RSA SECURID® ACCESS
Implementation Guide

Google Apps

Gina Salvalzo, RSA Partner Engineering
Last Modified: February 9, 2015

RSA READY

Solution Summary

Google Apps Business Edition enables companies of any size to leverage their existing corporate directories and authentication systems to authorize employee access to Google Apps. Google Apps Business Edition supports service-provider initiated single sign-on (SSO).

RSA SecurID Access Features	
Google Apps	
On Premise Methods	
RSA SecurID	✓
On Demand Authentication	✓
Risk-Based Authentication (AM)	-
Cloud Authentication Service Methods	
Authenticate App	✓
FIDO Token	✓
SSO	
SAML SSO	✓
HFED SSO	-

Identity Assurance	
Collect Device Assurance and User Behavior	✓

Configuration Summary

All of the supported use cases of RSA SecurID Access with Google Apps require both server-side and client-side configuration changes. This section of the guide includes links to the appropriate sections for configuring both sides for each use case.

RSA Cloud Authentication Service – Google Apps can be integrated with RSA Cloud Authentication Service in the following way:

SAML via RSA Identity Router (IdP)

Cloud Authentication Service – Identity Router IdP Configuration
Google Apps SAML Configuration

RSA READY

RSA SecurID Access Server Side Configuration

RSA Cloud Authentication Service Configuration

SAML via RSA Identity Router (IdP)

To configure a SAML Service Provider in RSA Identity Router, you must deploy the connector for Google Apps in the RSA SecurID Access Console. During configuration of the IdP you will need some Information from the SP. This information includes (but is not limited to) Assertion Consumer Service URL and Service Provider Entity ID.

Configure RSA Identity Router SAML IdP

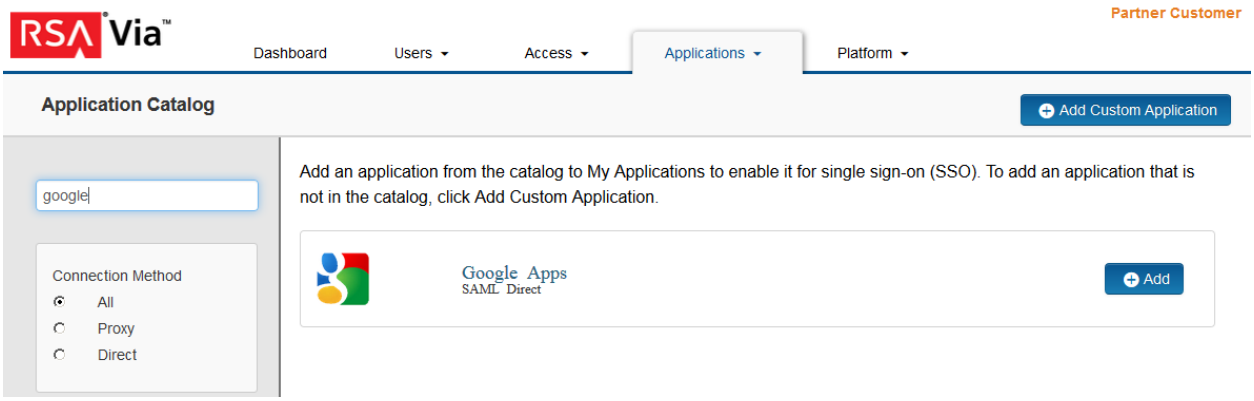
Before You Begin

- Acquire an administrator account to both RSA SecurID Access and Google.
- Obtain the ACS URL information from Google.
- Verify the RSA SecurID Access user account. Refer to the User, Rule, and Policy section of this manual.

The following was tested:

Google Calendar -> https://www.google.com/calendar/
Google Mail -> https://mail.google.com/mail/
Google Docs / Drive -> https://mail.google.com/drive/
Google Domain Management / Sites -> https://mail.google.com/sites/

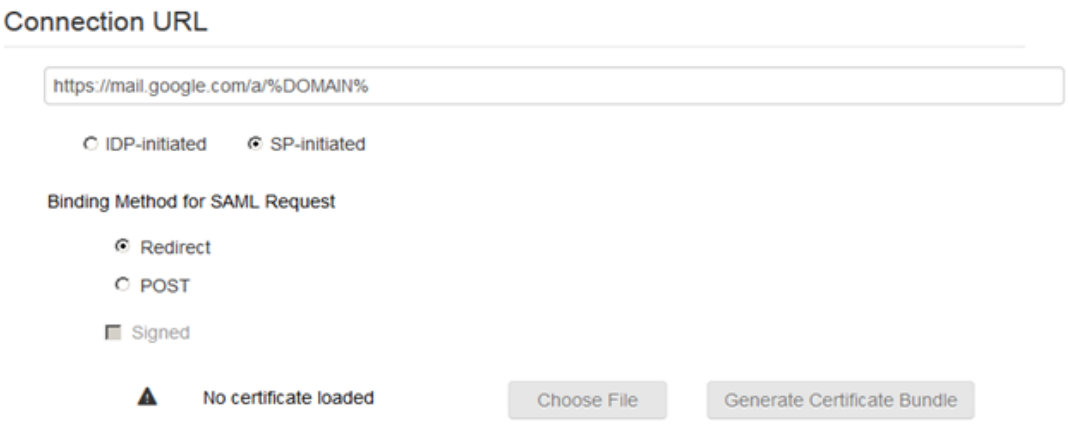
1. In the RSA SecurID Access Administration Console, click **Applications > Application Catalog**.
2. From the list of applications, select **Google Apps** and click **+Add**.



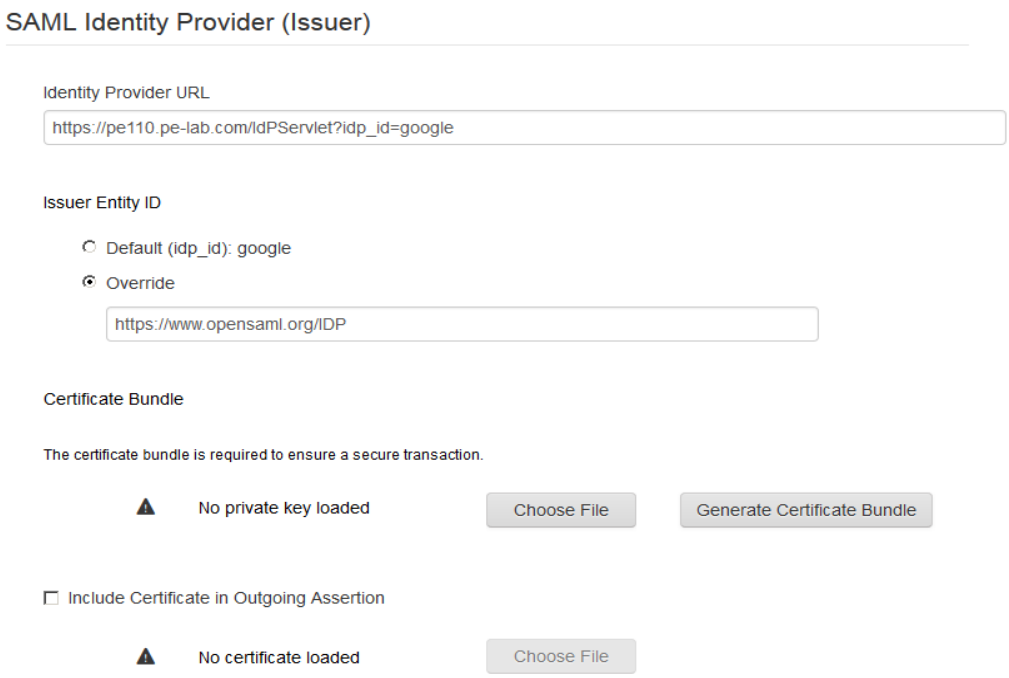
3. On the **Basic Information** page, specify the application name and click **Next Step**.

> **Note: The following SP -initiated configuration works for both SP -initiated and IDP -initiated connections.**

4. On the Connection Profile page, enter your site domain in place of the %DOMAIN% in the Connection URL. **https://mail.google.com/a/%DOMAIN%**.

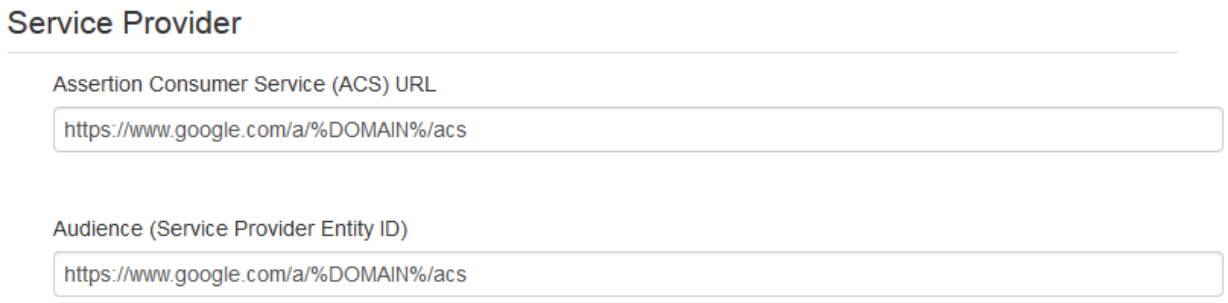


5. Scroll down to SAML Identity Provider (Issuer) section.



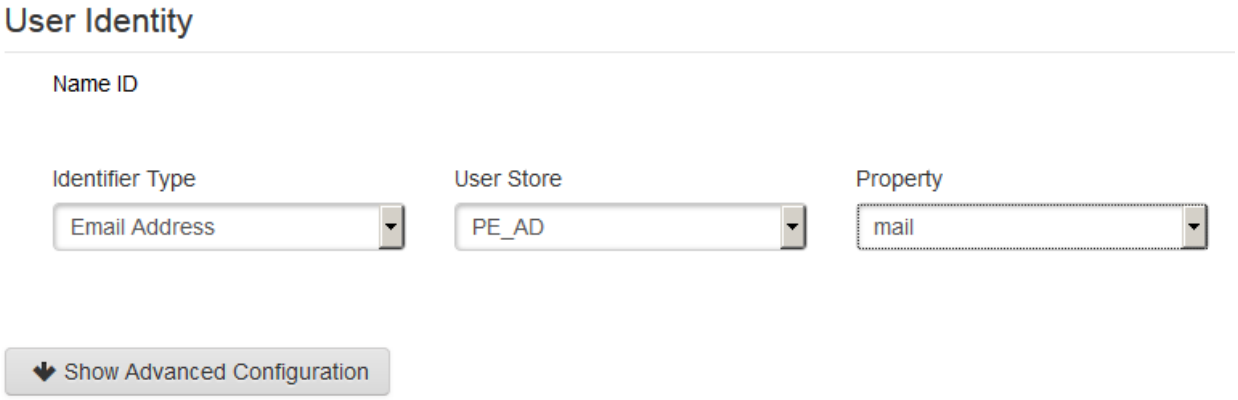
a. In the **Identity Provider URL** field, copy the URL which will be needed later to configure the Service Provider configuration.
b. Select **Override** and enter URL **https://www.opensaml.org/IDP**.
c. Select **Choose File** and upload the private key.

6. Scroll down to the **Service Provider** section.



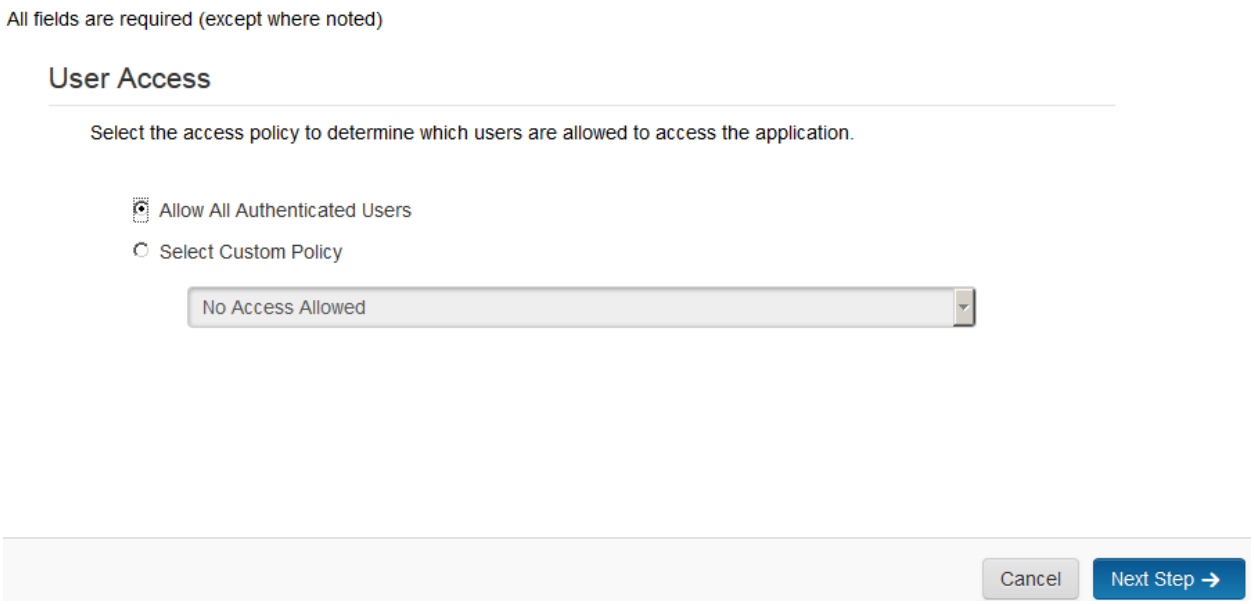
   a. In the **Assertion Consumer Service (ACS) URL** field, enter your site domain in place of %DOMAIN in the URL. **https://www.google.com/a/%DOMAIN%**
   b. In the **Audience (Service Provider Entity ID)** field, enter your site domain in place of %DOMAIN% in the URL. **https://www.google.com/a/%DOMAIN%**

7. Scroll down to the **User Identity** section. Verify the settings are correct for your environment. In this example, the username will be presented in email format and the user account will be validated against the User Store selected.

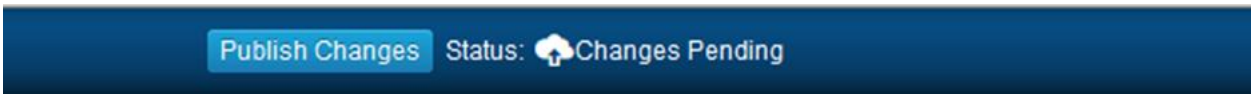


8. Click **Next Step**.

9. On the **User Access** page, select the desired user policy from the drop down list.



10. Click **Next Step**.
11. On the Portal Display page, select **Display in Portal**.
12. Click **Save and Finish**.
13. Click **Publish Changes**. Your application is now enabled for SSO.



Partner Product Configuration

Before You Begin

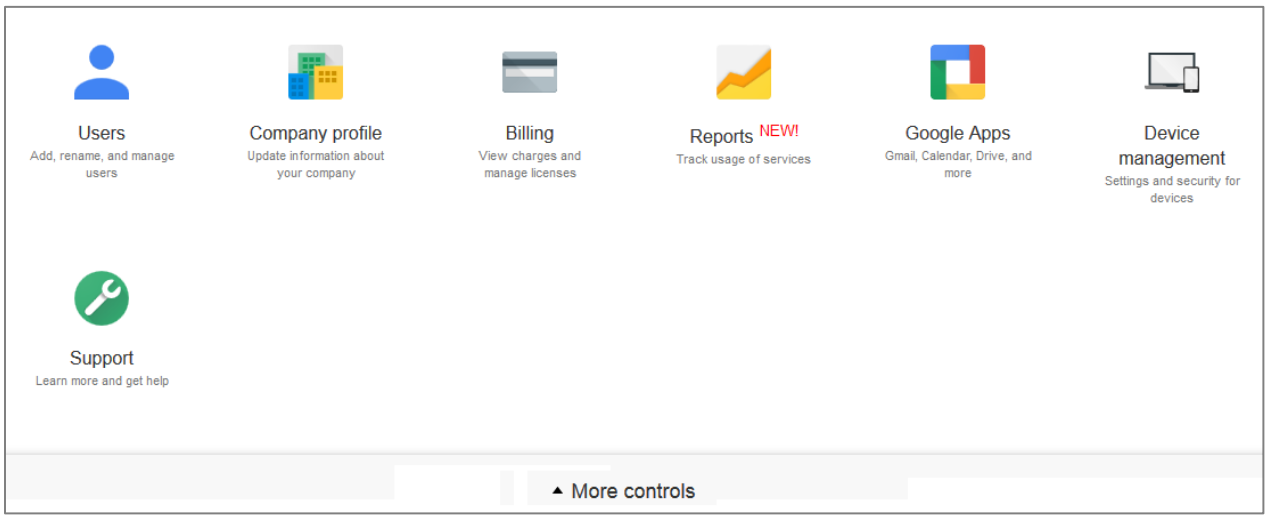
This section provides instructions for configuring Google Apps with RSA SecurID Access. This document is not intended to suggest optimum installations or configurations.

It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

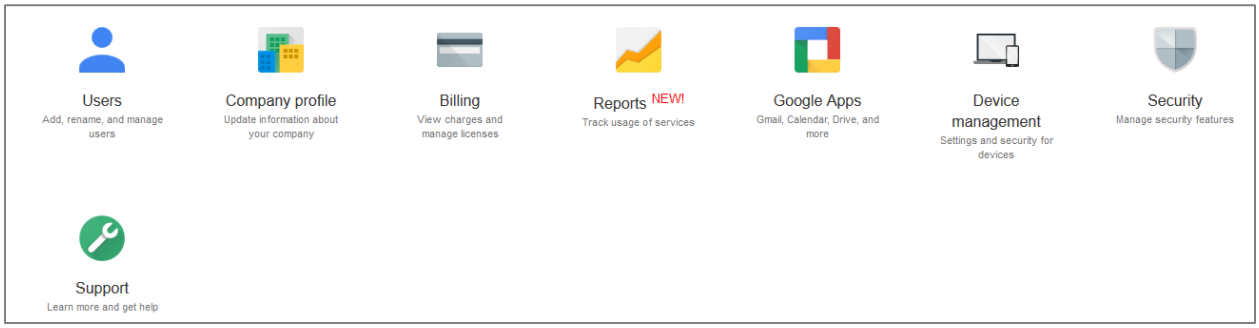
All Google Apps components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

Google Apps SAML Configuration

1. Launch a browser and login to the Google Apps administrator dashboard.
2. Click the **Start Setup** link and complete the verification of your domain.

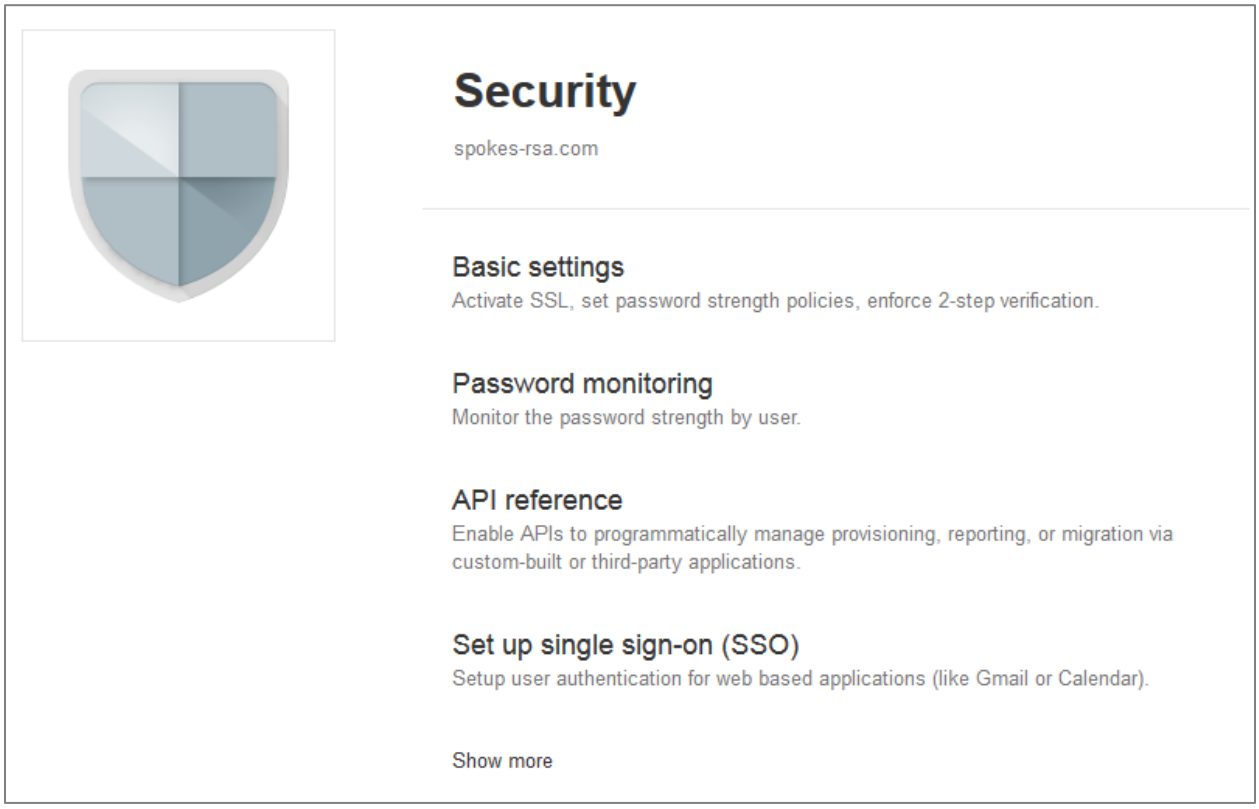


3. At the bottom of the dashboard, click on **More controls**.
4. Click the **Security** icon.

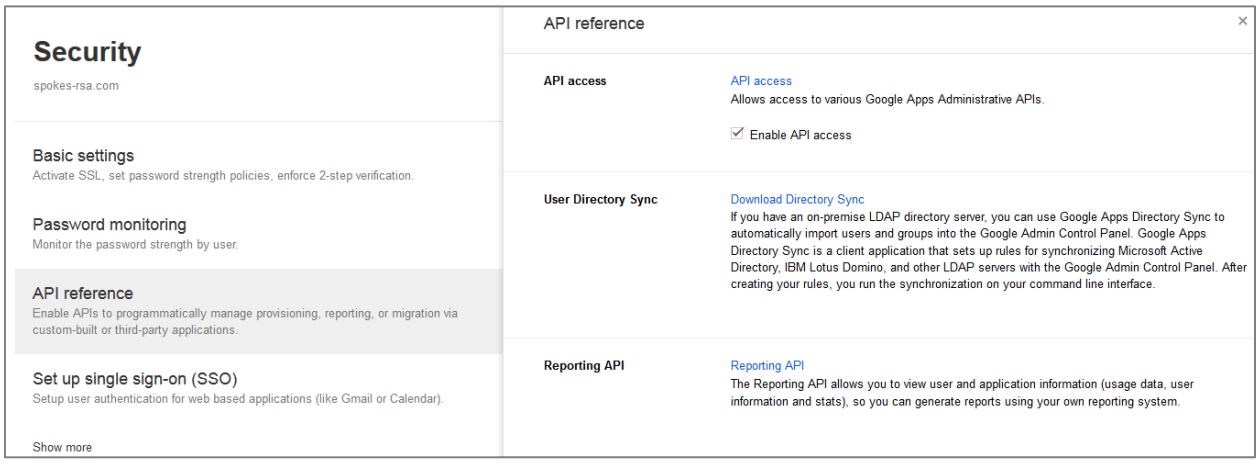


RSA READY

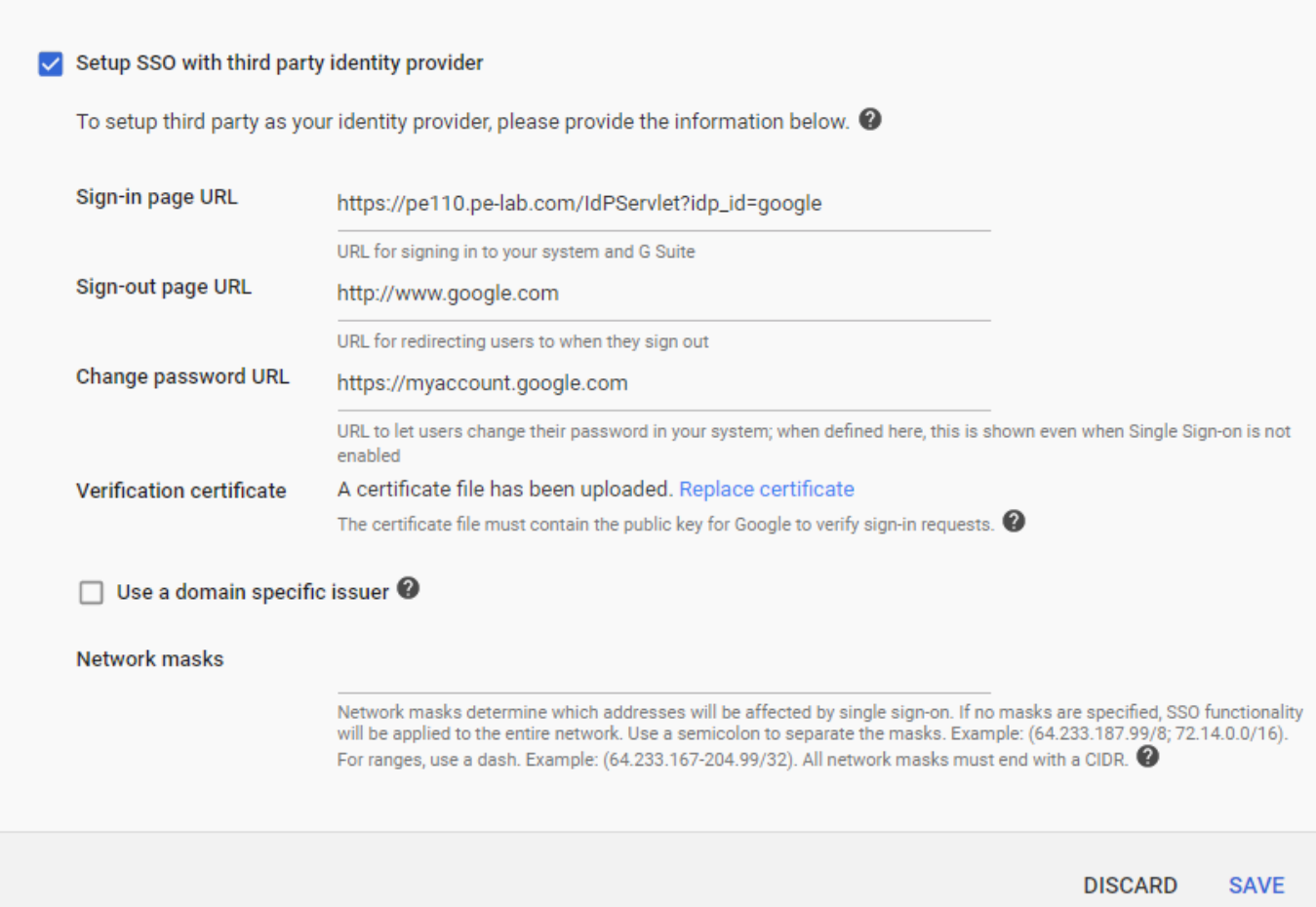
5. Select **API reference**.



6. Select the **Enable API access** check box to allow API provisioning.



7. Select **Set up single sign-on (SSO).**



a. Select the **Setup SSO with third party identity provider** check box.
b. Fill in the **Sign-in page URL** with the Identity Provider URL from step 5.
c. Fill in the **Sign-out page URL**.
d. Fill in the **Change password URL**.
e. Click the **Choose File** and browse to your X.509 public certificate and click **Upload**.
f. Click **Save**.