Ping Identity™

PingFederate®

PeopleSoft Integration Solution v2.4.5 (OpenToken Adapter)

User Guide

PingFederate PeopleSoft Integration Solution (OpenToken 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

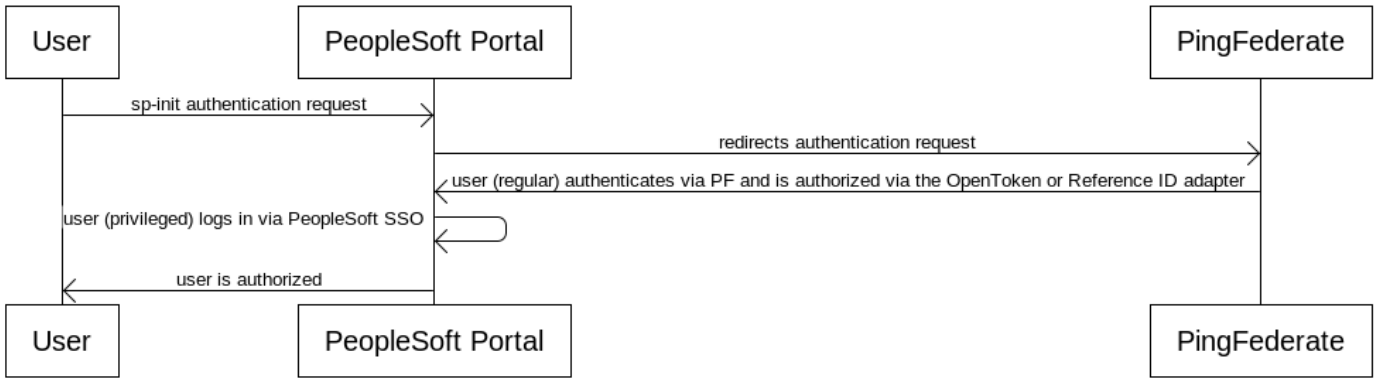
Disclaimer
This document is proprietary and not for general publication. It may be provided ad hoc for informational purposes only, and the information herein is subject to change without notice. Ping Identity does not provide any warranties and specifically disclaims any liability in connection with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



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

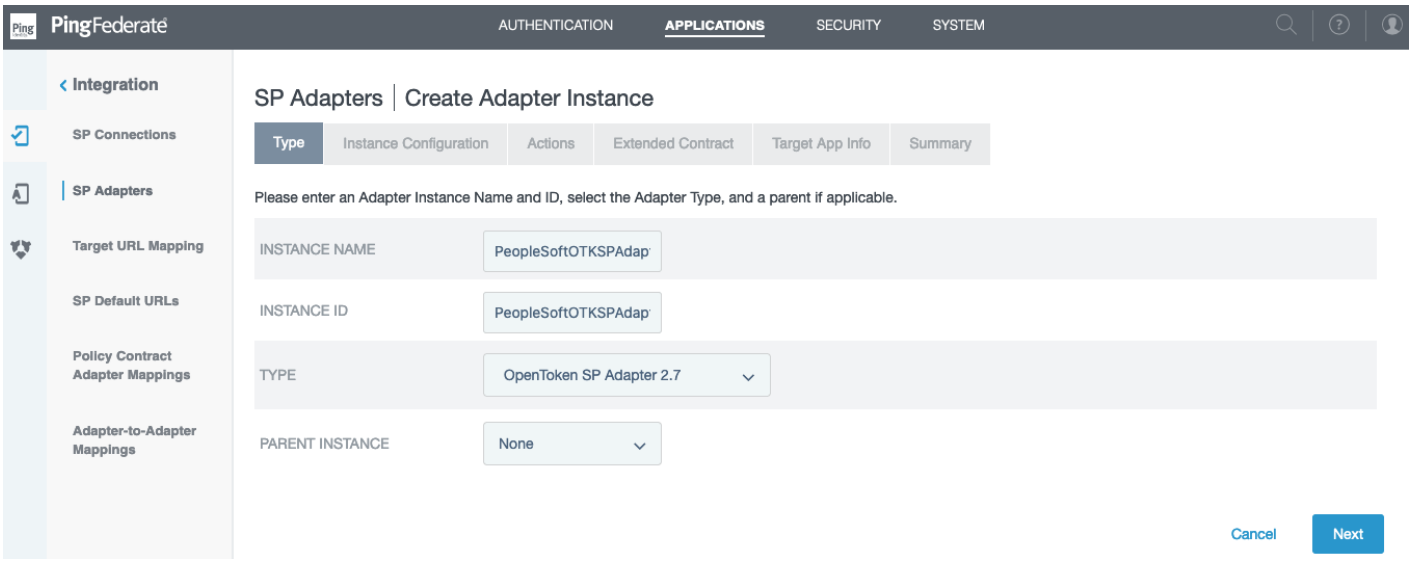
Note: It is recommended that a PeopleSoft environment with limited users should be used for the initial installation and configuration of the solution, as downtime is needed.

PINGFEDERATE CONFIGURATION

Configuring the OpenToken Adapter

Note: The *PingFederate Java Integration Kit* will need to be installed and deployed in your PingFederate environment prior to the below configuration steps.

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



4. Click the **Show Advanced Fields** link.
5. Configure the following:
    a. Password
    b. Confirm Password
    c. Transport Mode = Form POST
    d. Not Before Tolerance = 10 (leave a ‘0’ if all PeopleSoft and PingFederate server time clocks are in sync; otherwise, set it anywhere between 5-30 seconds)
    e. Send Extended Attributes = Query Parameters

SP Adapters | Create Adapter Instance

Type | Instance Configuration | Actions | Extended Contract | Target App Info | Summary

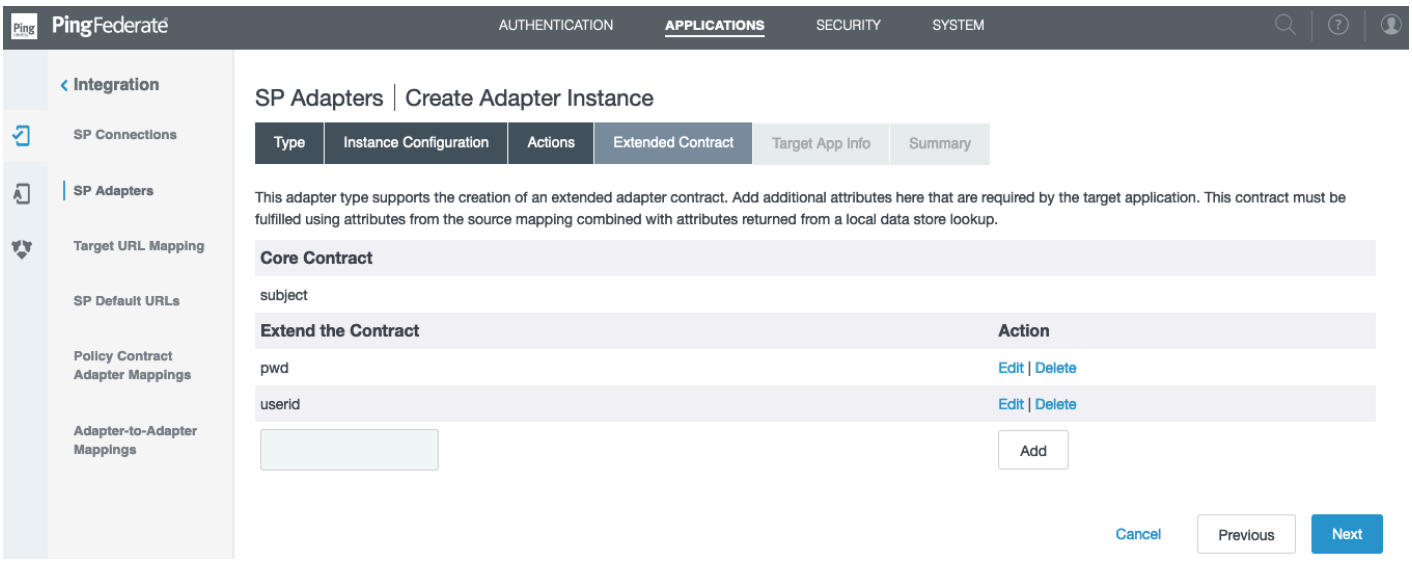
Complete the configuration necessary to set the appropriate security context for user sessions in your environment. This configuration was designed into the adapter for use at your site.

OpenToken Adapter 2.7

Field Name	Field Value	Description
PASSWORD	•••••••••	Password to use for generating the encryption key.
CONFIRM PASSWORD	•••••••••	Must match password field.
TRANSPORT MODE	○ Query Parameter ○ Cookie ● Form POST	How the token is transported to/from the application, either via a query parameter, a cookie, or as a form POST.
TOKEN NAME	opentoken	The name of the cookie or query parameter that contains the token. This name must be unique for each adapter instance.
CIPHER SUITE	○ Null ○ AES-256/CBC ● AES-128/CBC ○ 3DES-168/CBC	The algorithm, cipher mode, and key size that should be used for encrypting the token.
AUTHENTICATION SERVICE		The URL to which the user is redirected for an SSO event. This URL overrides the Target Resource which is sent as a parameter to the Authentication Service.
ACCOUNT LINK SERVICE		The URL to which the user is redirected for Account Linking. This URL is part of an external SP application. This external application performs user authentication and returns the local user ID inside the token.
LOGOUT SERVICE		The URL to which the user is redirected for a single-logout event. This URL is part of an external application, which terminates the user session.
SAMESITE COOKIE	○ Strict ○ Lax ○ None ● Nothing	The SameSite attribute for the cookie that contains the token. Selecting the option "Nothing" will not set SameSite attribute on the cookie.
COOKIE DOMAIN		The server domain should be in the format of example.com. If no domain is specified, the value is obtained from the request.
COOKIE PATH	/	The path for the cookie that contains the token.

TOKEN LIFETIME	300	The duration (in seconds) for which the token is valid. Valid range is 1 to 28800.
SESSION LIFETIME	43200	The number of seconds that a session is valid for. During this period, PingFederate can extend the lifetime of active tokens without requiring the user to authenticate again. If the token already expired or the session lifetime ended, PingFederate requires the user to authenticate again. Valid range is 1 to 259200.
NOT BEFORE TOLERANCE	10	The amount of time (in seconds) to allow for clock skew between servers. Valid range is 0 to 3600.
FORCE SUNJCE PROVIDER	☐	If checked, the SunJCE provider will be forced for encryption/decryption.
USE VERBOSE ERROR MESSAGES	☐	If checked, use verbose TokenException messages
OBFUSCATE PASSWORD	☑	If checked, the password will be obfuscated and password-strength validation will be applied. Clearing the checkbox allows backward compatibility with previous OpenToken agents.
SESSION COOKIE	☐	If checked, OpenToken will be set as a session cookie (rather than a persistent cookie). Applies only if Transport Mode is set as 'Cookie'.
SECURE COOKIE	☑	If checked, the OpenToken cookie will be set only if the request is on a secure channel (https). Applies only if Transport Mode is set as 'Cookie'.
HTTP ONLY FLAG	☑	Sets a flag for the cookie that it can only be read via http requests and disallows Javascript to access the cookie. Note: not all browsers respect the HTTP Only flag.
SEND SUBJECT AS QUERY PARAMETER	☐	Checking this box will send the Subject ID as a clear-text query parameter, if Transport Mode is set to "Query Parameter". If Transport Mode is set to "Form POST", the Subject ID is sent as POST data.
SUBJECT QUERY PARAMETER		The parameter name used for the Subject ID when the "Send Subject ID as Query Parameter" box is checked.
SEND EXTENDED ATTRIBUTES	Query Parameters	Extended Attributes are typically sent only within the token, but this option overrides the normal behavior and allows the attributes to be included in browser cookies or query parameters.
SKIP TRIMMING OF TRAILING BACKSLASHES	☐	If not checked, it prevents insecure content from affecting the security of your application/agent. We recommend to update your applications with the latest version of the agent. We recommend not to change the value of this flag.
URL ENCODE COOKIE VALUES	☑	If checked, the extended attribute cookie value will be URL encoded.

6. Click **Next**.
7. Click the **Invoke Download** link.
8. Click **Export** and save the **agent-config.txt** file. Then click **Next**.
9. Extend the contract by adding the following attributes:
    a. userid
    b. pwd



10. Click **Next**.
11. Review the **Summary**, and click **Done**.

SP Adapters | Create Adapter Instance

Type | Instance Configuration | Actions | Extended Contract | Target App Info | Summary

SP adapter instance summary information.

Create Adapter Instance

Type

Instance Name	PeopleSoftOTKSPAdapter
Instance ID	PeopleSoftOTKSPAdapter
Type	OpenToken SP Adapter 2.7
Class Name	com.pingidentity.adapters.opentoken.SpAuthnAdapter
Parent Instance Name	None

Instance Configuration

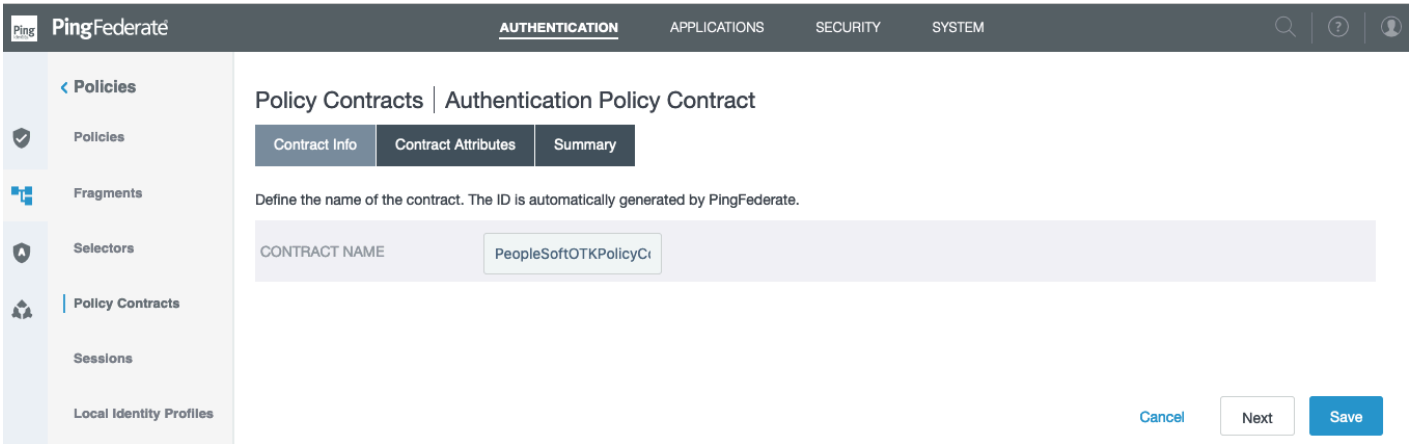
Transport Mode	Form POST
Token Name	opentoken
Cipher Suite	AES-128/CBC
Authentication Service	
Account Link Service	
Logout Service	
SameSite Cookie	Nothing
Cookie Domain	
Cookie Path	/
Token Lifetime	300
Session Lifetime	43200
Not Before Tolerance	10
Force SunJCE Provider	false
Use Verbose Error Messages	false
Obfuscate Password	true

Session Cookie	false
Secure Cookie	true
HTTP Only Flag	true
Send Subject as Query Parameter	false
Subject Query Parameter	
Send Extended Attributes	Query Parameters
Skip Trimming of Trailing Backslashes	false
URL Encode Cookie Values	true
Actions	
Download	Download the configuration file for the agent.
Extended Contract	
Attribute	subject
Attribute	pwd
Attribute	userid
Target App Info	

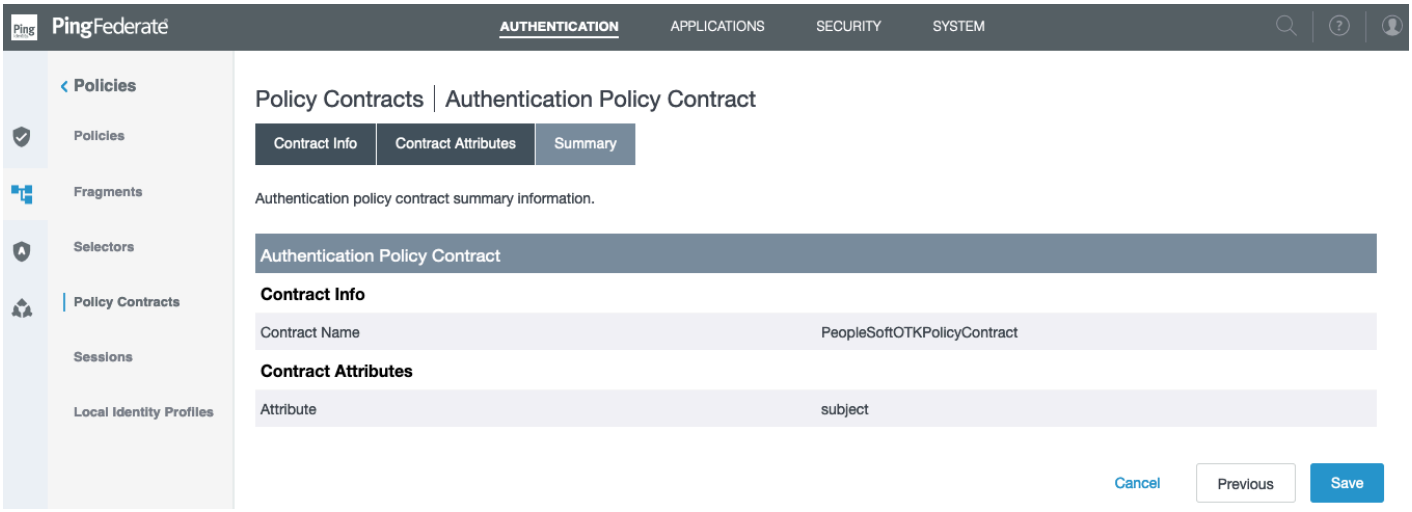
12. Click **Save**.

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**.



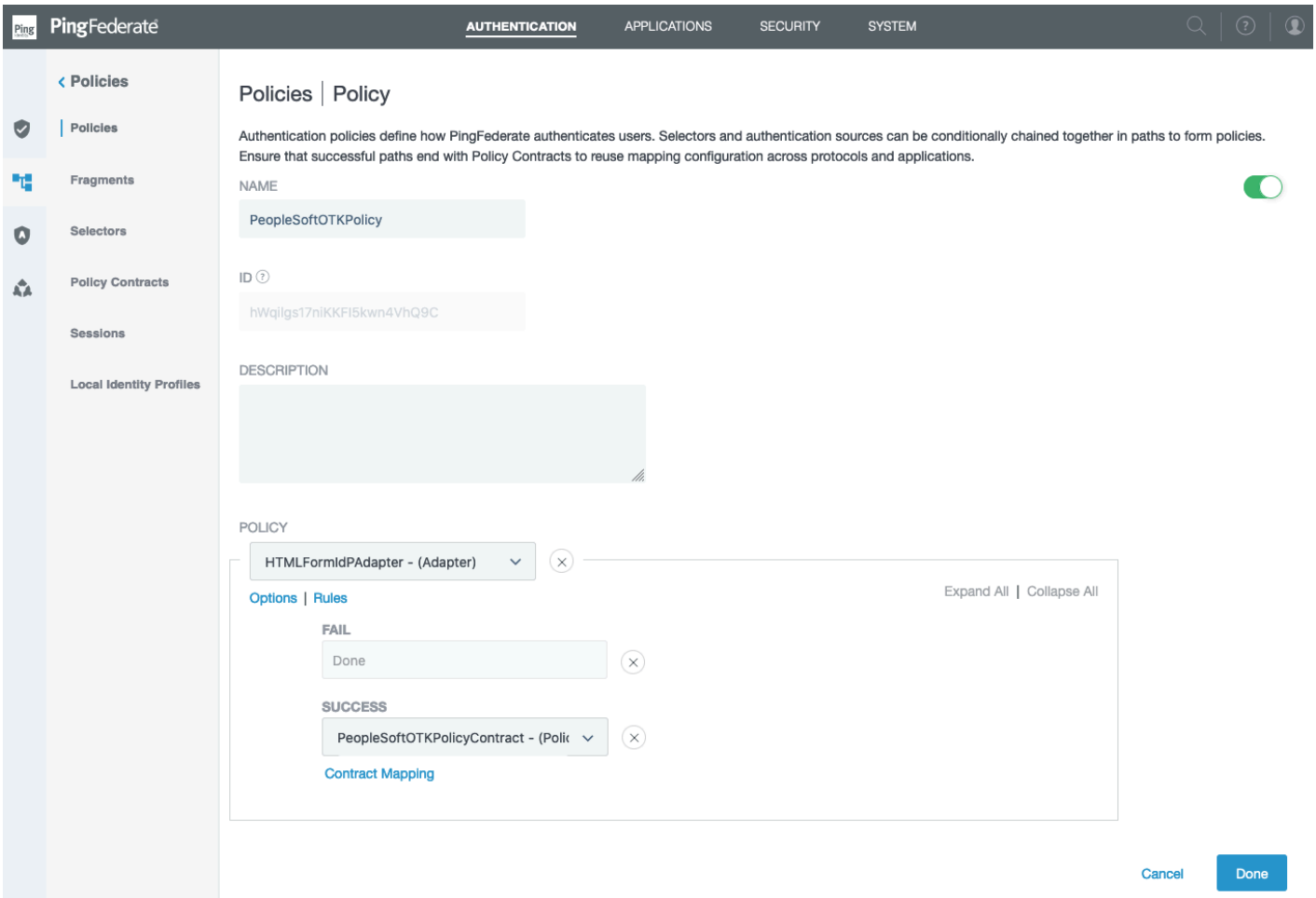
4. Click **Next**.
5. Review the **Summary** and click **Save**.



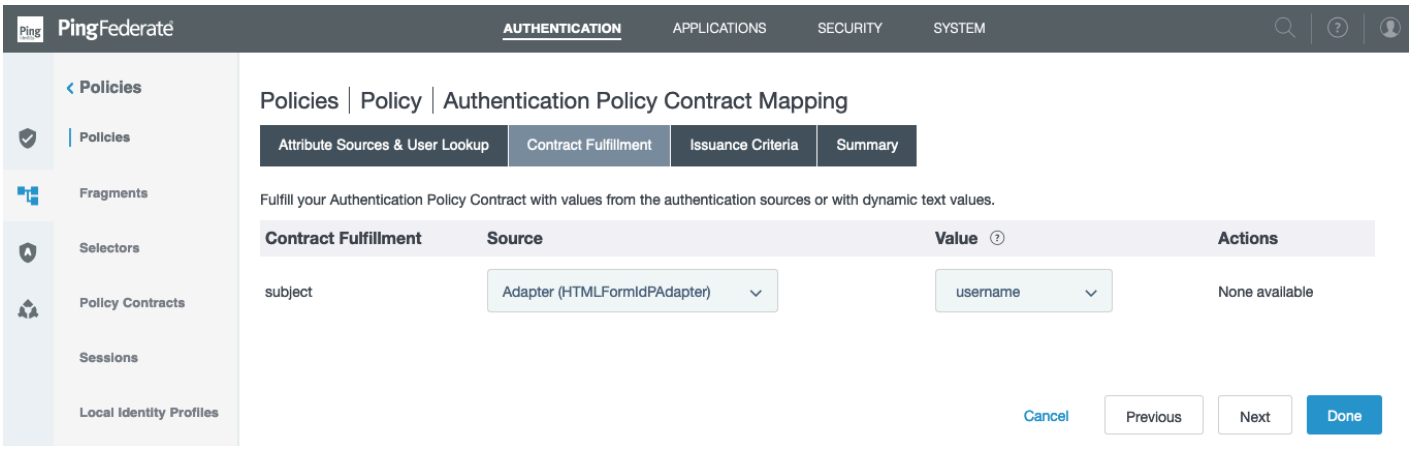
Configuring the Policy

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

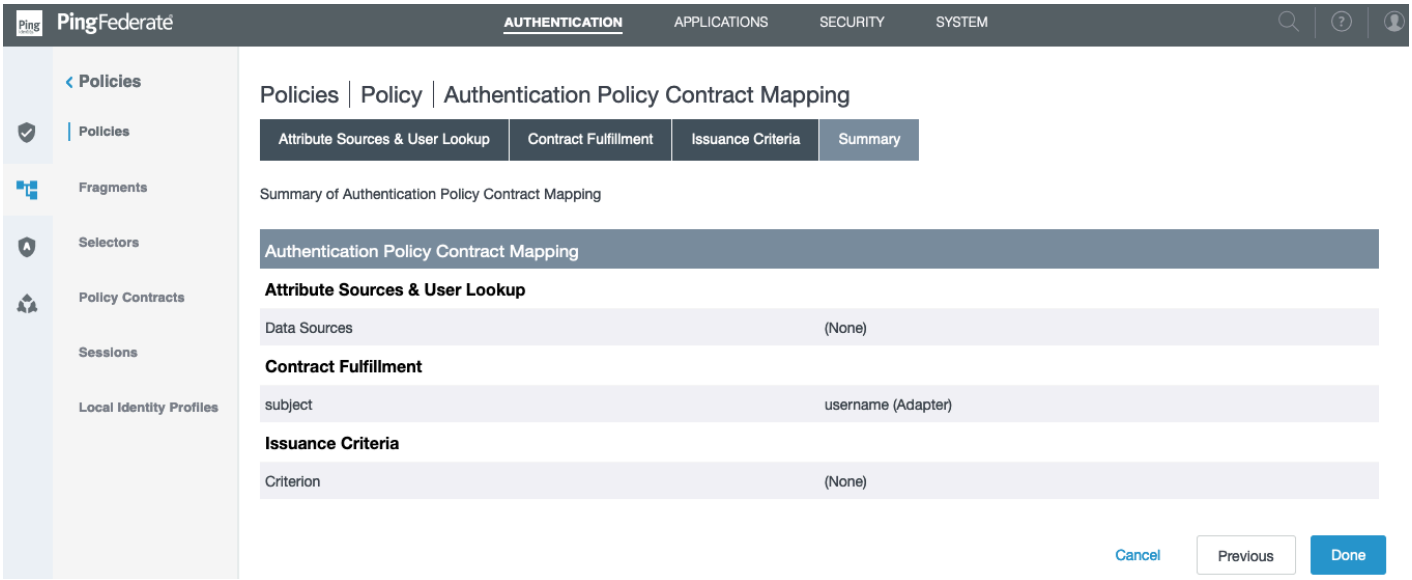
1. Log into the PingFederate admin console and click on **Authentication** >> **Policies**.
2. Click **Add Policy**.
3. Enter the **Name** and configure the policy flow. An HTML Form IdP Adapter is used for the first factor in this example.



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



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



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

Connection Type | Connection Options | Metadata URL | 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://localhost:9031/idp/startSSO.ping?PartnerSpId=peoplesoftotk-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)	peoplesoftotk-sp
Connection Name	peoplesoftotk-sp
Default Virtual Server ID	peoplesoftotk-idp
Base URL	https://localhost:9031

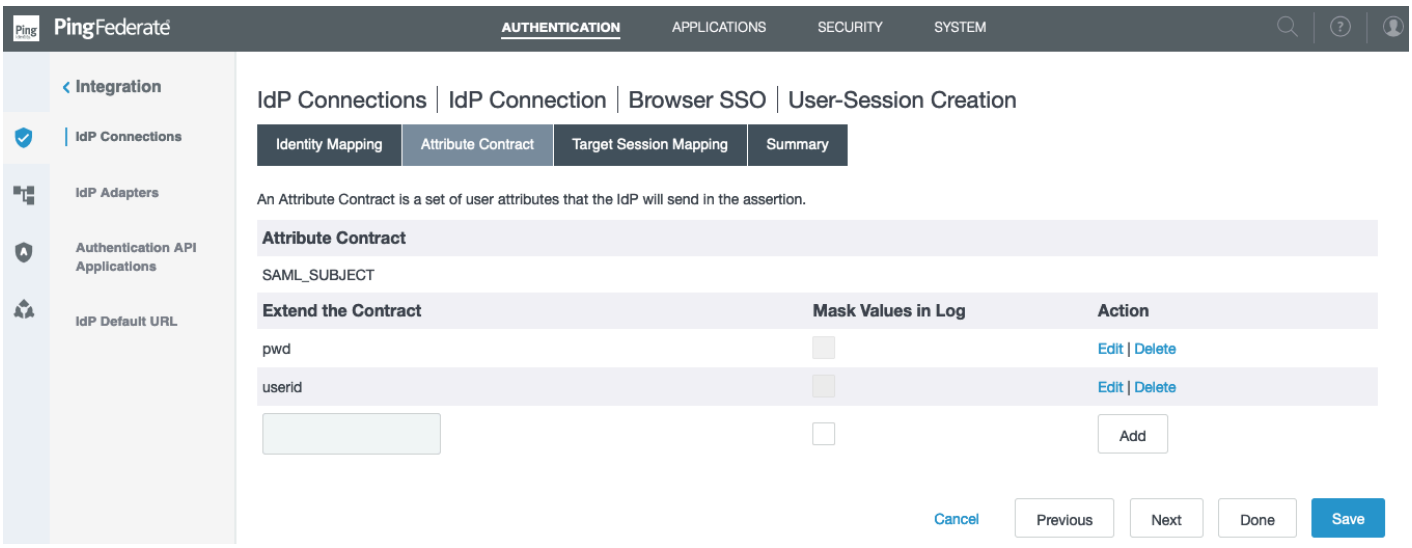
Browser SSO	
SAML Profiles	
IdP-Initiated SSO	true
IdP-Initiated SLO	false
SP-Initiated SSO	true
SP-Initiated SLO	false
Assertion Lifetime	
Valid Minutes Before	5
Valid Minutes After	5
Assertion Creation	
Identity Mapping	
Enable Standard Identifier	true
Attribute Contract	
Attribute	SAML_SUBJECT
Subject Name Format	urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
Authentication Source Mapping	
Authentication policy contract name	PeopleSoftOTKPolicyContract
Authentication Policy Contract	
Selected contract	PeopleSoftOTKPolicyContract
Virtual Server IDs	
Restricted Virtual Server ID	(none)
Mapping Method	
Authentication Policy Contract	PeopleSoftOTKPolicyContract
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

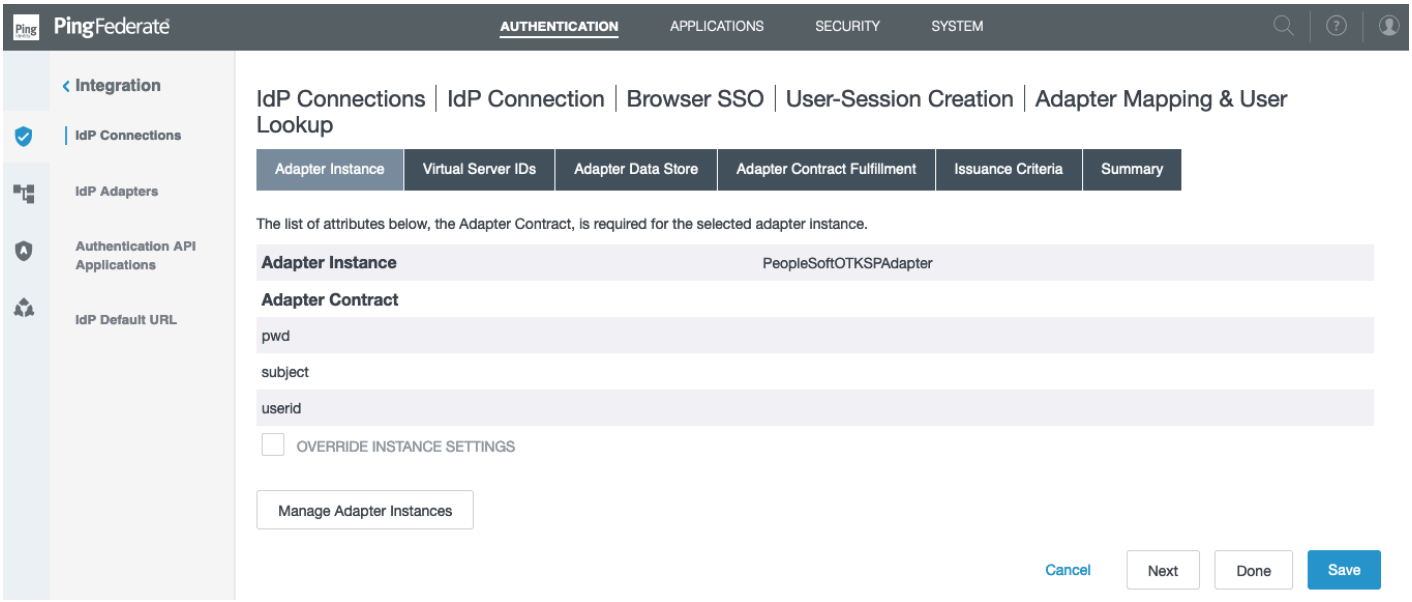
3. Click **Save** and confirm that the SP Connection is enabled.

Configuring the IdP Connection

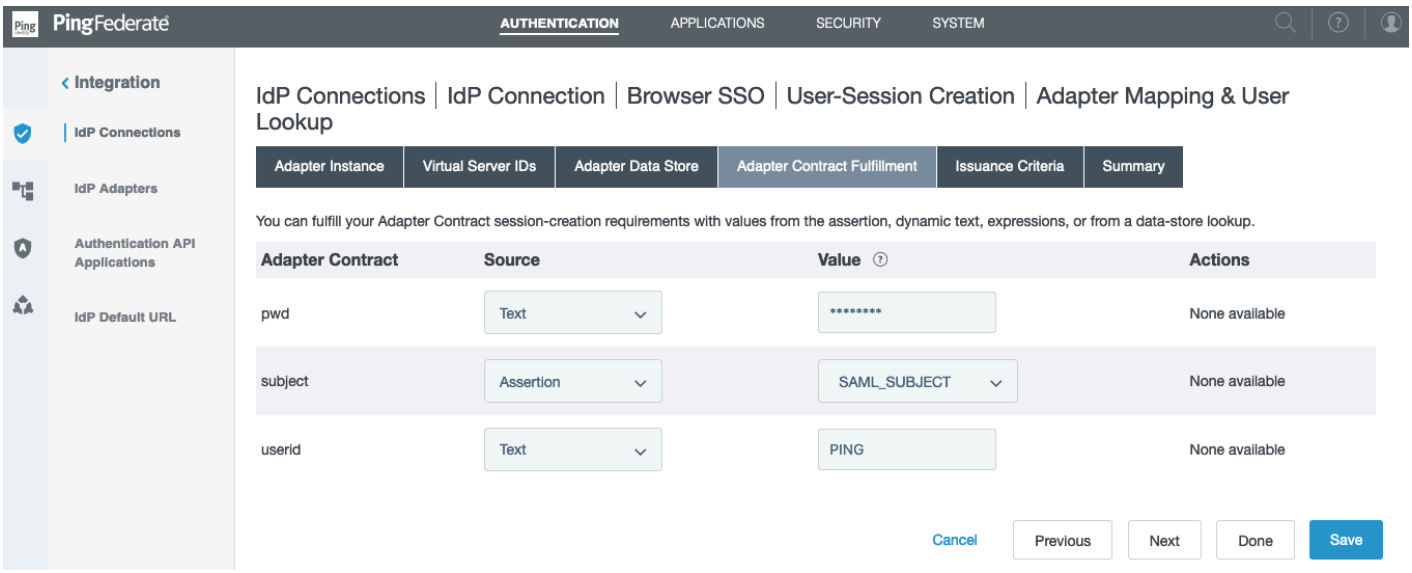
1. Log into the PingFederate admin console and click on **Authentication** >> **IdP Connections**.
2. Click **Create Connection**.
3. In the **Attribute Contract** section, extend the attributes to include ‘userid’ and ‘pwd’, and click **Next**.



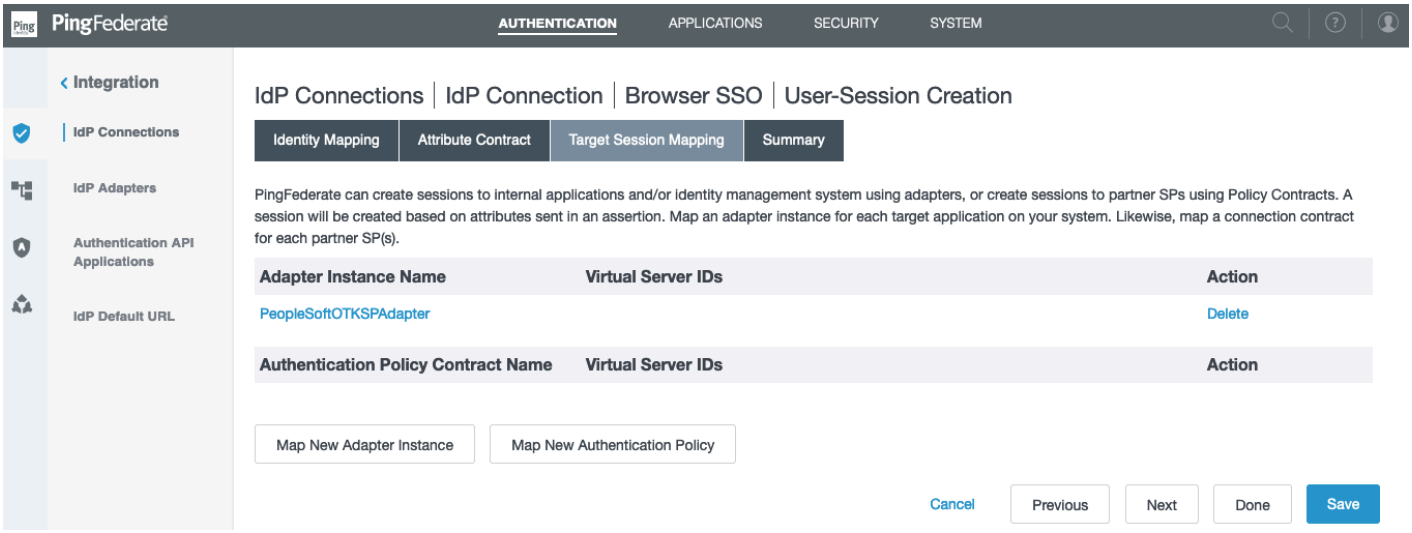
4. Click **Map New Adapter Instance** and select the OTK SP Adapter created above and click **Next**.



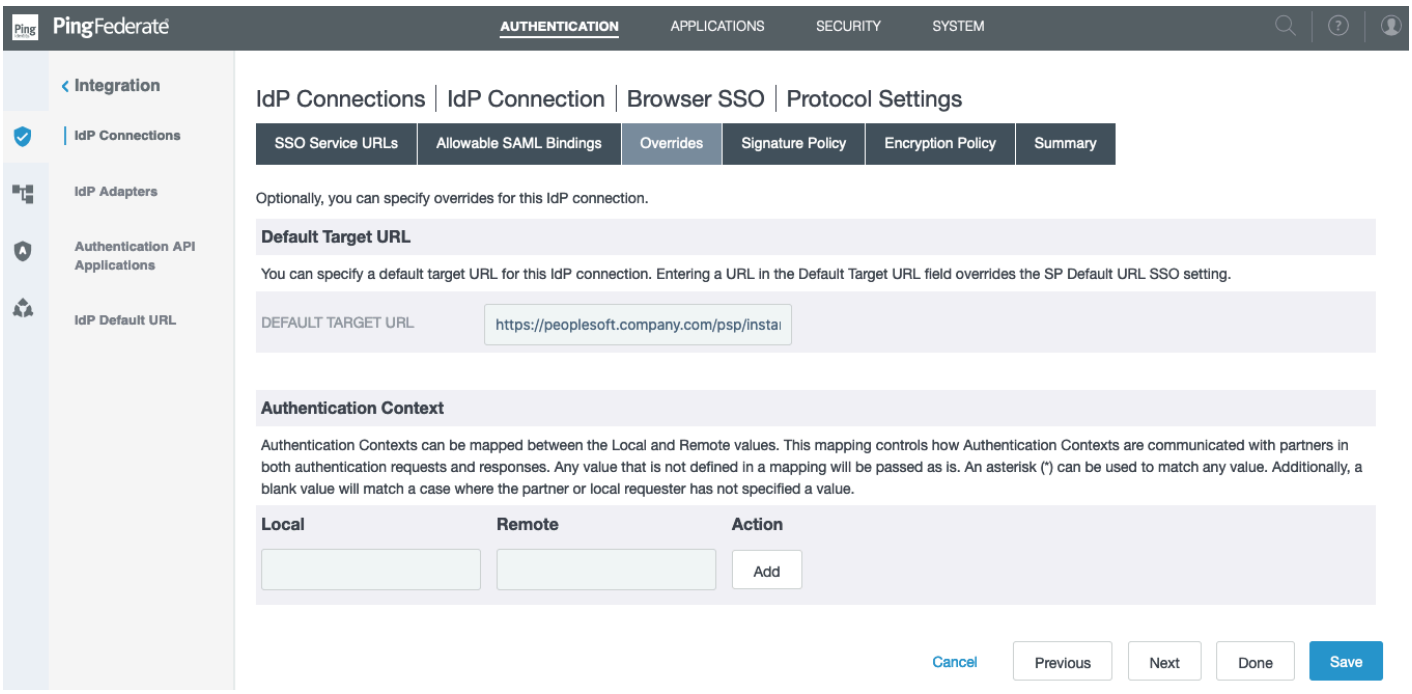
5. Click **Next**.
6. Click **Next**.
7. Fulfill the **Adapter Contract Fulfillment** with the following criteria:
    a. userid = PING
    b. pwd = ******



8. Click **Done**.



9. Continue on with configuring the IdP Connection until **Protocol Settings**.
10. 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.



11. Continue configuring the rest of the IdP Connection.
12. Review the **Summary** and click **Done**.

IdP Connections | IdP Connection

Connection Type | Connection Options | Metadata URL | General Info | Browser SSO | Credentials | Activation & Summary

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=PeopleSoftOTKSPAdapter

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)	peoplesoftotk-idp
Connection Name	peoplesoftotk-idp
Default Virtual Server ID	peoplesoftotk-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
Attribute	pwd
Attribute	userid
Target Session Mapping	
Adapter instance name	PeopleSoftOTKSPAdapter
Adapter Instance	
Selected adapter	PeopleSoftOTKSPAdapter
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	
pwd	******** (Text)
subject	SAML_SUBJECT (Assertion)
userid	PING (Text)
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)

13. 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 ***PSOpenTokenConversion.java*** file and modify the following:

    a. Line 36 – set *displayDebug* to either true or false to log open token transaction events:

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

    b. 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. From the */conf/peoplecode* folder, open up the ***PeopleCode_OpenToken.txt*** file and modify the following if needed:

    a. If only returning the User ID in the attribute contract, ensure that lines 47-48 are **not** commented out and lines 51-58 are commented out:

```
&psUserId = &Agent.GetUserId([True or False], &opentoken, &URL);
&logfile.WriteLine("     psUserId= " | &psUserId);
```

    b. If returning the User ID along with additional attributes in the attribute contract, ensure that lines 51-58 are **not** commented out, lines 47-48 are commented out, and modify accordingly to extract the additional attributes – for example:

```
&psAttrNames = "mail|displayName"; // attribute names must be separated by a pipe
&psUserData = Split(&Agent.GetUserData(True, &psAttrNames, &opentoken, &URL), "|");
&psUserId = &psUserData[1];
&logfile.WriteLine("    psUserId= " | &psUserId);
&psMail = &psUserData[2];
&logfile.WriteLine("    psMail = " | &psMail);
&psDisplayName = &psUserData[3];
&logfile.WriteLine("    psDisplayName = " | &psDisplayName);
```

    c. Please note that in line 68:

```
SetAuthenticationResult( True, Upper(&psUserId), "", False);
```

    The user ID (&psUserId) obtained from the open token will be converted to upper case. Please ensure that any case settings in PeopleSoft have been configured to match case comparison for the user ID. Otherwise, line 68 will need to be modified to match the case settings in PeopleSoft.

4. 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 */deploy/html* folder, open up *siginin.html* and do the following:
    i. Modify the following:

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

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

            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, remove 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);

    ii. Save the file.

    iii. Copy lines 52 to 135 from the *signin.html* that was just modified– basically everything between:

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

    iv. 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**
Exported from ***Configuring the OpenToken Adapter*** Step 8: • agent-config.txt	<YourPeopleSoftPath>
/deploy/	<YourPeopleSoftPath>/appserv/classes/

• commons-collections-X.X.X.jar • commons-logging-X.X.jar • javax.servlet-api-X.X.X.jar • log4j-api-X.X.X.jar • log4j-core-X.X.X.jar • otk-agents/opentoken-agent-2.X.X.jar (please make sure you have the correct version that matches your OpenToken Adapter version in PingFederate)	
/deploy/src/main/java/com/pingidentity/ps/pf/peoplesoft/ • PSOpenTokenConversion.java	<YourPeopleSoftPath>/appserv/classes/
/deploy/src/main/resources/ • log4j2.properties	<YourPeopleSoftPath>/appserv/classes/

4. Compile the *PSOpenTokenConversion.java* file and move the class file. For instance:
    a. cd /<YourPeopleSoftPath>/appserv/classes/
    b. For Linux:
        i. /usr/jdkX.X/bin/javac -classpath ./opentoken-agent-2.X.X.jar:./commons-collections-X.X.X.jar:./commons-logging-X.X.jar:./javax.servlet-api-X.X.X.jar:./log4j-api-X.X.X.jar:./log4j-core-X.X.X.jar PSOpenTokenConversion.java
    c. For Windows:
        i. D:\Java\javac.exe -cp ".;./opentoken-agent-2.X.X.jar;commons-collections-X.X.X.jar;commons-logging-X.X.jar;javax.servlet-api-X.X.X.jar;log4j-api-X.X.X.jar;log4j-core-X.X.X.jar;" PSOpenTokenConversion.java
    d. Move PSOpenTokenConversion.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.

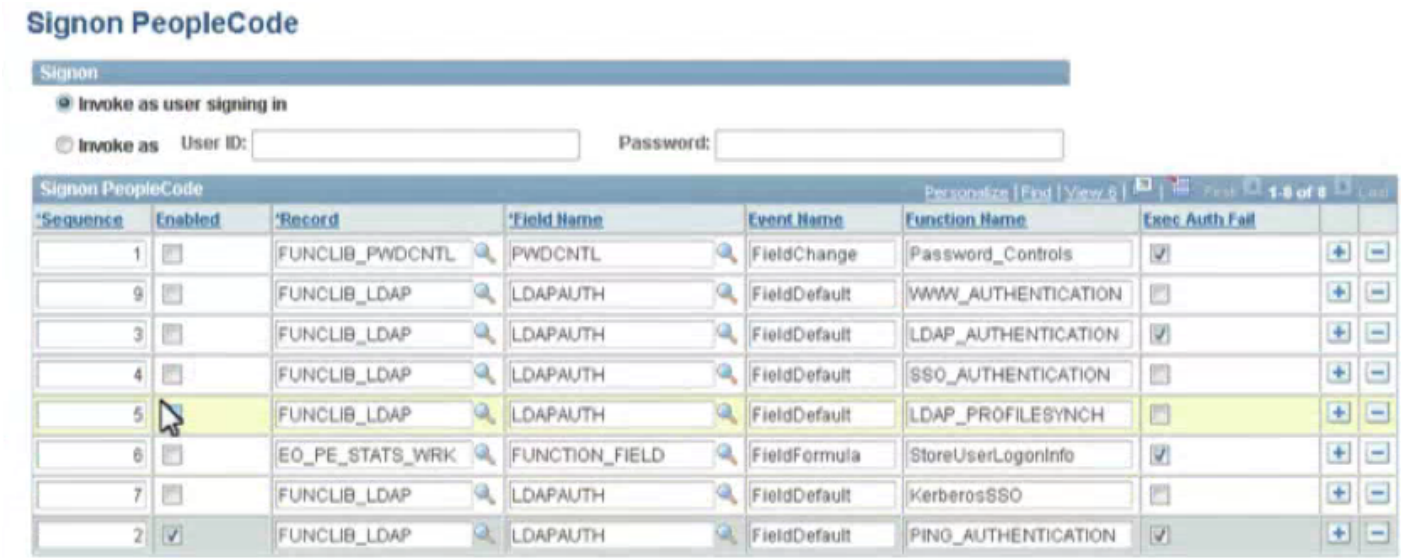
1. Log into the PeopleSoft application, and create an underprivileged account with the username of **PING**. Note that the username must match the **userid** entered in ***Configuring the Adapter-to-Adapter Mapping*** Step 5. The passwords should be different between the **PING** account in the PeopleSoft 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 a URL named **AGENT** with the path of where the agent-config.txt is located on the PeopleSoft application server, for example (do not forget the end forward slash):
    a. D:/psoft/<instance>/
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:



3. From the /conf/peoplecode/ folder in the *pf-peoplesoft-integration-solution-2.4.5.zip* solution, copy the contents from *PeopleCode_OpenToken.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>/instance/?cmd=login&languageCd=ENG&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 *PSOpenTokenConversion.java*, follow Steps 1 and 2 in ***Modifying the PeopleSoft Integration Solution Files***.

To enable/disable logging in the PeopleSoft login page, follow Step 4.c.i.b in ***Modifying the PeopleSoft Integration Solution Files***.