

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 <u>https://nexus.microsoftonline-p.com/federationmetadata/sam120/federationmetadata.xml</u>

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.

gringreuerate		
JN	License Warning: Approaching expiration date	
IdP Configuration	Server Configuration	
Server Configuration	SYSTEM SETTINGS	CERTIFICATE MANAGEMENT
	Server Settings	Trusted CAs
	Connect to PingOne	SSL Server Certificates
	Data Stores	SSL Client Keys & Certificates
	IdP Discovery	Signing & Decryption Keys & Certificates
	Redirect Validation	Certificate Revocation Checking
		Metadata URLs
	ADMINISTRATIVE FUNCTIONS	
	Metadata Export	AUTHENTICATION
	XML File Signatures	Application Authentication
	Configuration Archive	Password Credential Validators
	Account Management	Active Directory Domains/Kerberos Realms
	License Management	
right © 2003-2016	Virtual Host Names	

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

Ping Federate					
MAIN	License Warning: Approaching	expiration date			
IdP Configuration	Manage Credential	Validator Inst	ances		
Server Configuration	Credential Validators are plug-li instance must be configured in	ns used to verify use the appropriate con	rname and password pairs in various contexts throughou text as needed (e.g., OAuth Resource Owner Credentials I	the system. The actua Mapping).	I 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 All rights reserved					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 PingFederate					٩
MAIN	License Warning: Approact	hing 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	a "instances" of adapters that SP connections ma	y use to fulfill Attribute Contracts
	Instance Name 🗘	Instance Id	Туре	Parent Name	Action
	Test Create New Instance		HTML Form IdP Adapter		Delete I Check Usage
					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**.

UN	License Warning: Approaching expiration date		
IdP Configuration	Manage IdP Adapter Instances Create Adapter Instance		
	Type IdP Adapter Extended Contract Adapter Attributes Adapter Contract Mapping Summary		
Server Configuration	Complete the configuration necessary to look up user security contexts in your environment. This configuration was designed into the adapte	r for use at your site.	
	CREDENTIAL VALIDATORS (A list of Password Credential Validators to be used for authentication.)		
	PASSWORD CREDENTIAL VALIDATOR INSTANCE	Actio	n
	det v	Edit	Delete
	Add a new row to (Croniential Validatore)		

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



5. Click Configure Adapter Contract.

1214	Adversaria A	Rental Accord	ing argument data					
IdP Configuration	Manag	e IdP Adapt	ter Instances C	reate Adapter In	istance			
	Туре	MP Adapter	Extended Contract	Adapter Attributes	Adapter Centred Mapping	Summery		
CONTRACTOR STREET, STR								
Server Configuration	An Adapte Optionally	r Coritract may be additional attribut	used to fulfill the Attribut as from local data stores	e Contract passed to your can be used to fulfil the o	r SP partners. By default, the ads contract.	opter contract is fulfill	ed by the adigter bie	C
sever congustor	An Adapte Optionely Contig	r Contract way be additional athibut une Adapter Contr	used to fulfil the Athlbut es from local data stores art	e Contract passed to you can be used to fulfil the o	r SP partners, By Gefault, The add contract.	gder contract is fulfill	ed by the adaptor bie	e
	An Adulte Optionally Conto	r Contract may be additional attribut une Adapter Contr	used to fulfit the Athlout es from local data stores act	e Contract passed to you can be used to fulfil the r	e SP partners. By default, the sole contract.	pter contract is fulfit	ed by the adapter bar	¢

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

Ping PingFederate	٩
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
	Adapter Contract Mapping
	Attribute Sources & User Lookup
	Dets Sources (None) Adapter Contract Fulfiliment
	username username (Adapter)
	Issuance Criteria
	Criterian (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.

Organisation * 🛄 Training *		
PingFederate		
MAIN	License Warning: Approaching expiration date	
IdP Configuration	Server Configuration	
Server Configuration	SYSTEM SETTINGS	CERTIFICATE MANAGEMENT
/	Server Settings	Trusted CAs
	Connect to PingOne	SSL Server Certificates
	Data Stores	SSL Client Keys & Certificates
	IdP Discovery	Signing & Decryption Keys & Certificates
	Redirect Validation	Certificate Revocation Checking
		Metadata URLs
	ADMINISTRATIVE FUNCTIONS	
	Metadata Export	AUTHENTICATION
	XML File Signatures	Application Authentication
	Configuration Archive	Password Credential Validators
	Account Management	Active Directory Domains/Kerberos Realms
	License Management	
Copyright © 2003-2016	Virtual Hoet Namee	

- 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: Appr	oeching expiration date	
IdP Configuration	Certificate Man	agement Import Certificate	
Server Configuration	Import Certificate	Summary	
	Please select the file cor	ntaining the desired certificate.	
	FILENAME	No file selected Choose file	
	PASSWORD		
		ci	ancel 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:

- <u>Register Sentry to Access</u>
- Configure Access to create a Federated Pair
- Configure the Office 365 environment
- <u>Configure PingFederate environment</u>

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

- Clish Sentry. In the configuration mode, execute the following command for registration. (config)#accs registration https:/<FQDN of Access server><Admin Username of Access
- 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.

Server>

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 <u>https://nexus.microsoftonline-</u>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	
ederated F	Pairs					
now Descriptio	n	155				
ow to upload n	ny Access metadata i	o my IDP of SPr				
+ Add New Pa	ir -					
+ Add New Pa	ir					
+ Add New Pa	r		SF	^o Metadata Vie	w	
+ Add New Pa	ir DeFederate	Acces	SF SP Metadata (Uplo	PMetadata Vie bad to IDP) Vie	w w Download	
+ Add New Pa	r	Acces	Si ss SP Metadata (Upto IDf	P Metadata Vie bad to IDP) Vie P Metadata Vie	w w Download w	
+ Add New Pa O365 and Pir No description Policy Name: D	r naFederate Default Policy	Acces	Si ss SP Metadata (Upic Upi ss IDP Metadata (Upi	Metadata Vie ad to IDP) Vie Metadata Vie oad to SP) Vie	w w Download w w Download	i 10

Copyright 2017 Mobiletron Inc. All rights reserved. About Mobiletron | 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<="" td=""></alternate>
	sentry>/MobileIron/acc/17db9e36-4688-40ae-a981-
	15c8b81e76a7/idp
DefaultInteractiveAuthenticatio	
nMethod	
FederationBrandName	Company Name
IssuerUri	https:// <alternate fqdn="" of<="" td=""></alternate>
	sentry>/MobileIron/acc/17db9e36-4688-40ae-a981-
	15c8b81e76a7/idp
LogOffUri	https:// <alternate fqdn="" of<="" td=""></alternate>
	sentry>/MobileIron/acc/17db9e36-4688-40ae-a981-
	15c8b81e76a7/idp
MetadataExchangeUri	
NextSigningCertificate	
OpenIdConnectDiscoveryEndp	
oint	
PassiveLogOnUri	https:// <alternate fqdn="" of<="" td=""></alternate>
	sentry>/MobileIron/acc/17db9e36-4688-40ae-a981-
	15c8b81e76a7/idp
SigningCertificate	MIIDCjCCAfKgAwIBAgIGAVffQk9kMA0GCSqGSIb
	3DQEBCwUAMEYxCzAJBgNVBAYTAIVTMQswC
	QYDVQQIEwJDQTEWMBQGA1UEChMNbWlzZW5
	0cnkyLmNvbTESMBAGA1UEAxMJTUITRU5UUlky
	MB4XDTE2MTAxOTIzMjQwN1oXDTE3MTAxOTIz
	MjQwN1owRjELMAkGA1UEBhMCVVMxCzAJBgN
	VBAgTAkNBMRYwFAYDVQQKEw1taXNlbnRyeTI



uY29tMRIwEAYDVQQDEwlNSVNFTIRSWTIwggEi MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKA0IE AQCygNhcR9CH1OPFSyKBV/patqgmUemK6Lg9Aea HVFIi2cEdGRCIfHsYIpbJ2WISIT7Nrms48+z5abBwh SLoIjFHj0IT44UZP4JhHrG1frl6gkyNXgMVaSC8w8U NlfroEaOKqkt2bnLYIfPH/8gCupnb1SZQMhPbvjXWe ROb3tEMCd5k017DuCfrcj59h4xekUiy2tShL+O/JQ+C E3hyh+12+YfTbPw4tJrdJdUaN2wQ8r/EMJkQdaIm8W ALcgszGfWBjPr/b9jXXBL0GVXD4jtTuLZECMOIXF s6mkLeV1GJDUHtyt6rGUJ3FFbJjSj6meEoklZEya1V KyH7oc2WjjtAgMBAAEwDQYJKoZIhvcNAQELBQ ADggEBAJBgL5lXjFEW1y0hj2e4IWXK0hMCPu+8Q 0VHWAZ9XH+h9cDL1TWUmcfqrif5Em6KfOLP0vg GyvtGLpijyyd7eHBPTcNB9Ez+Tf/O62lKKVuIaK6F5 hpFrQSuqvjf9/UxM4NYIIGpU8M5q64Qqf8FQcIksys1 v7P1bTX+aDOq9NYhFkP6eety3uckv+hCQk4ix1MrD FKe17ZXHeJGadWxgfrnUSkTj6jY8PGwVAw9Smx5/ NQ2SIOtzR4MSPGZUf17EZToaIKFHWX2kTCRfw+		
MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKA0IEAQCygNhcR9CH1OPFSyKBV/patqgmUemK6Lg9AeaHVFIi2cEdGRCIfHsYIpbJ2WISIT7Nrms48+z5abBwhSLoIjFHj0IT44UZP4JhHrG1frl6gkyNXgMVaSC8w8UNlfroEaOKqkt2bnLYIfPH/8gCupnb1SZQMhPbvjXWeROb3tEMCd5k017DuCfrcj59h4xekUiy2tShL+O/JQ+CE3hyh+12+YfTbPw4tJrdJdUaN2wQ8r/EMJkQdaIm8WALcgszGfWBjPr/b9jXXBL0GVXD4jtTuLZECMOIXFs6mkLeV1GJDUHtyt6rGUJ3FFbJjSj6meEoklZEya1VKyH7oc2WjjtAgMBAAEwDQYJKoZIhvcNAQELBQADggEBAJBgL51XjFEW1y0hj2e4IWXK0hMCPu+8Q0VHWAZ9XH+h9cDL1TWUmcfqrif5Em6Kf0LP0vgGyvtGLpijyyd7eHBPTcNB9Ez+Tf/O62lKKVuIaK6F5hpFrQsuqvjf9/UxM4NYIIGpU8M5q64Qqf8FQcIksys1v7P1bTX+aDOq9NYhFkP6eety3uckv+hCQk4ix1MrDFKe17ZXHeJGadWxgfrnUSkTj6jY8PGwVAw9SmxS/NQ2SIOtzR4MSPGZUfI7EZToaIKFHWX2kTCRfw+		uY29tMRIwEAYDVQQDEwlNSVNFTlRSWTIwggEi
AQCygNhcR9CH10PFSyKBV/patqgmUemK6Lg9Aea HVFIi2cEdGRCIfHsYIpbJ2WISIT7Nrms48+z5abBwh SLoIjFHj0IT44UZP4JhHrG1frl6gkyNXgMVaSC8w8U NlfroEaOKqkt2bnLYIfPH/8gCupnb1SZQMhPbvjXWe ROb3tEMCd5k017DuCfrcj59h4xekUiy2tShL+O/JQ+C E3hyh+12+YfTbPw4tJrdJdUaN2wQ8r/EMJkQdaIm8W ALcgszGfWBjPr/b9jXXBL0GVXD4jtTuLZECMOIXF s6mkLeV1GJDUHtyt6rGUJ3FFbJjSj6meEoklZEya1V KyH7oc2WjjtAgMBAAEwDQYJKoZIhvcNAQELBQ ADggEBAJBgL51XjFEW1y0hj2e4IWXK0hMCPu+8Q 0VHWAZ9XH+h9cDL1TWUmcfqrif5Em6Kf0LP0vg GyvtGLpijyyd7eHBPTcNB9Ez+Tf/O62lKKVuIaK6F5 hpFrQSuqvjf9/UxM4NYIIGpU8M5q64Qqf8FQcIksysI v7P1bTX+aDOq9NYhFkP6eety3uckv+hCQk4ix1MrD FKe17ZXHeJGadWxgfrnUSkTj6jY8PGwVAw9SmxS/ NQ2SIOtzR4MSPGZUfI7EZToaIKFHWX2kTCRfw+		MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIB
HVFIi2cEdGRCIfHsYIpbJ2WISIT7Nrms48+z5abBwh SLoIjFHj0IT44UZP4JhHrG1frl6gkyNXgMVaSC8w8U NlfroEaOKqkt2bnLYIfPH/8gCupnb1SZQMhPbvjXWe ROb3tEMCd5k017DuCfrcj59h4xekUiy2tShL+O/JQ+C E3hyh+12+YfTbPw4tJrdJdUaN2wQ8r/EMJkQdaIm8W ALcgszGfWBjPr/b9jXXBL0GVXD4jtTuLZECMOIXF s6mkLeV1GJDUHtyt6rGUJ3FFbJjSj6meEoklZEya1V KyH7oc2WjjtAgMBAAEwDQYJKoZIhvcNAQELBQ ADggEBAJBgL51XjFEW1y0hj2e4IWXK0hMCPu+8Q 0VHWAZ9XH+h9cDL1TWUmcfqrif5Em6Kf0LP0vg GyvtGLpijyyd7eHBPTcNB9Ez+Tf/O62lKKVuIaK6F5 hpFrQSuqvjf9/UxM4NYIIGpU8M5q64Qqf8FQcIksysI v7P1bTX+aDOq9NYhFkP6eety3uckv+hCQk4ix1MrD FKe17ZXHeJGadWxgfrnUSkTj6jY8PGwVAw9SmxS/ NQ2SIOtzR4MSPGZUfI7EZToaIKFHWX2kTCRfw+		AQCygNhcR9CH1OPFSyKBV/patqgmUemK6Lg9Aea
SLoIjFHj0IT44UZP4JhHrG1frl6gkyNXgMVaSC8w8U NlfroEaOKqkt2bnLYIfPH/8gCupnb1SZQMhPbvjXWe ROb3tEMCd5k017DuCfrcj59h4xekUiy2tShL+O/JQ+C E3hyh+12+YfTbPw4tJrdJdUaN2wQ8r/EMJkQdaIm8W ALcgszGfWBjPr/b9jXXBL0GVXD4jtTuLZECMOIXH s6mkLeV1GJDUHtyt6rGUJ3FFbJjSj6meEoklZEya1V KyH7oc2WjjtAgMBAAEwDQYJKoZIhvcNAQELBQ ADggEBAJBgL51XjFEW1y0hj2e4IWXK0hMCPu+8Q 0VHWAZ9XH+h9cDL1TWUmcfqrif5Em6KfOLP0vg GyvtGLpijyyd7eHBPTcNB9Ez+Tf/O62lKKVuIaK6F5 hpFrQSuqvjf9/UxM4NYIIGpU8M5q64Qqf8FQcIksysl v7P1bTX+aDOq9NYhFkP6eety3uckv+hCQk4ix1MrD FKe17ZXHeJGadWxgfrnUSkTj6jY8PGwVAw9SmxS/ NQ2SIOtzR4MSPGZUfI7EZToaIKFHWX2kTCRfw+		HVFIi2cEdGRCIfHsYIpbJ2WISIT7Nrms48+z5abBwh
NlfroEaOKqkt2bnLYIfPH/8gCupnb1SZQMhPbvjXWe ROb3tEMCd5k017DuCfrcj59h4xekUiy2tShL+O/JQ+C E3hyh+12+YfTbPw4tJrdJdUaN2wQ8r/EMJkQdaIm8W ALcgszGfWBjPr/b9jXXBL0GVXD4jtTuLZECMOIXH s6mkLeV1GJDUHtyt6rGUJ3FFbJjSj6meEoklZEya1V KyH7oc2WjjtAgMBAAEwDQYJKoZIhvcNAQELBQ ADggEBAJBgL51XjFEW1y0hj2e4IWXK0hMCPu+8Q 0VHWAZ9XH+h9cDL1TWUmcfqrif5Em6Kf0LP0vg GyvtGLpijyyd7eHBPTcNB9Ez+Tf/O62lKKVuIaK6F5 hpFrQSuqvjf9/UxM4NYIIGpU8M5q64Qqf8FQcIksys1 v7P1bTX+aDOq9NYhFkP6eety3uckv+hCQk4ix1MrD FKe17ZXHeJGadWxgfrnUSkTj6jY8PGwVAw9SmxS/ NQ2SIOtzR4MSPGZUfI7EZToaIKFHWX2kTCRfw+		SLoIjFHj0IT44UZP4JhHrG1frl6gkyNXgMVaSC8w8U
ROb3tEMCd5k017DuCfrcj59h4xekUiy2tShL+O/JQ+C E3hyh+12+YfTbPw4tJrdJdUaN2wQ8r/EMJkQdaIm8V ALcgszGfWBjPr/b9jXXBL0GVXD4jtTuLZECMOIXI s6mkLeV1GJDUHtyt6rGUJ3FFbJjSj6meEoklZEya1V KyH7oc2WjjtAgMBAAEwDQYJKoZIhvcNAQELBQ ADggEBAJBgL51XjFEW1y0hj2e4IWXK0hMCPu+8Q 0VHWAZ9XH+h9cDL1TWUmcfqrif5Em6KfOLP0vg GyvtGLpijyyd7eHBPTcNB9Ez+Tf/O62lKKVuIaK6F5 hpFrQSuqvjf9/UxM4NYIIGpU8M5q64Qqf8FQcIksysI v7P1bTX+aDOq9NYhFkP6eety3uckv+hCQk4ix1MrD FKe17ZXHeJGadWxgfrnUSkTj6jY8PGwVAw9SmxS/ NQ2SIOtzR4MSPGZUfI7EZToaIKFHWX2kTCRfw+		NlfroEaOKqkt2bnLYIfPH/8gCupnb1SZQMhPbvjXWe
E3hyh+12+YfTbPw4tJrdJdUaN2wQ8r/EMJkQdaIm8W ALcgszGfWBjPr/b9jXXBL0GVXD4jtTuLZECMOIXF s6mkLeV1GJDUHtyt6rGUJ3FFbJjSj6meEoklZEya1V KyH7oc2WjjtAgMBAAEwDQYJKoZIhvcNAQELBQ ADggEBAJBgL51XjFEW1y0hj2e4IWXK0hMCPu+8Q 0VHWAZ9XH+h9cDL1TWUmcfqrif5Em6KfOLP0vg GyvtGLpijyyd7eHBPTcNB9Ez+Tf/O62lKKVuIaK6F5 hpFrQSuqvjf9/UxM4NYIIGpU8M5q64Qqf8FQcIksys1 v7P1bTX+aDOq9NYhFkP6eety3uckv+hCQk4ix1MrD FKe17ZXHeJGadWxgfrnUSkTj6jY8PGwVAw9SmxS/ NQ2SIOtzR4MSPGZUfI7EZToaIKFHWX2kTCRfw+		ROb3tEMCd5k017DuCfrcj59h4xekUiy2tShL+O/JQ+Ct
ALcgszGfWBjPr/b9jXXBL0GVXD4jtTuLZECMOIXH s6mkLeV1GJDUHtyt6rGUJ3FFbJjSj6meEoklZEya1V KyH7oc2WjjtAgMBAAEwDQYJKoZIhvcNAQELBQ ADggEBAJBgL5lXjFEW1y0hj2e4IWXK0hMCPu+8Q 0VHWAZ9XH+h9cDL1TWUmcfqrif5Em6Kf0LP0vg GyvtGLpijyyd7eHBPTcNB9Ez+Tf/O62lKKVuIaK6F5 hpFrQSuqvjf9/UxM4NYIIGpU8M5q64Qqf8FQcIksys1 v7P1bTX+aDOq9NYhFkP6eety3uckv+hCQk4ix1MrD FKe17ZXHeJGadWxgfrnUSkTj6jY8PGwVAw9SmxS/ NQ2SIOtzR4MSPGZUfI7EZToaIKFHWX2kTCRfw+		E3hyh+12+YfTbPw4tJrdJdUaN2wQ8r/EMJkQdaIm8W
s6mkLeV1GJDUHtyt6rGUJ3FFbJjSj6meEoklZEya1V KyH7oc2WjjtAgMBAAEwDQYJKoZIhvcNAQELBQ ADggEBAJBgL51XjFEW1y0hj2e4IWXK0hMCPu+8Q 0VHWAZ9XH+h9cDL1TWUmcfqrif5Em6KfOLP0vg GyvtGLpijyyd7eHBPTcNB9Ez+Tf/O62lKKVuIaK6F5 hpFrQSuqvjf9/UxM4NYIIGpU8M5q64Qqf8FQcIksys1 v7P1bTX+aDOq9NYhFkP6eety3uckv+hCQk4ix1MrD FKe17ZXHeJGadWxgfrnUSkTj6jY8PGwVAw9SmxS/ NQ2SIOtzR4MSPGZUfI7EZToaIKFHWX2kTCRfw+		ALcgszGfWBjPr/b9jXXBL0GVXD4jtTuLZECMOIXF
KyH7oc2WjjtAgMBAAEwDQYJKoZIhvcNAQELBQ ADggEBAJBgL51XjFEW1y0hj2e4IWXK0hMCPu+8Q 0VHWAZ9XH+h9cDL1TWUmcfqrif5Em6KfOLP0vg GyvtGLpijyyd7eHBPTcNB9Ez+Tf/O62lKKVuIaK6F5 hpFrQSuqvjf9/UxM4NYIIGpU8M5q64Qqf8FQcIksys1 v7P1bTX+aDOq9NYhFkP6eety3uckv+hCQk4ix1MrD FKe17ZXHeJGadWxgfrnUSkTj6jY8PGwVAw9SmxS/ NQ2SIOtzR4MSPGZUfI7EZToaIKFHWX2kTCRfw+		s6mkLeV1GJDUHtyt6rGUJ3FFbJjSj6meEoklZEya1V
ADggEBAJBgL51XjFEW1y0hj2e4IWXK0hMCPu+8Q 0VHWAZ9XH+h9cDL1TWUmcfqrif5Em6Kf0LP0vg GyvtGLpijyyd7eHBPTcNB9Ez+Tf/O62lKKVuIaK6F5 hpFrQSuqvjf9/UxM4NYIIGpU8M5q64Qqf8FQcIksys1 v7P1bTX+aDOq9NYhFkP6eety3uckv+hCQk4ix1MrD FKe17ZXHeJGadWxgfrnUSkTj6jY8PGwVAw9SmxS/ NQ2SIOtzR4MSPGZUfI7EZToaIKFHWX2kTCRfw+		KyH7oc2WjjtAgMBAAEwDQYJKoZIhvcNAQELBQ
0VHWAZ9XH+h9cDL1TWUmcfqrif5Em6KfOLP0vg GyvtGLpijyyd7eHBPTcNB9Ez+Tf/O62lKKVuIaK6F5 hpFrQSuqvjf9/UxM4NYIIGpU8M5q64Qqf8FQcIksys1 v7P1bTX+aDOq9NYhFkP6eety3uckv+hCQk4ix1MrD FKe17ZXHeJGadWxgfrnUSkTj6jY8PGwVAw9SmxS/ NQ2SIOtzR4MSPGZUfI7EZToaIKFHWX2kTCRfw+		ADggEBAJBgL51XjFEW1y0hj2e4IWXK0hMCPu+8Q
GyvtGLpijyyd7eHBPTcNB9Ez+Tf/O62lKKVuIaK6F5 hpFrQSuqvjf9/UxM4NYIIGpU8M5q64Qqf8FQcIksys1 v7P1bTX+aDOq9NYhFkP6eety3uckv+hCQk4ix1MrD FKe17ZXHeJGadWxgfrnUSkTj6jY8PGwVAw9SmxS/ NQ2SIOtzR4MSPGZUfI7EZToaIKFHWX2kTCRfw+		0VHWAZ9XH+h9cDL1TWUmcfqrif5Em6KfOLP0vg
hpFrQSuqvjf9/UxM4NYIIGpU8M5q64Qqf8FQcIksysl v7P1bTX+aDOq9NYhFkP6eety3uckv+hCQk4ix1MrD FKe17ZXHeJGadWxgfrnUSkTj6jY8PGwVAw9SmxS/ NQ2SIOtzR4MSPGZUfI7EZToaIKFHWX2kTCRfw+		GyvtGLpijyyd7eHBPTcNB9Ez+Tf/O62lKKVuIaK6F5
v7P1bTX+aDOq9NYhFkP6eety3uckv+hCQk4ix1MrD FKe17ZXHeJGadWxgfrnUSkTj6jY8PGwVAw9SmxS/ NQ2SIOtzR4MSPGZUfI7EZToaIKFHWX2kTCRfw+		hpFrQSuqvjf9/UxM4NYIIGpU8M5q64Qqf8FQcIksysN
FKe17ZXHeJGadWxgfrnUSkTj6jY8PGwVAw9SmxS/ NQ2SIOtzR4MSPGZUfI7EZToaIKFHWX2kTCRfw+		v7P1bTX+aDOq9NYhFkP6eety3uckv+hCQk4ix1MrD
NQ2SIOtzR4MSPGZUfI7EZToalKFHWX2kTCRfw+		FKe17ZXHeJGadWxgfrnUSkTj6jY8PGwVAw9SmxS/
		NQ2SIOtzR4MSPGZUfI7EZToaIKFHWX2kTCRfw+
AafB8rFhP1KObgMA9xuFNFXjcAMuHChXJJvav1V		AafB8rFhP1KObgMA9xuFNFXjcAMuHChXJJvav1Vj
sCcrs9j0mu7QhwtjZ2iNAg5CWZME=		sCcrs9j0mu7QhwtjZ2iNAg5CWZME=
SupportsMfa False	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**.



MAIN	SP Connection Browser SSO Assertion Creation				
IdP Configuration	Identity Mapping Attri	ibute Contract	Authentication Source Mapping	Summary	
Server Configuration	An Attribute Contract is a set of	of user attributes th	at this server will send in the assertion	n.	
	Attribute Contract	Subject Na	me Format		
	SAML_SUBJECT	urn:oasis:n	ames:tc:SAML:11:nameid-format:unspe	ecified	~
	Extend the Contract	Attribute N	ame Format		
	IDPEmail	urn:oasis:na	nes:tc:SAML:2.0:attrname-format:basi	c)	
	SAML_NAME_FORMAT	urn:oasis:na	nes:tc:SAML:2.0:attrname-format:unsp	pecified	
		urave esteur	emocile/AMErz.ccattrname-format:uri	~	

- 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.

P Connection	Browse	r SSO Protoco	Settings		
Assertion Consume	r Service URL	SLO Service URLs	Allowable SAML Bindings	Artifact Lifetime	Signature Policy
Encryption Policy	Summary				
the IdP, you may serve of several URLs, vi	nd SAML logout a different bindir	messages to the SP's Sir ngs. Please provide the e	igle Logout Service. Depending o indpoints that you would like to u	on the situation, the SF use.	^o may request that messages be sent
Binding	Endpoin	t URL	Response UR	łL.	Action
POST	/login.srf				Edit I 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.
- 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	STSContract1
Parameters to be provided in the request	
Parameter Name	Action
objectGUID	Edit I Delete
userPrincipalName	Edit I Delete
	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.



Туре	Instance Configura	tion Extende	ed Contract	Token Attributes	Summary
The values	of the selected Token	Processor Instan	ce.		
INSTANCE	NAME	Username	Token Proc		
INSTANCE ID		UsernameToke	nProcessor1		
TYPE		Username Tok	en Processor		
CLASS NA	ME	com.pingidenti	ty.pf.tokenpro	cessors.username.User	nameTokenProcesso
PARENT IN	NSTANCE	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 V		None available
UPN	Token	~	username V		None available

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

•	HTTP BASIC
 ✓ 	SSL CLIENT CERTIFICATE DIGITAL SIGNATURE (BROWSER SSO PROFILE ONLY)
~	REOLURE SSI

- 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.

<u>Task Result</u>

PingFederate and Office 365 setup with Access is complete.

Verification

Login to <u>https://login.microsoftonline.com</u>. 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.