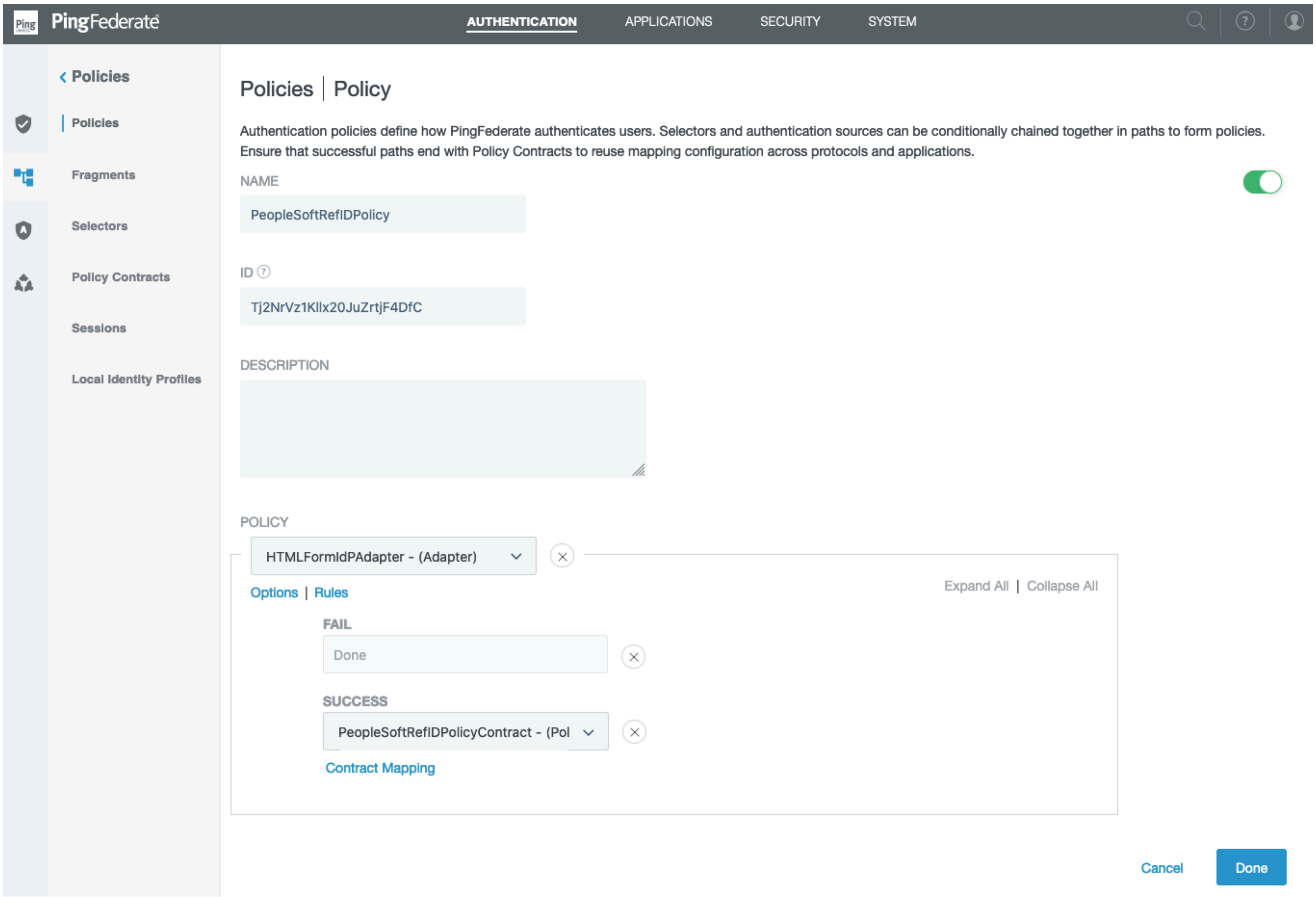
Authentication policy contract summary information.

Authentication Policy Contract	
Contract Info	
Contract Name	PeopleSoftRefIDPolicyContract
Contract Attributes	
Attribute	subject

Configuring the Policy

Note: An IdP adapter, such as Kerberos or HTML Form IdP, needs to be pre-configured prior to the below steps.

1. Log into the PingFederate admin console and click on **Authentication** >> **Policies**.
2. Click **Add Policy**.
3. Enter the **Name** and configure the policy flow. An HTML Form IdP Adapter is used for the first factor in this example.



Policies | Policy

Authentication policies define how PingFederate authenticates users. Selectors and authentication sources can be conditionally chained together in paths to form policies. Ensure that successful paths end with Policy Contracts to reuse mapping configuration across protocols and applications.

NAME: PeopleSoftRefIDPolicy

ID: Tj2NrVz1Kllx20JuZrtjF4DfC

DESCRIPTION:

POLICY: HTMLFormIdPAdapter - (Adapter)

Options | Rules

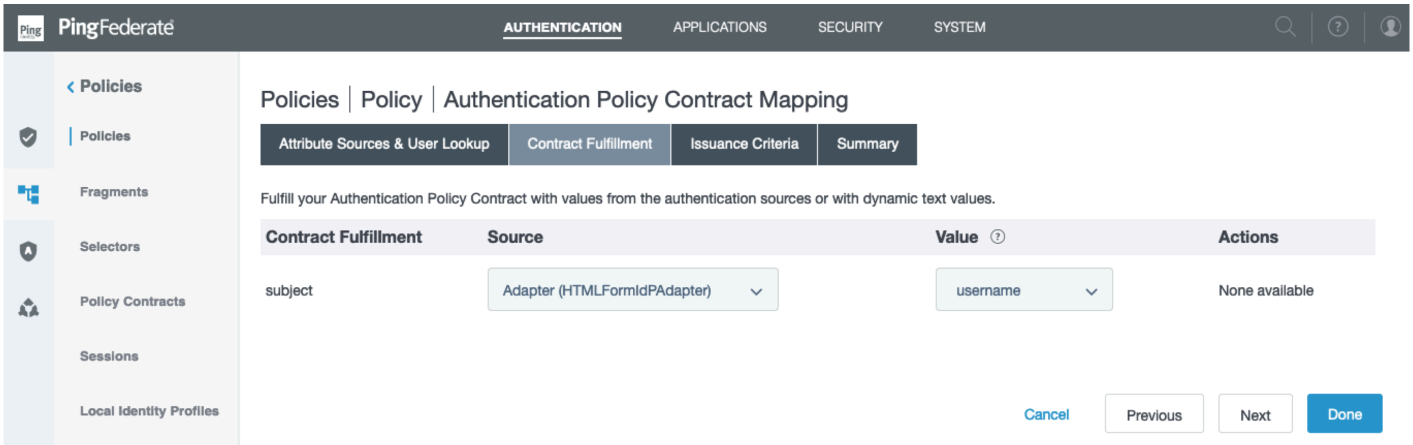
Expand All | Collapse All

FAIL: Done

SUCCESS: PeopleSoftRefIDPolicyContract - (Pol

Contract Mapping

4. Click **Contract Mapping** and click **Next**.
5. Configure the **Contract Fulfillment** and click **Next**.

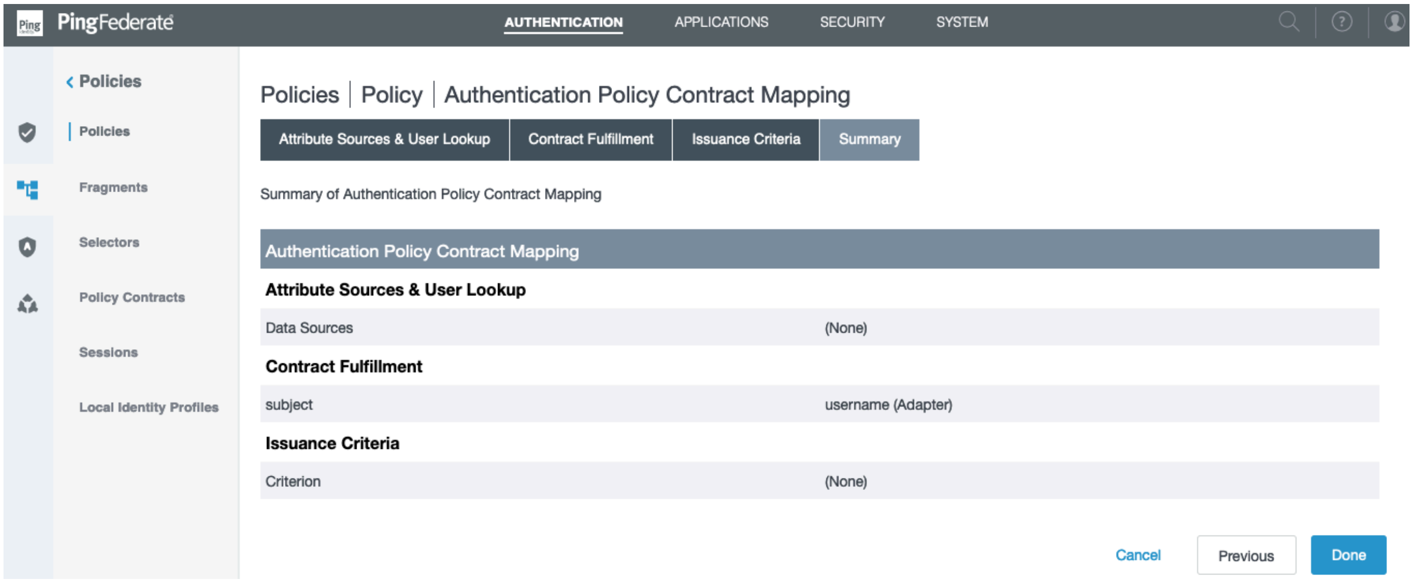


Policies | Policy | Authentication Policy Contract Mapping

Fulfill your Authentication Policy Contract with values from the authentication sources or with dynamic text values.

Contract Fulfillment	Source	Value	Actions
subject	Adapter (HTMLFormIdPAdapter)	username	None available

6. Click **Next**.
7. Review the **Summary** and click **Done**.



Policies | Policy | Authentication Policy Contract Mapping

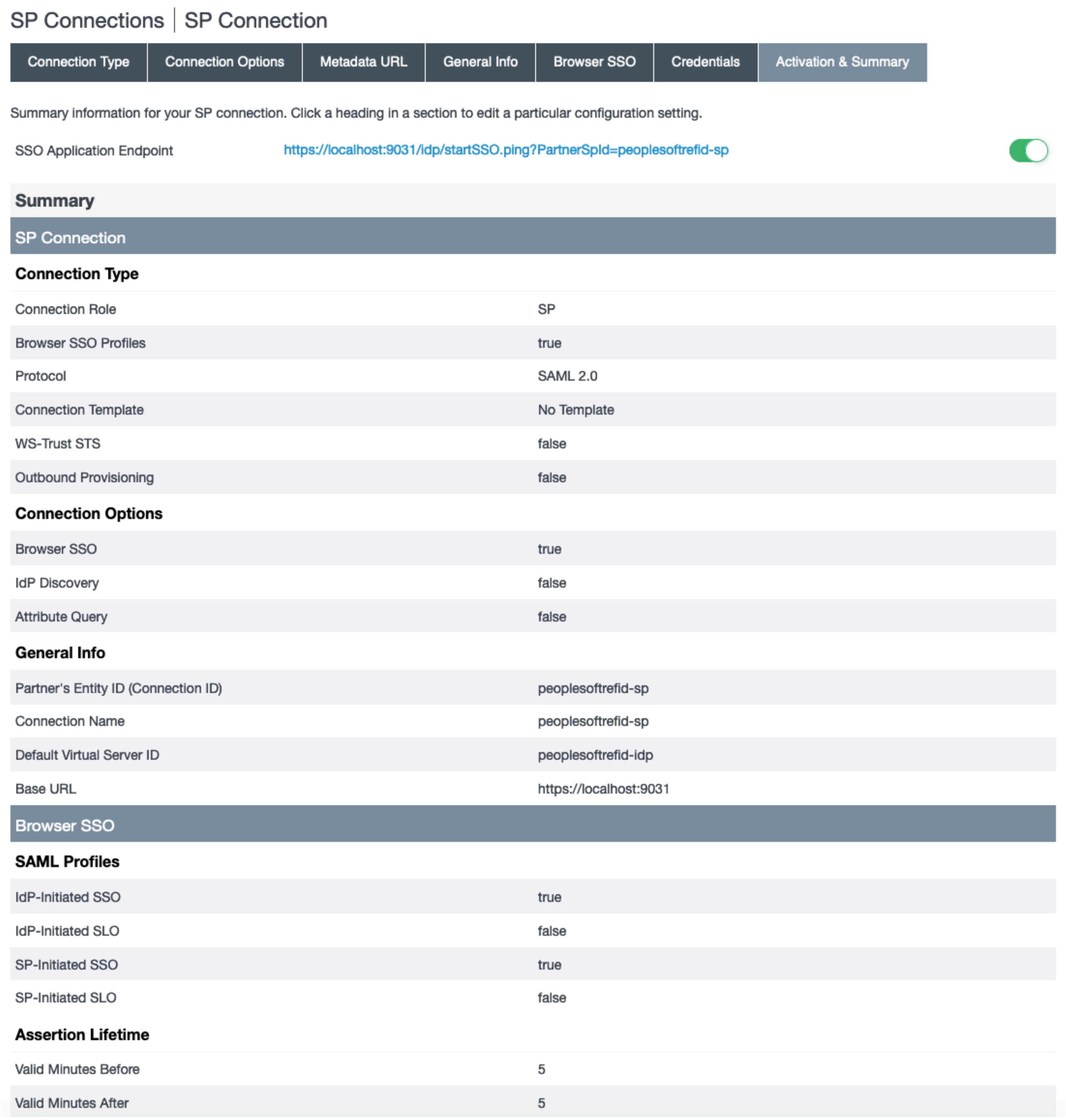
Summary of Authentication Policy Contract Mapping

Authentication Policy Contract Mapping	
Attribute Sources & User Lookup	
Data Sources	(None)
Contract Fulfillment	
subject	username (Adapter)
Issuance Criteria	
Criterion	(None)

8. Click **Done**.
9. Click **Save**.

Configuring the SP Connection

1. Log into the PingFederate admin console and click on **Applications** >> **SP Connections**.
2. Click **Create Connection** and configure the **Authentication Source Mapping** to the policy contract created above. For example:



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://localhost:9031/idp/startSSO.ping?PartnerSpId=peoplesoftrefid-sp

Summary

SP Connection

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

General Info

Partner's Entity ID (Connection ID)	peoplesoftrefid-sp
Connection Name	peoplesoftrefid-sp
Default Virtual Server ID	peoplesoftrefid-idp
Base URL	https://localhost:9031

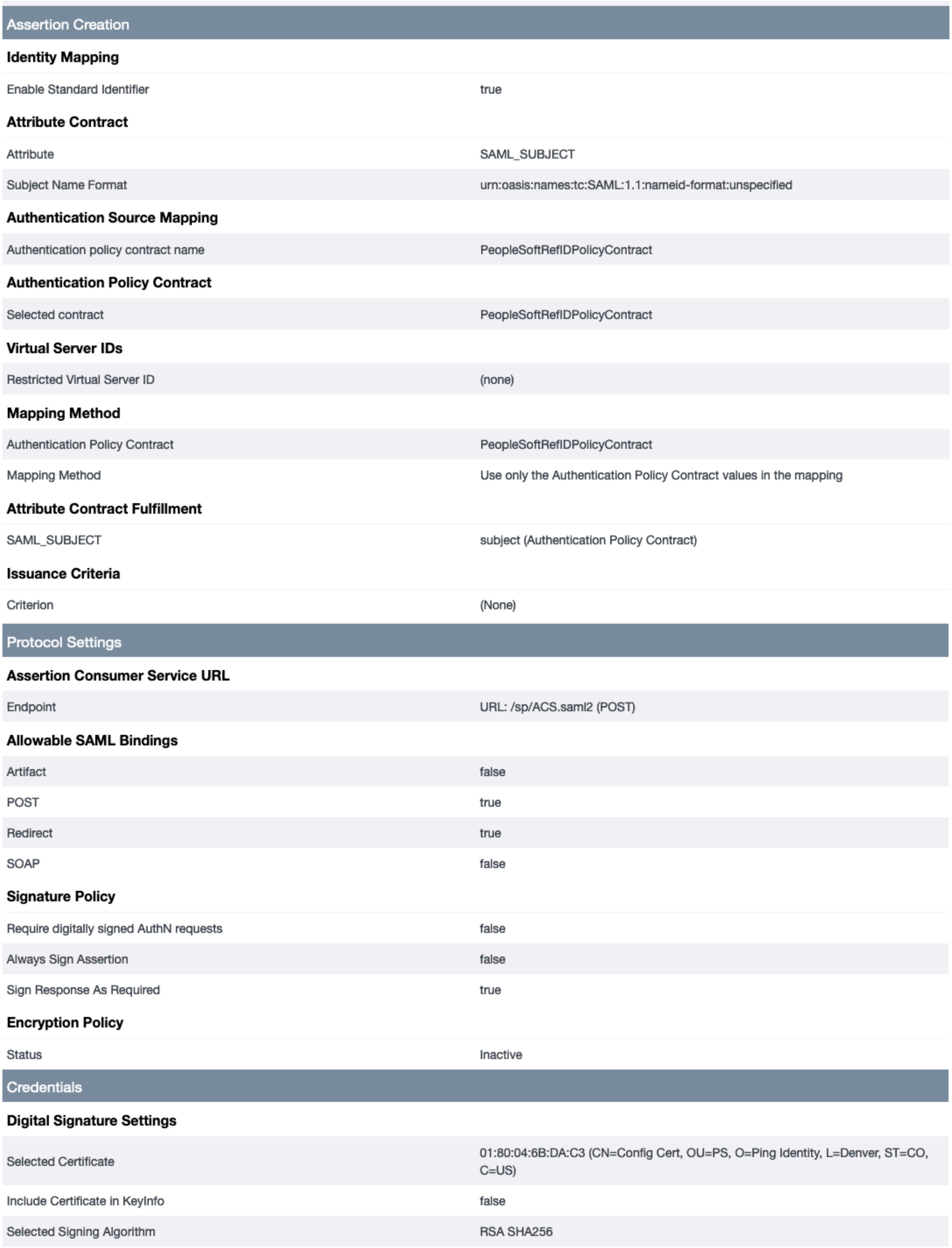
Browser SSO

SAML Profiles

IdP-Initiated SSO	true
IdP-Initiated SLO	false
SP-Initiated SSO	true
SP-Initiated SLO	false

Assertion Lifetime

Valid Minutes Before	5
Valid Minutes After	5



Assertion Creation

Identity Mapping

Enable Standard Identifier	true

Attribute Contract

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

Authentication Source Mapping

Authentication policy contract name	PeopleSoftRefIDPolicyContract

Authentication Policy Contract

Selected contract	PeopleSoftRefIDPolicyContract

Virtual Server IDs

Restricted Virtual Server ID	(none)

Mapping Method

Authentication Policy Contract	PeopleSoftRefIDPolicyContract
Mapping Method	Use only the Authentication Policy Contract values in the mapping

Attribute Contract Fulfillment

SAML_SUBJECT	subject (Authentication Policy Contract)

Issuance Criteria

Criterion	(None)

Protocol Settings

Assertion Consumer Service URL

Endpoint	URL: /sp/ACS.saml2 (POST)

Allowable SAML Bindings

Artifact	false
POST	true
Redirect	true
SOAP	false

Signature Policy

Require digitally signed AuthN requests	false
Always Sign Assertion	false
Sign Response As Required	true

Encryption Policy

Status	Inactive

Credentials

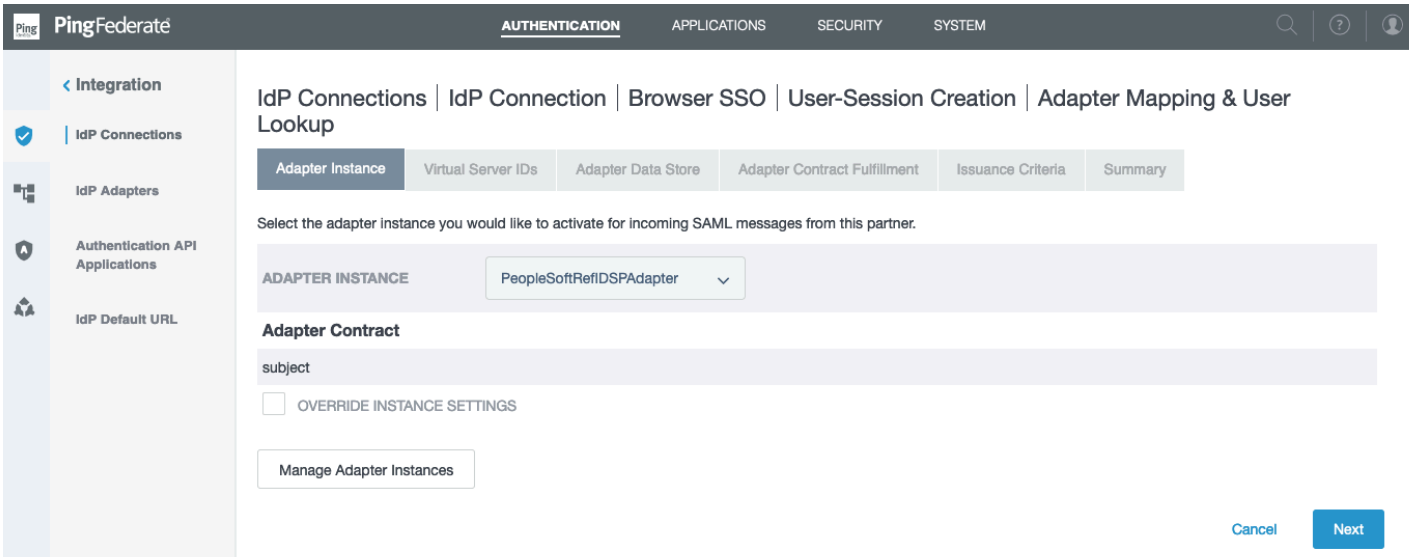
Digital Signature Settings

Selected Certificate	01:80:04:6B:DA:C3 (CN=Config Cert, OU=PS, O=Ping Identity, L=Denver, ST=CO, C=US)
Include Certificate in KeyInfo	false
Selected Signing Algorithm	RSA SHA256

3. Click **Save** and confirm that the SP Connection is enabled.

Configuring the IdP Connection

1. Log into the PingFederate admin console and click on **Authentication** >> **IdP Connections**.
2. Click **Create Connection**.
3. Click **Map New Adapter Instance** and select the Reference ID SP Adapter created above and click **Next**.



IdP Connections | IdP Connection | Browser SSO | User-Session Creation | Adapter Mapping & User Lookup

Select the adapter instance you would like to activate for incoming SAML messages from this partner.

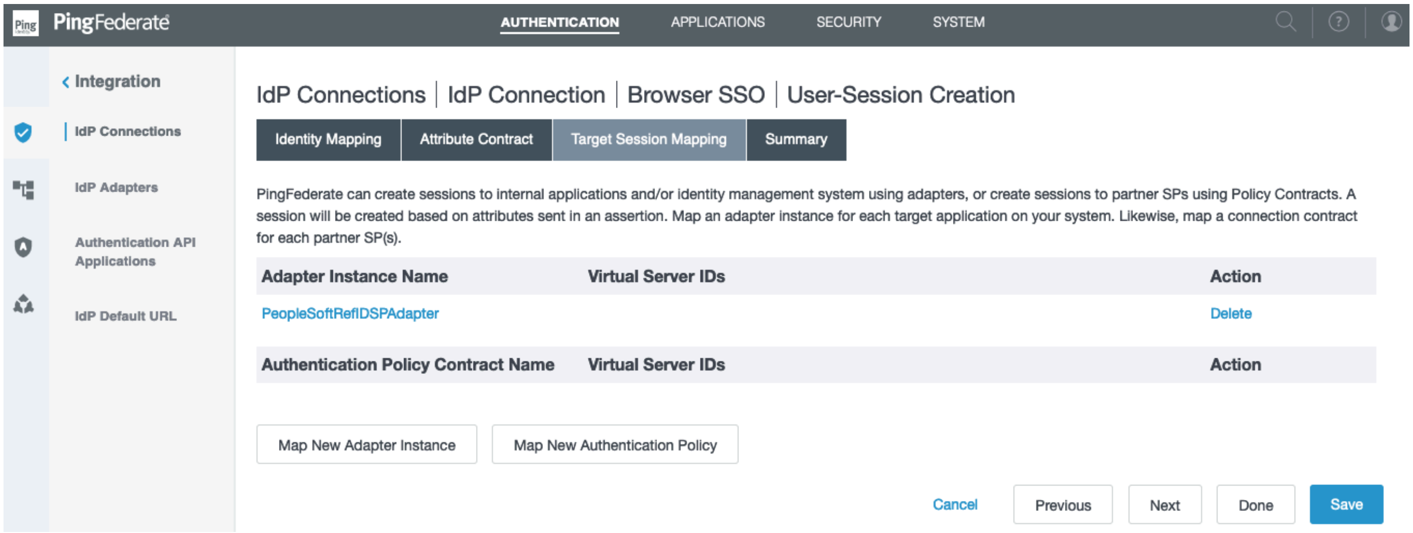
ADAPTER INSTANCE: PeopleSoftRefIDSPAdapter

Adapter Contract

subject

☐ OVERRIDE INSTANCE SETTINGS

4. Complete the adapter mapping configuration.
5. Click **Done**.



IdP Connections | IdP Connection | Browser SSO | User-Session Creation

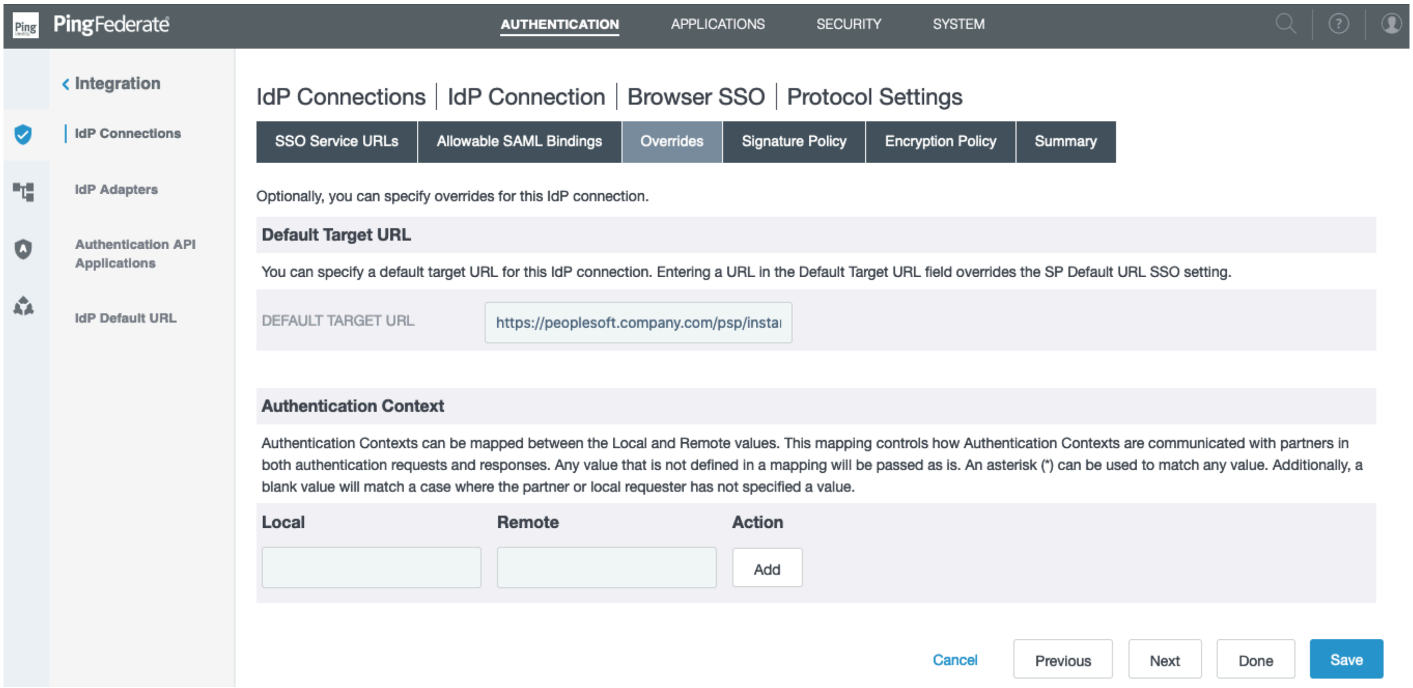
PingFederate can create sessions to internal applications and/or identity management system using adapters, or create sessions to partner SPs using Policy Contracts. A session will be created based on attributes sent in an assertion. Map an adapter instance for each target application on your system. Likewise, map a connection contract for each partner SP(s).

Adapter Instance Name	Virtual Server IDs	Action
PeopleSoftRefIDSPAdapter		Delete

Authentication Policy Contract Name	Virtual Server IDs	Action

6. Continue on with configuring the IdP Connection until **Protocol Settings**.
7. Under **Overrides** configure the **Default Target URL** with the PeopleSoft login URL, and click **Next**. For example:
   a. https://<YourPeopleSoftServer>/psp/<instance>/

Please note that the signin.html does not necessarily need to be a part of the default target Url, the below screenshot is just an example.



Optionally, you can specify overrides for this IdP connection.

Default Target URL

You can specify a default target URL for this IdP connection. Entering a URL in the Default Target URL field overrides the SP Default URL SSO setting.

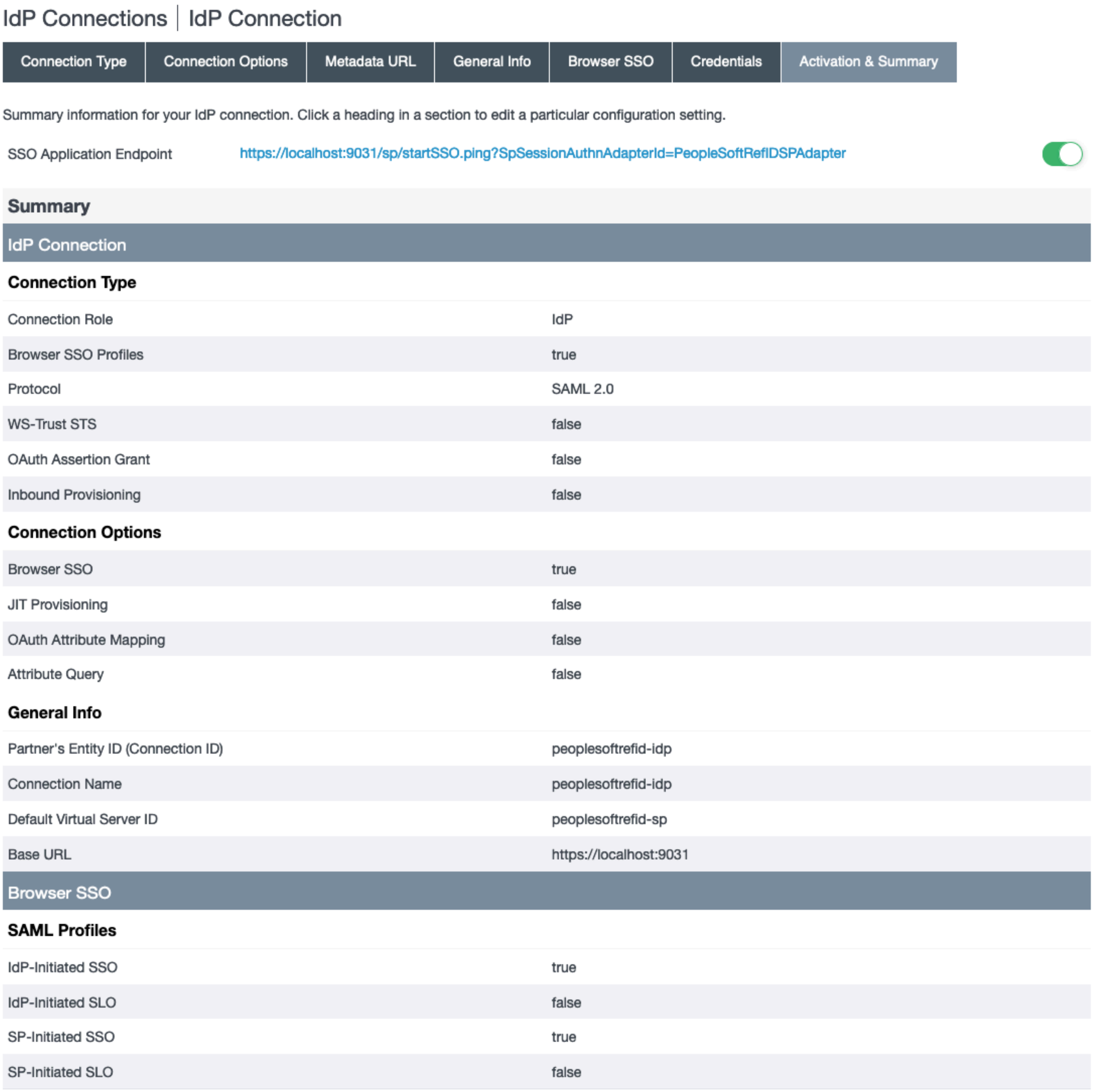
DEFAULT TARGET URL: https://peoplesoft.company.com/psp/instai

Authentication Context

Authentication Contexts can be mapped between the Local and Remote values. This mapping controls how Authentication Contexts are communicated with partners in both authentication requests and responses. Any value that is not defined in a mapping will be passed as is. An asterisk (*) can be used to match any value. Additionally, a blank value will match a case where the partner or local requester has not specified a value.

Local	Remote	Action
		Add

8. Continue configuring the rest of the IdP Connection.
9. Review the **Summary** and click **Done**.



IdP Connections | IdP Connection

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

SSO Application Endpoint https://localhost:9031/sp/startSSO.ping?SpSessionAuthnAdapterId=PeopleSoftRefIDSPAdapter

Summary

IdP Connection

Connection Type

Connection Role	IdP
Browser SSO Profiles	true
Protocol	SAML 2.0
WS-Trust STS	false
OAuth Assertion Grant	false
Inbound Provisioning	false

Connection Options

Browser SSO	true
JIT Provisioning	false
OAuth Attribute Mapping	false
Attribute Query	false

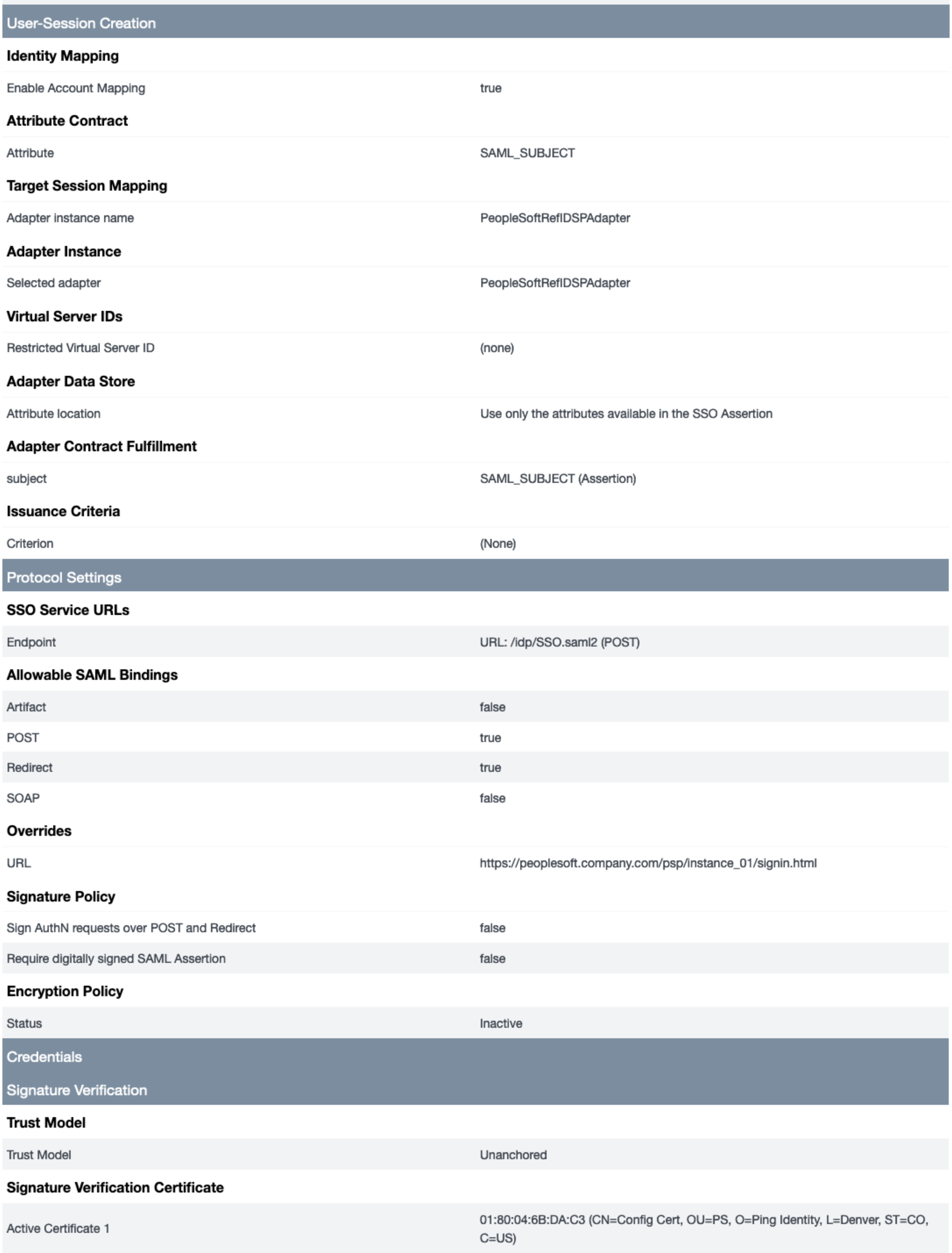
General Info

Partner's Entity ID (Connection ID)	peoplesoftrefid-idp
Connection Name	peoplesoftrefid-idp
Default Virtual Server ID	peoplesoftrefid-sp
Base URL	https://localhost:9031

Browser SSO

SAML Profiles

IdP-Initiated SSO	true
IdP-Initiated SLO	false
SP-Initiated SSO	true
SP-Initiated SLO	false



User-Session Creation	
Identity Mapping	
Enable Account Mapping	true
Attribute Contract	
Attribute	SAML_SUBJECT
Target Session Mapping	
Adapter instance name	PeopleSoftRefIDSPAdapter
Adapter Instance	
Selected adapter	PeopleSoftRefIDSPAdapter
Virtual Server IDs	
Restricted Virtual Server ID	(none)
Adapter Data Store	
Attribute location	Use only the attributes available in the SSO Assertion
Adapter Contract Fulfillment	
subject	SAML_SUBJECT (Assertion)
Issuance Criteria	
Criterion	(None)
Protocol Settings	
SSO Service URLs	
Endpoint	URL: /idp/SSO.saml2 (POST)
Allowable SAML Bindings	
Artifact	false
POST	true
Redirect	true
SOAP	false
Overrides	
URL	https://peoplesoft.company.com/psp/instance_01/signin.html
Signature Policy	
Sign AuthN requests over POST and Redirect	false
Require digitally signed SAML Assertion	false
Encryption Policy	
Status	Inactive
Credentials	
Signature Verification	
Trust Model	
Trust Model	Unanchored
Signature Verification Certificate	
Active Certificate 1	01:80:04:6B:DA:C3 (CN=Config Cert, OU=PS, O=Ping Identity, L=Denver, ST=CO, C=US)

10. Click **Save** and confirm that the IdP Connection is enabled.

PEOPLESOFT INSTALLATION AND CONFIGURATION

Modifying the PeopleSoft Integration Solution Files

Note: Extract the files from *pf-peoplesoft-integration-solution-2.4.5.zip* prior to the below steps.

1. From the */deploy/src/main/java/com/pingidentity/ps/pf/peoplesoft/* folder, open up the ***PSAgentlessConversion.java*** file and modify the following:

   a. Line 49 – set *displayDebug* to either true or false to log ReferenceID transaction events:

   ```
   private boolean displayDebug = [true or false];
   ```

   b. Line 52 – set *trustAllCertificates* to either true or false (setting the boolean flag to true is not recommended for production environments)

   ```
   private final static boolean trustAllCertificates = false;
   ```

   c. Line 166 – the ReferenceID SP Adapter User Name

```
urlConn.setRequestProperty("ping.uname", "<ReferenceID SP Adapter User Name>");
```

   d. Line 167 – the ReferenceID SP Adapter Pass Phrase

```
urlConn.setRequestProperty("ping.pwd", "<ReferenceID SP Adapter Pass Phrase>");
```

   e. Line 152 – the ReferenceID SP Adapter ID

```
urlConn.setRequestProperty("ping.instanceId", "<ReferenceID SP Adapter ID>");
```

   f. Save the file.

2. From the */deploy/src/main/resources/* folder, open up the ***log4j2.properties*** file and modify the following:

   a. Uncomment line 5 or 6 depending on which operating system is being used.
      i. Adjust the path where the *peoplesoft_pf.log* will be generated on the PeopleSoft server.

   b. Line 19 – the maximum file size for the log file, for example:

   ```
   appender.rolling.policies.size.size = 500KB
   ```

   c. Line 30 – the maximum number of days to back up the log files, for example:

   ```
   appender.rolling.strategy.delete.ifLastModified.age = 14d
   ```

   d. Line 34 – the log level, for example:

```
logger.rolling.level = debug
```

e. Review the rest of the properties as needed.
f. Save the file.

3. Modifying the ***signin.html*** file requires the following steps:
   a. Go to where the location of *signin.html* is located on your PeopleSoft web server.
   b. Make a back up copy of *signin.html* on your PeopleSoft web server (e.g., *signin.html.ORIG*).
   c. From the /conf/html/ folder, open up *siginin.html* and do the following:
      i. Modify the following (note that the line numbers may be different in the PeopleSoft web server *signin.html*):

         a. Line 127 – the PingFederate Adapter-2-Adapter URL:

            ```
            var pingUrl =
            "https://<YourPingFederateHost>/pf/adapter2adapter.ping?IdpAdapterId=<YourIdPAdapterId>&SpSessionAuthnAdapterId=<YourReferenceIDSPAdapterID>";
            ```

            Note: If a SP Connection was configured instead of the Adapter-2-Adapter mapping, use the SP Connection's SSO Application Endpoint for the URL.

         b. If logging should be enabled, uncomment the double forward slash in front of all lines of code that start with 'alert' in the PING IMPLEMENTATION JavaScript code. For example:

            ```
            alert("queryString: " + queryString);
            ```

         c. Save the file.
      ii. Copy lines 52 to 135 from the PeopleSoft Integration Solution *signin.html* – basically everything between:

      ```
      //** BEGIN PING IMPLEMENTATION **/
      …
      //** END PING IMPLEMENTATION **/
      ```

      iii. Paste lines 52 to 135 in the PeopleSoft web server *signin.html* between the <script language="JavaScript"></script> tags.

Deploying the PeopleSoft Integration Solution on the PeopleSoft Environment

Note: The above section, ***Modifying the PeopleSoft Integration Solution Files***, must be completed prior to the below steps. In addition, a compatible Java compiler (javac) must be installed on the PeopleSoft application server.

1. Shut down the PeopleSoft application server.
2. Create the following sub-directories in <YourPeopleSoftPath>/appserv/ directory:
   a. **conf** – for example: <YourPeopleSoftPath>/appserv/conf/
   b. **logs** – for example: <YourPeopleSoftPath>/appserv/logs/

    c. **com/pingidentity/ps/pf/peoplesoft/** - for example: <YourPeopleSoftPath>/appserv/classes/com/pingidentity/ps/pf/peoplesoft/

3. Copy the following files from the designated source to target location:

Source	**Target**
/deploy/ • javax.servlet-api-X.X.X.jar • json-simple-X.X.X.jar • log4j-api-X.X.X.jar • log4j-core-X.X.X.jar	<YourPeopleSoftPath>/appserv/classes/
/deploy/src/main/java/com/pingidentity/ps/pf/peoplesoft/ • PSAgentlessConversion.java	<YourPeopleSoftPath>/appserv/classes/
/deploy/src/main/resources/ • log4j2.properties	<YourPeopleSoftPath>/appserv/classes/

4. Compile the *PSAgentlessConversion.java* file and move the class file. For instance:
    a. cd /<YourPeopleSoftPath>/appserv/classes/
    b. For Linux:
        i. /usr/jdkX.X/bin/javac –classpath ./json-simple-X.X.X.jar:./javax.servlet-api-X.X.X.jar:./log4j-api-X.X.X.jar:./log4j-core-X.X.X.jar PSAgentlessConversion.java
    c. For Windows:
        i. D:\Java\javac.exe -cp ".;./json-simple-X.X.X.jar;javax.servlet-api-X.X.X.jar;log4j-api-X.X.X.jar;log4j-core-X.X.X.jar;" PSAgentlessConversion.java
    d. Move PSAgentlessConversion.class that was generated in <YourPeopleSoftPath>/appserv/classes/ to <YourPeopleSoftPath>/appserv/classes/com/pingidentity/ps/pf/peoplesoft/
5. Restart the PeopleSoft application server.

Creating the Underprivileged PeopleSoft Account

The purpose of the PING account is to intentionally fail authentication in the PeopleSoft application, so that the Ping Authentication PeopleCode (see next section) will be kicked off.

Note: These steps can be done in parallel with the above sections.

1. Log into the PeopleSoft application, and create an underprivileged account with the username of **PING**. Note that the username must match the **userid** in the ReferenceID PeopleCode (/conf/peoplecode/PeopleCode_ReferenceID.txt, line 40). The passwords should be different between the **PING** account in the PeopleSoft application and PingFederate.
2. Put **PING** into an underprivileged role that will allow the account:
    a. To have a password that never expires
    b. From becoming inactive or disabled
3. Create the following URLs in the PeopleSoft application; they will be used in the ReferenceID PeopleCode:
    a. URL.PING_DROPOFF – the PingFederate ReferenceID drop off URL (/conf/peoplecode/PeopleCode_ReferenceID.txt, line 18)
    b. URL.PING_ERROR – the error URL to redirect the user to if authentication fails (/conf/peoplecode/PeopleCode_ReferenceID.txt, line 38)

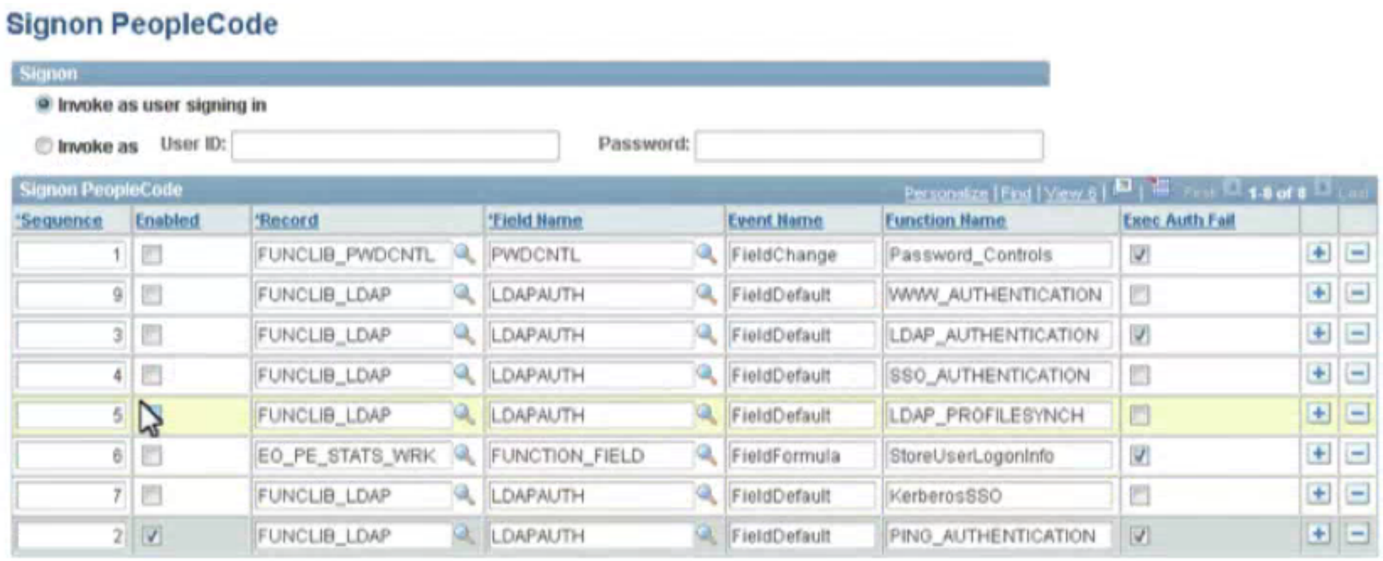
   c. URL.PING_SSO – the PingFederate SSO URL (/conf/peoplecode/PeopleCode_ReferenceID.txt, line 40)
4. Disable password controls in the PeopleSoft application (if applicable to your PeopleSoft version).
5. Disable anonymous authentication in the PeopleSoft application (if applicable to your PeopleSoft version).

Deploying the Ping Authentication PeopleCode

Note: These steps can be done in parallel with the above sections.

1. Log into the PeopleSoft application, and go to **PeopleTools** >> **Security** >> **Security Objects** >> **Signon PeopleCode**
2. Create a new PeopleCode record with the following properties:
   a. Sequence = 1 or 2
   b. Record = FUNCLIB_LDAP
   c. Field Name = LDAPAUTH
   d. Event Name = FieldDefault
   e. Function Name = PING_AUTHENTICATION
   f. Exec Auth Fail = checked

   For example:



Signon PeopleCode

Signon

● Invoke as user signing in

○ Invoke as User ID: Password:

Signon PeopleCode

*Sequence	Enabled	*Record	*Field Name	Event Name	Function Name	Exec Auth Fail
1	□	FUNCLIB_PWDCNTL	PWDCNTL	FieldChange	Password_Controls	☑
9	□	FUNCLIB_LDAP	LDAPAUTH	FieldDefault	WWW_AUTHENTICATION	□
3	□	FUNCLIB_LDAP	LDAPAUTH	FieldDefault	LDAP_AUTHENTICATION	☑
4	□	FUNCLIB_LDAP	LDAPAUTH	FieldDefault	SSO_AUTHENTICATION	□
5	□	FUNCLIB_LDAP	LDAPAUTH	FieldDefault	LDAP_PROFILESYNCH	□
6	□	EO_PE_STATS_WRK	FUNCTION_FIELD	FieldFormula	StoreUserLogonInfo	☑
7	□	FUNCLIB_LDAP	LDAPAUTH	FieldDefault	KerberosSSO	□
2	☑	FUNCLIB_LDAP	LDAPAUTH	FieldDefault	PING_AUTHENTICATION	☑

3. From the /conf/peoplecode/ folder in the *pf-peoplesoft-integration-solution-2.4.5.zip* solution, copy the contents from *PeopleCode_ReferenceID.txt* and place it in the newly created PING_AUTHENTICATION PeopleCode record.
4. Reorder the PeopleCode records by making the PING_AUTHENTICATION PeopleCode record one of the initial ones (i.e., 1 or 2).
5. Disable the old PeopleSoft authentication PeopleCode records.
6. Enable the PING_AUTHENTICATION PeopleCode record (Enabled = checked).

Testing

Please note: For all test cases below unless otherwise stated, please make sure to test with a new session (e.g., clear browser data, close and re-open the browser).

Test Case 1: Log into the PeopleSoft application as a regular user.

1. Open a browser and go to the PeopleSoft login page.
2. Log in as a regular user.

Results:

- The user should have been redirected to PingFederate for authentication.
- Upon successful authentication, the user should then be successfully authorized into the PeopleSoft application.
- A cookie named PS_TOKEN should have been created and set in the web browser.

Test Case 2: Log into the PeopleSoft application as a privileged user.

1. Open a browser and go to this PeopleSoft login link:
    a. https://<YourPeopleSoftPortalURL>/signin.html?locallogin=true
2. Log in as a privileged user.

Results:

- The user should not have been redirected to PingFederate for authentication.
- The user should have authenticated directly through the PeopleSoft login.
- Upon successful authentication, the user should then be successfully authorized into the PeopleSoft application.

Test Case 3: Re-log into the PeopleSoft application as a regular user.

1. Go through Test Case 1 steps.
2. In the same browser session, go to a different website and click around.
3. Go back to the PeopleSoft application.

Results:

- Should have the same results as Test Case 1.
- When the user returns to the PeopleSoft application after browsing another website in the same browser session, the user's session should have been preserved.

Logging

To enable/disable logging in *PSAgentlessConversion.java*, follow Steps 1a and 2 in ***Modifying the PeopleSoft Integration Solution Files***.

To enable/disable logging in the PeopleSoft login page, follow Step 3.c.i.b in ***Modifying the PeopleSoft Integration Solution Files***.