



MobileIron Access Cookbook

Access with Dropbox Business and Microsoft ADFS

Revised: November 02, 2017



Contents

Overview.....	3
Prerequisites.....	3
Configuring Dropbox-EMM and Microsoft ADFS with MobileIron Access	4
Configure Access to Create a Federated Pair	4
Configure the ADFS environment with MobileIron Access	5
Configure the Dropbox-EMM environment with MobileIron Access	8
Send Token to Dropbox-EMM app from Core.....	9
Configure Core to Apply App Restrictions	10
Register Sentry to Access	11
Verification	11



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 Microsoft ADFS for authentication. The user gets authentication from ADFS 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 ADFS as an authentication provider with Dropbox-EMM in a cloud environment.

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 ADFS in your environment.
- ADFS version 3.0
- **ADFS (IDP) Metadata Files**
You must download the ADFS metadata files for ADFS (IdP)
 - Download ADFS metadata file from <https://<ADFS Server FQDN>/FederationMetadata/2007-06/FederationMetadata.xml>
- **Dropbox Business (SP) Metadata Files**
 - **Entity ID:** https://www.dropbox.com/saml_login
 - **Assertion Consumer Service URL:** https://www.dropbox.com/saml_login



Configuring Dropbox-EMM and Microsoft ADFS with MobileIron Access

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

- [Configure Access to Create a Federated Pair](#)
- [Configure the ADFS environment with MobileIron Access](#)
- [Configure the Dropbox-EMM environment 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 **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
 - Assertion Consumer Service URL: 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 **Microsoft** 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, Add Metadata, or Metadata URL to provide the **IdP metadata** details that you saved. See [Prerequisites](#).
See <https://support.mobileiron.com/docs/curent/accs> for more information.
Click **Done**.



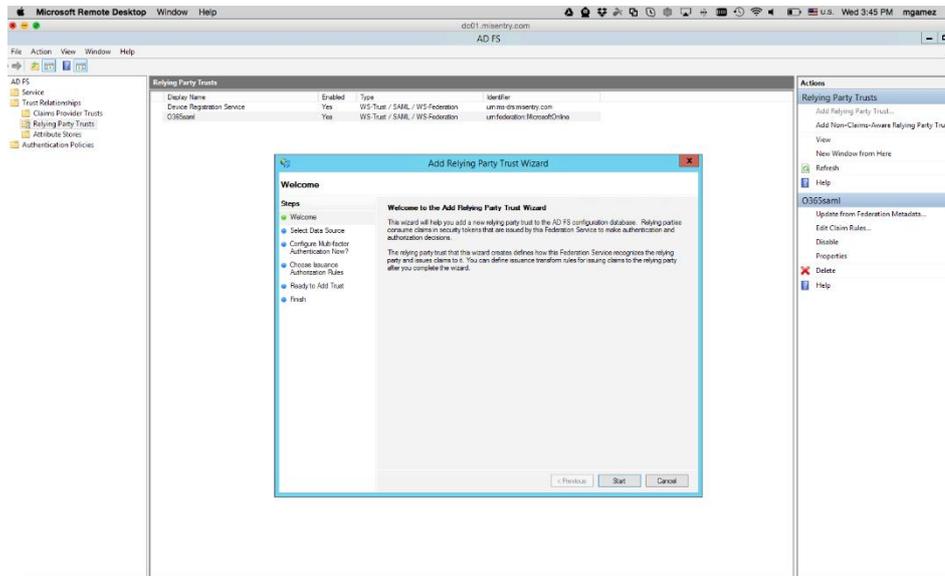
9. Download the **Access SP Metadata (Upload to IDP)** and **ACCESS IDP Metadata (Upload to SP)** metadata files.
10. Click **Publish** to publish the profile.

Configure the ADFS 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.

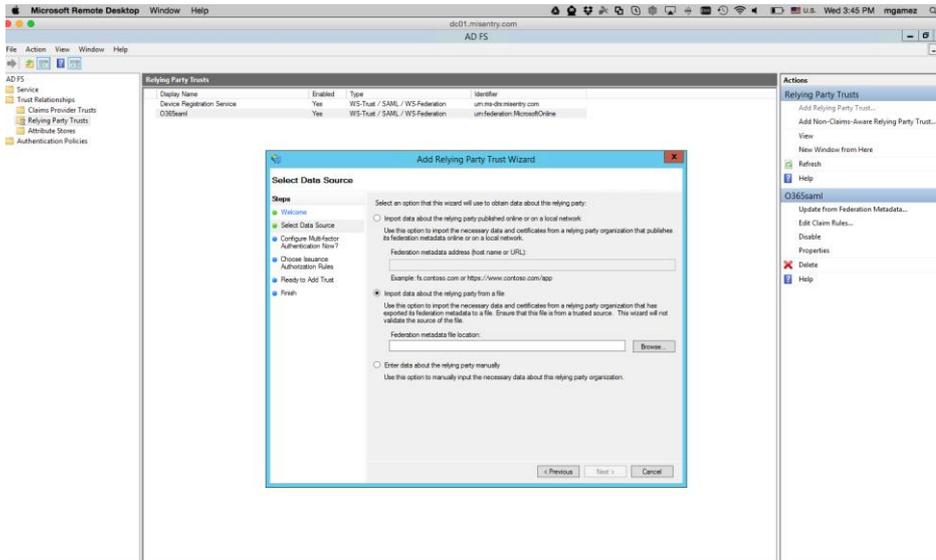
Procedure

1. Use Remote Desktop services to log into an ADFS machine with Admin credentials.
2. Click **Start > Administrative tools > ADFS Management > Expand Trust Relationships**.
3. Click **Relying Party Trust**. In the right-hand pane, under the **Actions** section click **Add Relying Party Trust** and follow the prompts.



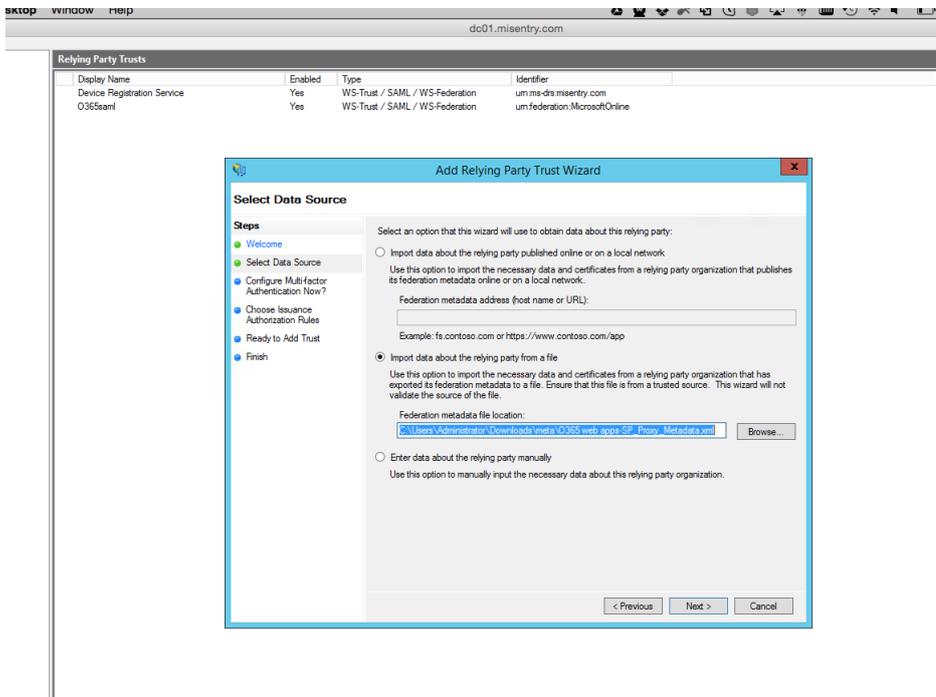


- Click **Start** and select **Import data about the relying party from a file**. Click **Next**.



- Click **Browse** and select the service provider metadata file that you downloaded and click **Next**.

Note: The filename for the proxy metadata file name ends with *UploadTo-Microsoft ADFS-IdP.xml*.



- Enter the **Display Name** and click **Next**.
All other fields are set to defaults. Follow the prompts.
- At the end, select **Open Edit Claim rules dialog for relying party trust**.
- Select SHA01 for encrypted algorithm.
- In the **Claim Rule Template** drop-down, select **Send LDAP Attributes as Claims** and click **Next**.



10. Configure **Claim rules** as follows:

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name:
email LDAP Query

Rule template: Send LDAP Attributes as Claims

Attribute store:
Active Directory

Mapping of LDAP attributes to outgoing claim types:

LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
E-Mail-Addresses	E-Mail Address
*	

11. Add another Claim Rule.

Select Rule Template

Steps

- Choose Rule Type
- Configure Claim Rule

Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.

Claim rule template:

Transform an Incoming Claim

Claim rule template description:

Using the Transform an Incoming Claim rule template you can select an incoming claim, change its claim type, and optionally change its claim value. For example, you can use this rule template to create a rule that will send a role claim with the same claim value of an incoming group claim. You can also use this rule to send a group claim with a claim value of "Purchasers" when there is an incoming group claim with a value of "Admins". Multiple claims with the same claim type may be emitted from this rule. Sources of incoming claims vary based on the rules being edited. For more information on the sources of incoming claims, click Help.



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:

Description:

BundleId:

File:

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:

Description:

EMAIL DOMAINS

No records to display

WEB DOMAINS

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

Buttons: Add+, 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.

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.

Verification

Single-sign-on service is now configured using SAML with Dropbox-EMM as the service provider and Microsoft ADFS 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 - 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.