

MobileIron Access Cookbook

Access with Box and Azure AD

01/02/2018

Contents

Overview.....	3
Prerequisites.....	3
Configuring Box and Azure AD with MobileIron Access	4
Registering Sentry to Access	4
Configuring Access to create a Federated Pair	4
Configuring Box with MobileIron Access.....	5
Configuring Azure AD with MobileIron Access.....	6
Verification	6

Overview

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

1. Ensure that you have a working setup of the Box and Azure AD pair without MobileIron Access.
2. **Metadata files for Box:**
Download the metadata file from the following location:
<https://cloud.app.box.com/shared/3isa8qvqgn>
3. **Metadata files for Azure AD**
 - Login to Azure portal with admin credentials.
 - In the Azure portal, on the left navigation pane, click **Azure Active Directory > App Registrations > Box > Box > Single Sign-On**.
 - Download the metadata file



Configuring Box and Azure AD with MobileIron Access

You must perform the following tasks to configure Box and Azure AD with MobileIron Access:

- [Registering Sentry to Access](#)
- [Configuring Access to create a Federated Pair](#)
- [Configuring Box with MobileIron Access](#)
- [Configuring Azure AD 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 Box and Azure AD natively. See [Prerequisites](#).

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 **Box** 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. Click **Upload Metadata** and upload the metadata file for Box 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 **Azure AD** as the Identity provider. Click **Next**.
8. Select the **Access Signing Certificate** or click **Advanced options** to create a new certificate.
9. Upload the Azure AD 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 Box with MobileIron Access

You must configure Box to use with Access.

Prerequisites

- Verify that you have created a federated pair with Box and Azure AD.
- Verify that you have configured Box and Azure AD natively.

Procedure

1. Login to the support portal for Box with admin credentials.
2. Click **Help** and select **Admin Forum**.
3. Under **Need Help?**, click on **Submit a case**
4. Upload the **Access IDP Metadata (Upload to SP)** downloaded in **Step 10** of [Configuring Access to create a Federated Pair](#).
5. Contact Box support for further configuration details.

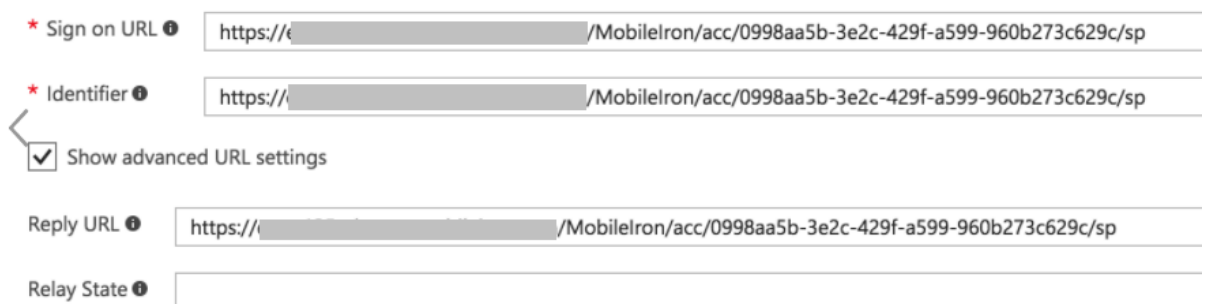
Task Result

Box is configured with Access.

Configuring Azure AD 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 Azure AD tenant portal with admin credentials.
2. On the left navigation pane, click **Azure Active Directory > App Registrations > Box > Box > Single Sign-On**.
3. Select **Mode as SAML-based Sign-on** to enable single sign-on.
4. Extract the following information from the proxy metadata file downloaded in **Step 10** of [Configuring Access to create a Federated Pair](#).



The screenshot shows a configuration form for a Single Sign-On application. It includes the following fields and options:

- Sign on URL**:
- Identifier**:
- Show advanced URL settings**
- Reply URL**:
- Relay State**:

5. Click **Save**.

Verification

- Open a browser and login to Box account. Verify the redirection in Sentry logs for SAML Request and Responses.
- Configure Box App on iOS/Android/Windows device and check the Sentry logs for SAML Request and Responses.

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.