



# MobileIron Access Cookbook

## Access with Dropbox Business and PingOne

**01/02/2018**



## Contents

Overview.....	3
Prerequisites.....	3
Configuring Dropbox-EMM and PingOne with MobileIron Access .....	4
Register Sentry to Access .....	4
Configure Access to Create a Federated Pair .....	4
Configure the PingOne environment with MobileIron Access.....	5
Configure the Dropbox-EMM environment with MobileIron Access .....	6
Send Token to Dropbox-EMM app from Core.....	7
Configure Core to Apply App Restrictions .....	8
Verification .....	9



# Overview

SAML provides single sign-on capability for users accessing their services hosted in a cloud environment. Generally, a service provider such as Dropbox-EMM 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 Dropbox-EMM.

This guide serves as step-by-step configuration manual for users using PingOne as an authentication provider with Dropbox-EMM 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 Dropbox Business and PingOne in your environment.
- **Dropbox Business (SP) Metadata Files**
  - **Entity ID:** [https://www.dropbox.com/saml\\_login](https://www.dropbox.com/saml_login)
  - **Assertion Consumer Service URL:** [https://www.dropbox.com/saml\\_login](https://www.dropbox.com/saml_login)
- **PingOne Metadata Files**
  - Login to PingOne with admin credentials.
  - Navigate to **Applications > Dropbox Business**.
  - Click the SAML Metadata download link to download the IdP metadata file.



# Configuring Dropbox-EMM 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 Dropbox-EMM 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 **Dropbox Business** option 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 or Add Metadata**
    - Entity ID: [https://www.dropbox.com/saml\\_login](https://www.dropbox.com/saml_login)
    - Assertion Consumer Service URL: [https://www.dropbox.com/saml\\_login](https://www.dropbox.com/saml_login)
  - (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 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 Dropbox 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 Dropbox-EMM environment with MobileIron Access

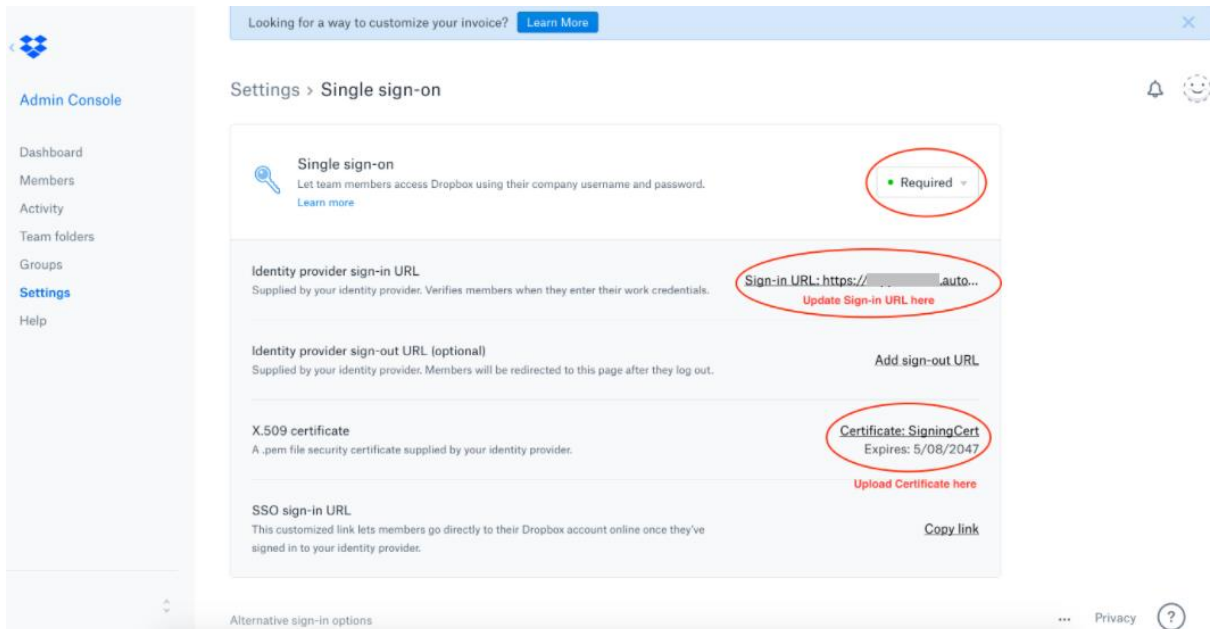
Dropbox-EMM does not let you upload a metadata file. The information must be extracted from the IDP Proxy metadata file. Extract the Entity ID from the IDP Proxy metadata file.

### Procedure

1. Login to Dropbox with admin credentials.
2. Open the SP Proxy metadata file that you downloaded when configuring Access for federated pair.
3. Extract the certificate from the IDP Proxy metadata file and save it in the .cer file.

```
</KeyDescriptor>
<KeyDescriptor use="signing">
  <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:X509Data>
      <ds:X509Certificate>MIIDZDCCAkwwCQCZVG/BcwYw0JANBgkqhkiG9w0BAQsFADB0MQswCQYDVQOCEwJVlZETMBEGA1UE
CAwKQ2FsaWZvcms5YTEWMBQGA1UEBwwNTW91bnRhaW4gVmlldzETMBEGA1UECgwKTW9laWw1S0N
bJFQMA4GA1UECwwHU3VwcC9ydERMABGA1UEAwww1SWRwUH1vesHkwHicNM1IzMDUzMDUzMDUzMDUz
MjRlbnRhaW4gVmlldzETMBEGA1UECgwKTW9laWw1S0NvbjE0MA4GA1UECwwHU3VwcC9ydERM
MABGA1UEAwww1SWRwUH1vesHkwHicEIMAGCCSgCS3DDEBAQUAA4IBDwAwggEKAoIBAQCu8ZUnrBrC
Yw3woT0Bn4yglJ1eXqe2Z7JRkmQWq1ySklJkTfshu3f6RUCXclbz7FaQzOCyKQnkKxYnmqVz
TpeBzYyB2XaYReTDTc40TEB8qUvm7C4UzIq1NhqCVC48TzLzMWsX+ngae5Vd/wso1PYbox5
CEXcQicTFG0IPAE8pPEhfT94cDGe7IDzie8IM8rshWczHdq6xDPZ18AZhNSkSD/Qz0551Qrv14
zFBR0yG0+oG-sawBC09opwd1Sh/Cz25zWEBuz+04Uv/VfUrh12EvY2IOF2dH1jvtmX0wTm6CTsKs09
fvj3XdrG15mbSdf225BOBynSH+VzAqMBAALwDQYJKoZIhvcNAQELBQADggELBAAgNp9RUK1TpxDfS
m6j5vR8Nv4lrdzrea0TeRTJNTSb/mA1ISRrMqYFnC91aJbdoSDlw6xhgAVjkyc/KKhu13hL9F3
TYy/wxhIU9DIXC4uTmVhUmp/gVm1/nyCINMSH1+9V0KWSyugfawBz96EYn8FX001psjtlpdhl
MTRDSeqETLq7fIocXE7PUcf15IHkV30xpBR4iuVoutJHbRqJKAK7M66wz2VYszmVvwD4+VzIVe
WY5GABrisdAB8OBLZQAuqib4SRsSvgn1IOYuvL0+aYXdkf9QhGDrLzIIDYluT3R15Pp8UzJfp1w8a7vIOIwx9Sg7q2RQfx3YA</ds:X509Certificate>
    </ds:X509Data>
  </ds:KeyInfo>
</KeyDescriptor>
```

4. Click **Settings > Single Sign On**, enter Sign-in URL and upload the extracted certificate.



5. Click **Settings > Devices > Enterprise Mobility Management** and copy the **Auth token** to setup Dropbox with the EMM vendor.



## Enterprise Mobility Management (EMM)

Enable EMM

Dropbox EMM works with third-party EMM vendors to give admins more control over how members use Dropbox on mobile devices. [Learn more](#)

**Auth token** ^

Use this token when setting up Dropbox with your EMM vendor

[Get new token](#)

**Deployment** ^

Test mode

All employees can still access company files using the regular Dropbox app.

[Create mobile app usage report](#)

Deploy

All employees will be required to install the Dropbox EMM app to access company files.

### 6. Create a *.plist* file and save the token.

```
<?xml
version="1.0"
encoding="UTF-8"?>
<!DOCTYPE
plist
PUBLIC
"-//Apple
Computer//DTD
PLIST
1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist
version="1.0">
<dict>
<key>team_emm_token</key>
<string><token></string>
</dict>
</plist>
```

### Send Token to Dropbox-EMM app from Core

1. Login to the Core with admin credentials.
2. Click **Policies & Configs > Configuration.**
3. Click **Add New > iOS & OSx.**
4. Select **Manage App Config > Configure Bundle ID.**



**New Managed App Config Setting**

Managed App Config allows you to specify a configuration dictionary to communicate with and configure third-party managed apps. It is supported only by iOS7 and later.

**License Required:** This feature requires a separate license. Prior to using this feature, ensure your organization has purchased the required licenses.

Name: emmtoken

Description:

BundleId: com.getdropbox.DropboxEMM

File: Browse... dpemm.plist

Save Cancel

5. Upload the *.plist* file and click **Save**.
6. Apply label to Managed App Config setting.

### Configure Core to Apply App Restrictions

You must configure Core to prevent access to documents from Dropbox to unmapped apps website on Safari Domain on an iOS device.

1. Login to Core with admin credentials.
2. Click **Policies & Configs > Configuration**.
3. Click **Add New > iOS & OSx**.
4. Select **Managed Domain**.
5. Click **Add+** to add a row under the **WEB DOMAINS** section such as `*.dropboxusercontent.com` or `*.dropbox.com`.

**Modify Managed Domains Configuration**

Name: Dropbox

Description:

EMAIL DOMAINS

No records to display

Add+

WEB DOMAINS

*.dropboxusercontent.com	=	✕
--------------------------	---	---

Cancel Save

6. Click **Save** to assign domain to an IOS Device.
7. Click **Policies & Configs > Configuration**.





8. Click **Add New > iOS & OSx > Restrictions**.
9. On the **Modify Restriction Settings** wizard, clear the following options:
  - Allow documents from managed apps to unmapped apps
  - Allow documents from unmapped apps to managed apps
10. Click **Save** to assign the configuration to an iOS device.

### **Task Result:**

This configuration does not allow users to open documents from Dropbox site through Safari browser. The *Open In* option displays Dropbox-EMM app or other managed apps.

## **Verification**

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

1. Register the device to core.
2. Open Dropbox for EMM application.
3. Observe the SAML SSO logs in sentry log file.
4. Login successfully to tenant from Dropbox for EMM application.
5. You must be unable to login to the tenant from other applications and browsers.



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.