

RSA SECURID[®] ACCESS

Implementation Guide

Google Apps

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



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 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

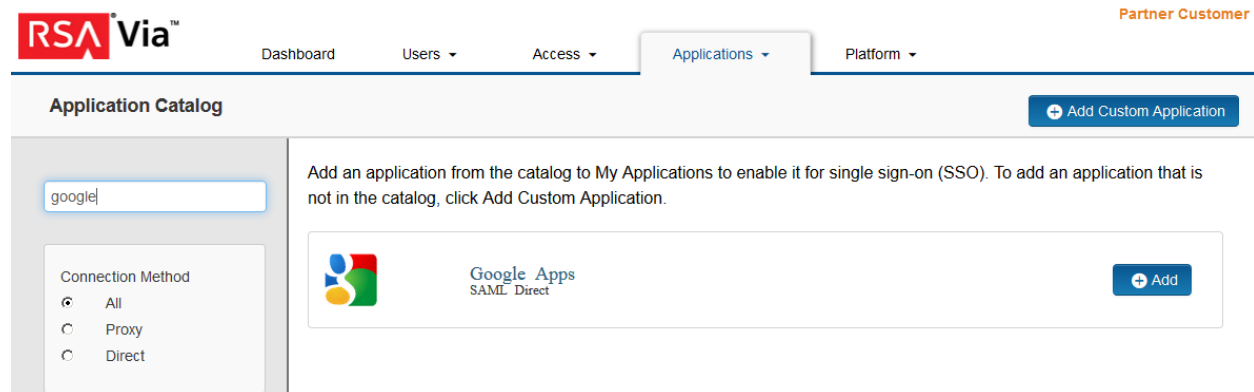
Before You Begin

- 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%>.

Connection URL

IDP-initiated SP-initiated

Binding Method for SAML Request

Redirect
 POST
 Signed

 No certificate loaded

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

SAML Identity Provider (Issuer)


Identity Provider URL

Issuer Entity ID


Default (idp_id): google
 Override

Certificate Bundle

The certificate bundle is required to ensure a secure transaction.

 No private key loaded

Include Certificate in Outgoing Assertion

 No certificate loaded

- 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.

Service Provider

Assertion Consumer Service (ACS) URL

<https://www.google.com/a/%DOMAIN%/acs>

Audience (Service Provider Entity ID)

<https://www.google.com/a/%DOMAIN%/acs>

- 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.

User Identity

Name ID

Identifier Type

Email Address

User Store

PE_AD

Property

mail

⌵ Show Advanced Configuration

8. Click **Next Step**.



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

All fields are required (except where noted)

User Access

Select the access policy to determine which users are allowed to access the application.

Allow All Authenticated Users

Select Custom Policy


No Access Allowed

Cancel

Next Step →

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.

Publish Changes

Status:  Changes Pending



Partner Product Configuration

Before You Begin

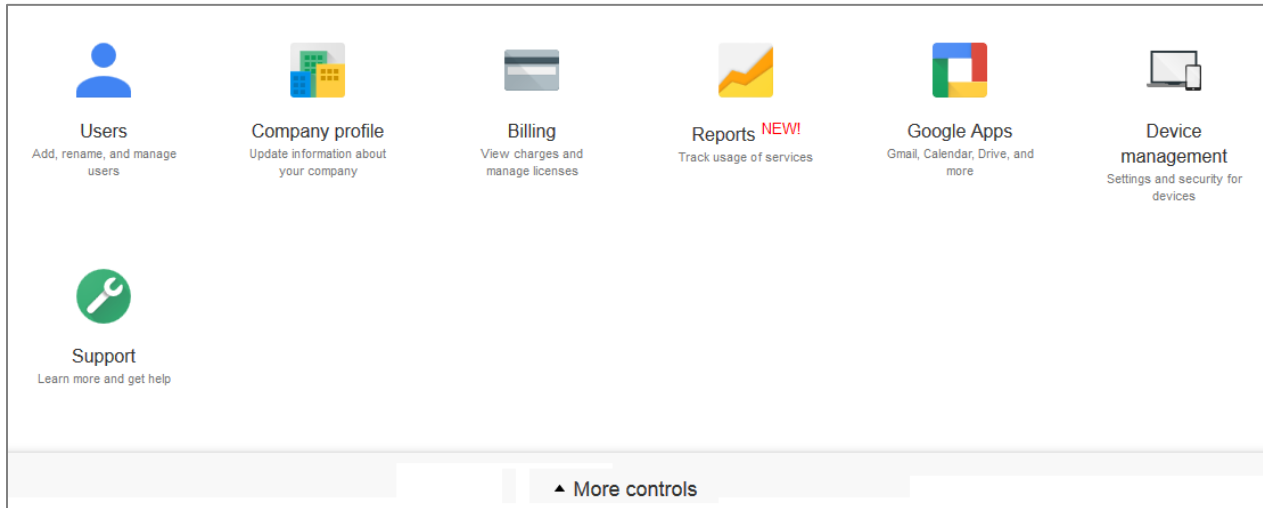
This section provides instructions for configuring Google Apps with RSA SecurID Access. This document is not intended to suggest optimum installations or configurations.

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.

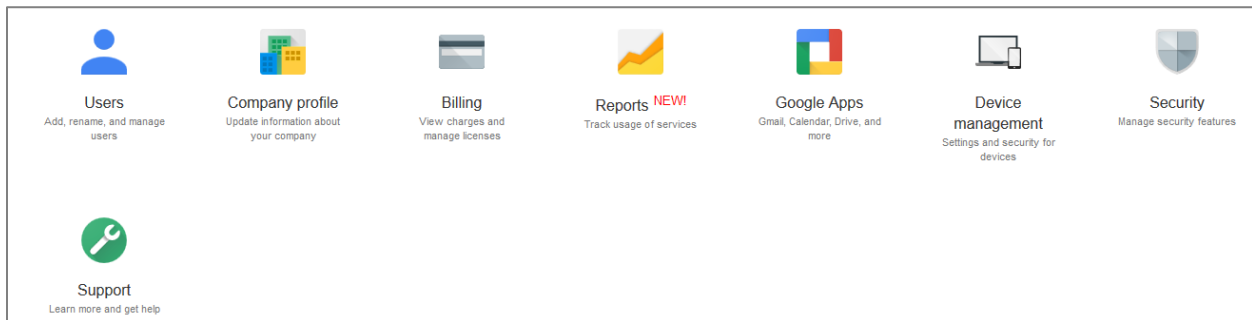
All Google Apps components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

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.





5. Select **API reference**.



Security

spokes-rsa.com

Basic settings

Activate SSL, set password strength policies, enforce 2-step verification.

Password monitoring

Monitor the password strength by user.

API reference

Enable APIs to programmatically manage provisioning, reporting, or migration via custom-built or third-party applications.

Set up single sign-on (SSO)

Setup user authentication for web based applications (like Gmail or Calendar).

Show more

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

<h3>Security</h3> <p>spokes-rsa.com</p> <hr/> <h4>Basic settings</h4> <p>Activate SSL, set password strength policies, enforce 2-step verification.</p> <h4>Password monitoring</h4> <p>Monitor the password strength by user.</p> <h4>API reference</h4> <p>Enable APIs to programmatically manage provisioning, reporting, or migration via custom-built or third-party applications.</p> <h4>Set up single sign-on (SSO)</h4> <p>Setup user authentication for web based applications (like Gmail or Calendar).</p> <p>Show more</p>	<h4>API reference</h4>
	<h4>API access</h4> <p>API access Allows access to various Google Apps Administrative APIs.</p> <p><input checked="" type="checkbox"/> Enable API access</p>
	<h4>User Directory Sync</h4> <p>Download Directory Sync If you have an on-premise LDAP directory server, you can use Google Apps Directory Sync to automatically import users and groups into the Google Admin Control Panel. Google Apps Directory Sync is a client application that sets up rules for synchronizing Microsoft Active Directory, IBM Lotus Domino, and other LDAP servers with the Google Admin Control Panel. After creating your rules, you run the synchronization on your command line interface.</p>
	<h4>Reporting API</h4> <p>Reporting API The Reporting API allows you to view user and application information (usage data, user information and stats), so you can generate reports using your own reporting system.</p>





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

Setup SSO with third party identity provider

To setup third party as your identity provider, please provide the information below. ?

Sign-in page URL	<input type="text" value="https://pe110.pe-lab.com/IdPServlet?idp_id=google"/>
	<small>URL for signing in to your system and G Suite</small>
Sign-out page URL	<input type="text" value="http://www.google.com"/>
	<small>URL for redirecting users to when they sign out</small>
Change password URL	<input type="text" value="https://myaccount.google.com"/>
	<small>URL to let users change their password in your system; when defined here, this is shown even when Single Sign-on is not enabled</small>
Verification certificate	A certificate file has been uploaded. Replace certificate <small>The certificate file must contain the public key for Google to verify sign-in requests. ?</small>

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. ?

DISCARD [SAVE](#)

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