MobileIron Access Cookbook

Access with G Suite and Azure AD

01/02/2018

Contents

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

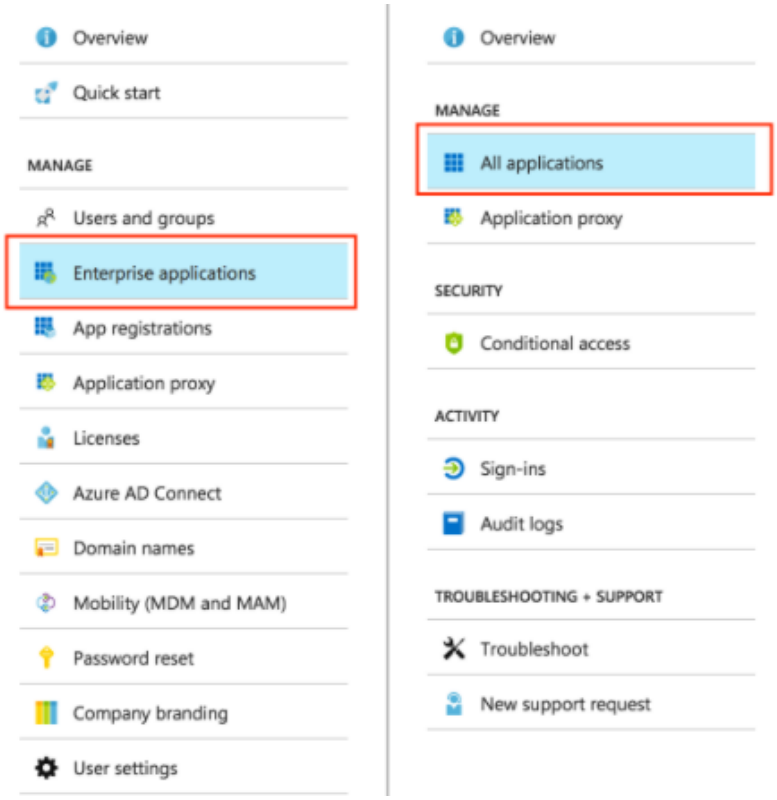
1. Ensure that you have a working setup of the G Suite and Azure AD pair without MobileIron Access.
2. Ensure that you verify the configuration at https://support.onelogin.com/hc/en-us/articles/201173424-Configuring-SAML-for-G-Suite

3. **Metadata files and configuration for Azure AD**

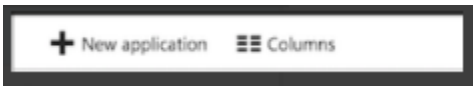
   Metadata files for Azure AD:
   Entity ID: https://sts.windows.net
   Post SSO URL: https://login.microsoftonline.com/
   Redirect SSO Url: https://login.microsoftonline.com/

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

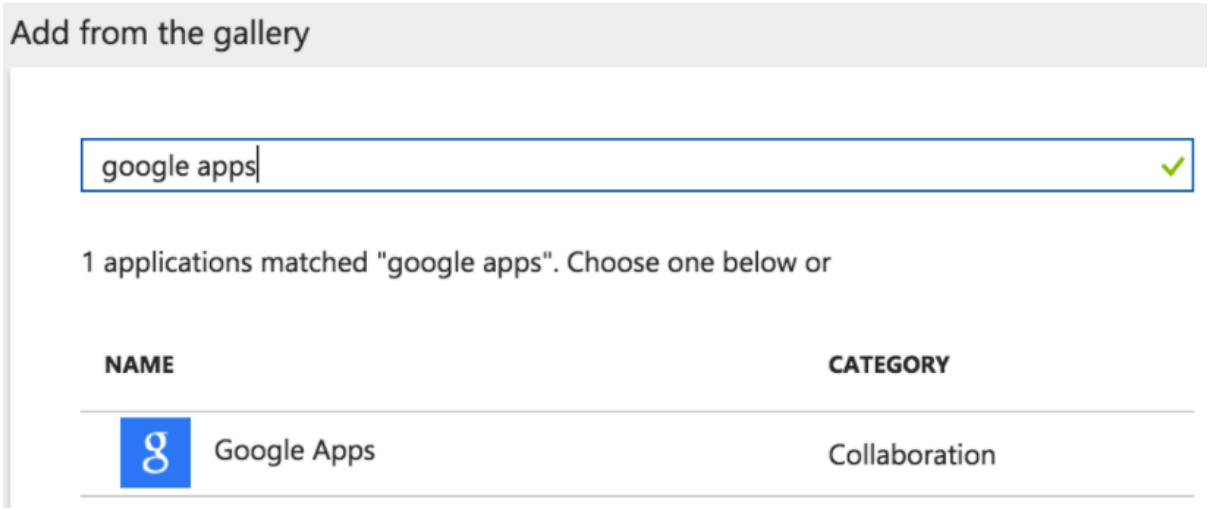
   c) Navigate to **Enterprise application** > **All Applications**.



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

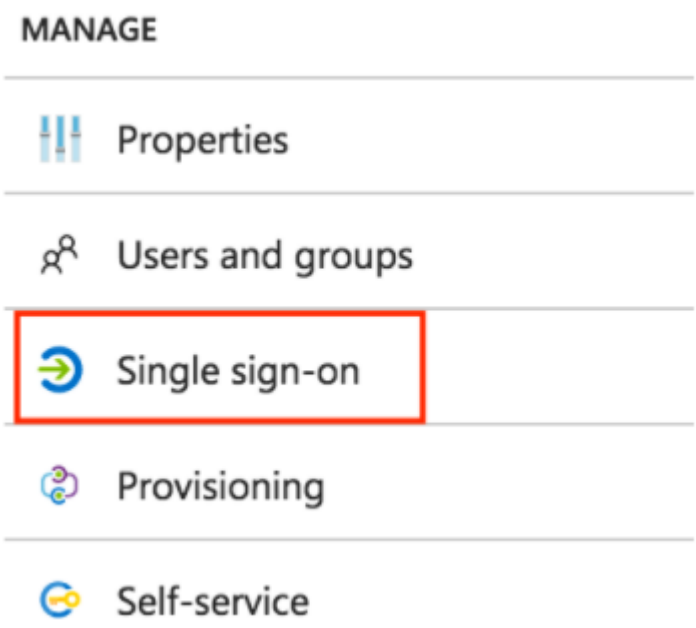


e) In the **Search** box, type **Google Apps**.



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

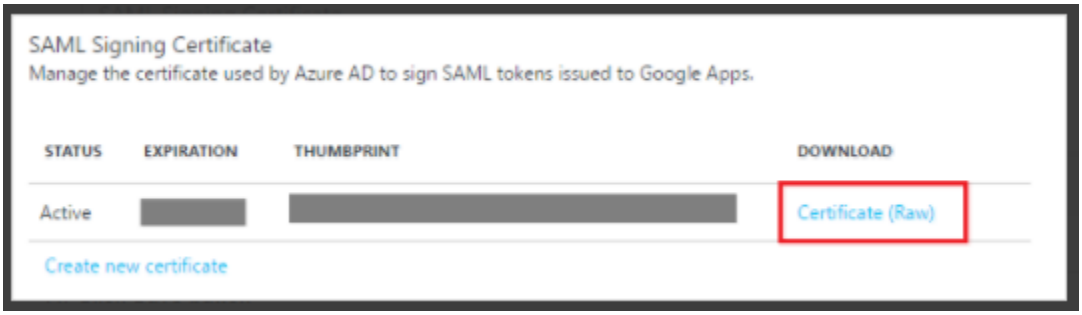
g) On the Google Apps application integration page, click **Single sign-on**.



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:

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:

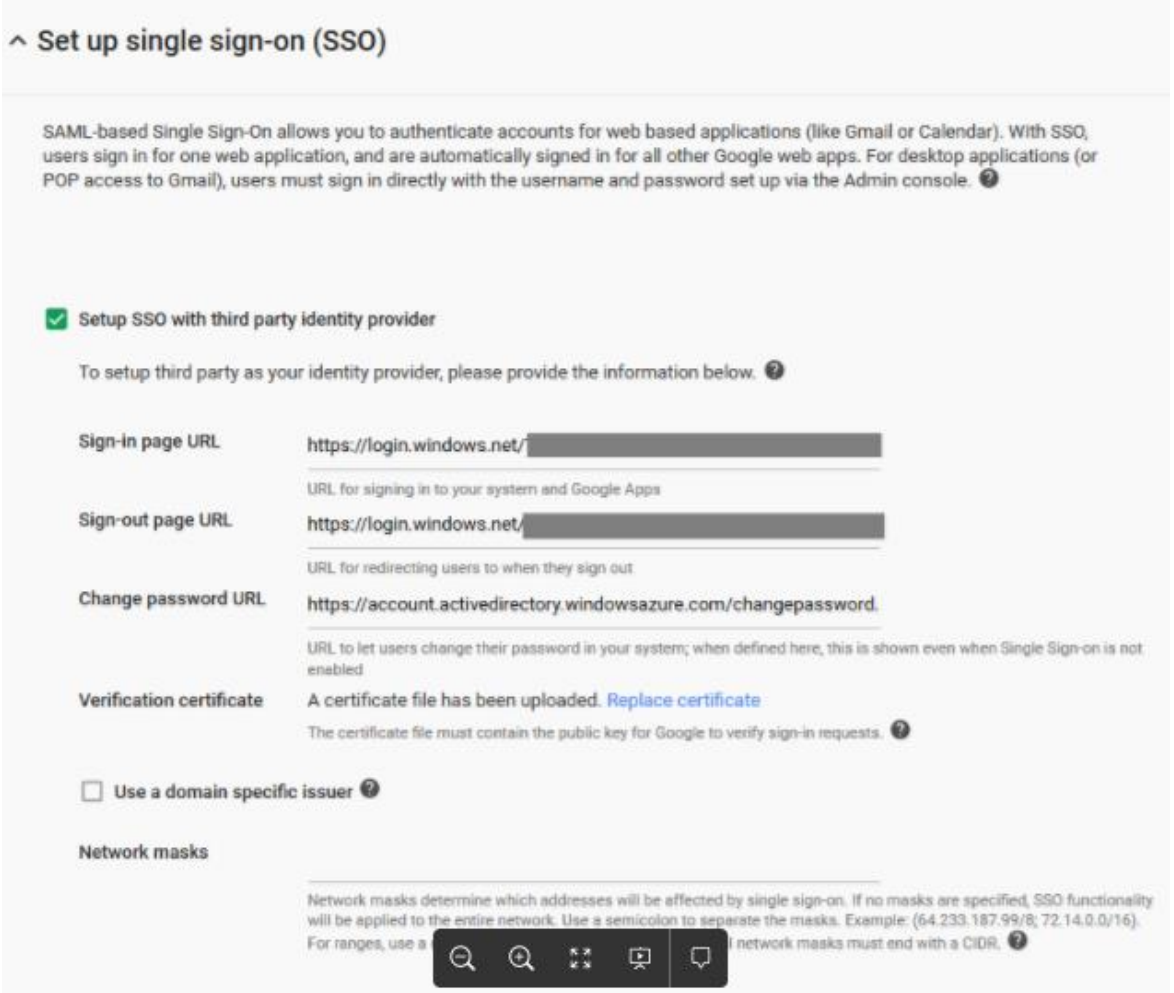
Entity ID: https://docs.google.com/a/<domain_name>
Assertion Consumer Service URL: https://www.google.com/a/domain_name/acs

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



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

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.

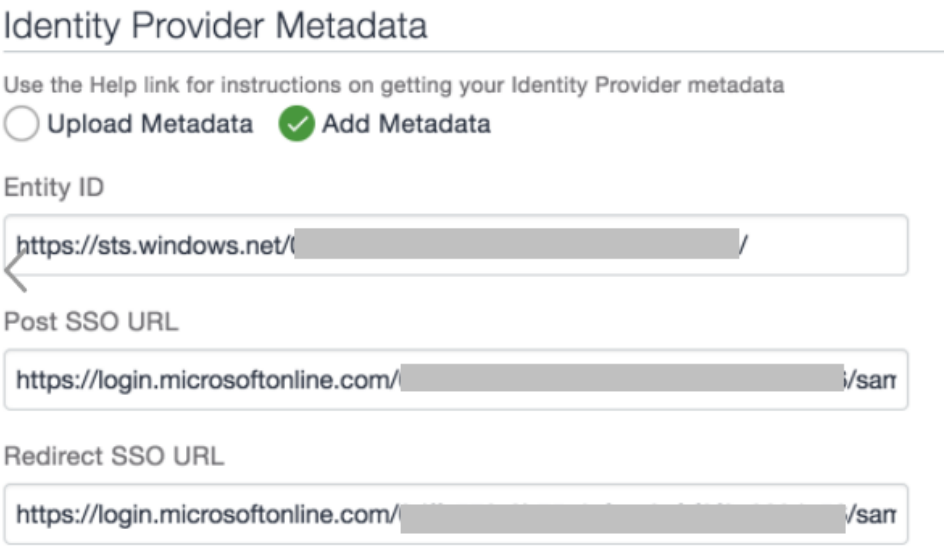
Prerequisites

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**.



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

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).

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**.

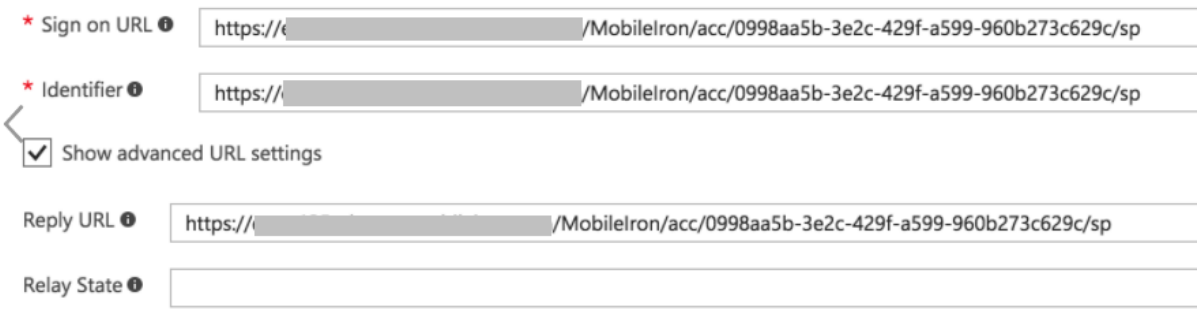
Task Result

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.



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.