MobileIron Access Cookbook

Access with G Suite and OneLogin

November 21, 2017

Contents

Overview

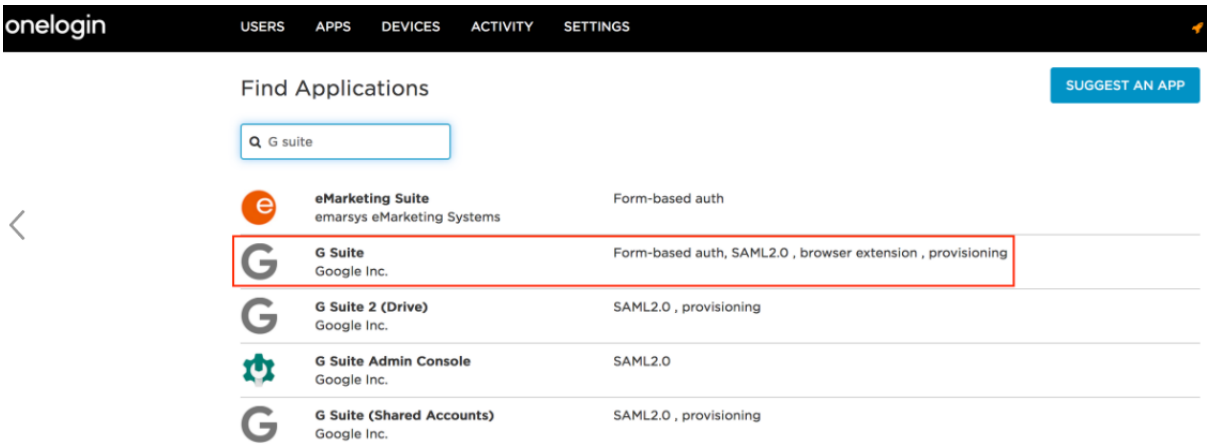
SAML provides single sign-on service for users accessing their services hosted in a cloud environment. Generally, a service provider such as G Suite is federated with an identity provider such as Onelogin for authentication. The user gets authenticated by Onelogin and obtains a SAML token for accessing applications in a cloud environment, such as G Suite. This guide serves as step-by-step configuration manual for users using Onelogin as an authentication provider with G Suite in a cloud environment.

Prerequisites

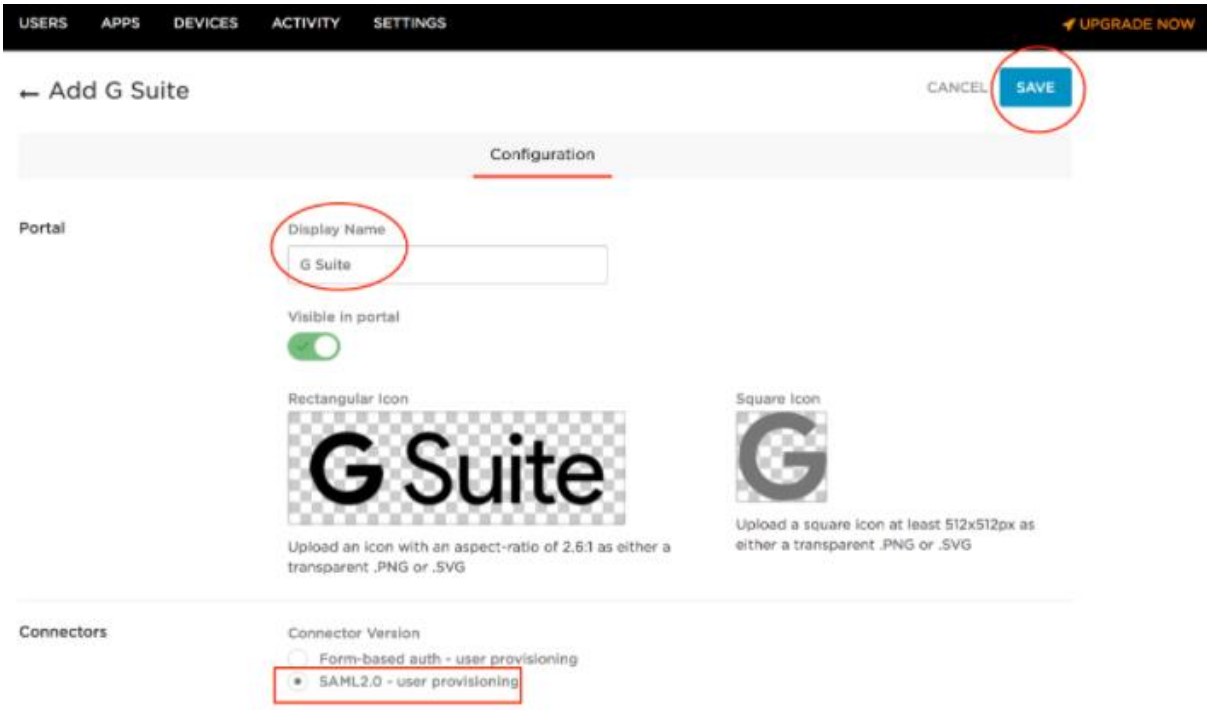
1. Ensure that you have a working setup of the G Suite and Onelogin pair without MobileIron Access.
2. Ensure that you verify the configuration at https://support.onelogin.com/hc/en-us/articles/201173424-Configuring-SAML-for-G-Suite

3. **Metadata files and configuration for Onelogin**

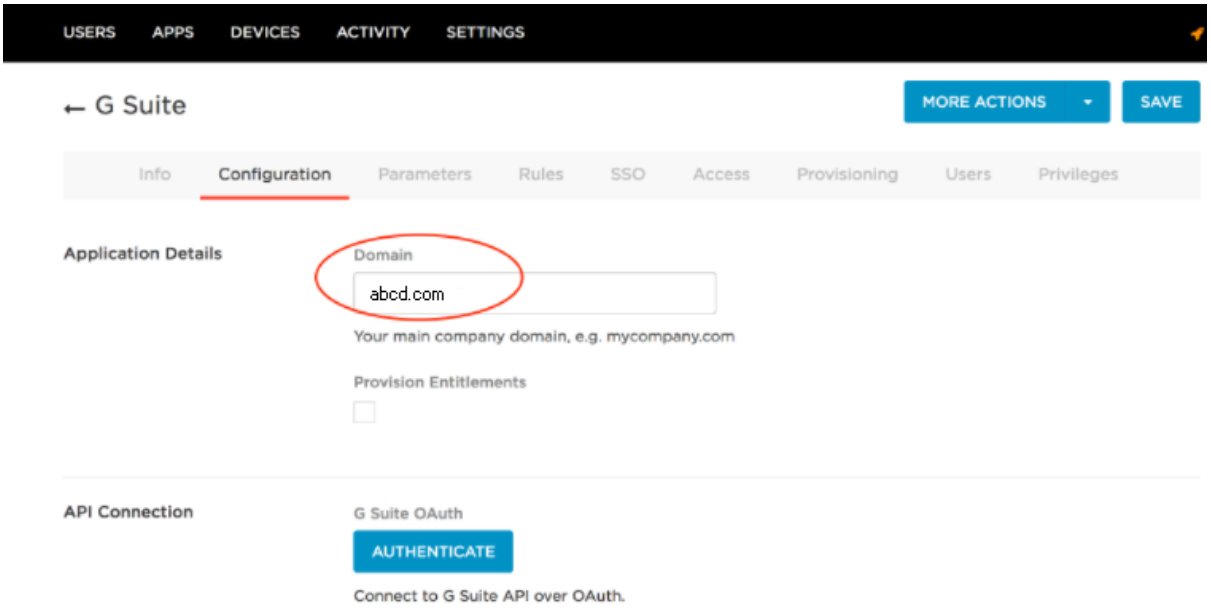
    1. Login to Onelogin tenant portal with admin credentials.
    2. Click **Apps** > **Add Apps**. Search for **G Suite** and select it.



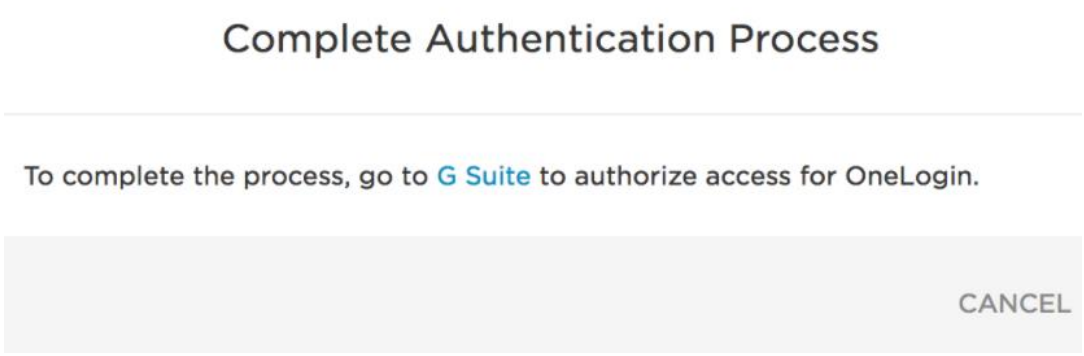
    3. On the **Add App** page > **Configuration** tab, select *SAML 2.0 – user provisioning*. Click **Save** to display additional configuration tabs.



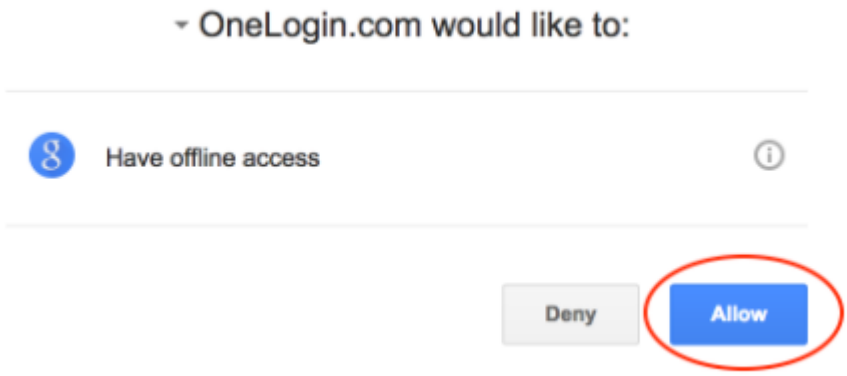
4. On the **Configuration** tab, enter the **G Suite** domain.



5. On the **Configuration** tab, authenticate to the G Suite API.
    a. On the **Configuration** tab, click **Authenticate**.
    b. On the **Complete Authentication Process** dialog, click the **G Suite** link.

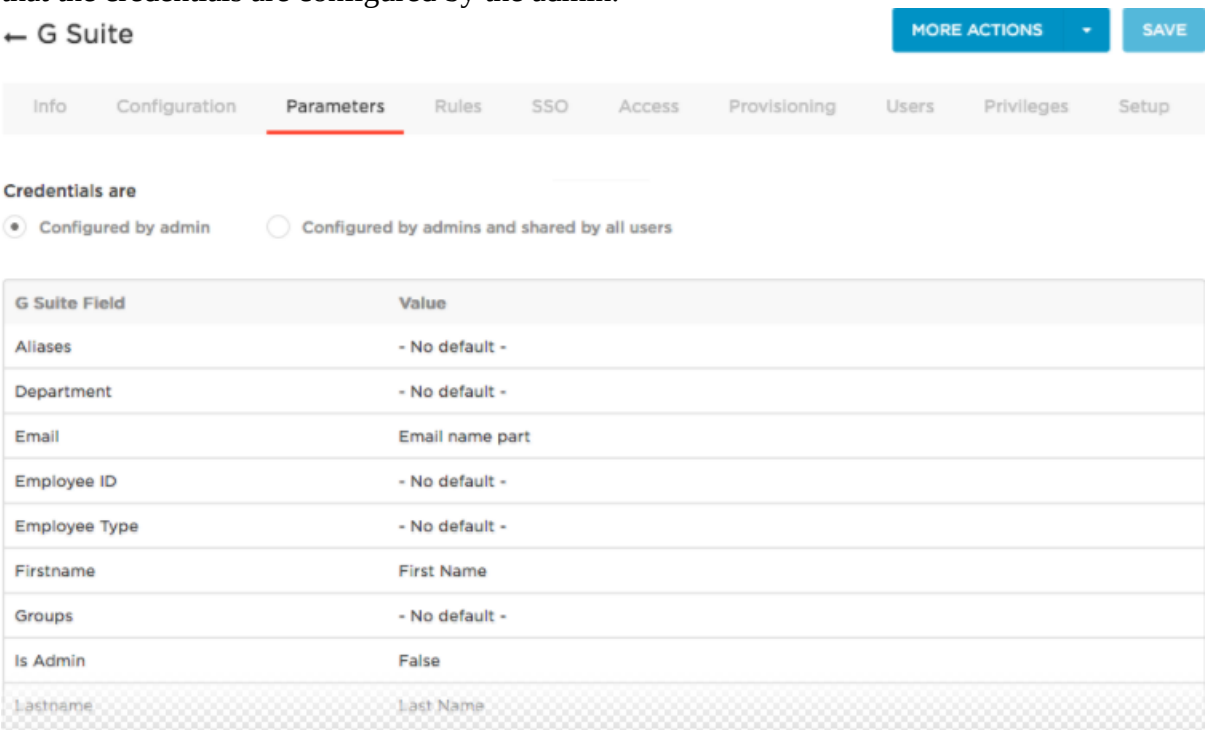


c. Click Allow on Google's Request Permission Page.

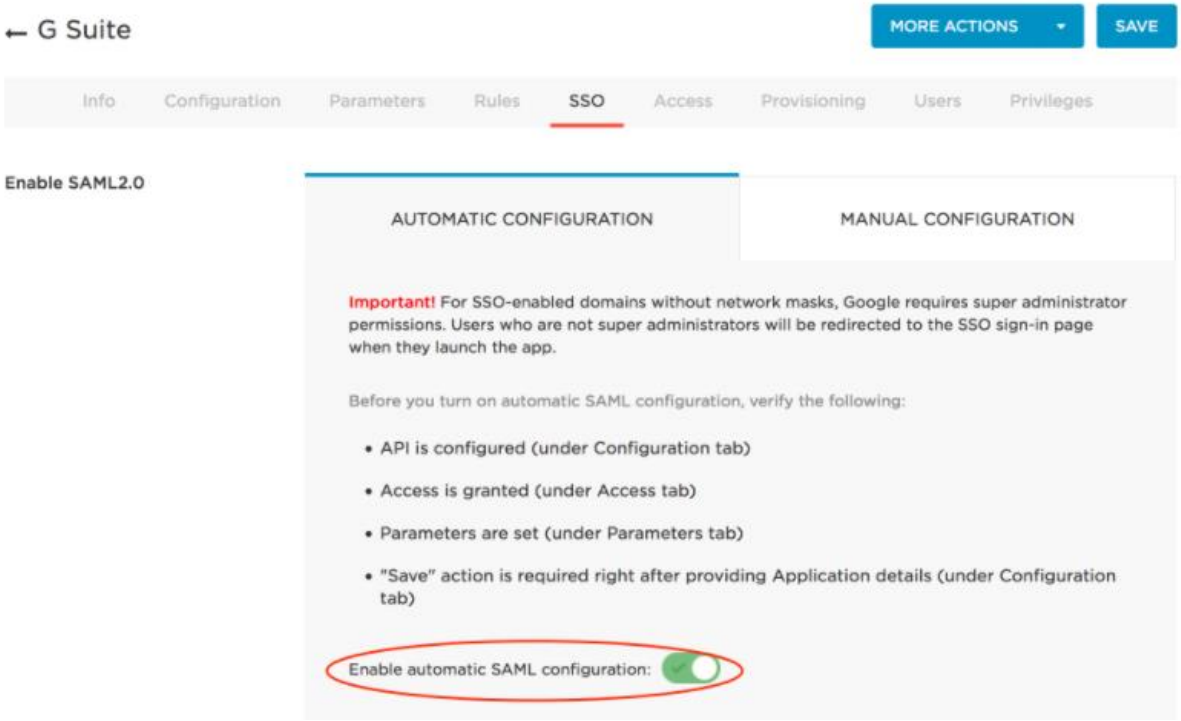


d. Onelogin returns to the G Suite app setup page and displays a brief message that the authorization was successful.

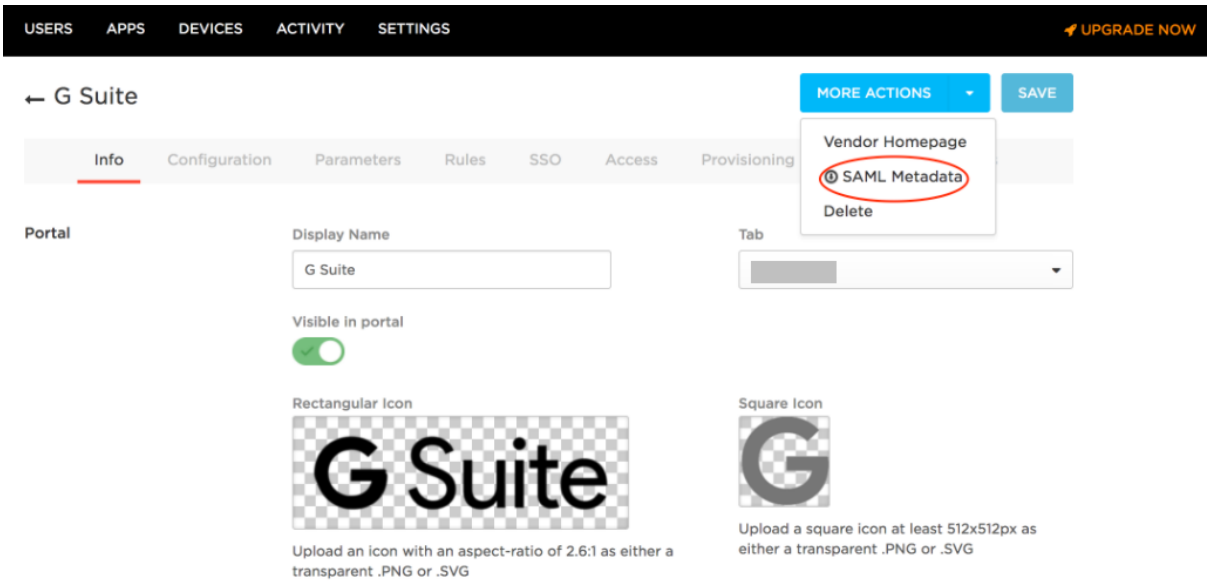
6. On the **Parameters** tab, map G Suite user attributes to Onelogin attributes. Verify that the credentials are configured by the admin.



7. Click **Save** to save the settings and enable the verification part of the SAML setup.
8. On the **SSO** tab, configure the SAML settings automatically.



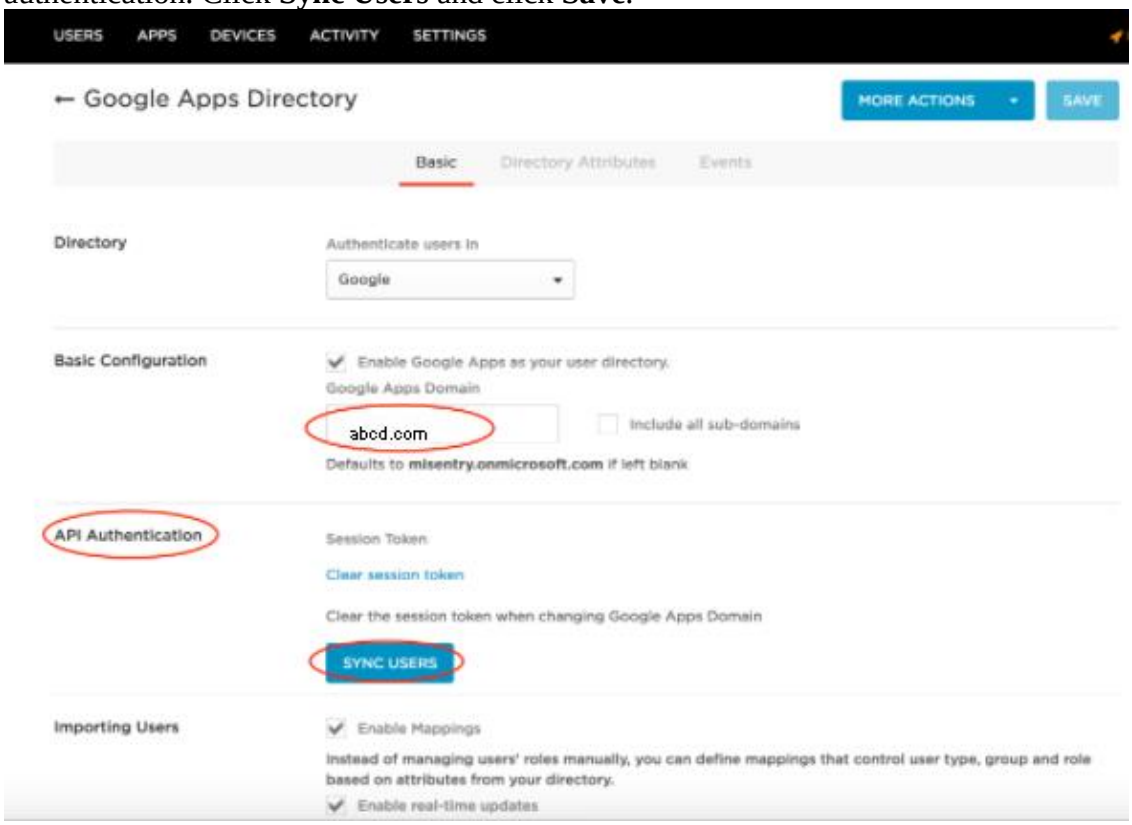
9. On the **Manual Configuration** sub-tab, copy the SAML 2.0 Endpoint (HTTP) URL and download the X.509 PEM Certificate.
   Note: To download the certificate, click **View Details** and select X.509 PEM from the drop-down list below X.509 Certificate field.
   * For a different certificate, click **Change** > select the new certificate and follow the above instructions.
   * To create new X.509 certificates, select **Settings** > **Certificates** > **New**.
10. Download the metadata file - Click **More Actions** > **SAML Metadata** > **Save** the file.



11. Importing Users from Google Directory

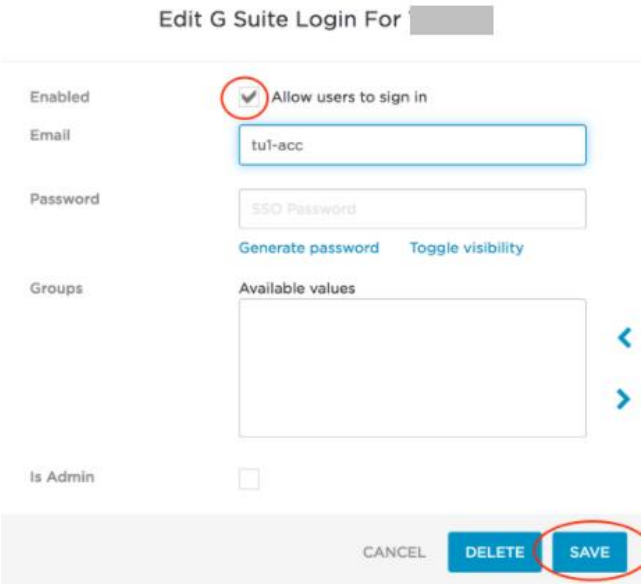
a. Click **User** > **All Users** > **Directory**.

b. Click **New Directory**.
Enter the domain information and click Authenticate for API authentication. Click **Sync Users** and click **Save**.



12. Click **User** > **All Users** > select the **User imported from Google Directory** > Click **Application** tab > select **G Suite** > **Continue**.
13. Click **Save**.
Note: If the Save button is grayed out, then deselect the *Enabled: Allow users to*

sign in option and select it again.



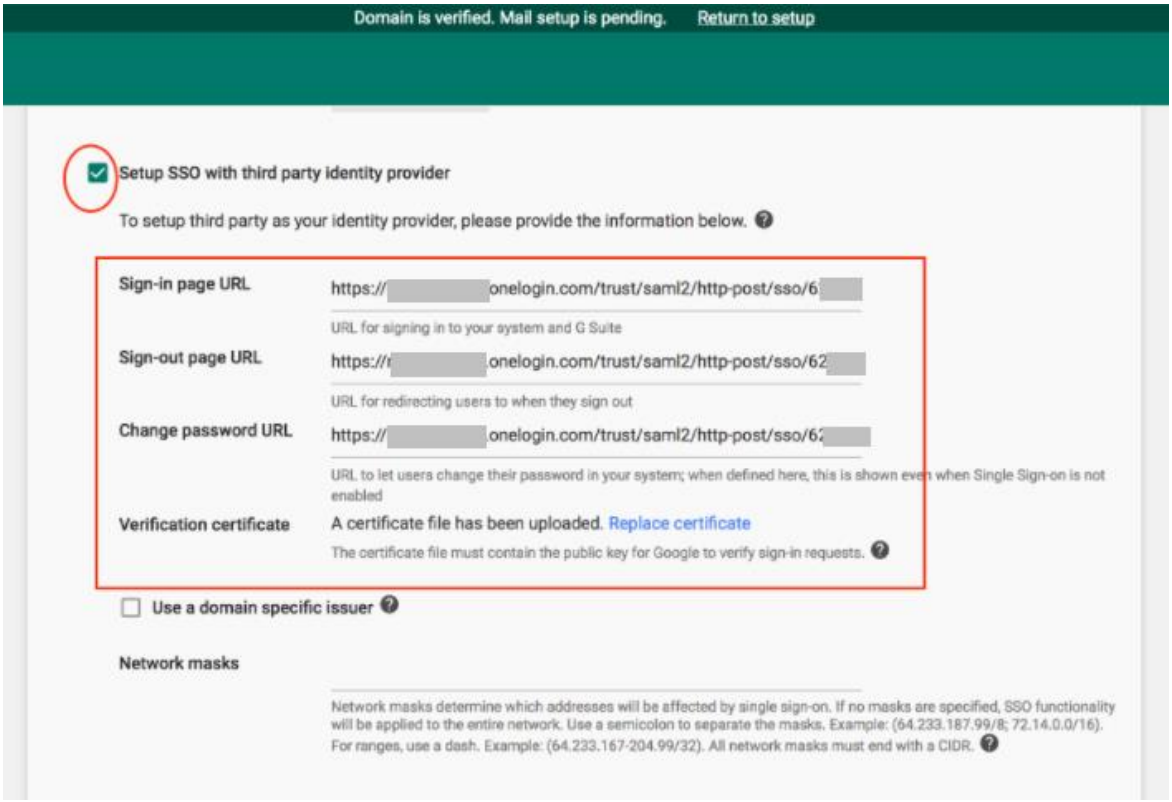
4. **Metadata files and configuration for G Suite**:

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:

1. Login to G Suite admin console.
2. Click **Security** > **Set up single sign-on** (SSO).
3. Upload the Onelogin X.509 PEM Certificate that you downloaded in Step 9 in the Metadata files for Onelogin section. See Prerequisites.
4. Click Setup SSO with third party identity provider.
5. Enter the following information:
   - **Sign-in page URL**: The SAML2.0 Endpoint (HTTP) URL that you copied from the Manual Configuration sub-tab in Onelogin in Step 9 in the above section.
   - **Sign-out page URL**: https://app.onelogin.com/client/apps
   - **Change password URL**: https://app.onelogin.com/password



6. Click **Save Changes**.

Verification: At this point, the SAML SSO should work fine between G Suite and Onelogin. Access G Suite services such as Google Drive or Google Docs from browser or applications on desktop or mobile devices.
Access to SPs must be successful.

Configuring G Suite and Onelogin with MobileIron Access

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

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 Onelogin 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
    You can also choose to **Upload Metadata** or select **Metadata URL** option to add metadata.
    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 **Onelogin** 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**.

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

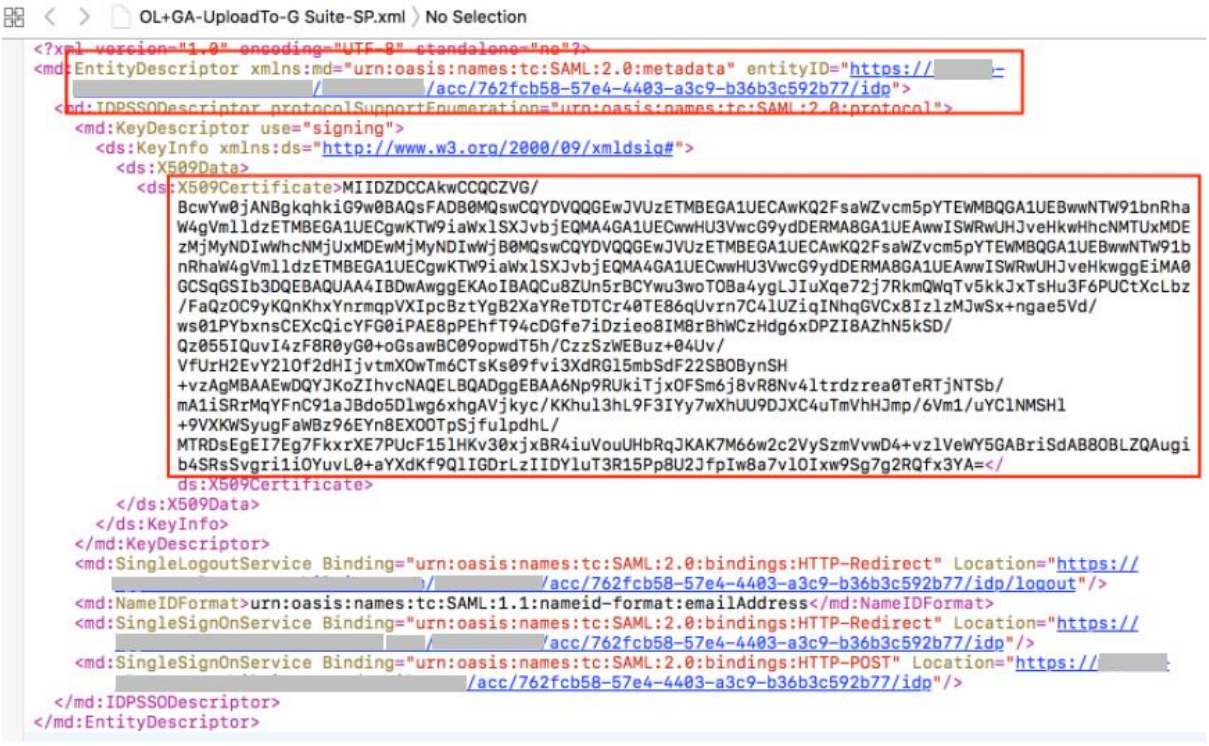
You must configure G Suite to use with Access.

Prerequisites

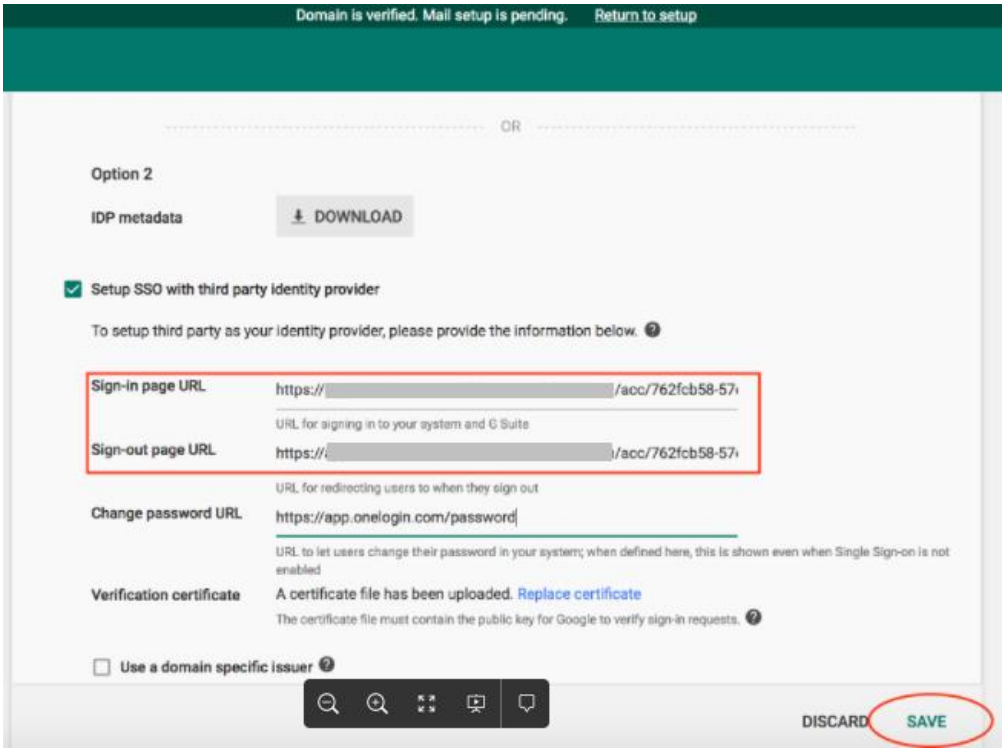
- Verify that you have created a federated pair with Google Suite and Onelogin.
- Verify that you have configured G Suite and Onelogin natively.

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)**" that you 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**: https://app.onelogin.com/password



6. Click Save.

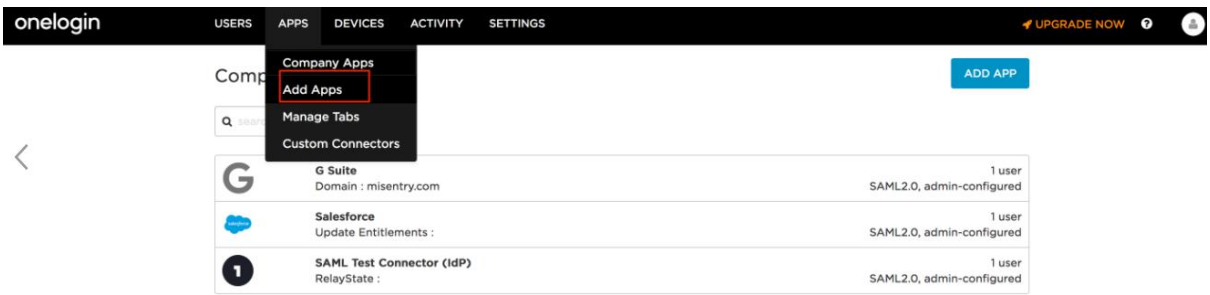
Task Result

G Suite is configured with Access.

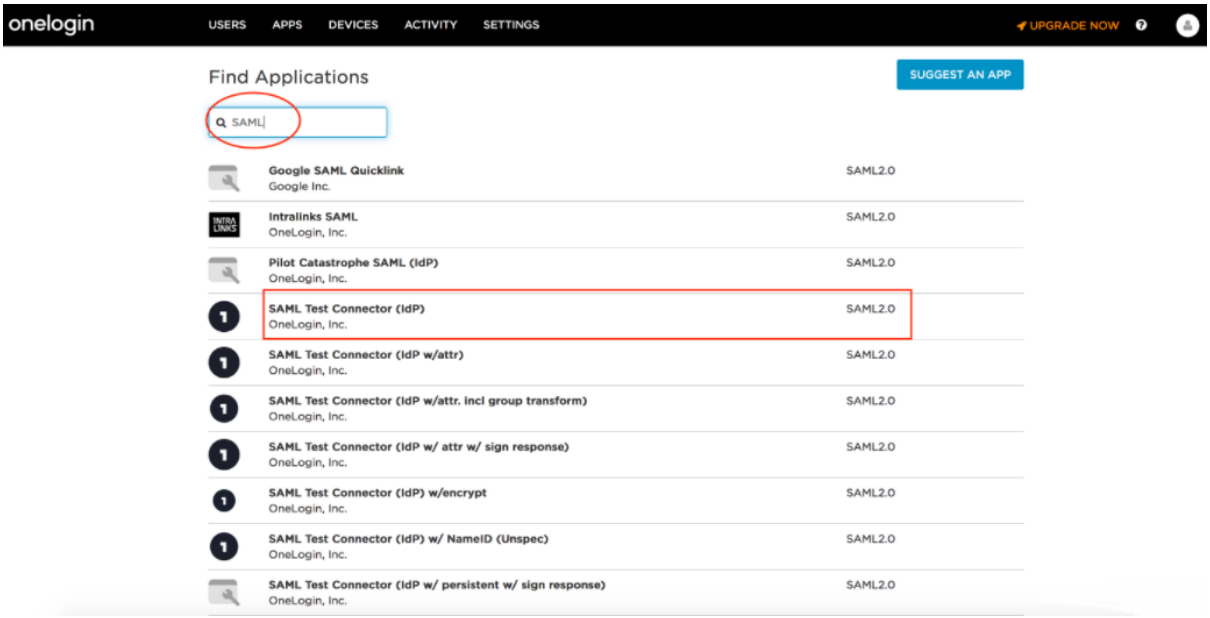
Configuring Onelogin with MobileIron Access

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

1. Login to Onelogin tenant portal with admin credentials and click Add Apps.

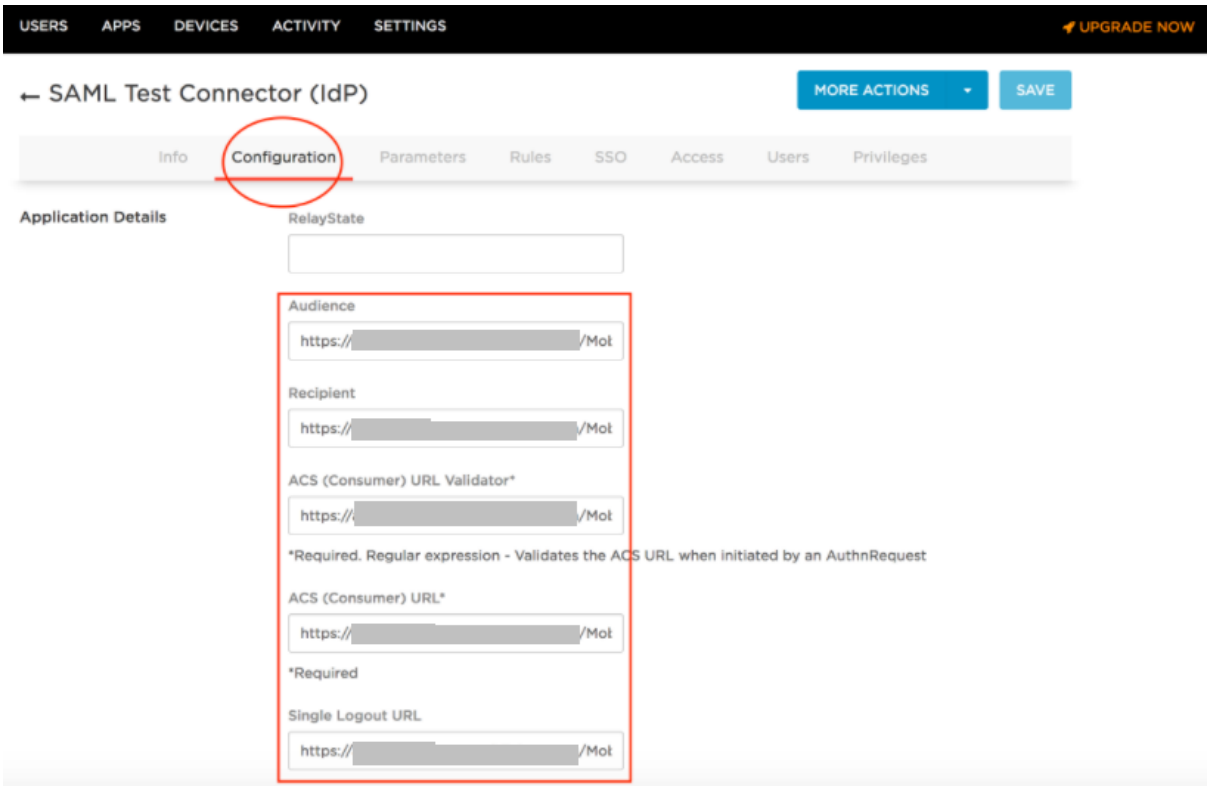


2. Search for SAML and select SAML Test Connector (IdP)

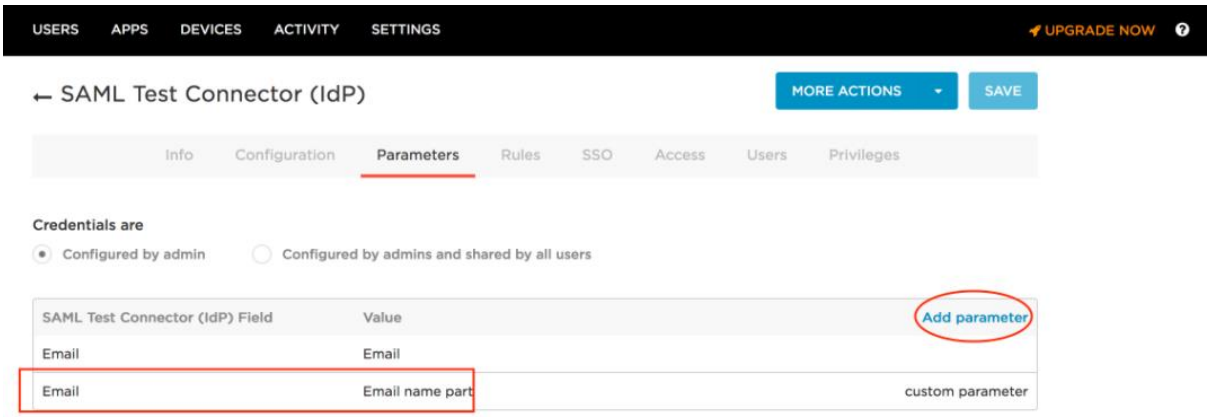


3. (Optional): Change the display name and click Save to enable other tabs.
4. On the configuration tab, enter the following information that is extracted from the Access SP Metadata (Upload to IDP) file from **Step 10** of Configuring Access to create a Federated Pair.

- Audience: <Entity ID of SP>
- Recipient: <Entity ID of SP>
- ACS (Consumer) URL Validator*: <Entity ID of SP>
- ACS (Consumer) URL*: <Entity ID of SP>
- Single Logout URL: <Entity ID of SP>



5. On the Parameters tab, Add custom parameter “Email” with value “Email Name Part”



6. Click **Save**.
7. Click **Users** > **All Users** > select the **User** and **Assign the Application**.
8. Click **Continue** and **Save**.

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.

Verification

Login to G Suite using the test account and verify the redirection in Sentry logs.