

MobileIron Access Cookbook

Access with G Suite and OneLogin

November 21, 2017

Contents

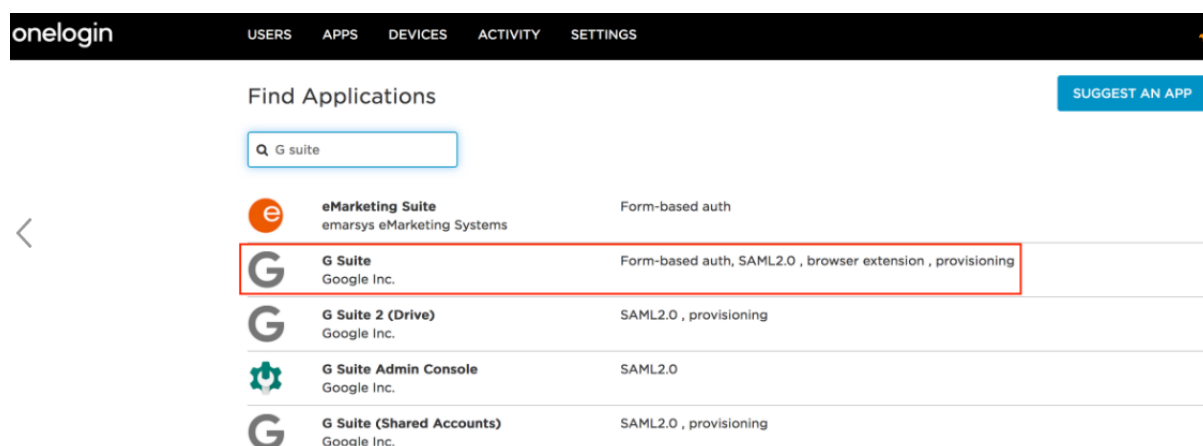
Overview	3
Prerequisites	3
Configuring G Suite and Onelogin with MobileIron Access.....	10
Configuring Access to create a Federated Pair	10
Configuring G Suite with MobileIron Access	11
Configuring Onelogin with MobileIron Access	12
Registering Sentry to Access	14
Verification	15

Overview

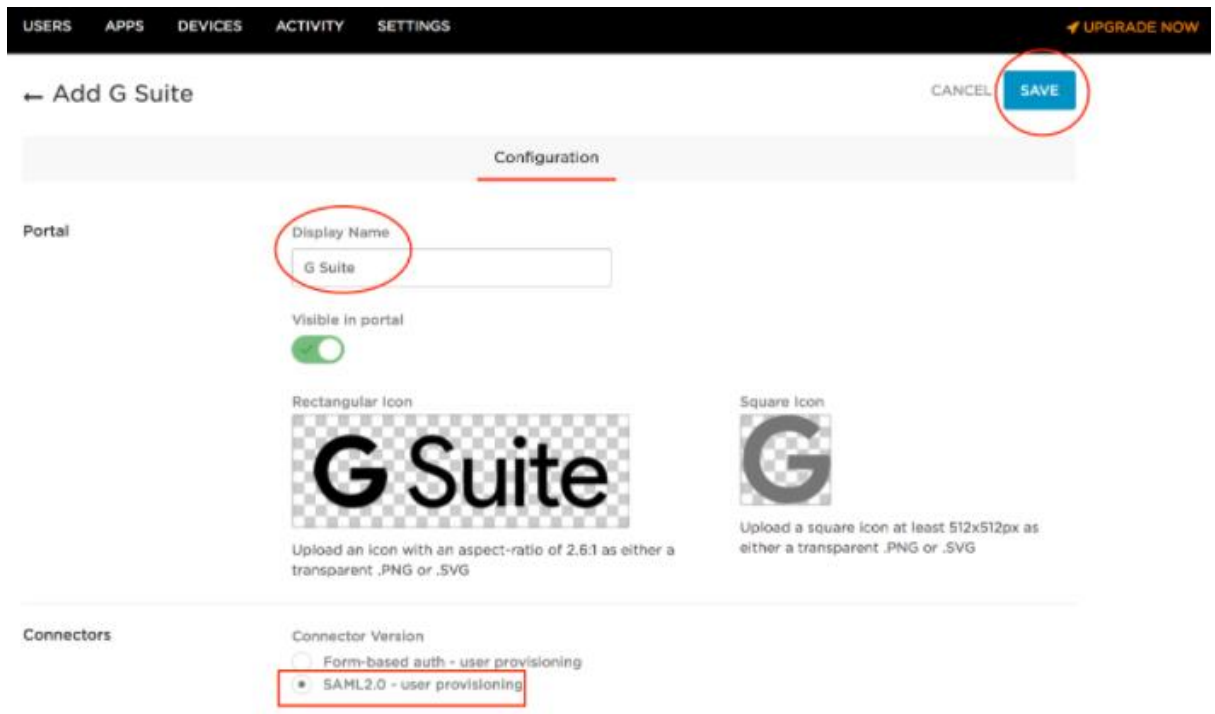
SAML provides single sign-on service for users accessing their services hosted in a cloud environment. Generally, a service provider such as G Suite is federated with an identity provider such as Onelogin for authentication. The user gets authenticated by Onelogin and obtains a SAML token for accessing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

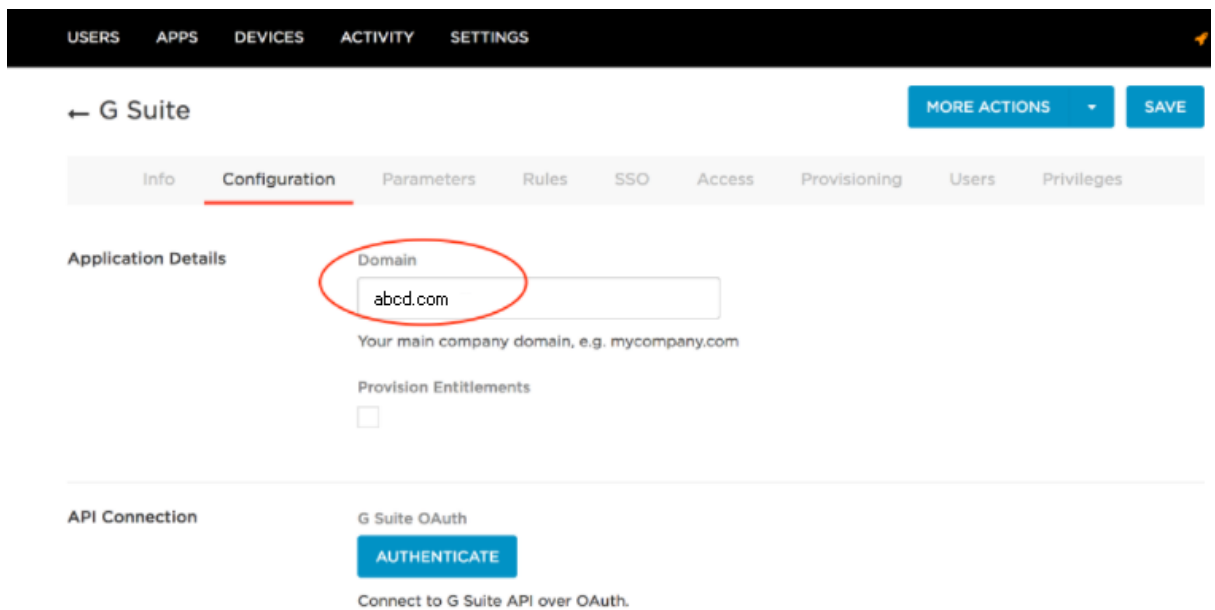
1. Ensure that you have a working setup of the G Suite and Onelogin pair without MobileIron Access.
2. Ensure that you verify the configuration at <https://support.onelogin.com/hc/en-us/articles/201173424-Configuring-SAML-for-G-Suite>
3. **Metadata files and configuration for Onelogin**
 1. Login to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



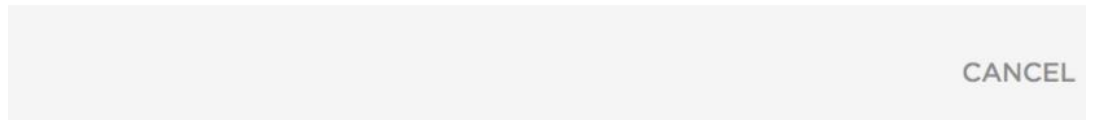
4. On the **Configuration** tab, enter the **G Suite** domain.



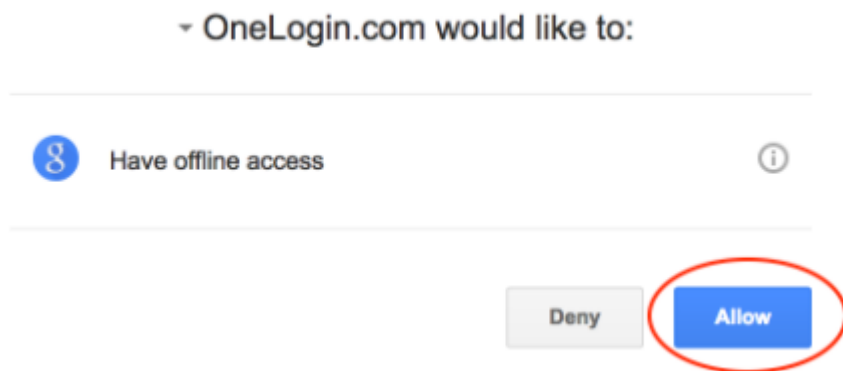
5. On the **Configuration** tab, authenticate to the G Suite API.
 - a. On the **Configuration** tab, click **Authenticate**.
 - b. On the **Complete Authentication Process** dialog, click the **G Suite** link.

Complete Authentication Process

To complete the process, go to [G Suite](#) to authorize access for OneLogin.



- 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.

← G Suite MORE ACTIONS ▾ SAVE

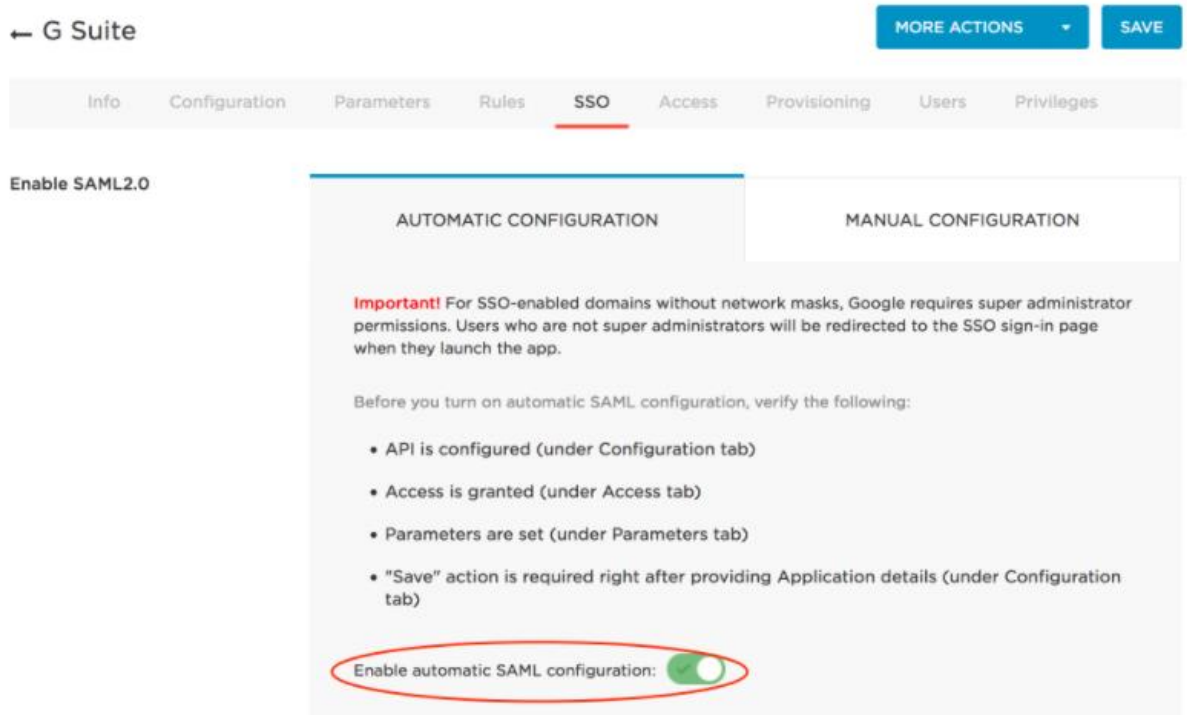
Info Configuration **Parameters** Rules SSO Access Provisioning Users Privileges Setup

Credentials are

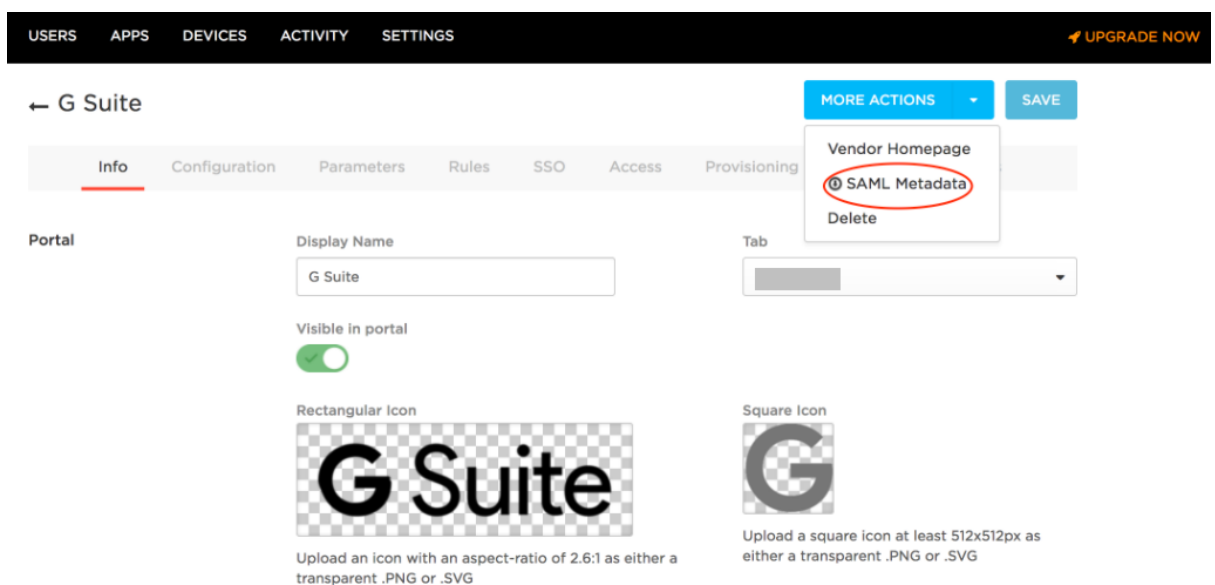
Configured by admin Configured by admins and shared by all users

G Suite Field	Value
Aliases	- No default -
Department	- No default -
Email	Email name part
Employee ID	- No default -
Employee Type	- No default -
Firstname	First Name
Groups	- No default -
Is Admin	False
Lastname	Last Name

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



- 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**.
- 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**.

The screenshot shows the 'Google Apps Directory' configuration page. At the top, there is a navigation bar with 'USERS', 'APPS', 'DEVICES', 'ACTIVITY', and 'SETTINGS'. Below the navigation bar, the page title is '← Google Apps Directory' with 'MORE ACTIONS' and 'SAVE' buttons. The page is divided into three tabs: 'Basic', 'Directory Attributes', and 'Events'. The 'Basic' tab is selected. Under the 'Directory' section, 'Authenticate users in' is set to 'Google'. The 'Basic Configuration' section has a checked checkbox for 'Enable Google Apps as your user directory'. The 'Google Apps Domain' is set to 'abcd.com', which is circled in red. There is an unchecked checkbox for 'Include all sub-domains'. Below this, it says 'Defaults to misentry.onmicrosoft.com if left blank'. The 'API Authentication' section is circled in red and contains a 'Session Token' field, a 'Clear session token' link, and a 'Clear the session token when changing Google Apps Domain' checkbox. A 'SYNC USERS' button is circled in red. The 'Importing Users' section has checked checkboxes for 'Enable Mappings' and 'Enable real-time updates'. A note explains that mappings control user type, group, and role based on directory attributes.

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.

Edit G Suite Login For [redacted]

Enabled Allow users to sign in

Email

Password
Generate password Toggle visibility

Groups Available values
< >

Is Admin

CANCEL DELETE SAVE

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>

Domain is verified. Mail setup is pending. [Return to setup](#)

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://[redacted].onelogin.com/trust/saml2/http-post/sso/6[redacted] URL for signing in to your system and G Suite
Sign-out page URL	https://[redacted].onelogin.com/trust/saml2/http-post/sso/62[redacted] URL for redirecting users to when they sign out
Change password URL	https://[redacted].onelogin.com/trust/saml2/http-post/sso/6[redacted] 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 affected 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 dash. Example: (64.233.167-204.99/32). All network masks must end with a CIDR. ?

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](#)
- [Configuring G Suite with MobileIron Access](#)
- [Configuring Onelogin with MobileIron Access](#)
- [Registering Sentry to Access](#)

Configuring Access to create a Federated Pair

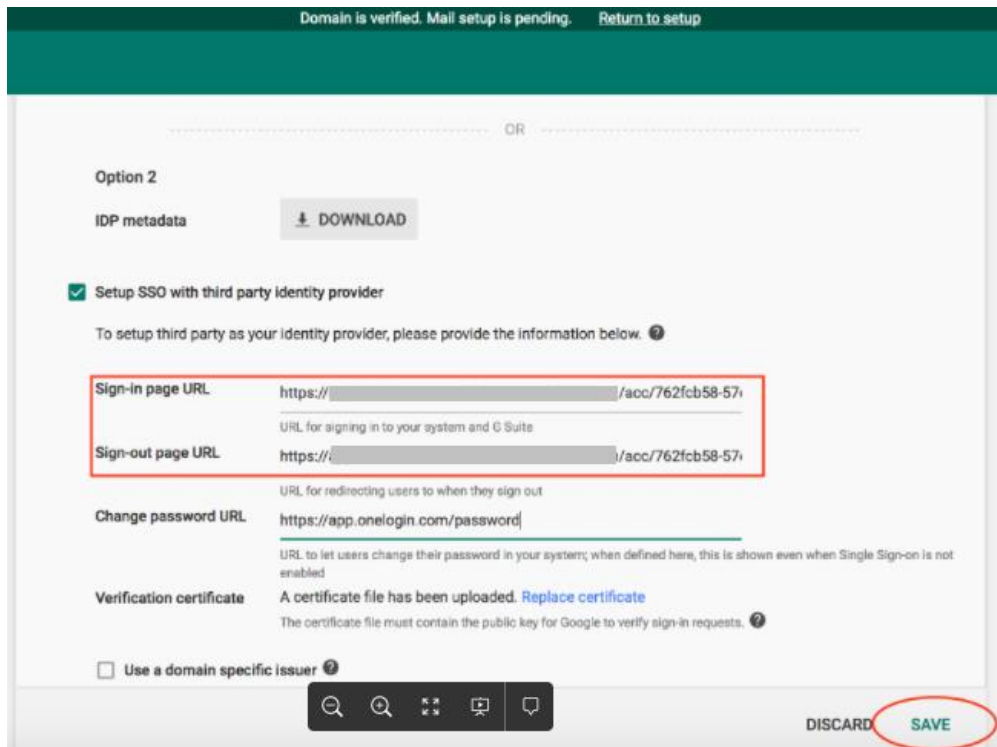
You must configure Access to create a federated pair.

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**.



6. Click Save.

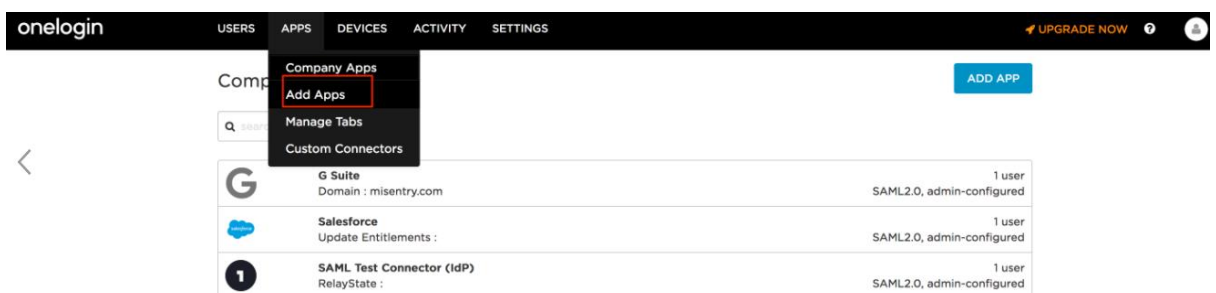
Task Result

G Suite is configured with Access.

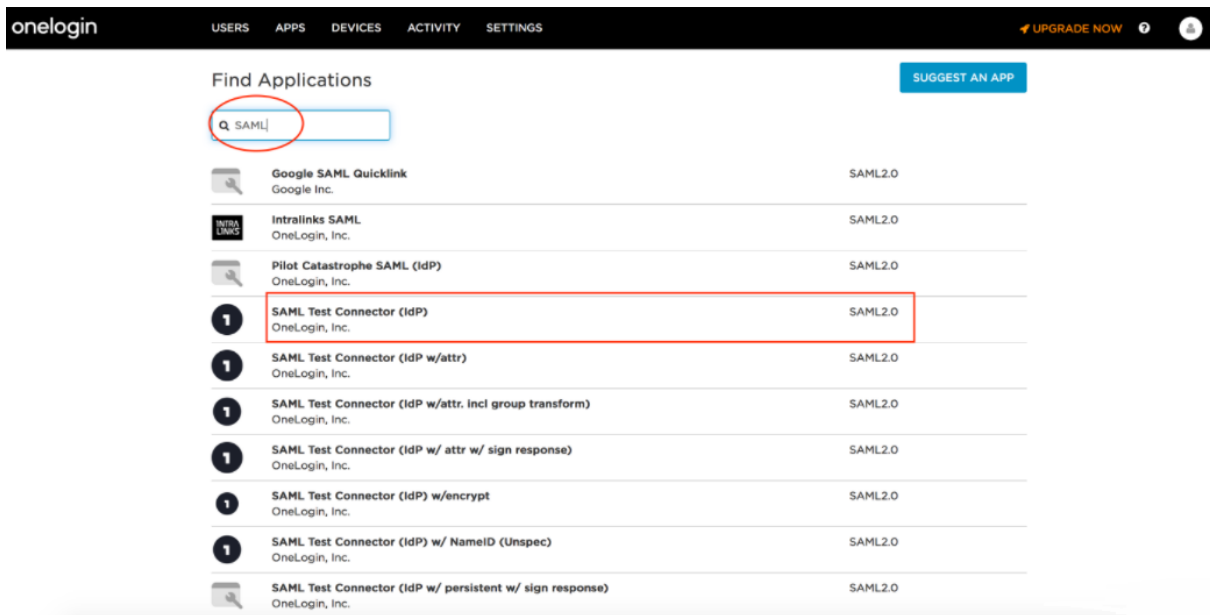
Configuring OneLogin with MobileIron Access

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.

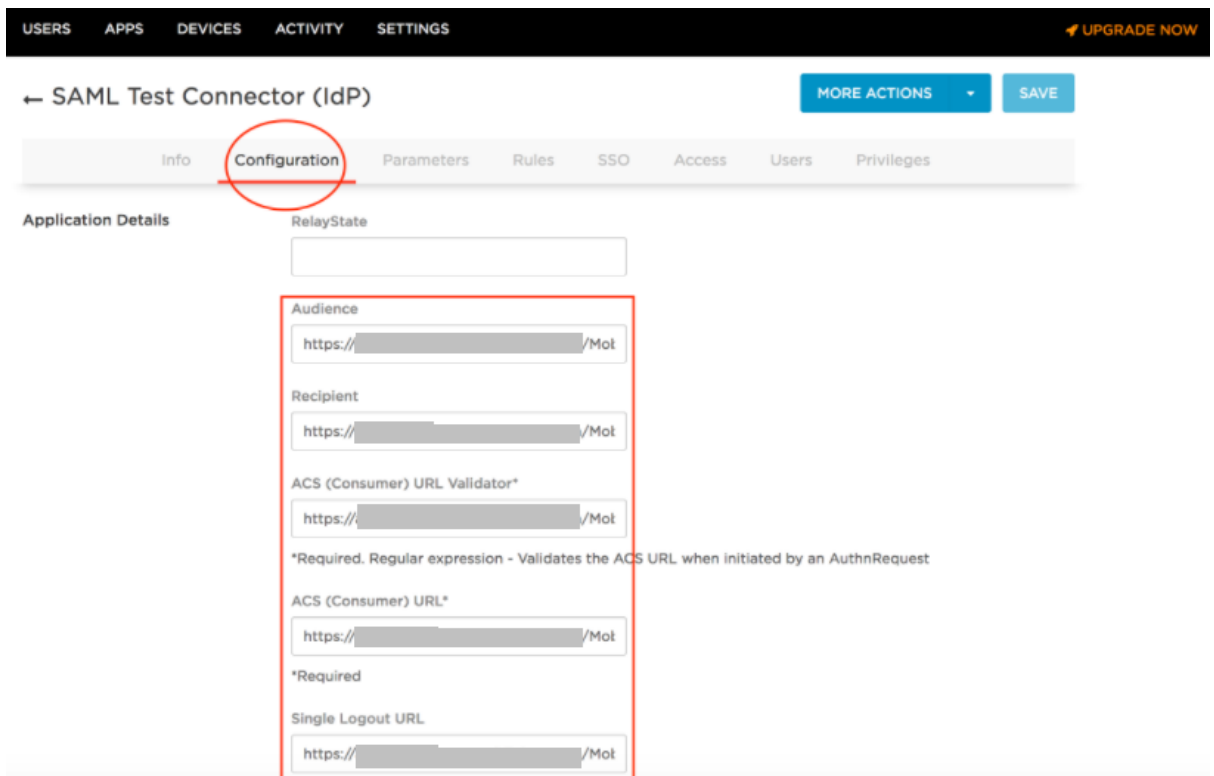


2. Search for SAML and select SAML Test Connector (IdP)

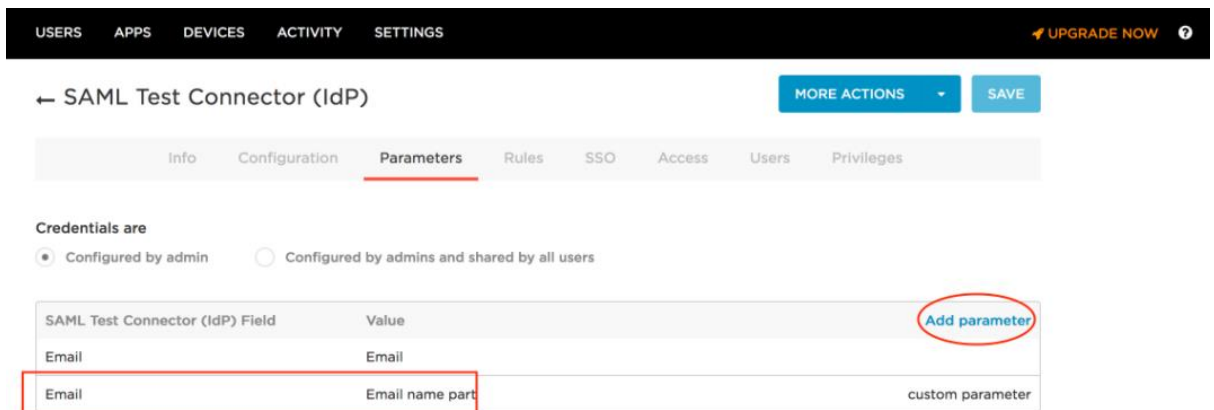


- (Optional): Change the display name and click Save to enable other tabs.
- On the configuration tab, enter the following information that is extracted from the Access SP Metadata (Upload to IDP) file from **Step 10** of [Configuring Access to create a Federated Pair](#).

- 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.

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.