

MobileIron Access Cookbook

Access with G Suite and Azure AD

01/02/2018

Contents

Overview	3
Prerequisites	3
Configuring G Suite and Azure AD with MobileIron Access	8
Registering Sentry to Access	8
Configuring Access to create a Federated Pair	8
Configuring G Suite with MobileIron Access	10
Configuring Azure AD with MobileIron Access	11
Verification	12

Overview

SAML provides single sign-on service for users accessing their services hosted in a cloud environment. Generally, a service provider such as G Suite 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 G Suite. This guide serves as step-by-step configuration manual for users using Azure AD as an authentication provider with G Suite 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 G Suite and Azure AD pair without MobileIron Access.
2. Ensure that you verify the configuration at <https://support.onelogin.com/hc/en-us/articles/201173424-Configuring-SAML-for-G-Suite>
3. **Metadata files and configuration for Azure AD**

Metadata files for Azure AD:

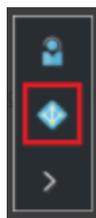
Entity ID: <https://sts.windows.net>

Post SSO URL: <https://login.microsoftonline.com/>

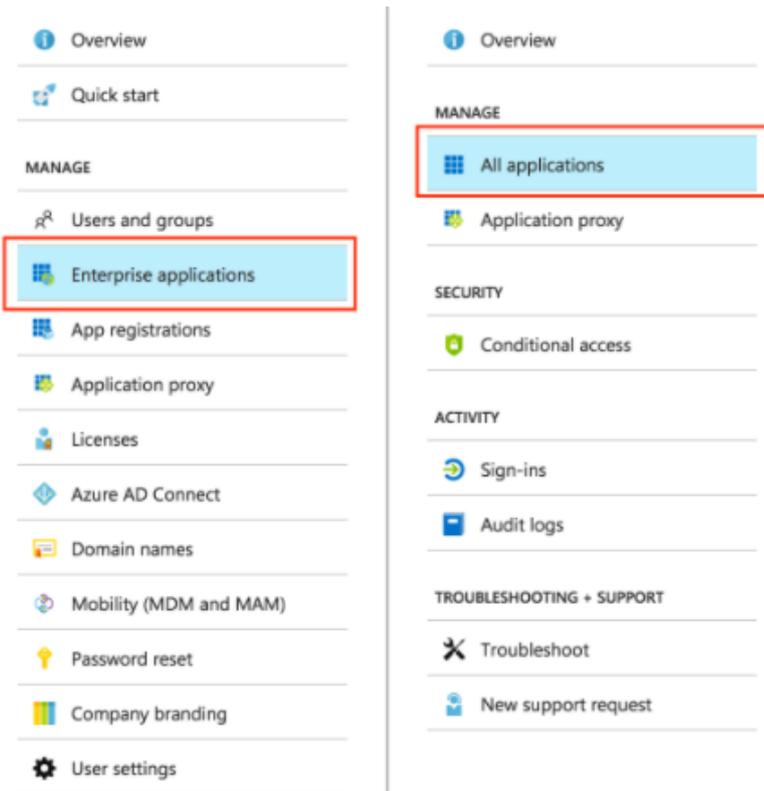
Redirect SSO Url: <https://login.microsoftonline.com/>

Configuration for Azure AD

- a) Login to Azure portal with admin credentials.
- b) On the left navigation pane, click **Azure Active Directory** icon.



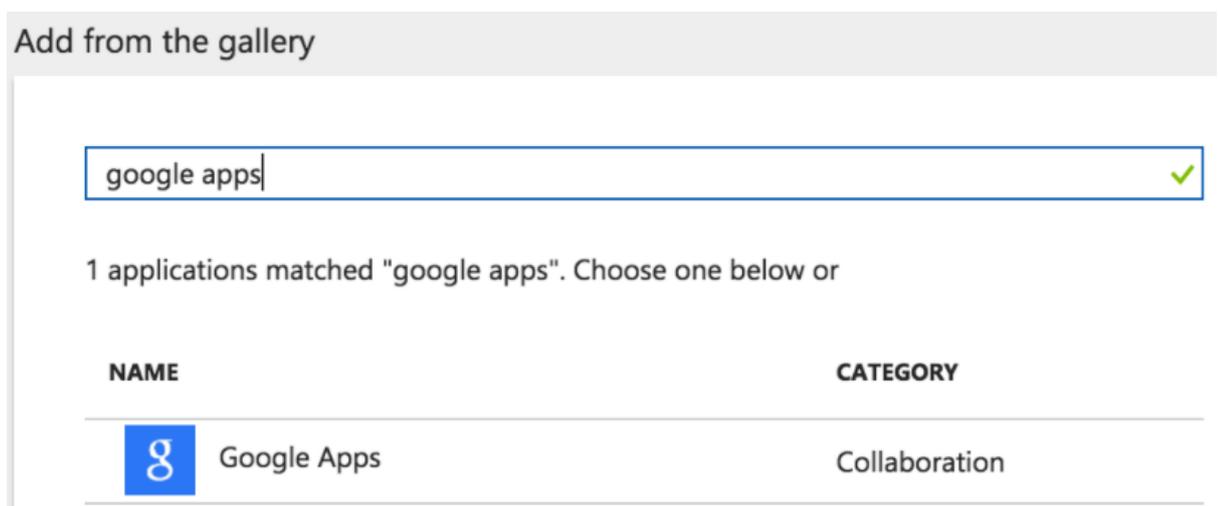
- c) Navigate to **Enterprise application > All Applications**.



d) On top of the window, click **New application**.



e) In the **Search** box, type **Google Apps**.



f) In the results panel, select **Google Apps** and click **Add**.

Google

Use Microsoft Azure AD to enable user access to Google Apps.
Requires an existing Google Apps subscription.

Name 

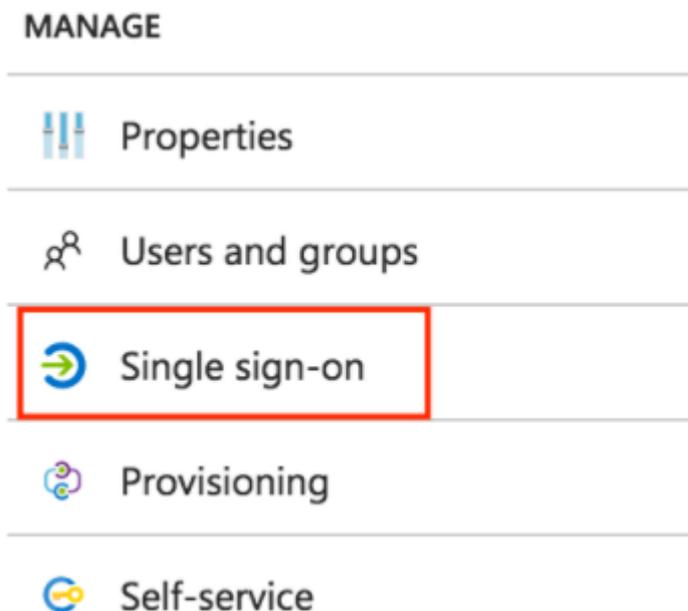
Publisher 
Google

URL 
[http://www.google.com/enterprise/apps/business,](http://www.google.com/enterprise/apps/business)

Logo 


[Add](#)

g) On the Google Apps application integration page, click **Single sign-on**.



h) On the Single sign-on dialog, select **Mode as SAML-based Sign-on** to enable single sign-on.



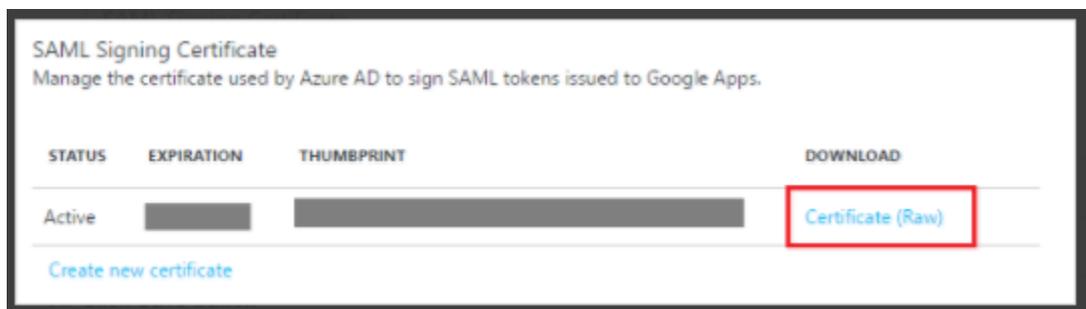
- i) On the **Google Apps Domain and URLs** section, enter the following details:

Google Apps Domain and URLs
Input the URLs and other details about your Google Apps tenant into Azure AD.

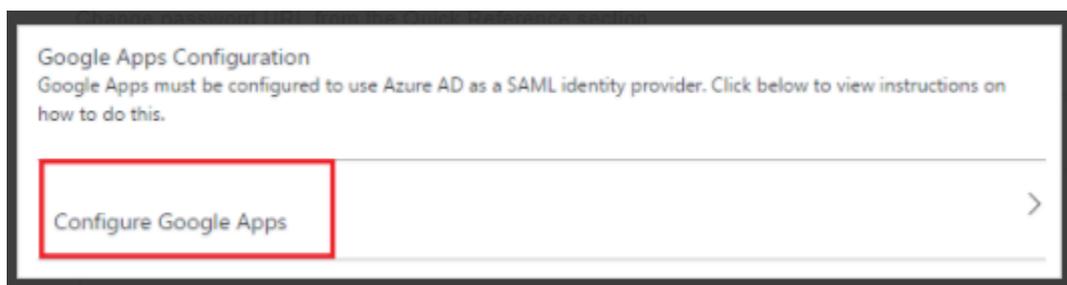
* Sign on URL

* Identifier

- j) On the **SAML Signing Certificate** section, click **Certificate** and then save the certificate on your computer. Click **Save**.



- k) On the **Google Apps Configuration** section, click **Configure Google Apps** to open Configure sign-on window.
Copy the **Sign-Out URL**, **SAML Single Sign-On Service URL** and **Change password URL** from the Quick Reference section.



4. Metadata files and configuration for G Suite:

Metadata for G Suite:

Entity ID: https://docs.google.com/a/<domain_name>

Assertion Consumer Service URL: https://www.google.com/a/domain_name/acs

Configuration for G Suite

1. Login to G Suite admin console.
2. Click **Security** > **Set up single sign-on (SSO)**.

3. Click Setup SSO with third party identity provider.
4. Enter the following information:
 - **Sign-in page URL:** <https://login.windows.net/>
 - **Sign-out page URL:** <https://login.windows.net/>
 - **Change password URL:**
<https://account.activedirectory.windowsazure.com/changepassword>

NOTE: The Change password URL field can be left empty

^ Set up single sign-on (SSO)

SAML-based Single Sign-On allows you to authenticate accounts for web based applications (like Gmail or Calendar). With SSO, users sign in for one web application, and are automatically signed in for all other Google web apps. For desktop applications (or POP access to Gmail), users must sign in directly with the username and password set up via the Admin console. ?

Setup SSO with third party identity provider

To setup third party as your identity provider, please provide the information below. ?

Sign-in page URL	https://login.windows.net/
	URL for signing in to your system and Google Apps
Sign-out page URL	https://login.windows.net/
	URL for redirecting users to when they sign out
Change password URL	https://account.activedirectory.windowsazure.com/changepassword
	URL to let users change their password in your system; when defined here, this is shown even when Single Sign-on is not enabled
Verification certificate	A certificate file has been uploaded. Replace certificate
	The certificate file must contain the public key for Google to verify sign-in requests. ?

Use a domain specific issuer ?

Network masks

Network masks determine which addresses will be effected by single sign-on. If no masks are specified, SSO functionality will be applied to the entire network. Use a semicolon to separate the masks. Example: (64.233.187.99/8; 72.14.0.0/16). For ranges, use a [bracket] network masks must end with a CIDR. ?

5. Click **Save Changes**.

Configuring G Suite and Azure AD with MobileIron Access

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

- [Registering Sentry to Access](#)
- [Configuring Access to create a Federated Pair](#)
- [Configuring G Suite 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 G Suite 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 **G Suite** 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 **Add Metadata** and enter the entity ID and Assertion consumer Service URL:
Entity ID: https://docs.google.com/a/<domain_name>
Assertion Consumer Service URL:
https://www.google.com/a/domain_name/acs
 - 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 IdP metadata file that you downloaded. See [Prerequisites](#). Click **Done**.

Identity Provider Metadata

Use the Help link for instructions on getting your Identity Provider metadata

Upload Metadata Add Metadata

Entity ID

<https://sts.windows.net/>

Post SSO URL

<https://login.microsoftonline.com/>/saml

Redirect SSO URL

<https://login.microsoftonline.com/>/saml

For the Base64 Encoded cert, extract the certificate downloaded from the SAML Signing Certificate in Azure portal. Run the following commands in a terminal:
`$openssl x509 -inform der -in certificate.cer -out certificate.pem`
`$vi certificate.pem` and copy certificate and paste it in the Base64 Encoded field

Base64 Encoded Cert

```
MIIC8DCCAdigAwIBAgIQEmLM2PB+NpZE2IGaGpTStzANBgqhkiG9w0BAQsFADA0
MTIwMAYDVQQDEylNaWNyb3NvZnQgQXp1cmUgRmVhZG9wYXN0eS0wDQYJKoZIhvcNAQEL
Y2F0ZTAeFw0xNzA4MTcwODU4MTVaFw0yMDA4MTcwODU4MTVaMDQxMjAwBgNVBAMT
KU1pY3Jvc29mdCBBenVzZSBGZWRIcmF0ZWQgU1NPIENlcnRpZmljYXRIMiBljAN
BgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAmH/H8bWwvOv5oeKS25nAQ3Lb47Y6
0SSRT98j8SLPOHcaUFHWBz3nOn/1VIW1xG5jn0uY7WcuGYWS0Ez2qkFg7zNuXAKL
lhJ3V6YUPhSKi1ZERrTo5K4BOuh+1LXrbNKoViysl+lojgm6MK5C9WDXtUHOgr2T
DSJzNLwptS8tfvizZOqJ00lbsPNjHu5eoqMmfDqjSm4l+MGDDOXhr8NutF1fJTW0
```

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 G Suite with MobileIron Access

You must configure G Suite to use with Access.

Prerequisites

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

Procedure

1. Login to the G Suite domain with admin credentials.
2. Click **Security**, and select **Single Sign-On Settings**.
3. Upload the “**Access IDP Metadata (Upload to SP)**” downloaded in **Step 10** of [Configuring Access to create a Federated Pair](#).
4. Extract the Sign-in page URL from Access IDP Metadata (Upload to SP).

```

<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" entityID="https://[redacted]
.com/MobileIron/acc/0998aa5b-3e2c-429f-a599-960b273c629c/idp">
  <md:IDPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <md:KeyDescriptor use="signing">
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>
          <ds:X509Certificate>MIIDazCCA10gAwIBAgIFAppA7e8wDQYJKoZIhvcNAQELBQAwZDZEUmBGA1UEAwLU2lnbmLuZ0NlcnQxE
          DA0BgNVBAsMB1N1cHBvcnQxEzARBgNVBAoMCK1vYmVsZUlyb24xZjAUBgNVBACMDU1vdW50YWluIFZpZCcxZzZxczEzARBgNVBAgMCKNhbg
          lmb3JuaWExCzAJBgNVBAYTALVTMB4XDTE3MDgyMjA1NTgwMloXDTE3MDgyMjA1NTgwMlowdW50YWluIFZpZCcxZzZxczEzARBgNVBAgMCKNh
          bG1mb3JuaWExCzAJBgNVBAYTALVTMIIIBIjANBgkqhkiG9w0BAQEFAAQCAQ8AMIIBcGKCAQEAgj5Y1IVKKQVCiIEDDtifNeyr1FJGj1
          GwJqRkNrwTwcZDuG+0vJWqUnrjUo7k4kieWwYX01HYePLrbjtVyyqG+8j08BrY8SYsdzHwX55agVfkeNCLwxXNvfeYB5HLMti/
          hmZ1f0I6FggN36pWkpyojUlokR0ZSioJLNAU/NXq8qhfK/VHfVzWricGpp0YptxFw6Y1tEMIIIfzXcl+xIhVpzvUTR1B/
          nzbq3LBUu5XgsRfBu6Tr0AuhEJYdesw5LT8rbUusu17WejyS0QXlXTofZgM+60ysyLPWyyZ4NC/
          NUSsgtWhsuwp942+RdNIvua0ij5fPNMu5lc53q+EXiG5AqwIDAQABMA0GCsqGS1b3DQEBCwUAA4IBAQA7rDDMTdNivw/
          6NS6zW8YoC/Z5ABh8rNLInowNUHMA0+SNZzgbBYFREgCSobXXic8BwydjwQCV4v4VNroMYgBxaYRueHqVquR0dC5Zva
          +pjMkdcxjexGvK6y3CLBMXNkvJLhRr5jKhJwWkQnyF8RkScjs9e
          +wL8d4jjVP1S0k7c7OhijlvbJQP83p0DAvL4zRtJEjux5HciKuVw6fouQu5t5yC30MA08FTP53Zac2ITFIIf/0yg0lcnUENiyBLZE
          +iT+G0w5R87pWSQ76THKeQiptJevAQcVSwVI4m9dEV0qBDCZve0B40AwqFBOEq9ao0w0G9UWlnB6uJLNEmKAHO</ds:
          X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </md:KeyDescriptor>
    <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://[redacted]
.com/MobileIron/acc/0998aa5b-3e2c-429f-a599-960b273c629c/idp"/>
    <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://[redacted]
.com/MobileIron/acc/0998aa5b-3e2c-429f-a599-960b273c629c/idp"/>
  </md:IDPSSODescriptor>
</md:EntityDescriptor>

```

5. Enter the following information from the certificate:
 - a. **Sign-in page URL:** <Entity ID from above screenshot>
 - b. **Sign-out page URL:** <Entity ID from above screenshot>
 - c. **Change password URL**
6. Click **Save**.

Task Result

G Suite 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 Google Apps application integration page, click **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](#).

* Sign on URL ⓘ

* Identifier ⓘ

Show advanced URL settings

Reply URL ⓘ

Relay State ⓘ

5. Click **Save**.

Verification

Login to G Suite using the test account and verify the redirection in Sentry logs. All the incoming and outbound SAML messages flow through Access Sentry.

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.