MobileIron Access Cookbook Access with Salesforce and Pingone

07 February 2018

Contents

Overview	.3
Prerequisites	3
Configuring Salesforce and Pingone with MobileIron Access	5
Registering Sentry to Access	.5
Configuring Access to create a Federated Pair	5
Configuring Salesforce with MobileIron Access	6
Configuring Pingone with MobileIron Access	.7
Verification	.9

Overview

SAML provides single sign-on service 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 Pingone for authentication. The user gets authenticated by Pingone 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 Pingone as an authentication provider with Salesforce in a cloud environment.

Prerequisites

- Ensure that you have a working setup of the Salesforce and Pingone pair without MobileIron Access.
- Metadata files for Salesforce
 - 1. Login to Salesforce with admin credentials.
 - 2. Click Security Control > SAML Single Sign-On Settings > Pingone record.
 - 3. Click **Download Metadata** and save the metadata file.

salesforce	earch Search					Hashmath Rehman 🔹	Setup	Help	Sales •
Home Chatter Campaigns	Leads Accounts Contacts	Opportunities Forecasts	Contracts Order	s Cases Solutions	Products Reports	Dashboards +			
Take Sales Run your busine	sforce with you ess from any mobile device	wherever yo the with the Salesform	DU go. ce1 Mobile App	salesforce	Download on the App Store	Get IT ON Coogle play	×		
Quick Find / Search O Q Expand All Collapse All	SAML Single Sign-O Back to Single Sign-On Settings	On Settings						Printable Vie	w Help for this Page 🥑
ॐ → ≯		E	dit Delete Clone Dov	mioad Metadata) SAML As	sertion Validator				
Lightning Experience	Name	ADFS			API Name	UniqueName			
Migration Assistant	SAML Version	2.0							
Switch to the modern, intelligent	Issuer	https://s01-secureauth-01.dev	.mobileiron.com		Entity ID	https://saml.salesforce.c	m		
Get Started	Identity Provider Certificate	(Expiration: 16 May 2025 20:1	, OU=IT, O=Mob 4:06 GMT	ileiron, L=Mountain View, S	T=California, C=US				
Con Oranio	Request Signing Certificate	SelfSignedCert 19Jan2016 2	211116						
	Request Signature Method	RSA-SHA256							
Salesforce1 Quick Start	Assertion Decryption Certificate	Assertion not encrypted							
	SAML Identity Type	Federation ID							
Force.com Home	SAML Identity Location	Subject							
Administar	Service Provider Initiated Request Binding	HTTP Redirect							
Administer	Identity Provider Login URL	https://	/securear	uth2/secureauth.aspx					
 Manage Users 	Identity Provider Logout URL								
Manage Apps	Custom Error URL								

- Metadata files for Pingone:
 - 1. Login to Pingone with admin credentials.
 - 2. Click Applications and select Salesforce application.

3. Scroll down and download the metadata file for Pingone.

saasid	
Issuer	https://pingone.com/idp/
Signing Algorithm	RSA_SHA256
ACS URL	-3b9a-4d43- b479-0c4b52328c49/sp
SP entityId	-3b9a-4d43-
Initiate Single Sign-On (SSO) URL @	
Single Sign-On (SSO) Relay State @	
Single Logout Endpoint	
Single Logout Response Endpoint	
Force Re-authentication @	false
Signing Certificate	Download
SAML Metadata	Download

Configuring Salesforce and Pingone with MobileIron Access

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

- <u>Registering Sentry to Access</u>
- Configuring Access to create a Federated Pair
- <u>Configuring Salesforce with MobileIron Access</u>
- Configuring Pingone with MobileIron Access

Registering 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
- *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.

Configuring Access to create a Federated Pair

You must configure Access to create a federated pair.

Prerequisites

Verify that you have configured Salesforce and Pingone natively.

Procedure

- 1. Log in to Access.
- 2. Click **Profile** > **Get Started**.
- 3. Enter the Access host information, and upload the **ACCESS SSL certificate** in p12 format. All the other fields are set to default. Click **Save**.
- 4. On the **Federated Pairs** tab, click **Add New Pair** and select **Salesforce** as the service provider.
- 5. Enter the following details:
 - a. Name
 - b. Description
 - c. Upload the Access Signing Certificate or click **Advanced Options** to create a new certificate.
 - d. Upload the metadata file of service provider that you downloaded. See <u>Prerequisites</u>.
 - e. (Optional) Select *Use Tunnel Certificates for SSO* to configure Cert SSO on MobileIron Core. See *Appendix* in the *MobileIron Access Guide* at <u>https://support.mobileiron.com/docs/current/accs/</u>
- 6. Click Next.
- 7. Select **Pingone** as the Identity provider. Click **Next**.
- 8. Select the Access signing Certificate or click **Advanced options** to create a new certificate.
- 9. Upload the IdP metadata file that you downloaded. See <u>Prerequisites</u>. Click **Done**.
- 10. Download the ACCESS SP Metadata (Upload to IDP) and the ACCESS IDP Metadata (Upload to SP) files from the federated pair page.
- 11. On the **Profile** tab, click **Publish** to publish the profile.

Configuring Salesforce with MobileIron Access

You must configure Salesforce to use with Access.

Prerequisites

- Verify that you have created a federated pair with Salesforce and Pingone.
- Verify that you have configured Salesforce and Pingone natively.

Procedure

- 1. Login to the Salesforce admin portal.
- 2. Expand Security Controls, and select Single Sign-On Settings.
- 3. On the SAML Single Sign-On Settings, click New from Metadata file.

salesforce	earch Search Hashmath Rehman * Setu	p Help	Sales •
Home Chatter Campaigns	Leads Accounts Contacts Opportunities Forecasts Contracts Orders Cases Solutions Products Reports Dashboards +		
Take Sales	sforce with you wherever you go. ess from any mobile device with the Salesforce? Mobile App.		
Quick Find / Search O Q	Single Sign-On Settings		Help for this Page 🥑
Expand All Collapse All	Configure single sign-on in order to authenticate users in salesforce.com from external environments. Your organization has the following options available for single sign	-on:	
ॐ → ≯	Federated authentication, a single sign-on method that uses SAML assertions sent to a Salesforce endpoint.		
Lightning Experience	Edit SAML Assertion Validator		
Migration Assistant	Federated Single Sign-On Using SAML		
Switch to the modern, intelligent Salesforce.	SAML Enabled 🗸		
Get Started			
	SAML Single Sign-On Settings New New from Metadata File New from Metadata URL		
Salesforce1 Quick Start	Action Name SAML Version Issuer Entity ID		

- Upload the Access IDP Metadata (Upload to SP) downloaded in Step 10 of Configuring Access to create a Federated Pair. Note: If certificate-based SSO is enabled, Request Signature method must be set to RSA-SHA256.
- 5. Click Save.
- On the admin portal, Click Domain Management > My Domain > Edit Authentication configuration and select Access as the new federated authentication service instead of Pingone.

Task Result

Salesforce is configured with Access.

Configuring Pingone with MobileIron Access

You must configure the identity provider with the service provider metadata file. This builds the trust relationship with the service provider.

- 1. Login to Pingone with admin credentials.
- 2. Click My Applications and select Salesforce.

Ny App	lications			A / A	pplications / My Applications
pplications	you've added to your acc	ount are listed here.			
Active a Details	pplications are enabled for fisplays the application de	r single sign-on (SSO). Itails			
- Dorano (approver and approximation at	No.		98. H1000	
	Application Name	Туре	Status	Enabled	
	ACC Dropbox	SAML	Active	Yes	Remove
bax	Box	SAML with Provisioning (API)	Active	Yes	Remove
E	Google Docs	SAML	Active	Yes	Remove
	Google Drive	SAML	Active	Yes	Remove
					1.000

- 3. Click **Edit** > **Continue to Next Step**.
- 4. Upload the Access SP Metadata (Upload to IDP) metadata file downloaded in Step 10 of Configuring Access to create a Federated Pair.

Upload Metadata	Select File Or use URL
ACS URL	· · · · ·
Entity ID	· · · · · · · · · · · · · · · · · · ·
Target Resource @	
Single Logout Endpoint @	example.com/slo.endpoint
Single Logout Response Endpoint @	example.com/sloresponse.endpoint
Verification Certificate @	Browse No file selected. saml20metadata.cer
Force Re-authentication @	
PingOne dock URL	
Default PingOne dock URL	
	Use Custom URL @
Set Up Provisioning	This application also supports User Provisioning, User Provisioning integrates the directory services for your IdP with a SaaS provider provisioning API to automatically create, update and delete user accounts in the service provider directory.
NEXT: Attribute Mapping	Cancel Back Continue to Next Step

- 5. Click Continue to Next Step > Save > Publish.
- 6. Click **Finish**.

Verification

Salesforce and Pingone is now configured with MobileIron Access. You must validate the new federation settings.

- Register a device to Core.
- Download Salesforce applications from App Store.
- Opening this application triggers the per-app-vpn.
- Verify that SAML SSO is working.

Copyright © 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.