MobileIron Access Cookbook

Access with Salesforce and Pingone

07 February 2018

Proprietary and Confidential | Do not Distribute

Contents

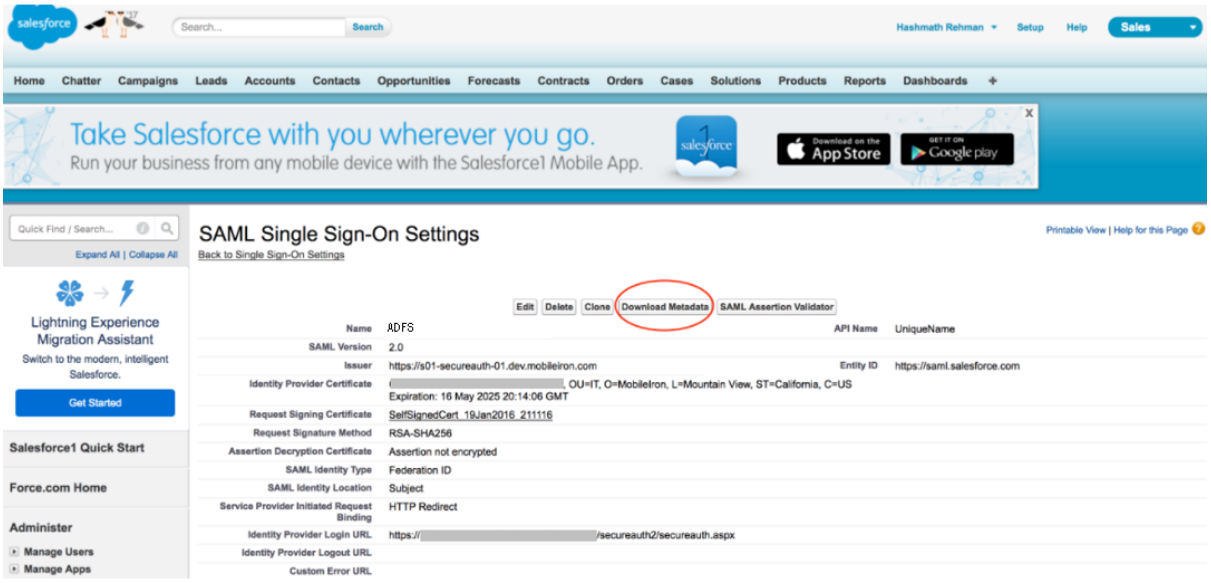
Overview 3
Prerequisites 3
Configuring Salesforce and Pingone with MobileIron Access 5
Registering Sentry to Access 5
Configuring Access to create a Federated Pair 5
Configuring Salesforce with MobileIron Access 6
Configuring Pingone with MobileIron Access 7
Verification 9

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

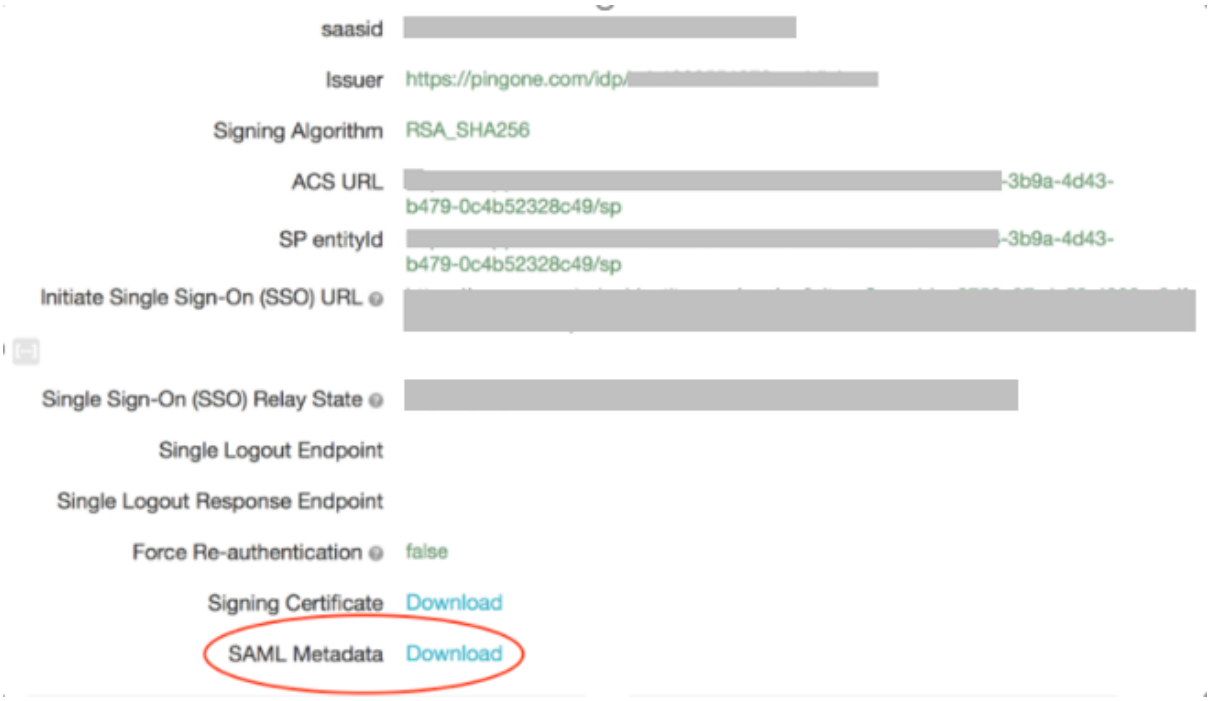
- Ensure that you have a working setup of the Salesforce and Pingone pair without MobileIron Access.
- **Metadata files for Salesforce**
  1. Login to Salesforce with admin credentials.
  2. Click **Security Control** > **SAML Single Sign-On Settings** > Pingone record.
  3. Click **Download Metadata**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



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

Proprietary and Confidential | Do not Distribute

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



Proprietary and Confidential | Do not Distribute

Configuring Salesforce and Pingone with MobileIron Access

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

- Registering Sentry to Access
- Configuring Access to create a Federated Pair
- Configuring Salesforce with MobileIron Access
- 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

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.

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.

Proprietary and Confidential | Do not Distribute

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 Prerequisites.
    e. (Optional) Select *Use Tunnel Certificates for SSO* to configure Cert SSO on MobileIron Core. See *Appendix* in the *MobileIron Access Guide* at https://support.mobileiron.com/docs/current/accs/
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 Prerequisites. 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

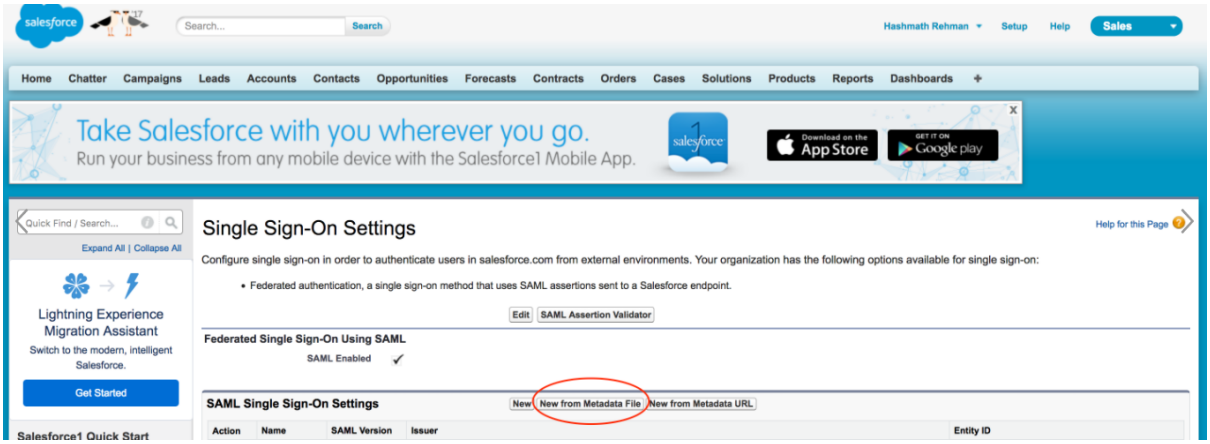
You must configure Salesforce to use with Access.

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**.



4. 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**.
6. On the admin portal, Click **Domain Management** > **My Domain** > **Edit Authentication configuration** and select Access as the new federated authentication service instead of Pingone.

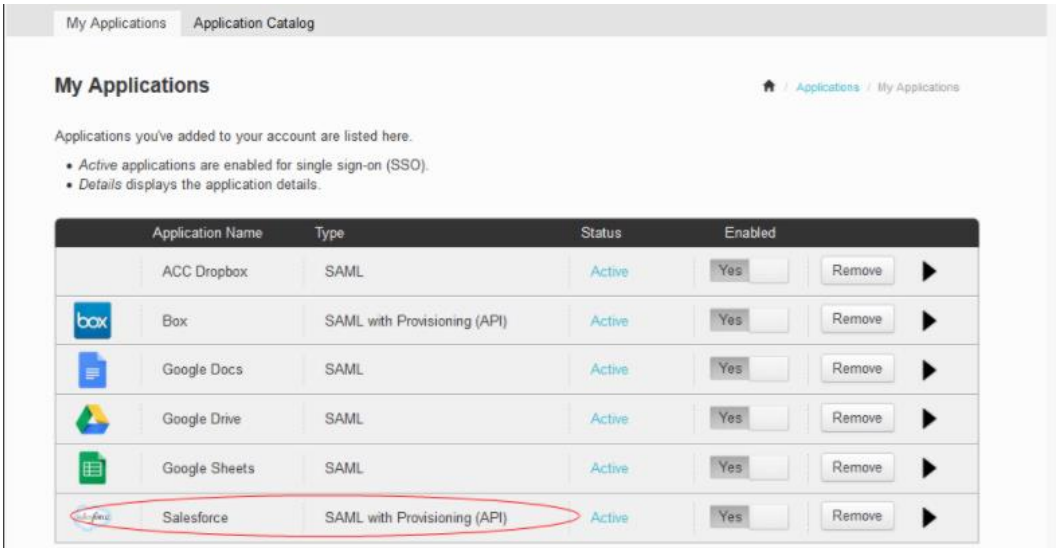
Task Result

Salesforce is configured with Access.

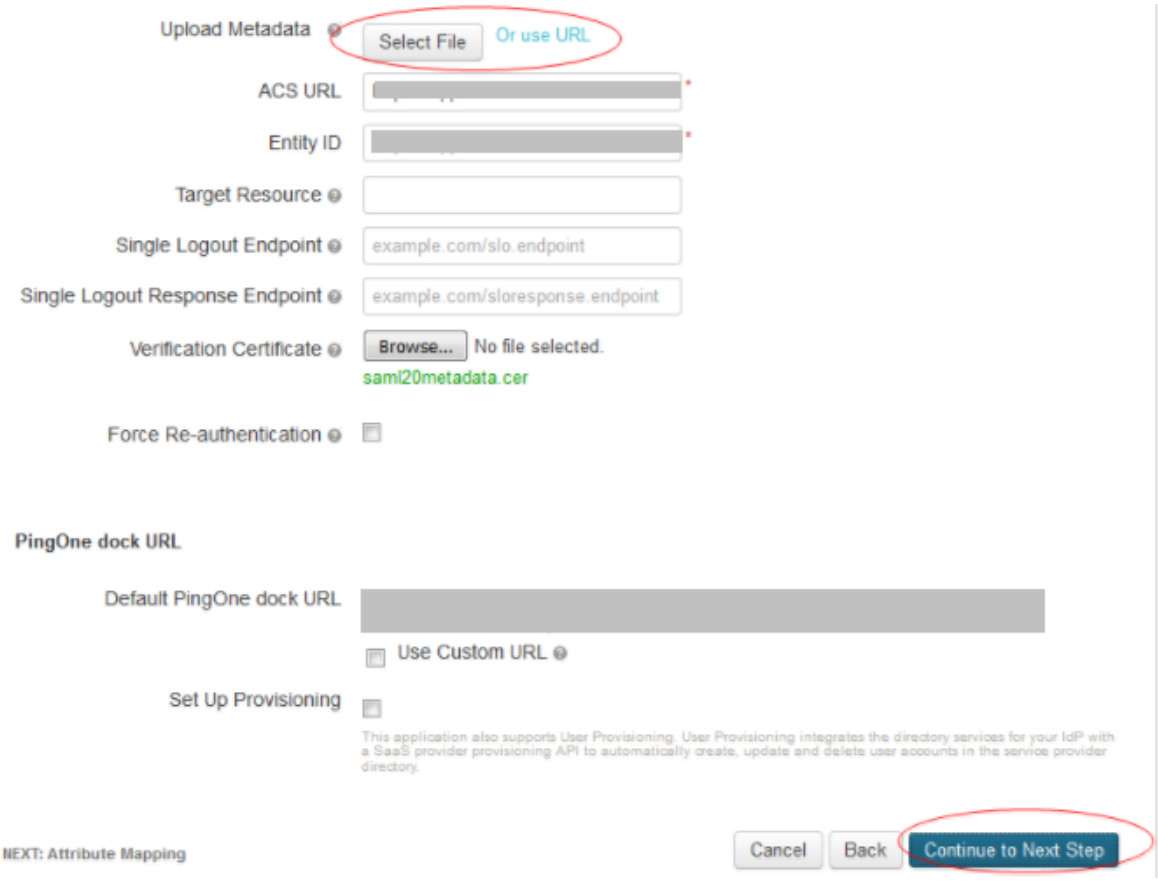
Configuring Pingone with MobileIron Access

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**.



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.



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

Proprietary and Confidential | Do not Distribute

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.

Proprietary and Confidential | Do not Distribute

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.