MobileIron Access Cookbook

Access with Salesforce and PingFederate

Revised: April 03, 2018

Contents

Overview

SAML provides single sign-on capability for users accessing their services hosted in a cloud environment. Generally, a service provider such as Salesforce is federated with an identity provider such as PingFederate for authentication. The user gets authentication from PingFederate and obtains a SAML token for accessing applications in a cloud environment, such as Salesforce.
This guide serves as step-by-step configuration manual for users using PingFederate as an authentication provider with Salesforce in a cloud environment.

Prerequisites for PingFederate

You must perform the following steps before you configure Salesforce:

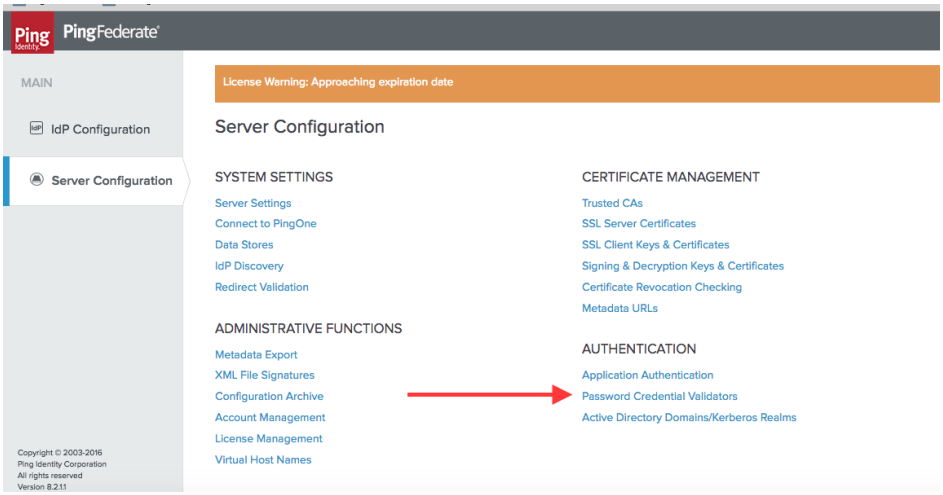
1. Create a Validator
2. Create an Adapter
3. Create a Signing Certificate
4. Add an LDAP Datastore

Create a Validator

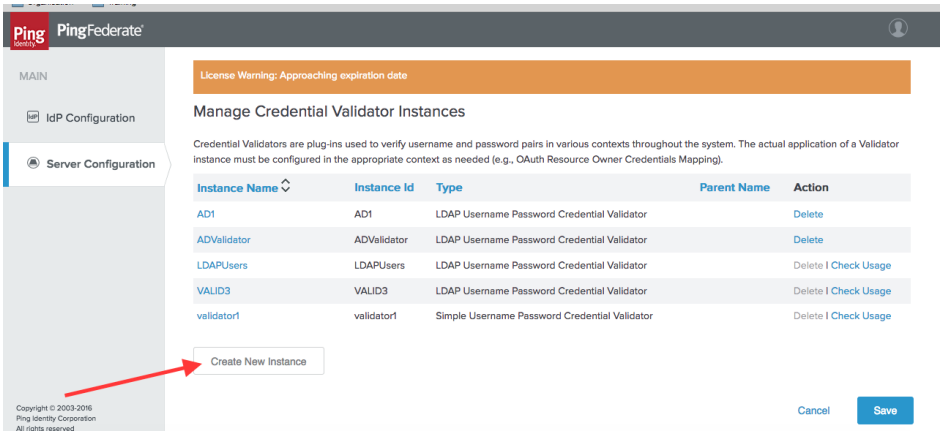
A validator authenticates the user. A user can authenticate in multiple ways with PingFederate such as AD authentication (sync users in AD), local user authentication (create local users in PingFederate), and so on.

Procedure

1. On the **Server Configuration** tab in PingFederate, click **Password Credential Validators**.



2. Click **Create New Instance**. The **Manage Credential Validator Instances** page opens.



3. Enter the following details for the new instance and click **Next**.

Field	Value
Instance Name	Enter an appropriate instance name
Instance ID	Enter an ID
Type	Select *LDAP username and password Credential validator* from the drop-down list.

4. Select the appropriate values for LDAP and click **Next**.

Field	Value
LDAP Datastore	dc.example.com
Search Base	DC=example,DC=com
Search Filter	userPrincipalName=${username}
Scope of Search	Subtree

5. Click **Next** > **Done**.

Task Result

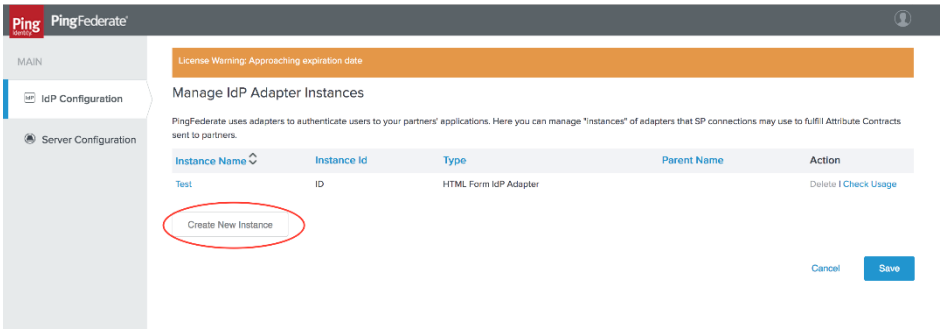
A validator is created. You must use this validator while creating federation data.

Create an Adapter

An adapter is a simulator for the authentication page. It can be form-based or pop-up based. PingFederate uses terms such as *HTMLFORM* for form-based and *httpBasic* for pop-up based adapters. You must create a new adapter instance.

Procedure

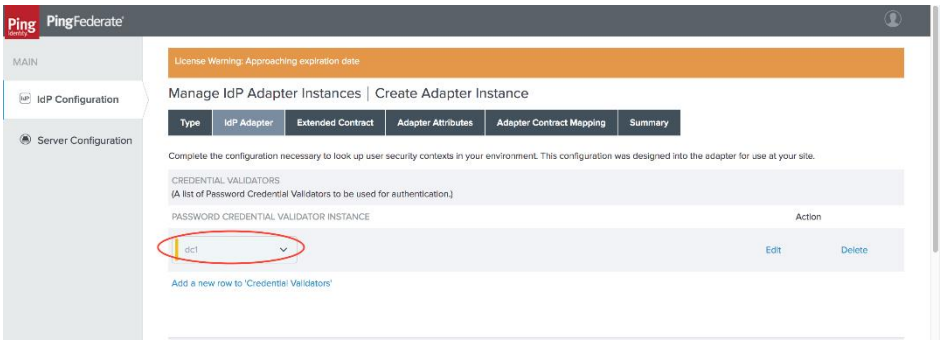
1. On **IDP Configuration** tab, click **Adapters** > **Create New Instance**.



2. Enter the following details for the new instance and click **Next**.

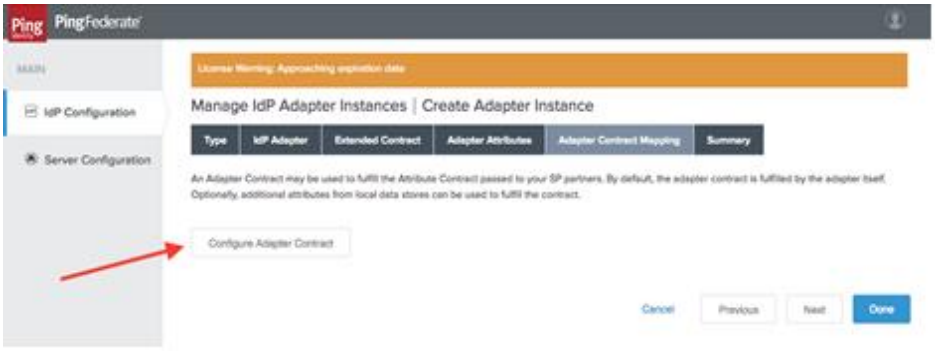
Field	**Value**
Instance Name	Enter an appropriate instance name
InstanceID	Enter an ID
Type	HTML Form IDP Adapter

3. On the next screen, select the validator created using **Create a Validator** and click **Update**.

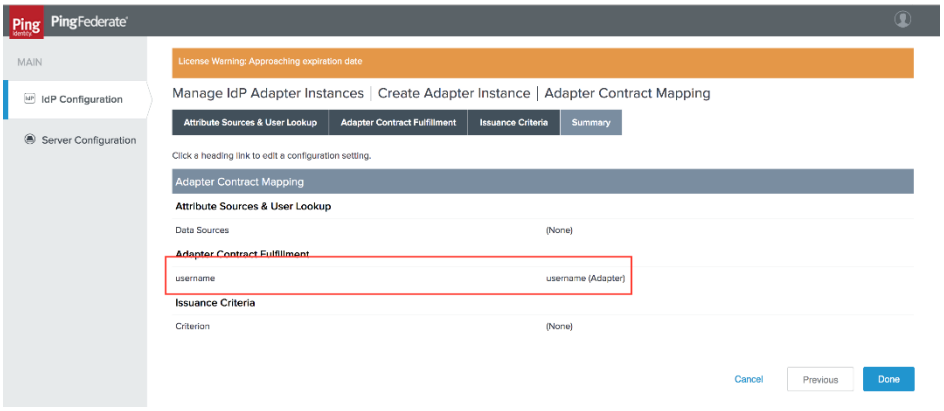


4. Click **Next** > **Next** and select **Pseudonym**. Click **Next**.

5. Click **Configure Adapter Contract**.



6. Click **Adapter Contract Fulfillment** and select **Source** as Adapter**.** Click **Next** > **Next** > **Done**.



Task Result

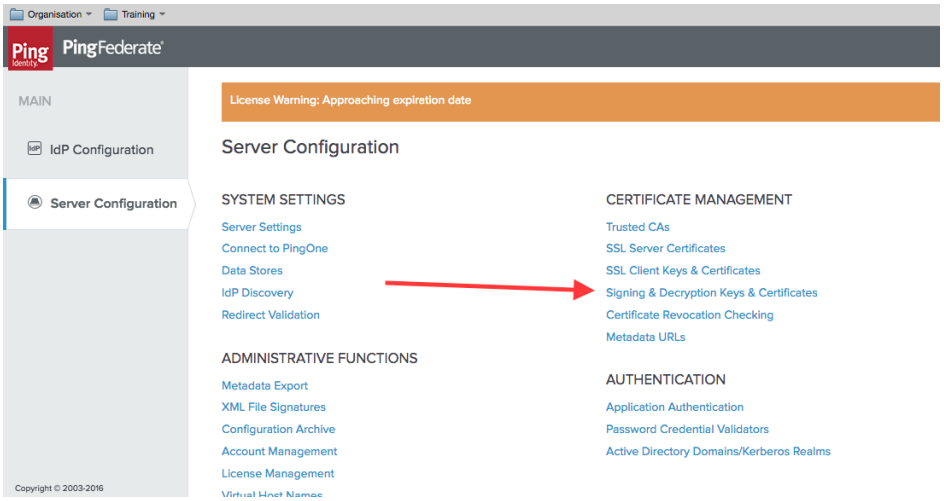
An adapter is created. You must use this adapter while creating the federation pair.

Create a Signing Certificate

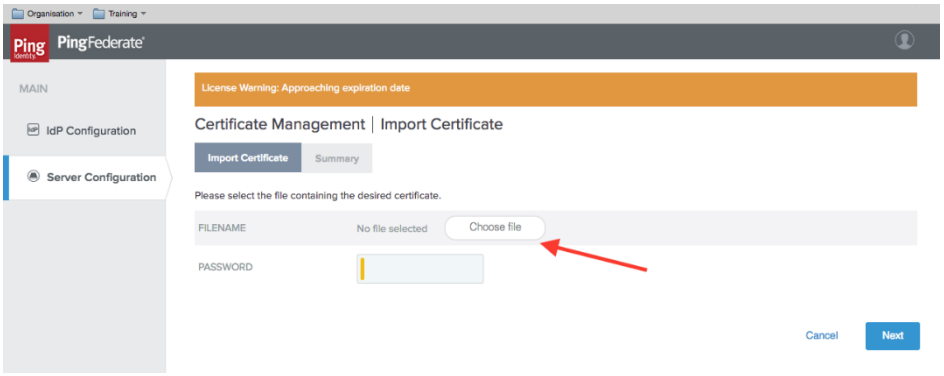
If you are using any self-signed certificate as a signing certificate, you must upload the same certificate to PingFederate such that the uploaded certificate is used as a signing certificate.

Procedure

1. On the **Server Configuration** tab, click **Signing & Decryption Keys & Certificates**.



2. Click **Import** if you already have signing certificates.
3. Click **Choose file** and browse to import the existing **p12 certificate**.
4. Enter the **Password** and click **Next**.



5. Click **Save**.

Task Result

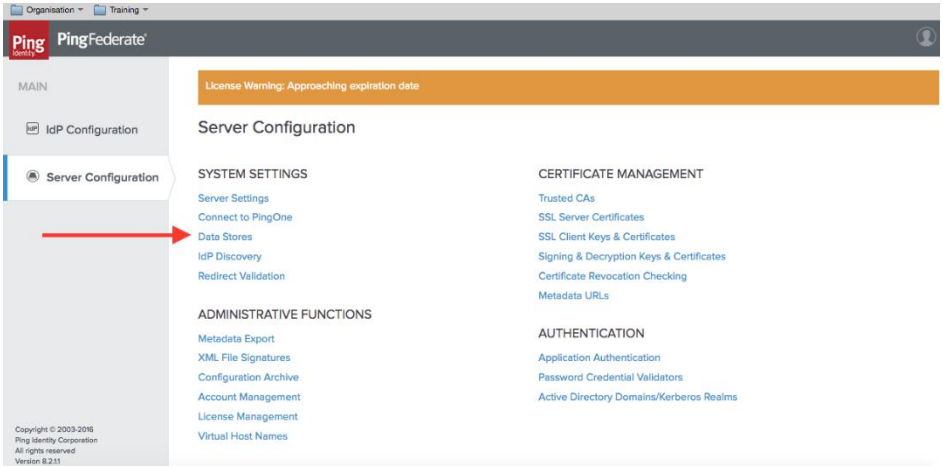
A signing certificate is created. You must use the same exported certificate while creating federation pairs in Access.

Add an LDAP Datastore

PingFederate lets you add an existing LDAP Datastore.

Procedure

1. On the **Server Configuration** tab, click **Data Stores**.



2. Click **Add Data Store**.
3. Enter the following details for Data Store and click **Save**.

Field	Value
Hostname	dc.example.com
User DN	domain\administrator
Password	Enter an appropriate password

Task Result

An LDAP Datastore is added. The same data store is referred to in **Create a Validator**.

Configuring Salesforce and PingFederate with MobileIron Access

You must perform the following tasks to configure Salesforce and PingFederate with MobileIron Access:

Register Sentry to Access

You must register Sentry to Access to fetch the latest configuration from Access.

Prerequisite

Verify that you have registered Sentry earlier. If so, then do not perform this step.

Procedure

1. **Clish** Sentry. In the configuration mode, execute the following command for registration.
   (config)#accs registration https:/<FQDN of Access server><Admin Username of Access Server>
2. Enter the **Tenant password** and complete the registration.
3. In **Access**, click the **Sentry** tab.
4. Select the appropriate Sentry instance, then click **Action** > **Assign**.
5. Click **OK**.
6. **Clish** Sentry and execute the following command in configuration mode to fetch the latest configuration from Access immediately:

   (config)# accs config-fetch update

   Note: All the published configuration changes are fetched by Sentry assigned to the profile in fifteen minutes. However, if you want to see the changes immediately, then perform Step 6.

Task Result

Registering Sentry to Access lets you fetch the latest configuration from Access.

Configuring Access to create a Federated Pair

You must configure Access to create a Federated Pair. You must create a service provider and then associate the identity provider with Access.

Procedure

1. Log in to **Access**.
2. Click **Profiles** > **Get Started**.
3. Enter the Access host information, and upload the **ACCESS SSL certificate**. All other fields are set to default. Click **Save**.
4. On the **Federated Pairs** tab, click **Add** and select **Salesforce** as the service provider.
5. Enter the following details:
    a. Name
    b. Description
    c. Upload the signing certificate from the drop-down list.
    d. Upload the metadata file of service provider downloaded from https://nexus.microsoftonline-p.com/federationmetadata/saml20/federationmetadata.xml
6. Click **Next**.
7. Select **PingFederate** as the Identity provider. Click **Next**.
8. Upload the **IdP certificate** and the **IdP metadata file** download. Click **Done**.
9. Download the **ACCESS SP Proxy** and the **ACCESS IDP Proxy** metadata file.
10. On the **Profile** tab, click **Publish** to publish the profile.

Task Result

The Federated Pair is created.

Configuring Salesforce to use PingFederate

You must configure Salesforce to use PingFederate natively.

Prerequisites

Verify that you have the credentials for Salesforce admin portal.

Procedure

You must configure Salesforce to use PingFederate natively with all the services. This means that there is no Access Sentry configuration yet.

1. On the Salesforce admin portal, go to **Security Controls** > **Single Sign-On Settings** > **New from Metadata File**.
2. Upload the **PingFederate IPD** metadata to Salesforce. The metadata file is available at https://<PingFederateDomainName>FederationMetadata/2007-06/FederationMetadata.xml
3. Enter the details for the **SAML Single Sign-On Settings**.

Field	Value
Name	Enter an appropriate name for PingFederate.
Request Signing Certificate	Default Certificate
Request Signature Method	RSA-SHA256
Assertion Decryption Certificate	Assertion not encrypted
SAML Identity Type	Assertion contains User's salesforce.com username
SAML Identity Location	Identity is in the NameIdentifier element of the subject statement
Service Provider Initiated Request Binding	HTTP Redirect
Identity Provider Login URL	<PingFederate Server> URL

4. Click **Save**.
5. Expand **Domain Management** > **My Domain** > **Edit**.
6. Select an authentication service. This service is the SSO profile that is already created.

Configuring PingFederate to use Salesforce

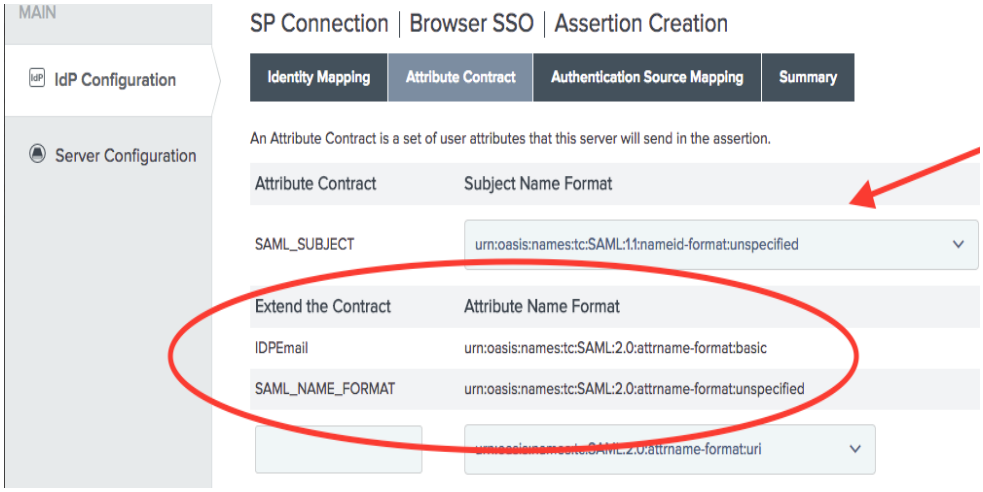
You must configure PingFederate natively to use Salesforce.

Prerequisites

Verify that you have the credentials to the PingFederate admin portal.

Procedure

1. Log in to **PingFederate** admin portal and click **Create New** to create a new connection in PingFederate.
2. Select **Browser SSO Profiles** (SAML 2.0 is selected by default) as the connection type and click **Next**.
3. Select **Browser SSO** as the connection option and click **Next**.
4. Select **File** to import the metadata and click **Choose File**. Upload the Salesforce metadata file that you have downloaded.
5. On the **Metadata URL** tab, click **Next**.
6. On the **General Info** tab, click **Next**.
7. On the **Browser SSO** tab, click **Configure Browser SSO**.
    a. On the **SAML Profiles** tab, select **IDP-Initiated SSO** and **SP-Initiated SSO**. Click **Next**.
    b. On the **Assertion Lifetime** tab, Click **Next**.
    c. On the **Assertion Creation** tab, click **Configure Assertion**.
        i. On the **Identity Mapping** tab, select **Standard** and click **Next**.
        ii. On the **Attribute Contract** tab, select the SAML-Subject, IDPEmail, SAML_NAME_FORMAT as follows and click **Next**.



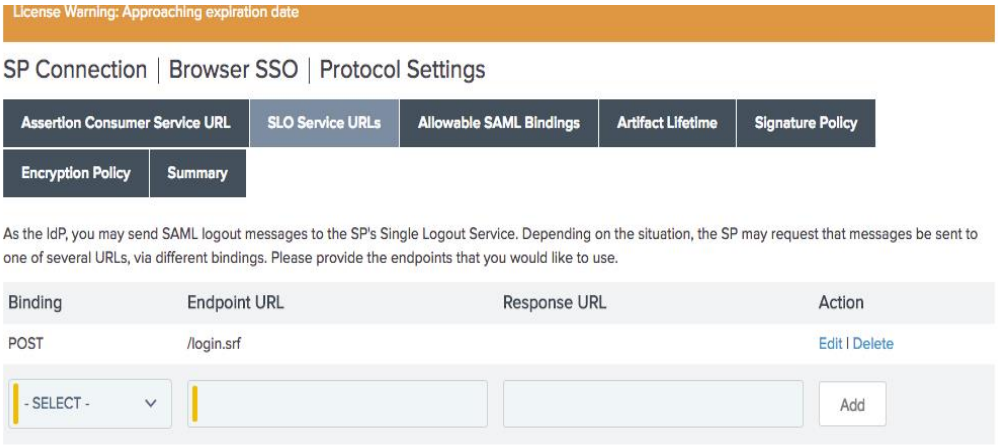
iii. On the **Authentication Source Mapping** tab, Click **Map New Adapter Instance.**

1. Select **HTTPForm** from the **Adapter Instance** drop-down and click **Next**.
2. On the **Mapping Method** tab, click **Next**.
3. On the **Attribute Contract Fulfillment** tab, select the following attributes and click **Next**.
   - Source – Adapter
   - Value – username for SAML_SUBJECT under attribute contract filling
4. On the **Issuance Criteria** tab, click **Next**.
5. On the **Summary** tab, click **Save**. **Assertion Creation** is complete.

d. On the **Protocol Settings** tab, click **Configure Protocol Settings**.

i. On the **Assertion Consumer Service URL** tab, select **POST** as the **Binding** method and the **Endpoint URL** as your Salesforce URL.

e. On the **SLO Service URLs** tab, select the endpoint URL.



f. On **Allowable SAML Bindings** tab, select **POST** and **REDIRECT** as the allowable bindings, and click **Next**.

g. On the **Signature Policy** tab, select both the check boxes and click **Next**.
h. On the **Encryption Policy** tab, select **NONE**. Click **Next** and then click **Done.**

8. On the **Credentials** tab, click **Configure Credentials**. Select the signing certificate from the drop-down list and click **Next**.
9. On the **Activation & Summary** tab, select **Active** to activate the profile. Click **Save**.

Task Result

PingFederate is configured natively to use Salesforce.
You must verify SSO access to Salesforce at this point.

- Open your Salesforce domain in a browser and log in as a user existing in both PingFederate and Salesforce domains. The browser must be redirected to the PingFederate login page.
- Enter the user credentials. The browser must be redirected to Salesforce and you must have access to Salesforce.