



MobileIron Access Cookbook

Access with Box and PingFederate

Jun 05, 2017



Contents

Overview	3
Prerequisites for PingFederate	3
Create a Validator	3
Create an Adapter	4
Create a Signing Certificate	6
Add an LDAP Datastore	7
Download metadata files for Box and PingFederate	8
Configuring Box and PingFederate with MobileIron Access	9
Configure Access to create a Federated Pair	9
Configure the Box environment.....	10
Configure the PingFederate environment	10
Register Sentry to Access	12



Overview

SAML provides single sign-on capability for users accessing their services hosted in a cloud environment. Generally, a service provider such as Box 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 Box. This guide serves as step-by-step configuration manual for users using PingFederate as an authentication provider with Box in a cloud environment.

Prerequisites for PingFederate

You must perform the following steps before you configure Box:

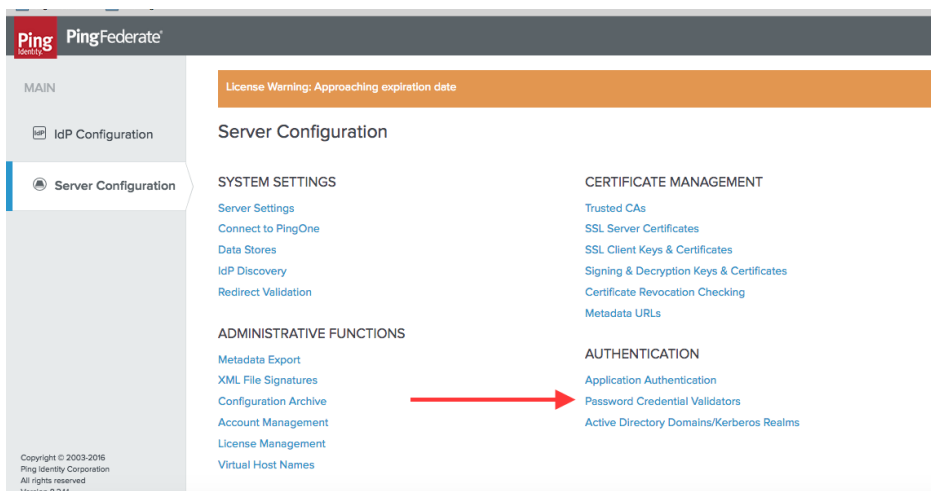
1. [Create a Validator](#)
2. [Create an Adapter](#)
3. [Create a Signing Certificate](#)
4. [Add an LDAP Datastore](#)
5. [Download metadata files for Box and PingFederate](#)

Create a Validator

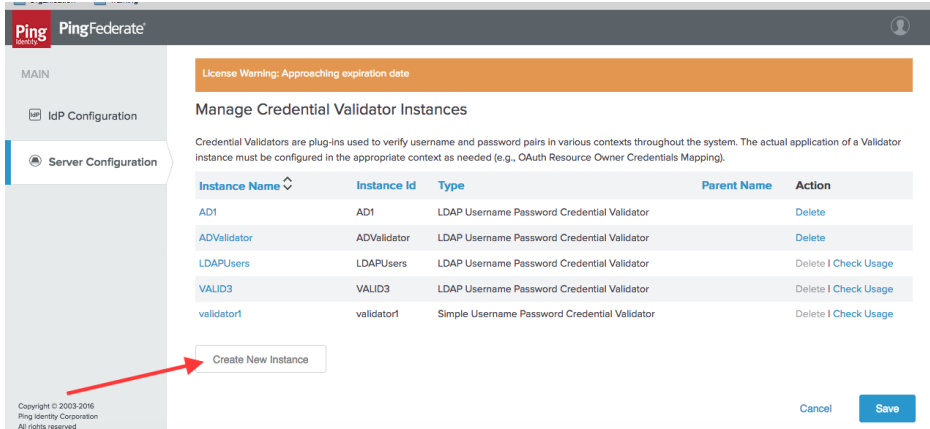
A validator authenticates the user. A user can authenticate in multiple ways with PingFederate such as AD authentication (sync users in AD), local user authentication (create local users in PingFederate), and so on.

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 <i>LDAP username and password Credential validator</i> 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

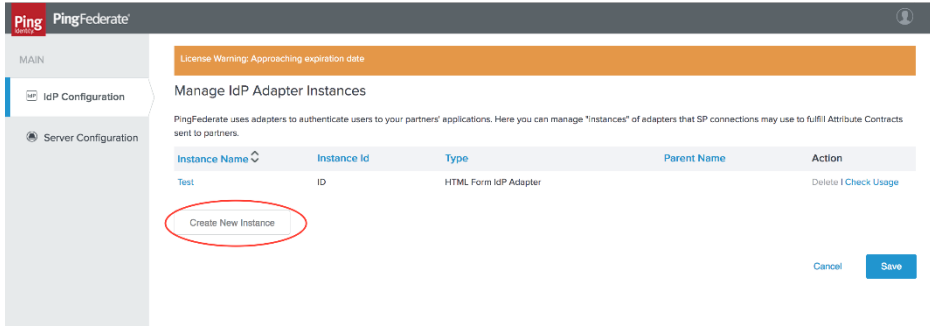
A validator is created. You must use this validator while creating federation data.

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

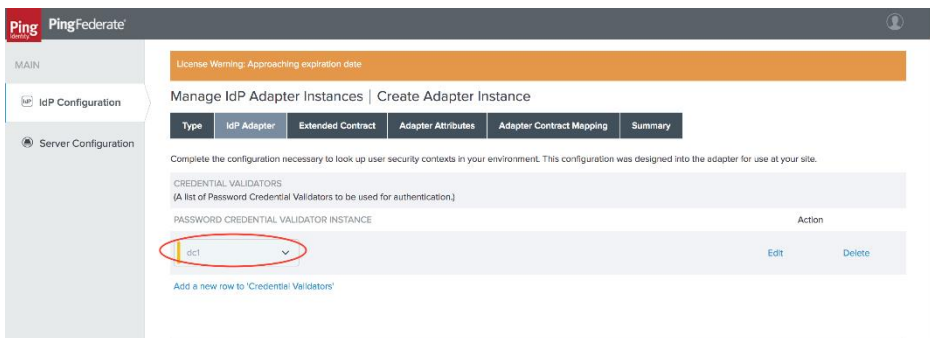
1. On **IDP Configuration** tab, click **Adapters > Create New Instance**.



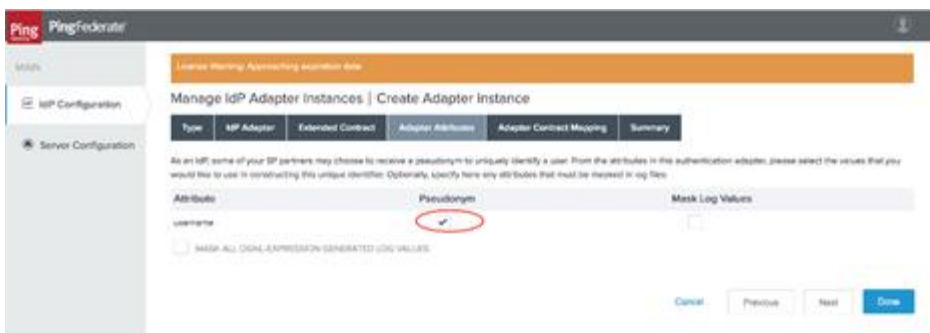
2. Enter the following details for the new instance and click **Next**.

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**.



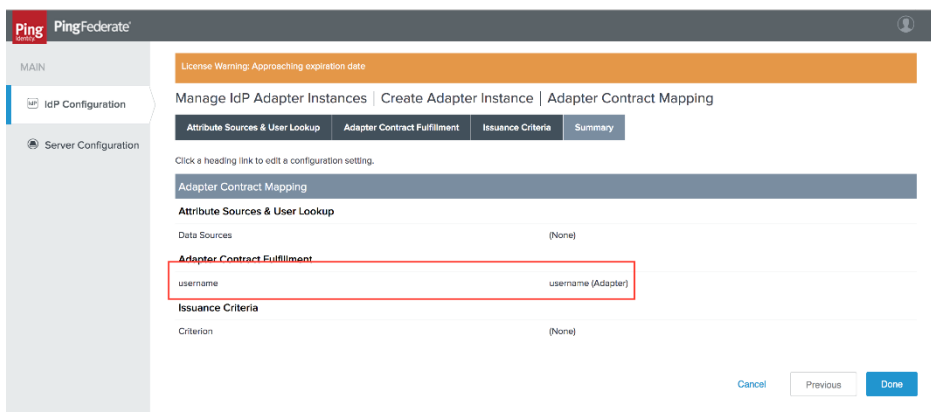
4. Click **Next** > **Next** and select **Pseudonym**. Click **Next**.



5. Click **Configure Adapter Contract**.



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



Task Result

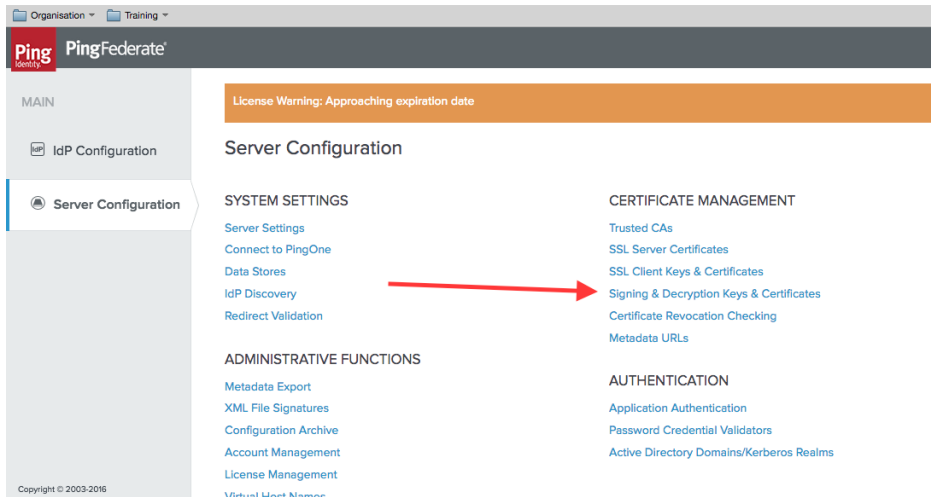
An adapter is created. You must use this adapter while creating the federation pair.

Create a Signing Certificate

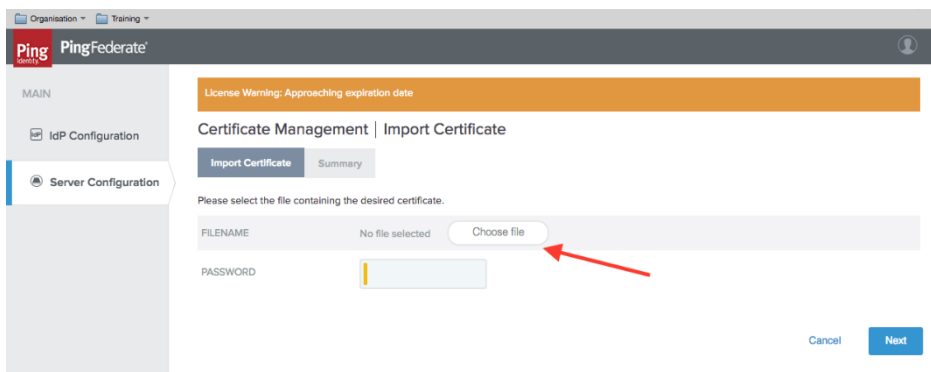
If you are using any self-signed certificate as a signing certificate, you must upload the same certificate to PingFederate such that the uploaded certificate is used as a signing certificate.

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

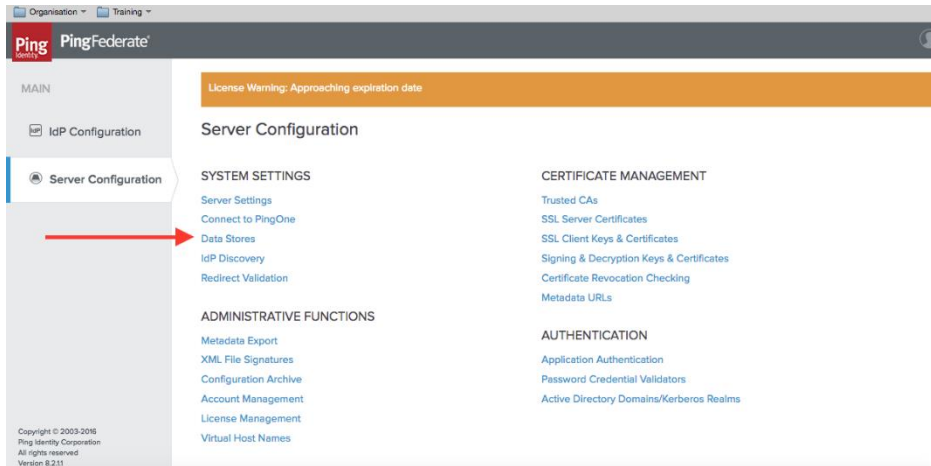
A signing certificate is created. You must use the same exported certificate while creating federation pairs in Access.

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**.

Download metadata files for Box and PingFederate

Box:

Download the metadata file from the following location:

<https://cloud.app.box.com/shared/3isa8qvvn>

PingFederate:

1. Login to PingFederate server with admin credentials.
2. Click **Server Configuration**.
3. Click **Metadata Export**
4. On the **Metadata Mode** tab, click **Next**.
5. On the **Connection Metadata** tab, select **Box.net** from the drop-down list and click **Next**.
6. On the **Metadata Signing** tab, click **Next**.
7. On the **Export & Summary** tab, click **Export** and save the metadata file.
8. Click **Done**.



Configuring Box and PingFederate with MobileIron Access

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

- [Configure Access to create a Federated Pair](#)
- [Configure the Box environment](#)
- [Configure the PingFederate environment](#)
- [Register Sentry to Access](#)

[Configure 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 **Box** as the service provider.
5. Enter the following details:
 - a. Name
 - b. Description
 - c. Upload the SPProxy certificate from the drop-down list.
 - d. Upload the metadata file of service provider downloaded from <https://cloud.app.box.com/shared/3isa8qvvqn>
6. (Optional): Select **Use Tunnel Certificates for SSO** for users to be authenticated automatically. This leverages the user's authentication in the MobileIron Tunnel VPN. See *Appendix* in the *MobileIron Access Guide* at <https://support.mobileiron.com/docs/curent/accs>.
7. Click **Next**.
8. Select **PingFederate** as the Identity provider. Click **Next**.
9. Upload the **IdP certificate** and the **IdP metadata file** download. Click **Done**.
10. Download the **ACCESS SP Proxy** and the **ACCESS IDP Proxy** metadata file.
11. On the **Profile** tab, click **Publish** to publish the profile.

Task Result

The Federated Pair is created.

For information on Cert SSO, see MobileIron Access guide @



[Configure the Box environment](#)

You must configure Box to use PingFederate natively.

Prerequisites

Verify that you have the credentials for Box admin portal.

Procedure

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

1. Login to the Box support portal <https://support.box.com>.
2. On the **Help** tab, select **Admin Forum**.
3. Click **Submit a case** under **Need Help?**
4. Upload Access IDP Metadata (Upload to SP) file that you downloaded when a creating a federated pair.
5. Contact Box support to complete the configuration.

Task Result

Box configuration is complete to use PingFederate.

[Configure the PingFederate environment](#)

You must configure PingFederate natively to use Box.

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 Box 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 as email address 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 entityID from SP Proxy (**SF+PI Federation-UploadTo-PingFederate-IdP.xml**) custom URL.
- e. On the **SLO Service URLs** tab, select the endpoint URL.

License Warning: Approaching expiration date

SP Connection | Browser SSO | Protocol Settings

Assertion Consumer Service URL	SLO Service URLs	Allowable SAML Bindings	Artifact Lifetime	Signature Policy
Encryption Policy	Summary			

As the IdP, you may send SAML logout messages to the SP's Single Logout Service. Depending on the situation, the SP may request that messages be sent to one of several URLs, via different bindings. Please provide the endpoints that you would like to use.

Binding	Endpoint URL	Response URL	Action
POST	/login.srf		Edit Delete

- 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 Box.
You must verify SSO access to Box at this point.



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

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. Enter the tenant password for the profile.
6. Click **OK**.
7. **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

Single-sign-on service is now configured using SAML with Box and PingFederate. This configuration lets you fetch the latest configuration from Access.



Copyright © 2016 - 2017 MobileIron, Inc. All Rights Reserved.

Any reproduction or redistribution of part or all of these materials is strictly prohibited. Information in this publication is subject to change without notice. MobileIron, Inc. does not warrant the use of this publication. For some phone images, a third-party database and image library, Copyright © 2007-2009 Aeleeta's Art and Design Studio, is used. This database and image library cannot be distributed separate from the MobileIron product.

“MobileIron,” the MobileIron logos and other trade names, trademarks or service marks of MobileIron, Inc. appearing in this documentation are the property of MobileIron, Inc. This documentation contains additional trade names, trademarks and service marks of others, which are the property of their respective owners. We do not intend our use or display of other companies’ trade names, trademarks or service marks to imply a relationship with, or endorsement or sponsorship of us by, these other companies.