MobileIron Access Cookbook
Access with Box and PingOne

01/02/2018

Contents

Overview

SAML provides single sign-on capability 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 PingOne for authentication. The user gets authentication from PingOne 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 PingOne 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

Verify that you have the following components in your environment:

- Ensure that you have a working setup of native federation for Box and PingOne in your environment.

- **Box (SP) Metadata Files**
  - Download Metadata file from the following URL:
    https://cloud.app.box.com/shared/3isa8qvvqn

- **PingOne (IdP) Metadata Files**
  - Login to PingOne with admin credentials.
  - Navigate to **Applications** > **My Applications > Add Application**.
  - Select Search Application Catalog.
  - Type **Box** and click **Search**.
  - Select Box with SAML Provisioning and click the Arrow.
  - Click Setup > Continue > Next.
  - In Attribute Mapping, select Email and click Continue to Next Step.
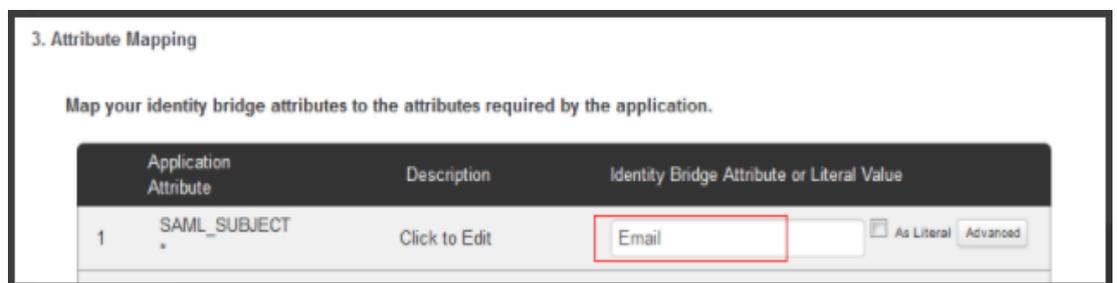
  - Click **Save** > **Publish**.
  - Click the SAML Metadata download link to download the IdP metadata file and click **Finish**.

Configuring Box and PingOne with MobileIron Access

You must perform the following tasks to accomplish the configuration between Dropbox-EMM and PingOne:

- Register Sentry to Access
- Configure Access to Create a Federated Pair
- Configure the PingOne environment with MobileIron Access
- Configure the Box environment with MobileIron Access

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.

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 **Profile** > **Get Started**.
2. Enter the Access host information and upload the ACCESS SSL Certificate. Use the default values for the other fields. Click **Save**.
   Note: Perform the above steps only if a profile is not available.
3. Click **Profiles** > **Federated Pair** > **Add New Pair.**
4. Select **Box** under the **Choose Service Provider**.
5. Enter the following details:

   - Name for the Federated Pair
   - Description
   - Select the **Access Signing Certificate** or use the **Advanced Options** to create a new Access Signing Certificate.
   - **Upload** the metadata file for Box that you downloaded in Prerequisites.
   - (Optional): Select **Use Tunnel Certificates for SSO** for users to be authenticated automatically. This leverages the user's authentication in the MobileIron Tunnel VPN. See *Appendix* in the *MobileIron Access Guide* at https://support.mobileiron.com/docs/curent/accs.

6. Click **Next** and select **PingOne** as the identity provider.
7. Select the **Access Signing Certificate** or use the **Advanced Options** to create a new self-signed Access Signing Certificate.
8. Select Upload Metadata or Add Metadata to provide the **IdP metadata** details for PingOne that you saved. See Prerequisites.
   See https://support.mobileiron.com/docs/curent/accs for more information.
   Click **Done**.
9. Download the **Access SP Metadata (Upload to IDP)** and **ACCESS IDP Metadata (Upload to SP)** metadata files.
10. Click **Publish** to publish the profile.

Configure the PingOne environment with MobileIron Access

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

Procedure

1. Login to PingOne portal with admin credentials.
2. Navigate to **Applications** > **My Application** > select the Box application.
3. Click **Edit** > **Continue** to Next.
4. Upload the metadata file **Access SP Metadata (Upload to IDP)** that you downloaded in **Step 9** of Configure Access to Create a Federated Pair.
5. Click **Continue**.
6. All other fields are set to default. Click **Save** and **Publish**.
7. Click **Finish**.

Configure the Box environment with MobileIron Access

Procedure

1. Login to Box support portal with admin credentials.
   https://support.box.com
2. On the **Help** tab, select **Admin Forum**.
3. Under **Need Help**?, click **Submit a Case**.
4. Upload the metadata file **Access IDP Metadata (Upload to SP)** that you downloaded in **Step 9** of Configure Access to Create a Federated Pair.
5. Follow-up with Box support for further clarification.

Verification

Single-sign-on service is now configured using SAML with Box as the service provider and PingOne as the identity provider. This configuration lets you fetch the latest configuration from Access.

1. Open a browser and log in to Box account.
2. Observe the SAML SSO logs in sentry log file for SAML Requests and Responses.
3. Configure Box application on iOS/Android/Windows device and check Sentry Logs for SAML Request and Responses.