

# 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



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.

PingFederate					
MAIN	License Warning: Approachi	ng expiration date			
IdP Configuration	Manage Credential	Validator Inst	ances		
Server Configuration	Credential Validators are plug- instance must be configured in	ins used to verify use the appropriate con	rname and password pairs in various contexts throughon text as needed (e.g., OAuth Resource Owner Credentials	ut the system. The actua Mapping).	al application of a Validator
	Instance Name 🗘	Instance Id	Туре	Parent Name	Action
	AD1	AD1	LDAP Username Password Credential Validator		Delete
	ADValidator	ADValidator	LDAP Username Password Credential Validator		Delete
	LDAPUsers	LDAPUsers	LDAP Username Password Credential Validator		Delete I Check Usage
	VALID3	VALID3	LDAP Username Password Credential Validator		Delete I Check Usage
	validator1	validator1	Simple Username Password Credential Validator		Delete I Check Usage
	Create New Instance				
Copyright © 2003-2016 Ping identity Corporation					Cancel Save

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
Туре	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**.



Ping Federate					0
MAIN	License Warning: Approact	ning expiration date			
IdP Configuration	Manage IdP Adap	ter Instances			
Server Configuration	PingFederate uses adapters sent to partners.	to authenticate users to your	partners' applications. Here you can manage	"instances" of adapters that SP connections may	use to fulfill Attribute Contracts
	Instance Name 🗘	Instance Id	Туре	Parent Name	Action
	Test	ID	HTML Form IdP Adapter		Delete I Check Usage
	Create New Instance	>			
					Cancel Save

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
Туре	HTML Form IDP Adapter

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

Ping PingFederate			٢
MAIN	License Warning: Approaching expiration date		
IdP Configuration	Manage IdP Adapter Instances   Create Adapter Instance		
Castar Castaratian	Type IdP Adapter Extended Contract Adapter Attributes Adapter Contract Mapping Summary		
Server Conliguration	Complete the configuration necessary to look up user security contexts in your environment. This configuration was designed into the adapter for use	e at your site.	
	CREDENTIAL VALIDATORS (A list of Password Credential Validators to be used for authentication.)		
	PASSWORD CREDENTIAL VALIDATOR INSTANCE	Action	
	det v	Edit	Delete
	Add a new row to 'Credential Validators'		

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

10.01	Inner Perry Association	expression data			
E MP Configuration	Manage IdP Adapter	Instances   Create Adapter is	istance		
	Type All Adaptar	Extended Contract Adapter Risthame	Adapter Contract Mapping	Summery	
<ul> <li>Server Configuration</li> </ul>	As an IdP, some of your DP party would find to use in conversioning	ert may channe la receive a pseudintym to pr Mis unique intercelles: Optionally, specify here	iquely identify a user. From the en- iny etc bodies that multiple means	ettudes in this authentication adapter, please se of in op Taps	fect the verses that you
	Attribute	Pseudorym		Mask Log Values	
	Attribute	Pseudonym		Mask Log Values	
	Athibute usersate balle AL (Sol, Arres)			Mask Log Values	

5. Click Configure Adapter Contract.



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

Ping PingFederate		
MAIN	License Warning: Approaching expiration date	
IdP Configuration	Manage IdP Adapter Instances   Create Adapter Instance   Adapter Contract Mapping	
Server Configuration	Attribute Sources & User Lookup Adapter Contract Fulfilment Issuance Criteria Summary Click e heading link to edit a configuration setting. Adapter Contract Mapping	
	Attribute Sources & User Lookup Data Sources (None) Adapter Contract Eufiliment	
	username username (Adapter) Issuance Criteria	
	Criterion (None)	
	Cancel Previous	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**.

Crganisation - 🦳 Training -			
Ping PingFederate			
MAIN	License Warning: Approachin	ng expiration date	
IdP Configuration	Certificate Manager	ment   Import Certificate	
Server Configuration	Please select the file containin	nmary	
	FILENAME	No file selected Choose file	
	PASSWORD		
		Cance	el 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/3isa8qvvqn

#### **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
- <u>Configure the PingFederate environment</u>
- <u>Register Sentry to Access</u>

# **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 <a href="https://support.mobileiron.com/docs/curent/accs">https://support.mobileiron.com/docs/curent/accs</a>.
- 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 <u>https://support.box.com</u>.
- 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 enail 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.

Connection	Browser	SSO   Protoco	l Settings		
ssertion Consumer S	ervice URL	SLO Service URLs	Allowable SAML Bindings	Artifact Lifetime	Signature Policy
ncryption Policy	Summary				
the IdP, you may send	SAML logout I	messages to the SP's Sir	ale Logout Service. Depending	on the situation, the SI	<sup>o</sup> may request that messages b
the IdP, you may send e of several URLs, via d nding	SAML logout i lifferent bindir Endpoin	messages to the SP's Sir Igs. Please provide the e t URL	igle Logout Service. Depending indpoints that you would like to i Response UR	on the situation, the Sf use.	<sup>o</sup> may request that messages b Action
the IdP, you may send e of several URLs, via d Inding DST	SAML logout i lifferent bindir Endpoin /login.srf	messages to the SP's Sir igs. Please provide the e t URL	igle Logout Service. Depending Indpoints that you would like to t Response UR	on the situation, the Sf use. L	P may request that messages to Action 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.