

# MobileIron Access Cookbook

## Access with G Suite and Pingone

**07 February 2018**

## Contents

Overview .....	3
Prerequisites .....	3
Configuring G Suite and Pingone with MobileIron Access .....	4
Registering Sentry to Access .....	4
Configuring Access to create a Federated Pair .....	4
Configuring G Suite with MobileIron Access .....	5
Configuring Pingone with MobileIron Access .....	6
Verification .....	6

# 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 Pingone for authentication. The user gets authenticated by Pingone 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 Pingone 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

- Ensure that you have a working setup of the G Suite and Pingone pair without MobileIron Access.
- **Metadata files for G Suite**
  1. **Entity ID:** google.com/a/<domain name>
  2. **Assertion Consumer Service URL:** https://google.com/a/<domain name>/acs
- **Metadata files and configuration for Pingone**
  1. Login to Pingone with admin credentials.
  2. Click **Applications > G Suite >** scroll-down and download the **SAML metadata**.

# Configuring G Suite and Pingone with MobileIron Access

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

- [Registering Sentry to Access](#)
- [Configuring Access to create a Federated Pair](#)
- [Configuring G Suite with MobileIron Access](#)
- [Configuring Pingone 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 Pingone 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**. See [Prerequisites](#).  
**Entity ID:** [https://google.com/a/<domain\\_name>](https://google.com/a/<domain_name>)  
**Assertion Consumer Service URL:**  
[https://www.google.com/a/domain\\_name/acs](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 **Pingone** 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 Pingone.
- Verify that you have configured G Suite and Pingone natively.

### Procedure

1. Login to the G Suite domain with admin credentials.
2. Click **Security**, and select **Single Sign-On Settings**.
3. Enter the following information from the certificate available in **Step 10** of [Configuring Access to create a Federated Pair](#):
  - a. **Sign-in page URL:** <Entity ID >
  - b. **Sign-out page URL:** <Entity ID >
  - c. **Change password URL**

#### d. Verification certificate

The screenshot shows the Google Security console interface for setting up a third-party identity provider. The main section is titled "Setup SSO with third party identity provider" and includes instructions to provide information for the provider. The form contains the following fields and controls:

- Sign-in page URL:** A text input field with a red border. Below it, a small text label reads "URL for signing in to your system and Google Apps".
- Sign-out page URL:** A text input field with a red border. Below it, a small text label reads "URL for redirecting users to when they sign out".
- Change password URL:** A text input field with a red border. Below it, a small text label reads "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 section containing a "CHOOSE FILE" button, the text "No file chosen", and an "UPLOAD" button. Below this, a small text label reads "The certificate file must contain the public key for Google to verify sign-in requests.".
- Use a domain specific issuer:** A checkbox that is currently unchecked.
- Network masks:** A section header at the bottom of the form.

4. Click **Save**.

## Configuring Pingone 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. Login to Pingone with admin credentials.
2. Click **My Applications** and select **G Suite** application.
3. Click **Edit > Continue to Next Step**.
4. Upload the **Access SP Metadata (Upload to IDP)** metadata file downloaded in **Step 10** of [Configuring Access to create a Federated Pair](#).
5. Click **Continue to Next Step > Save > Publish**.
6. Click **Finish**.

## Verification

1. Register a device to Core.
2. Download G Suite application from App Store.
3. Opening this application triggers the per-app-vpn.
4. Verify that SAML SSO is working.

Copyright © 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.