



# MobileIron Access Cookbook

## Access with Office 365 and PingFederate

**Revised:** 01/02/2018



## Contents

Overview .....	3
Prerequisites for Office 365 .....	3
Prerequisites for PingFederate .....	3
Create a Validator .....	3
Create an Adapter .....	5
Create a Signing Certificate .....	6
Add an LDAP Datastore .....	7
Configuring Office 365 and PingFederate with MobileIron Access .....	9
Register Sentry to Access .....	9
Configure Access to create a Federated Pair .....	9
Configure the Office 365 environment .....	10
Configure PingFederate environment .....	12
Verification .....	16



# Overview

SAML provides single sign-on capability for users accessing their services hosted in a cloud environment. Generally, a service provider such as Office 365 is federated with an identity provider such as PingFederate for authentication. The user gets authenticated by PingFederate and obtains a SAML token for accessing applications in a cloud environment, such as Office 365.

This guide serves as step-by-step configuration manual for users using PingFederate as an authentication provider with Office 365 in a cloud environment.

## **Disclaimer:**

This cookbook is informational to help with the setup flow and actual screenshots. The steps might vary in your deployment scenario due to changes in SP/IdP versions.

## Prerequisites for Office 365

- Ensure to download the metadata files for Office 365 from <https://nexus.microsoftonline-p.com/federationmetadata/saml20/federationmetadata.xml>

## Prerequisites for PingFederate

You must perform the following steps before you configure Office 365:

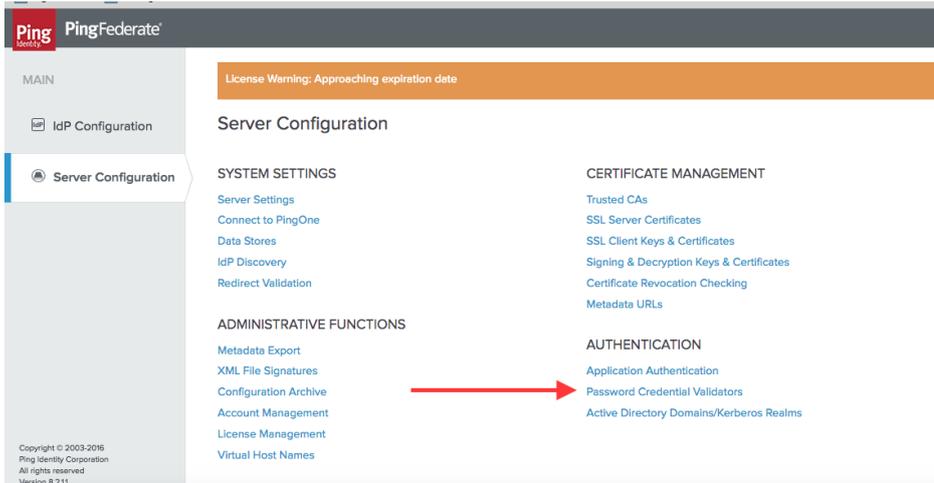
1. Create a Validator
2. Create an Adapter
3. Create a Signing Certificate
4. Add an LDAP Datastore

### Create a Validator

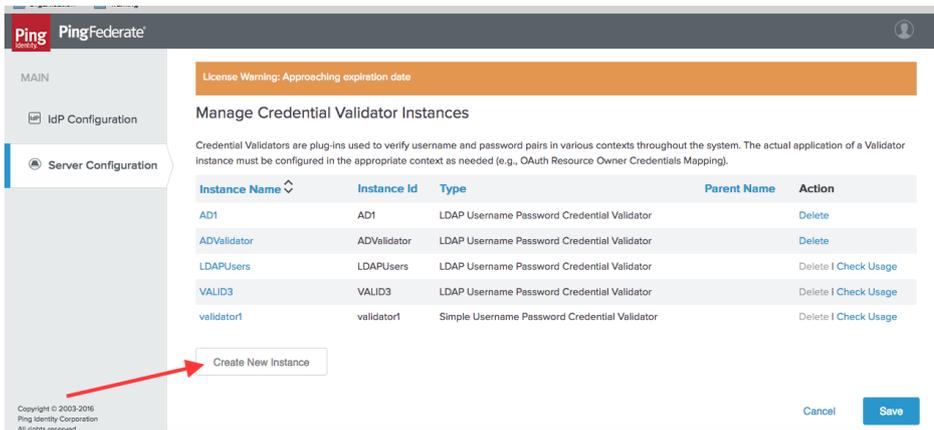
A validator authenticates the user. A user can authenticate in multiple ways with PingFederate such as AD authentication (sync users in AD), local user authentication (create local users in PingFederate), and so on.

## **Procedure**

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



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

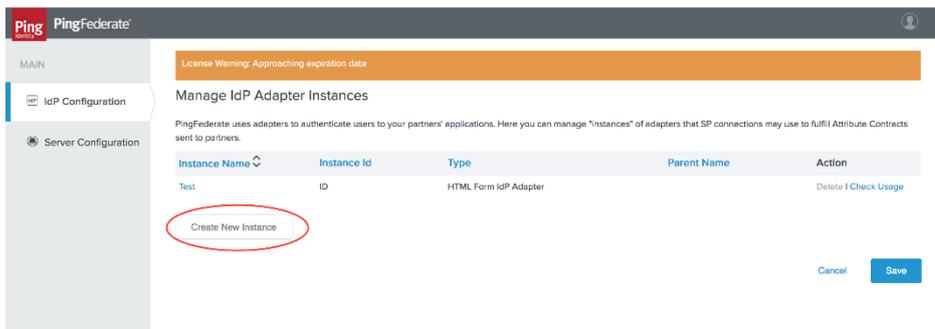
A validator is created. You must use this validator while creating federation data.

## 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

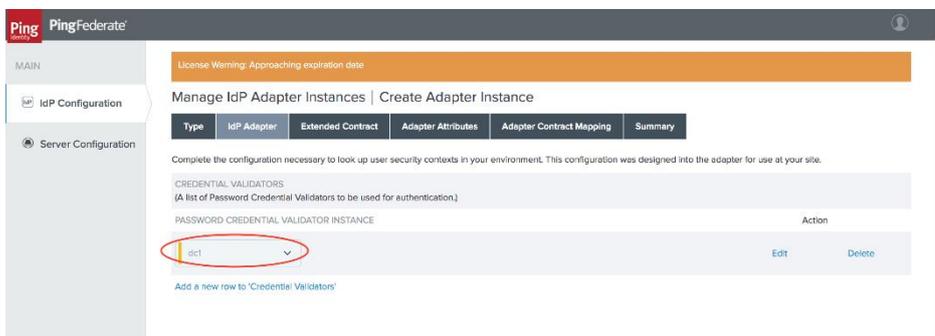
1. On **IDP Configuration** tab, click **Adapters > Create New Instance**.



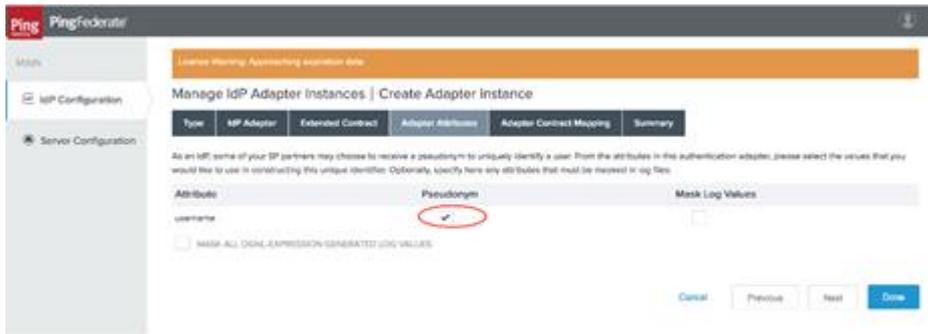
2. Enter the following details for the new instance and click **Next**.

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

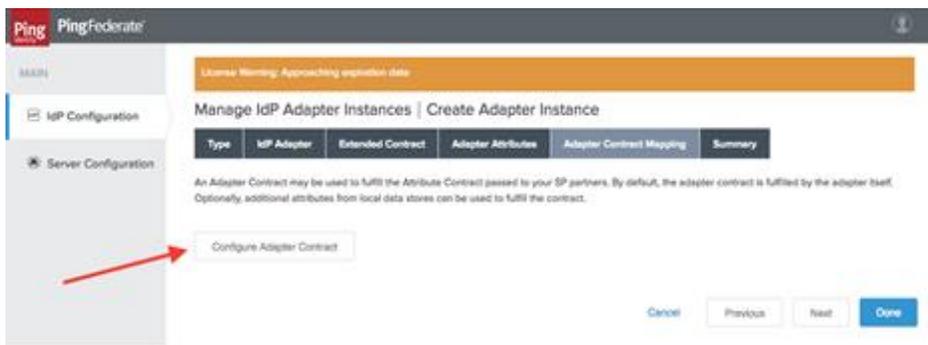
3. On the next screen, select the validator created using **Create a Validator** and click **Update**.



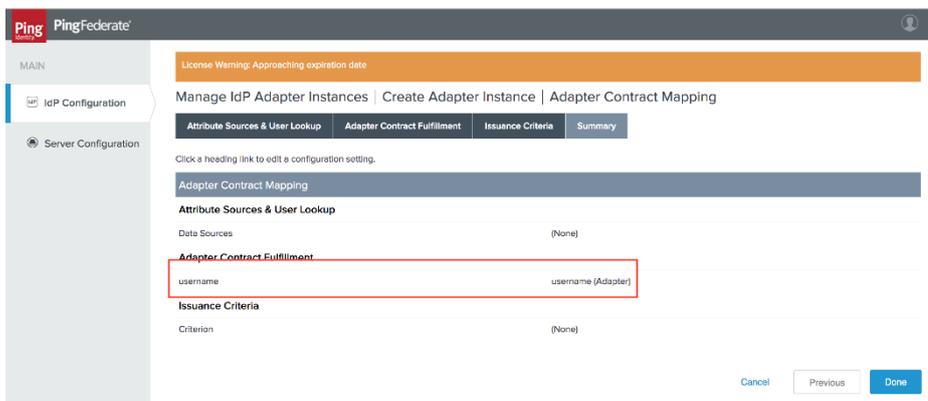
4. Click **Next > Next** and select **Pseudonym**. Click **Next**.



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.

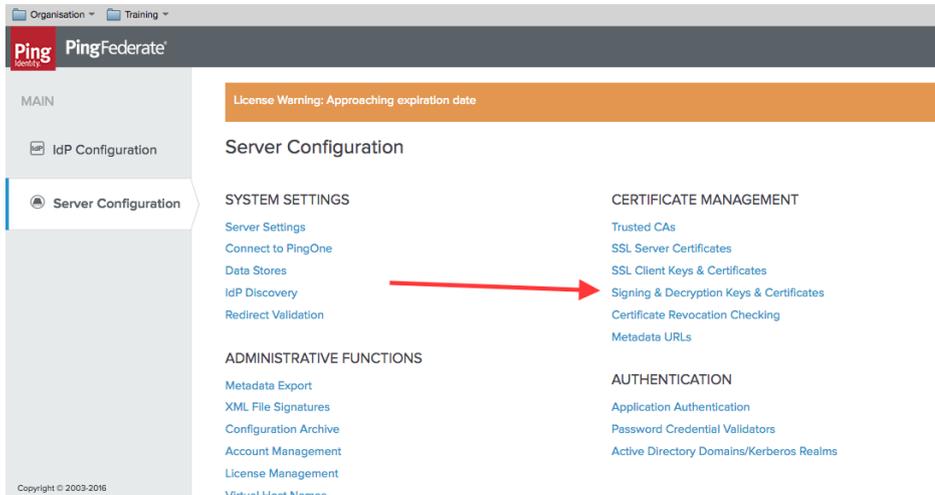
## **Create a Signing Certificate**

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.

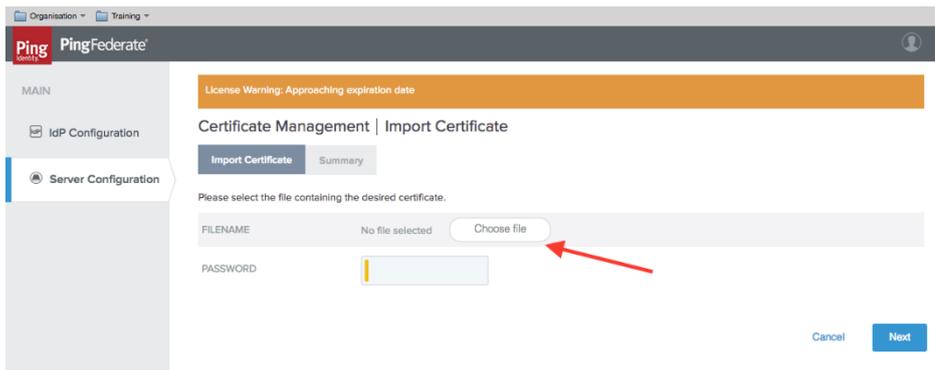
## **Procedure**



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**

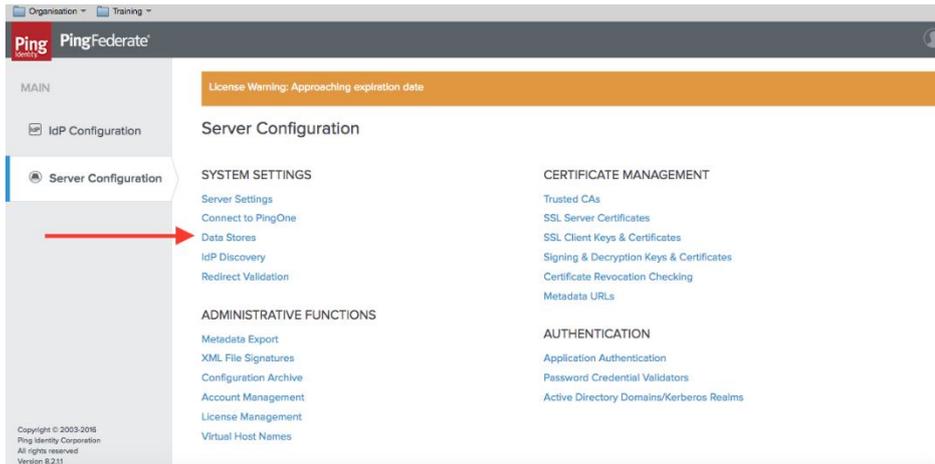
A signing certificate is created. You must use the same exported certificate while creating federation pairs in Access.

## **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**.



# Configuring Office 365 and PingFederate with MobileIron Access

You must perform the following tasks to configure Office 365 and PingFederate with MobileIron Access:

- [Register Sentry to Access](#)
- [Configure Access to create a Federated Pair](#)
- [Configure the Office 365 environment](#)
- [Configure PingFederate environment](#)

## [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.

## [Configure Access to create a Federated Pair](#)

You must configure Access to create a Federated Pair. For this, 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 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 **Office 365** as the service provider.
5. Enter the following details:
  - a. Name
  - b. Description
  - c. Upload the SPProxy Certificate
  - d. Select **WS Trust 13** in Office 365 specifics
  - e. Enter value for Federated Domain
  - f. Enter the original IdP Active Logon URL
  - g. 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.

## **Configure the Office 365 environment**

You must configure Office 365 to use Access.

1. Open Powershell and enter the following command:  
**Note:** Run the PowerShell script in a Windows server as Administrator.

*Connect-MsolService*

**Note:** Download the PowerShell script from MobileIron Access for Office 365 and PingFederate federated pair to avoid manual editing.

Overview Federated Pairs Conditional Access Split Tunneling Branding Certificates

### Federated Pairs

Show Description  
How to upload my Access metadata to my IDP or SP?

+ Add New Pair

Name	Description	Policy Name	SP Metadata	IDP Metadata	Access IDP Metadata
O365 and PingFederate	No description	Policy Name: Default Policy	View	View	View

Access SP Metadata (Upload to IDP) View | Download  
IDP Metadata View  
Access IDP Metadata (Upload to SP) View | Download  
PowerShell Commands for Office 365 View | Download

© Copyright 2017 MobileIron Inc. All rights reserved. About MobileIron | Terms of Use | Privacy Policy



2. Fetch the existing settings by executing the following command:

```
saml= Get-MsolDomainFederationSettings -DomainName example.com
```

3. Edit the settings for the following components:

- **ActiveLogOnUri** - saml.ActiveLogOnUri= https://<Alternate fqdn of sentry>/MobileIron/acc/17db9e36-4688-40ae-a981-15c8b81e76a7/idp
- **IssuerUri** - saml.IssuerUri=https://<Alternate fqdn of sentry>/MobileIron/acc/17db9e36-4688-40ae-a981-15c8b81e76a7/idp
- **LogOffUri** - saml.LogOffUri=https://<Alternate fqdn of sentry>/MobileIron/acc/17db9e36-4688-40ae-a981-15c8b81e76a7/idp/logout
- **PassiveLogonUri** - saml.PassiveLogOnUri=https://<Alternate fqdn of sentry>/MobileIron/acc/17db9e36-4688-40ae-a981-15c8b81e76a7/idp

4. PS C:\Users\Administrator\Documents> Get-MsolDomainFederationSettings - DomainName |fl

Field	Value
ActiveLogOnUri	https://<Alternate fqdn of sentry>/MobileIron/acc/17db9e36-4688-40ae-a981-15c8b81e76a7/idp
DefaultInteractiveAuthenticationMethod	
FederationBrandName	Company Name
IssuerUri	https://<Alternate fqdn of sentry>/MobileIron/acc/17db9e36-4688-40ae-a981-15c8b81e76a7/idp
LogOffUri	https://<Alternate fqdn of sentry>/MobileIron/acc/17db9e36-4688-40ae-a981-15c8b81e76a7/idp
MetadataExchangeUri	
NextSigningCertificate	
OpenIdConnectDiscoveryEndpoint	
PassiveLogOnUri	https://<Alternate FQDN of sentry>/MobileIron/acc/17db9e36-4688-40ae-a981-15c8b81e76a7/idp
SigningCertificate	MIIDCjCCAfKgAwIBAgIGAVffQk9kMA0GCSqGSIb3DQEBCwUAMEYxCzAJBgNVBAYTAIVTMQswCQYDVQQIEwJDQTEWMBQGA1UEChMNbWlzZW50cnkyLmNvbTESMBAGA1UEAxMJTUI TRU5UUIkyMB4XDTE2MTAxOTIzMjQwN1oXDTE3MTAxOTIzMjQwN1owRjELMAkGA1UEBhMCVVMxCzAJBgNVBAGTAKNBMRywFA YDVQQKEw1taXNlbnRyeTI



	uY29tMRIwEAYDVQQDEwINSVNFTIRSWTIwggEi MA0GCSqGSIB3DQEBAQUAA4IBDwAwggEKAoIB AQCygNhcR9CH1OPFSyKBV/patqgmUemK6Lg9Aea HVFLi2cEdGRCIfHsYIpbJ2WISIT7Nrms48+z5abBwh SLoIjFHj0IT44UZP4JhHrG1frl6gkyNXgMVaSC8w8U NlfroEaOKqkt2bnLYIfPH/8gCupnb1SZQMhPbvjXWe ROb3tEMCd5k017DuCfrcj59h4xekUiy2tShL+O/JQ+Ct E3hyh+12+YfTbPw4tJrdJdUaN2wQ8r/EMJkQdaIm8W ALcgszGfWBjPr/b9jXXBLOGVXD4jtTuLZECMOIXF s6mkLeV1GJDUHtyt6rGUJ3FFbJjSj6meEoklZEya1V KyH7oc2WjttAgMBAAEwDQYJKoZIhvcNAQELBQ ADggEBAJBgLS1XjFEW1y0hj2e4IWXK0hMCPu+8Q 0VHWAZ9XH+h9cDL1TWUmcfqrif5Em6KfOLP0vg GyvtGLpijyyd7eHBPTcNB9Ez+Tf/O62IKK VuIaK6F5 hpFrQSuqvjf9/UxM4NYIIGpU8M5q64Qqf8FQcIksysN v7P1bTX+aDOq9NYhFkP6eety3uckv+hCQk4ix1MrD FKel7ZXHeJGadWxgfrnUSkTj6jY8PGwVAw9SmxS/ NQ2SI0tZR4MSPGZUfi7EZToaIKFHwx2kTCRfw+ AafB8rFhP1KObgMA9xuFNFXjcAMuHChXJJvav1Vj sCcrs9j0mu7QhwtjZ2iNAG5CWZME=
SupportsMfa	False

### [Configure PingFederate environment](#)

You must configure PingFederate with Access for the setup to complete.

#### **Procedure**

1. Login 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 metadata and click **Choose File**. Upload the Office 365 metadata file that you downloaded.
5. On the **Metadata URL** tab, select **File to import metadata** and select the file.
6. Upload the **Access SP Metadata (Upload to IDP)** file which is downloaded when Configure Access to create a Federated Pair and click **Next**.
7. On the **General Info** tab, click **Next**.
8. 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**.
    - On the **Identity Mapping** tab, select **Standard** and click **Next**.
    - On the **Attribute Contract** tab, select the SAML\_Subject, IDPEmail, SAML\_NAME\_FORMAT as follows and click **Next**.



- 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**.
  - On the **Assertion Consumer Service URL** tab, select **POST** as the **Binding** method and the **Endpoint URL** as your Office 365.
- 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**.
- i. On **WS-Trust STS Policy** tab, click **Configure WS-Trust STS**.
  - On the **Protocol Settings** tab, configure the **Service Identifier**. Extract the information from Access SP Metadata (Upload to IDP) file which is the Entity ID. Click **Next**.
  - Configure **Token lifetime** timeframe with 5 minutes before and 30 minutes after issuance.
  - On **Token Creation** tab, click **Configure Token Creation**. On the **Attribute Contract** tab, enter the below details:

An Attribute Contract is a set of user attributes that this server will send in the token.

Attribute Contract	
SAML_SUBJECT	
Extend the Contract	Attribute Namespace
ImmutableId	http://schemas.microsoft.com/LiveID/Federation/2008/05
UPN	http://schemas.xmlsoap.org/claims
	ns:unspecified

- On the **Request Contract** tab, click **Manage STS Request Parameters**.
- Click **Add New Request Contract** and enter the details for **Contract Name** and **ID** as below.

Specify one or more parameters that will be included in RSTs applicable to a connection partner (or partners). during partner-connection configuration.

CONTRACT NAME	STS Contract
CONTRACT ID	STSTContract1
Parameters to be provided in the request	
Parameter Name	Action
objectGUID	Edit   Delete
userPrincipalName	Edit   Delete
<input type="text"/>	<input type="button" value="Add"/>

- Click **Done > Save > Next**.
- On **IDP Token Processor Mapping**, click **Map New Token Processor Instance > Manage Token Processor Instance > Create New Instance**. Configure the settings as below and click **Next**.



Type	Instance Configuration	Extended Contract	Token Attributes	Summary
------	------------------------	-------------------	------------------	---------

The values of the selected Token Processor Instance.

INSTANCE NAME	Username Token Prox
INSTANCE ID	UsernameTokenProcessor1
TYPE	Username Token Processor
CLASS NAME	com.pingidentity.pf.tokenprocessors.username.UsernameTokenProcessor
PARENT INSTANCE	None

- Configure the **Password Credential Validator** and click **Next**.
- Configure the **Extended Contract** and click **Next**.
- Configure **Token Attributes** and click **Next**. Click **Save > Next**.
- Configure **Attribute Retrieval** by selecting “Use only the token processor contract values in the outgoing token” option.
- Configure **Attribute Contract Fulfillment** as show below

Fulfill your Attribute Contract with values from the incoming token, data stores, or dynamic text values.

Attribute Contract	Source	Value	Actions
ImmutableId	Context	Authentication Context	None available
SAML_SUBJECT	Token	username	None available
UPN	Token	username	None available

- Click **Next > Save > Done > Done > Next > Done**.
- Click **Configure Credentials > Back Channel Authentication**.
- Configure the **Inbound Authentication Type** and click **Next**.

<input checked="" type="checkbox"/>	HTTP BASIC
<input type="checkbox"/>	SSL CLIENT CERTIFICATE
<input checked="" type="checkbox"/>	DIGITAL SIGNATURE (BROWSER SSO PROFILE ONLY)
<input checked="" type="checkbox"/>	REQUIRE SSL

- Configure **Basic Authentication** (Inbound) an enter the username and password. Click **Next > Done > Next**.
- Configure **Digital Signature Settings** and select the **Signing Certificate** and the **Signing Algorithm**. Click **Next**.
- Click **Signature Verification >** and configure the **Trust Model**. Select **Unanchored** option.
- Configure **Signature Verification Certificate** from the **Certificate** dropbox.



- Click **Next > Done > Next > Done**.

9. On the **Activation & Summary** tab, select **Active** to activate the profile. Click **Save**.

### **Task Result**

PingFederate and Office 365 setup with Access is complete.

## **Verification**

Login to <https://login.microsoftonline.com>. You are now redirected from IdP Proxy to PingFederate.



Copyright © 2016 - 2018 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.