



MobileIron Access Cookbook

Access with Test SP and Test IDP

Revised: 28 September, 2017



Contents

Overview.....	3
Prerequisites.....	3
Working with Test SP and Test IDP without MobileIron Access.....	5
Configuring Test SP and Test IDP with MobileIron Access.....	6
Configure Access to Create a Federated Pair.....	6
Configure the SP (Test SP) with MobileIron Access.....	8
Configure the IDP (Test IDP) with MobileIron Access.....	8
Register Sentry to Access.....	9
Verifying the setup.....	10



Overview

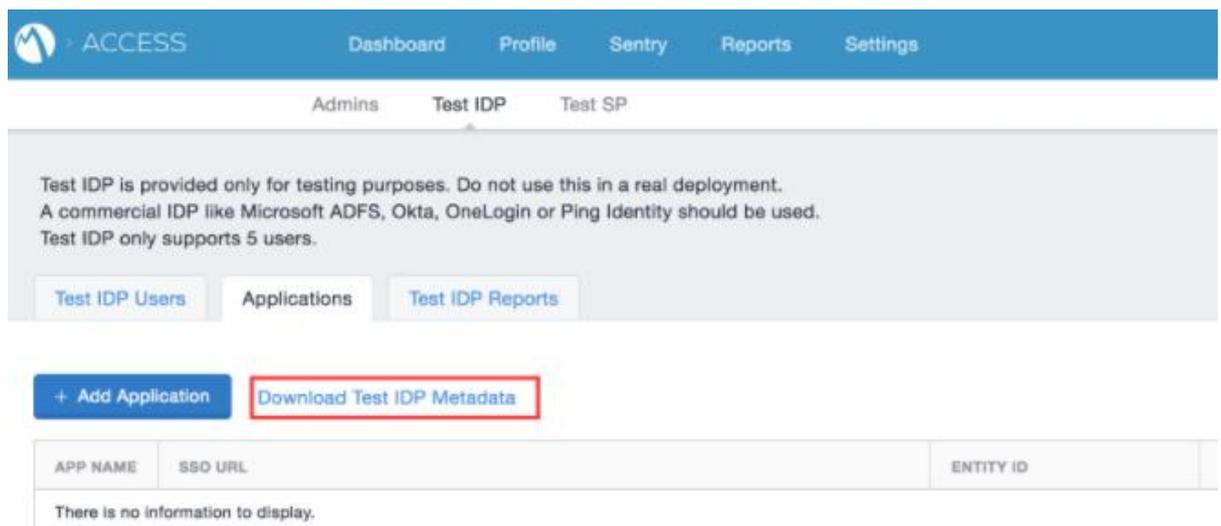
SAML provides single sign-on capability for users accessing their services hosted in a cloud environment. Generally, a service provider such as Test SP is federated with an identity provider such as Test IDP for authentication. The user gets authentication from Test IDP and obtains a SAML token for accessing applications in a cloud environment, such as Test SP. This guide serves as step-by-step configuration manual for users using Test IDP as an authentication provider with Test SP in a cloud environment.

Prerequisites

Verify that you have the following metadata available in your environment:

- **Test IDP Metadata Files**

1. Login to MobileIron Access with admin credentials.
2. Click **Settings > Test IDP > Applications**.
3. Click **Download Test IDP Metadata**.

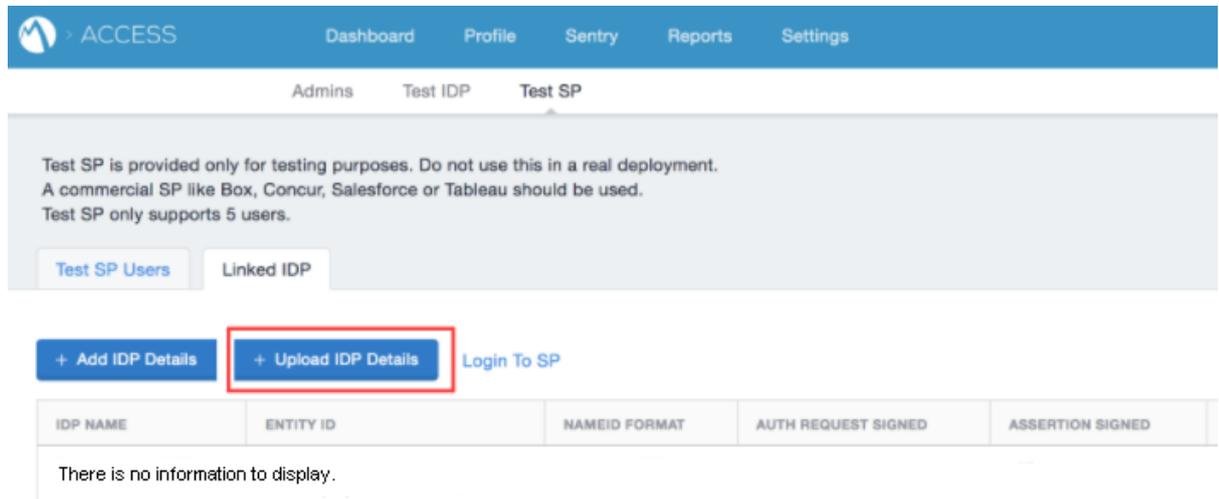


4. Save the metadata file.
5. Click **Test IDP Users** tab and + **Add Test IDP User**.



- **Test SP Metadata Files**

1. Login to MobileIron Access with admin credentials.
2. Click **Settings > Test SP > Linked IDP**.
3. Click on + **Upload IDP Details** and enter the IDP name.



4. Click **Choose File** or **Drag and drop the file** that you saved from Test IDP procedure above.
5. Click **Done**.
6. Click **Download Test SP Metadata** in **Actions** from the new IDP entry created.
7. Click **Test SP Users** tab and + **Add Test SP User**.
Note: The username and email address must be the same as Test IDP user that is created in the **Test IDP Metadata Files** procedure.



Working with Test SP and Test IDP without MobileIron Access

You can test the service providers and identity providers without creating a federated pair in MobileIron Access. You must download the metadata files for SP and IDP as described in the [Prerequisites](#) section.

Procedure

1. Login to MobileIron Access with admin credentials.
2. Navigate to **Settings > Test IDP > Applications**.
3. Click + **Add Application**.
4. Upload the Test SP metadata file downloaded from [Prerequisites](#) section.
5. Navigate to **Test SP > Linked IDP** and click **Login to SP**.
The page redirects to Test IDP login page.
6. Enter the user credentials.
The Test SP home page is displayed with successful login.



Configuring Test SP and Test IDP with MobileIron Access

You must perform the following tasks to accomplish the configuration between Test SP and Test IDP:

- [Configure Access to Create a Federated Pair](#)
- [Configure the SP \(Test SP\) with MobileIron Access](#)
- [Configure the IDP \(Test IDP\) with MobileIron Access](#)
- [Register Sentry to Access](#)

Configure Access to Create a Federated Pair

You must configure Access to select your service provider and the identity provider. You can apply the configuration settings for the service provider and the identity provider. It creates a federated pair.

Procedure

1. In Access, click **Profiles > Get Started**.
2. Enter the Access host information and upload the ACCESS SSL Certificate. Use the default values for the other fields. Click **Save**.
3. Click **Profiles > Federated Pair > Add New Pair**.
4. Select **Custom SAML Service Provider** option under the **Choose Service Provider**.
5. Enter the following details:
 - Name for the Federated Pair
 - Description
 - Select or upload the SP Proxy Signing Certificate
 - Upload the Test SP metadata downloaded from the Prerequisites section and click **Next**.
 - Click Advanced options and enter the following configuration:



- Advanced Options

Assertion Validity: (minutes)

Enter information here only if you would like the SAML assertions generated by MobileIron Access to have a structure different than the default configured for this SP.

You can select values from the certificate Subject or Subject Alternative Name fields to go into the SAML Response Subject or Attributes in an Attribute Assertion in the SAML Response.

SAML Subject Configuration

Type:

Value:

SAML Attribute Configuration

1 Attribute(s) [Add New](#)

6. Click **Next**.
7. Select **Custom Identity Provider** as the identity provider.
8. Select or Upload the **IdP Proxy certificate** and the **IdP metadata** file that you downloaded from the Prerequisites section.
9. Click **Done**.
10. Download the **Access SP Metadata and Upload to IDP** and **ACCESS IDP Metadata and Upload to SP** metadata files.
11. Click **Profile > Publish** to publish the profile.

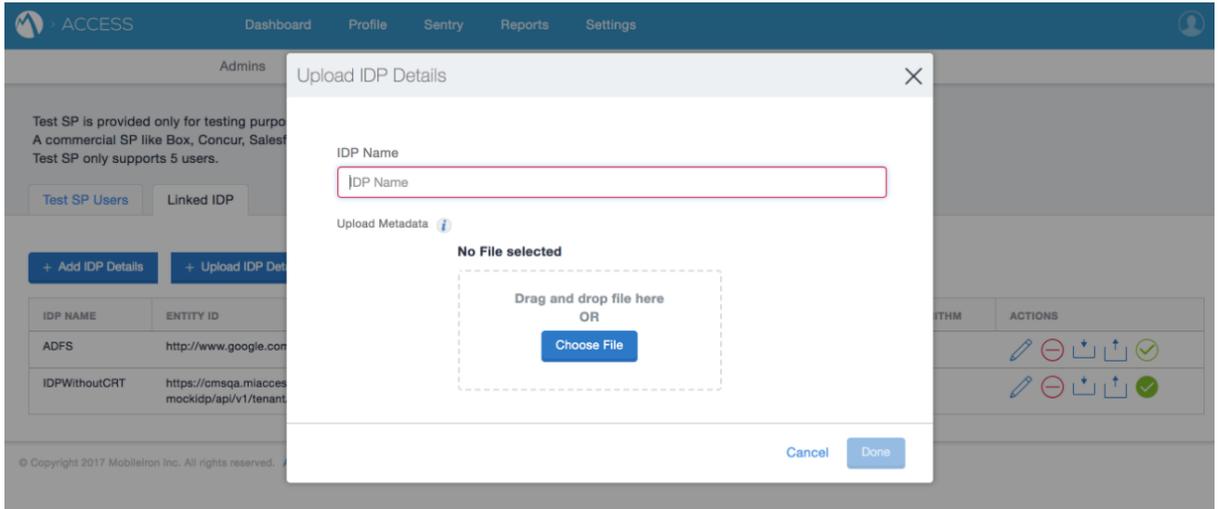


Configure the SP (Test SP) with MobileIron Access

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

Procedure

1. Login to MobileIron Access with admin credentials.
2. Click **Settings** > **Test SP** > **Linked IDP**.
3. Click + **Upload IDP Details**.



4. Upload the Access IDP Metadata downloaded from [Working with Test SP and Test IDP without MobileIron Access](#)

You can test the service providers and identity providers without creating a federated pair in MobileIron Access. You must download the metadata files for SP and IDP as described in the [Prerequisites](#) section.

Procedure

7. Login to MobileIron Access with admin credentials.
8. Navigate to **Settings** > **Test IDP** > **Applications**.
9. Click + **Add Application**.
10. Upload the Test SP metadata file downloaded from [Prerequisites](#) section.
11. Navigate to **Test SP** > **Linked IDP** and click **Login to SP**.
The page redirects to Test IDP login page.
12. Enter the user credentials.
The Test SP home page is displayed with successful login.

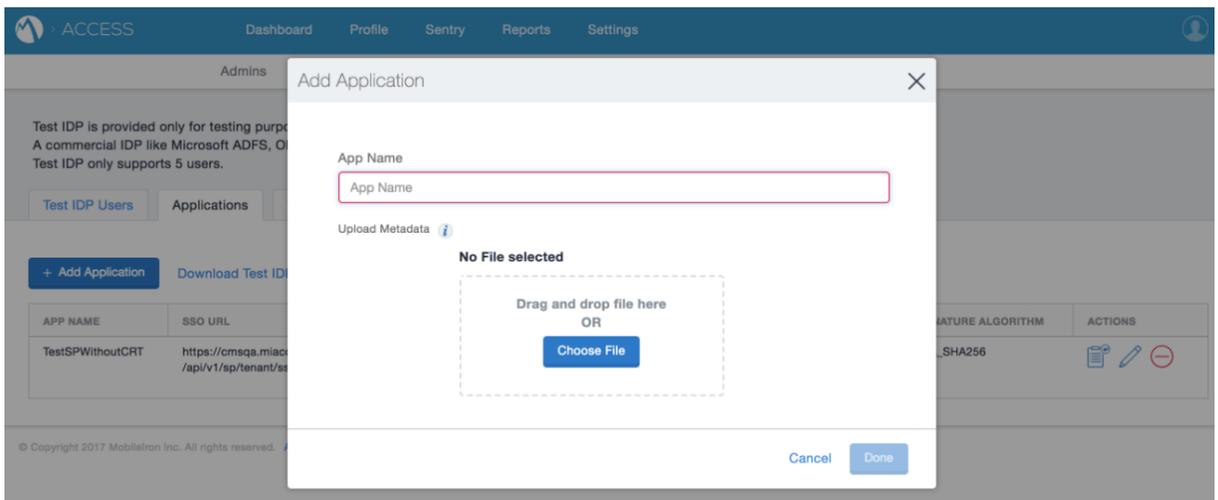


5. Configuring Test SP and Test IDP with MobileIron Access section.
6. Click **Done**.

Configure the IDP (Test IDP) with MobileIron Access

Procedure

1. Login to MobileIron Access with admin credentials.
2. Click **Settings > Test IDP > Applications**.
3. Click + **Add Application**.



4. Enter a name for the application and upload the Access SP Metadata downloaded from [Working with Test SP and Test IDP without MobileIron Access](#)

You can test the service providers and identity providers without creating a federated pair in MobileIron Access. You must download the metadata files for SP and IDP as described in the [Prerequisites](#) section.

Procedure

13. Login to MobileIron Access with admin credentials.
14. Navigate to **Settings > Test IDP > Applications**.
15. Click + **Add Application**.
16. Upload the Test SP metadata file downloaded from [Prerequisites](#) section.
17. Navigate to **Test SP > Linked IDP** and click **Login to SP**.
The page redirects to Test IDP login page.
18. Enter the user credentials.
The Test SP home page is displayed with successful login.



5. Configuring Test SP and Test IDP with MobileIron Access.
6. Click **Done**.

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 Test SP as the service provider and Test IDP as the identity provider. This configuration lets you fetch the latest configuration from Access.

Verifying the setup

After the setup is configured with Access, you must verify the authentication.

Procedure

1. Login to MobileIron Access with admin credentials.
2. Navigate to **Settings** > **Test SP**.
3. Click **Login to SP**. The Test IDP login page displays.



4. Enter the username and password.
After successful authentication, the Test SP home page displays.

The Test SP and Test IDP expects the username to be an email address in User Creation flow.



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.