

Directory Password Synchronization with G Suite Configuration Guide

Introduction

Use this guide to enable directory (AD, SQL, Oracle, etc.) to G Suite (formerly Google Apps) password synchronization via SecureAuth IdP.

This enables users' passwords to change in both the directory and G Suite once modified in one location.

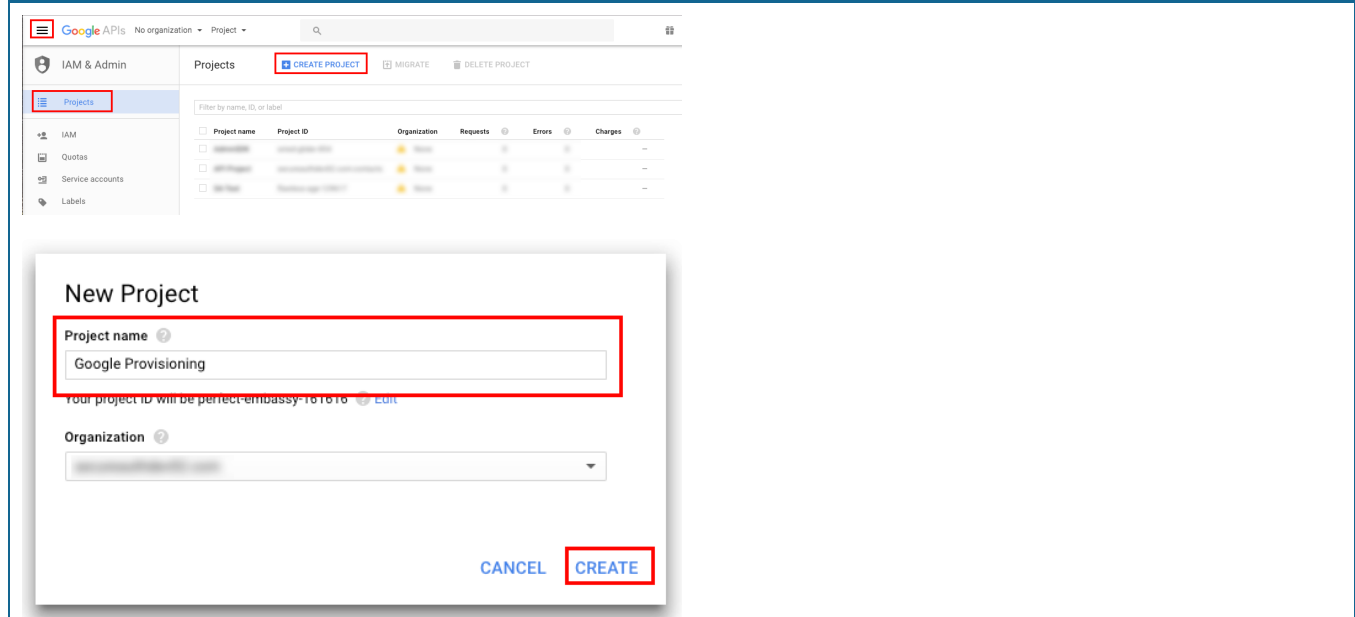
Prerequisites

1. Create a **Service Account** with G Suite
2. Delegate **domain-wide authority** to the G Suite Service Account
3. Have a directory **Service Account** with **read and write** access for SecureAuth IdP
4. Have an Active Directory field to which SecureAuth IdP can map a **Profile Property**

For other data stores, the field mapping will need to be configured through the directory

G Suite API Configuration Steps

Create Project

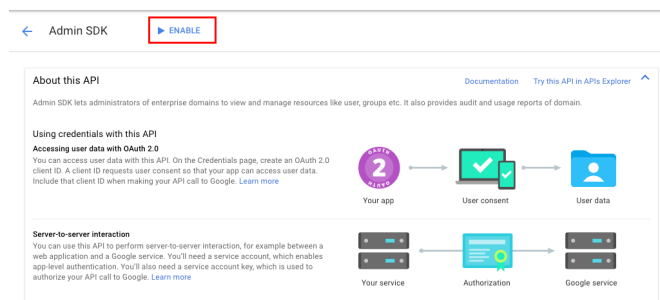


1. Log into the [Google Developers' Console](#) , and navigate to **IAM & Admin > Projects** from the three bars menu
2. Select **Create Project**

These steps can also be completed by opening the **Projects** dropdown menu at the top, and selecting **Create project**

3. Provide a **Project Name**, and select an **Organization** if the project is not already being created within one
4. Click **Create**

Enable Admin SDK

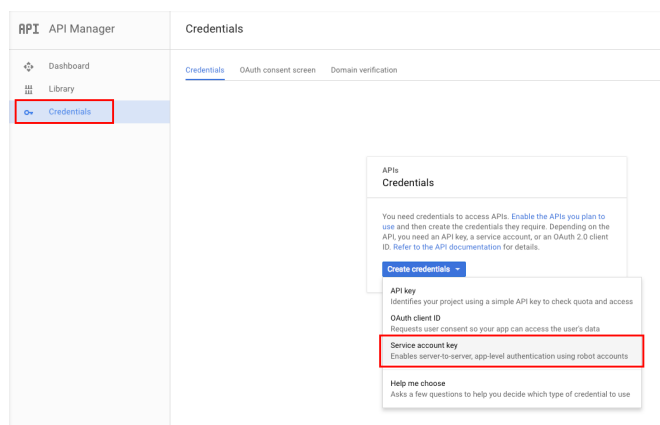


The screenshot shows the 'Admin SDK' page in the Google Cloud console. At the top, there is a navigation bar with a back arrow and the text 'Admin SDK'. To the right of this text is a red-bordered button labeled 'ENABLE'. Below the navigation bar, the page content includes a section titled 'About this API' with a 'Documentation' link and a 'Try this API in APIs Explorer' link. The main text describes the Admin SDK's purpose. There are two diagrams: one for 'Using credentials with this API' showing a flow from 'Your app' to 'User consent' to 'User data', and another for 'Server-to-server interaction' showing a flow from 'Your service' to 'Authorization' to 'Google service'.

5. In the **Libraries** section, search for **Admin SDK**, and select the option

6. On the **Admin SDK** page, click **Enable**

Create Service Account



The screenshot shows the 'API Manager' page in the Google Cloud console. The left sidebar has a menu with 'Dashboard', 'Library', and 'Credentials' (highlighted with a red box). The main content area is titled 'Credentials' and has sub-sections for 'Credentials', 'OAuth consent screen', and 'Domain verification'. A 'Create credentials' dialog box is open, showing options: 'API key', 'OAuth client ID', 'Service account key' (highlighted with a red box), and 'Help me choose'. The 'Service account key' option is described as 'Enables server-to-server, app-level authentication using robot accounts'.

7. On the **API Manager** page (accessible via the three bars menu), navigate to the **Credentials** section, and click **Create Credentials**

8. Select **Service Account Key**

Create Service Account Key



Create service account key

Service account

New service account

Service account name ?

service-account

Role ?

Owner

Service account ID

service-account @iam.gserviceaccount.c

Key type

Downloads a file that contains the private key. Store the file securely because this key can't be recovered if lost.

JSON

Recommended

P12

For backward compatibility with code using the P12 format

Create

Cancel

9. Select **New service account** from the **Service Account** dropdown, and provide a **Service Account Name**

10. Select **Project > Owner** from the **Role** dropdown

11. Select **P12**, and click **Create**

12. Save the p12 file that downloads, which is uploaded to the SecureAuth appliance (see steps below), note the **Private Key Password**, and click **Close**

New private key

Google Provisioning-cb22b8fbf390.p12 has been saved on your computer. This is the only copy of the key, so store it securely.

This is the private key's password. It will not be shown again. You must present this password to use the private key. [Learn more](#)

notasecret

CLOSE

Manage Service Account

IAM & Admin

Service Accounts CREATE SERVICE ACCOUNT DELETE PERMISSIONS

Service accounts for project "Google Provisioning"

A service account represents a Google Cloud service identity, such as code running on Compute Engine VMs, App Engine apps, or systems running outside Google. [Learn more](#)

Service account name	Service account ID	Key ID	Key creation date	Options
Compute Engine default service account	941071411006-compute@developer.gserviceaccount.com	No keys		
service-account	service-account@iam.gserviceaccount.com	6822b8fbf3901470axk1	Mon 14, 2017	Edit Delete Create key

13. On the **Credentials** page, click **Manage Service Accounts**

14. Click the three dots on the newly-created service account, and select **Edit**

Edit Service Account

Edit service account

Service account name [?](#)

Enable G Suite Domain-wide Delegation
Grants a client access to all users' data on a G Suite domain without manual authorization on their part. [Learn more](#)

i To change settings for G Suite domain, product name for the OAuth consent screen must be configured. Assign the product name below or configure the OAuth consent screen.

Product name for the consent screen

[CANCEL](#) [SAVE](#) [CONFIGURE CONSENT SCREEN](#)

15. Check **Enable G Suite Domain-wide Delegation** and provide a **Product name for the consent screen**

16. Click **Save**

Click **Configure Consent Screen** to set additional (optional) preferences for the consent page; or access the configuration at **API Manager > Credentials > OAuth Consent Screen**

Service accounts for project "Google Provisioning"

A service account represents a Google Cloud service identity, such as code running on Compute Engine VMs, App Engine apps, or systems running outside Google. [Learn more](#)

Find a service account

Service account name	Service account ID	Key ID	Key creation date	Options
Compute Engine default service account	941671411006-compute@developer.gserviceaccount.com	No keys		
service-account	service-account@iam.gserviceaccount.com	db2268f9951673ad179a17...	Mar 15, 2017	View Client ID

Back on the **Service Accounts** page, a new **DwD** section appears for the service account

17. Click **View Client ID**

Credentials

Credentials

[←](#) [Download JSON](#) [Delete](#)

Client ID for Service account client

i Service account clients are created when **domain-wide delegation** is enabled on a service account. [Manage service accounts](#)

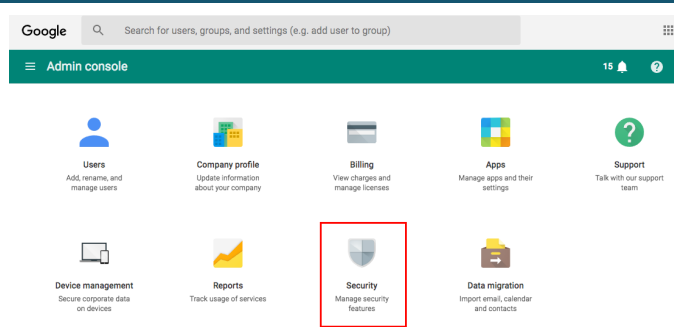
Client ID	1166612500697452
Service account	service-account@iam.gserviceaccount.com
Creation date	Mar 15, 2017, 10:27:40 AM

Name

[Save](#) [Cancel](#)

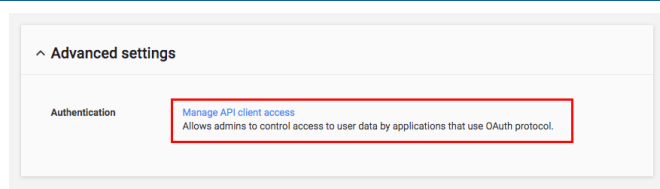
18. Note the **Client ID**, which is used in the G Suite Administrative Configuration Steps (below), and the **Service Account** email address, which is used in the SecureAuth IdP Configuration Steps (below)

G Suite Administration Configuration Steps



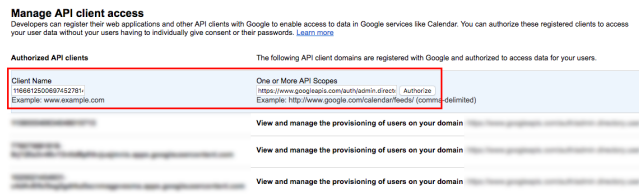
19. Log into the **G Suite Administrative Console** and select **Security**

Security - Advanced Settings



20. Under **Advanced Settings**, select **Manage API Client Access**

Manage API Client Access



21. Set the **Client Name** to the **Client ID** obtained in the G Suite API Configuration Steps (step 18)

22. Set the **One or More API Scopes** to **https://www.googleapis.com/auth/admin.directory.user** and click **Authorize**

SecureAuth IdP Configuration Steps

▼ Profile Fields

Property	Source	Field	Data Format	Writable
Groups	Default Provider	memberOf		<input type="checkbox"/>
First Name	Default Provider	givenName		<input type="checkbox"/>
Last Name	Default Provider	sn		<input type="checkbox"/>
Phone 1	Default Provider	telephoneNumber		<input checked="" type="checkbox"/>
Phone 2	Default Provider	mobile		<input checked="" type="checkbox"/>
Phone 3	Default Provider	homePhone		<input checked="" type="checkbox"/>
Phone 4	Default Provider	Pager		<input checked="" type="checkbox"/>
Ext. Sync Pwd Date	Default Provider	Directory Field	Plain Text	<input checked="" type="checkbox"/>
Hardware Token	Default Provider		Plain Text	<input checked="" type="checkbox"/>



This step is for Active Directory data stores only

1. In the **Profile Fields** section, map a directory field to **Ext. Sync Pwd Date Profile Property**, and check **Writable**

This is to contain the date on which the G Suite password was last synchronized with AD



Click **Save** once the configurations have been completed and before leaving the **Data** page to avoid losing changes

▼ Google Apps Functions

Google Apps Domain Name:	<input type="text"/>
Admin Email:	<input type="text" value="admin@company.com"/>
Service Email:	<input type="text" value="service-account@project.iam.gse"/>
	<input type="button" value="Choose File"/> No file chosen
P12 Password:	<input type="password" value="*****"/> <input checked="" type="checkbox"/> Hidden
Create User:	<input type="text" value="Enabled"/>
Sync Password:	<input type="text" value="Enabled"/>
Mail Forwarding:	<input type="text" value="Not Set"/>
Forwarding Email Address:	<input type="text" value="Authenticated User ID"/>

2. Leave the **Google Apps Domain Name** field blank
3. Set the **Admin Email** to the G Suite Administrative email account
4. Set the **Service Email** to the **Service Account** email address obtained from the G Suite Steps above (step 18)
5. Click **Choose File** and select the **p12 File** obtained in the G Suite Steps above (step 12)
6. Set the **P12 Password** to the **Private Key Password** obtained in the G Suite Steps above (step 12)
7. Select **Enabled** from the **Create User** dropdown if SecureAuth IdP is to automatically create the G Suite user account (if it does not already exist)
8. Select **Enabled** from the **Sync Password** dropdown if SecureAuth IdP is to conduct a one-way synchronization of the user's directory password to G Suite

To synchronize on specific dates versus every time the password changes, map a directory field to the **Ext. Sync Pwd Date** property in the **Data** tab

If no field is mapped, then the password synchronizes every time

G Suite requires passwords with a minimum of 8 characters

9. Select **Enabled** from the **Mail Forwarding** dropdown if another email address will receive messages; select **Disabled** to disable the feature; or select **Not Set** if SecureAuth IdP is to not be included in this feature
10. Select the **Profile Field** that contains the user's **Forwarding Email Address**



Click **Save** once the configurations have been completed and before leaving the **Post Authentication** page to avoid losing changes