

# Preparation for Google Workspace by enabling domain-wide delegation using OAuth service

## Table of Contents

[Step 1: Create the access key](#)

[Step 2: Enable the API Services](#)

[Step 3: Enable domain-wide delegation](#)

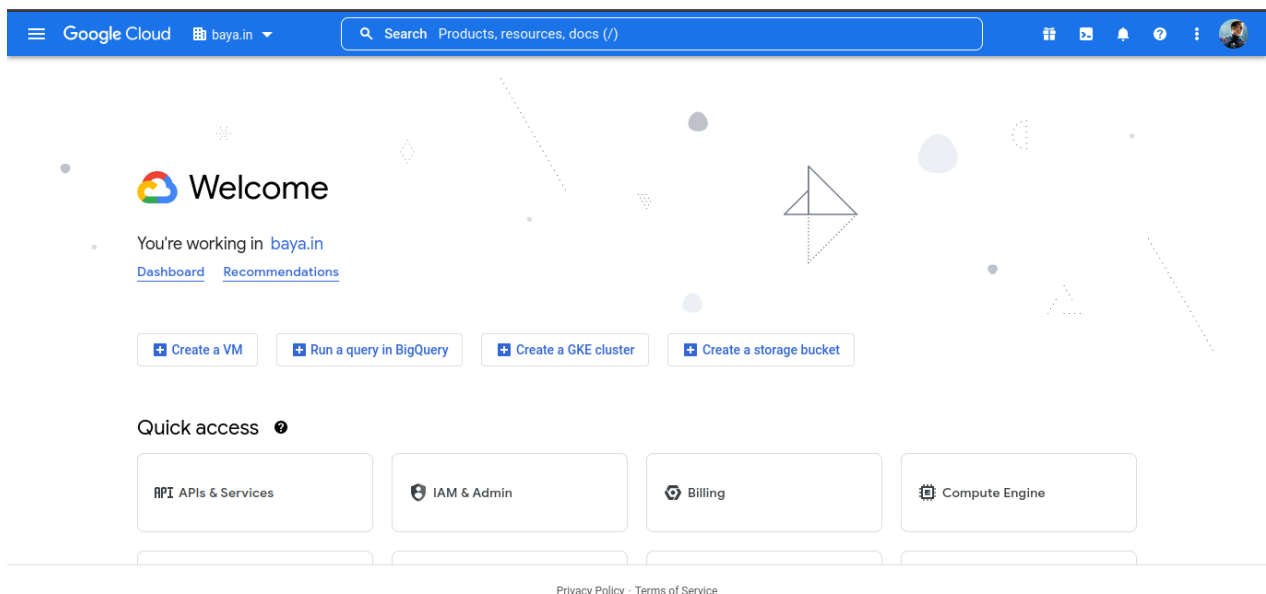
[Step 4: Register with LegacyFlo](#)

## Step 1: Create the access key

1. Login to Google Workspace Admin account and navigate to [Google developers console](#)

(<https://console.developers.google.com/>).

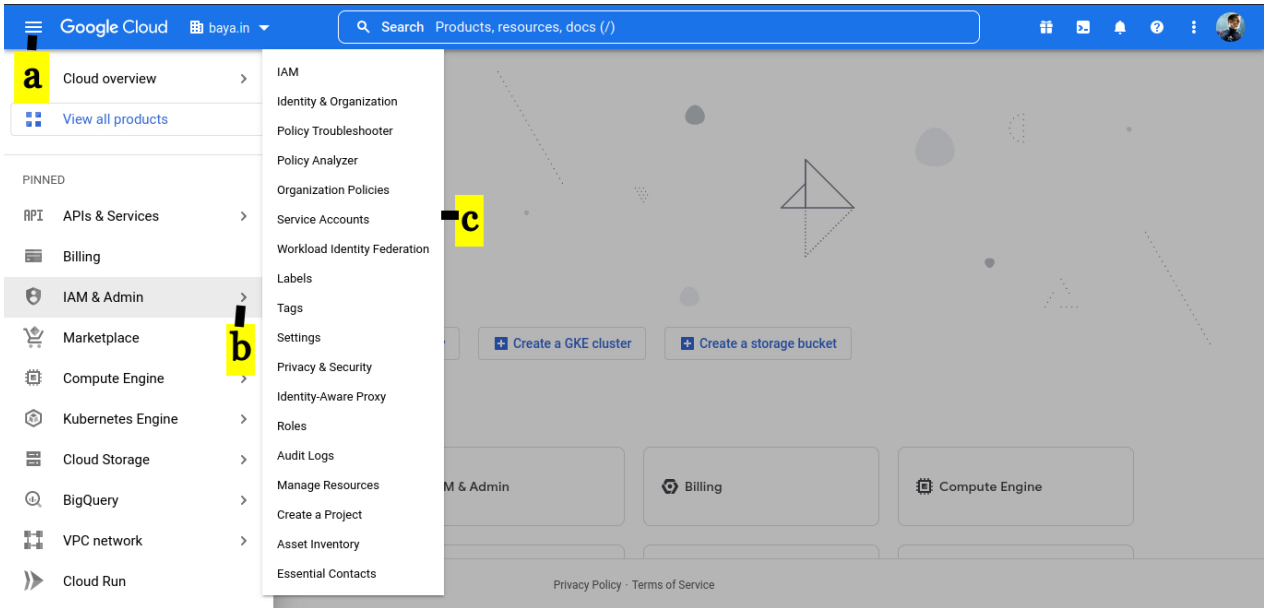
Http link: <https://console.developers.google.com> (<https://console.developers.google.com/>)



a. Select top left panel.

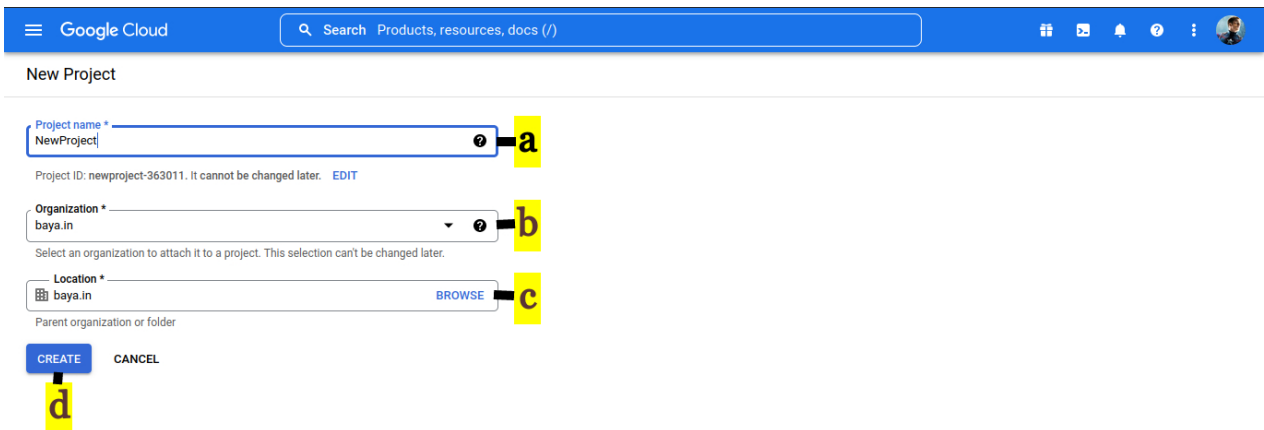
b. Select **IAM & Admin**.

c. Select **Service Accounts**.



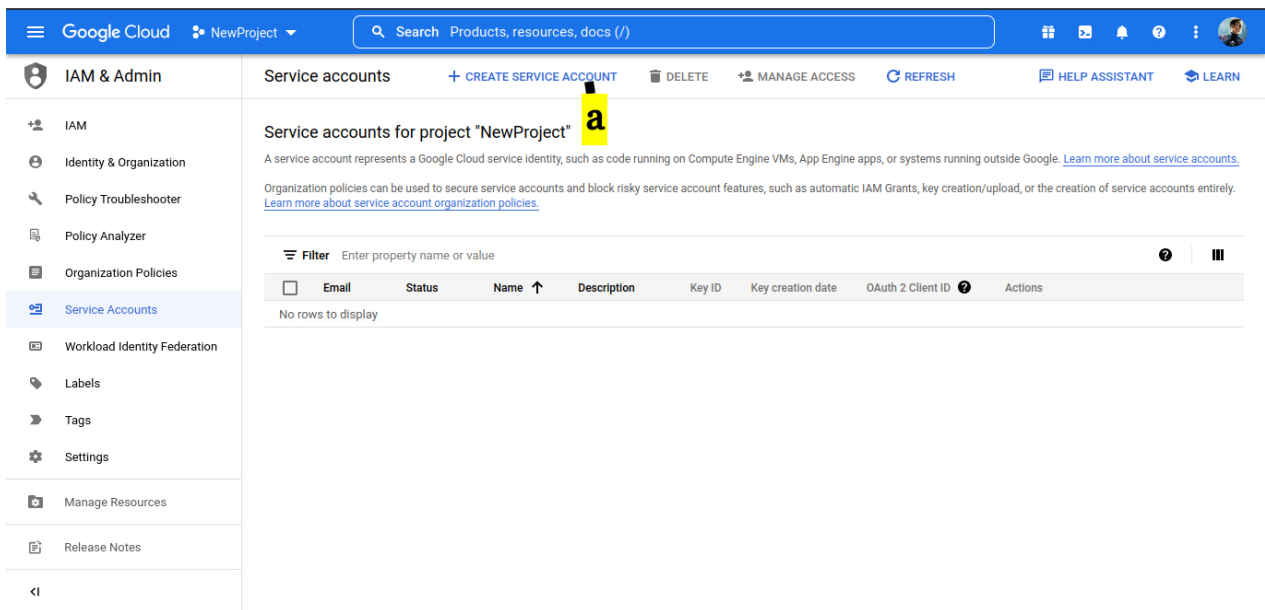
2. CREATE A PROJECT

- a. Provide **Project name**.
- b. Select the **Organization**.
- c. Browse for the **Location**.
- d. Click on **CREATE**.



### 3. Create a service account

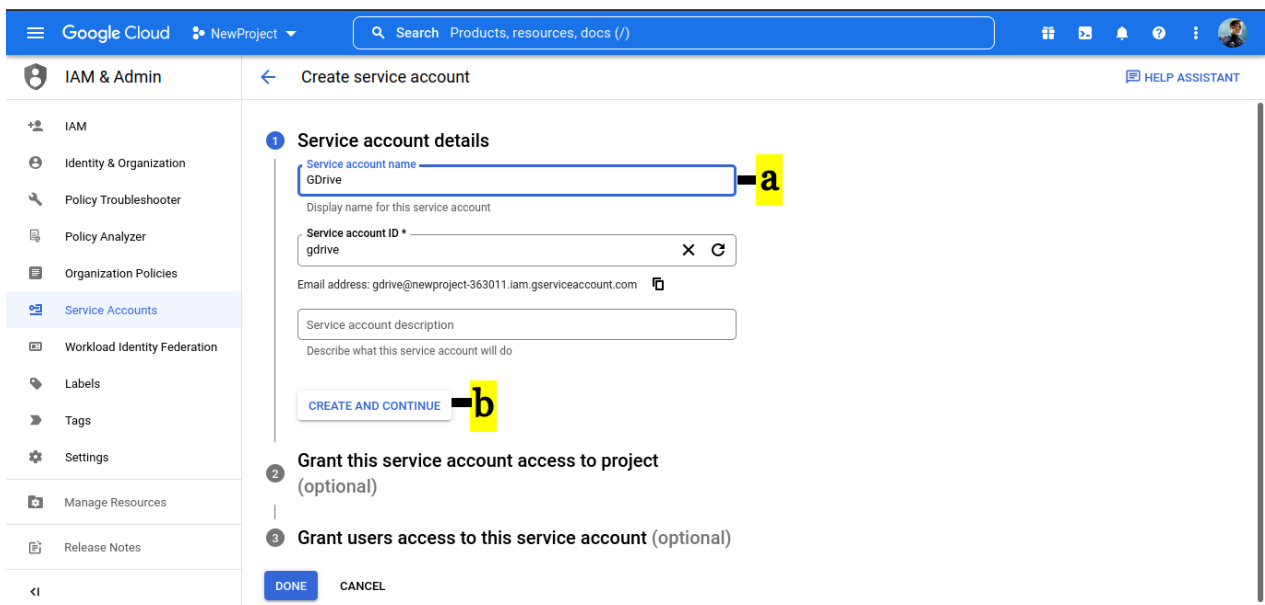
a. Click **CREATE SERVICE ACCOUNT**.



### 4. On the service account details window.

a. Provide **Service account name**.

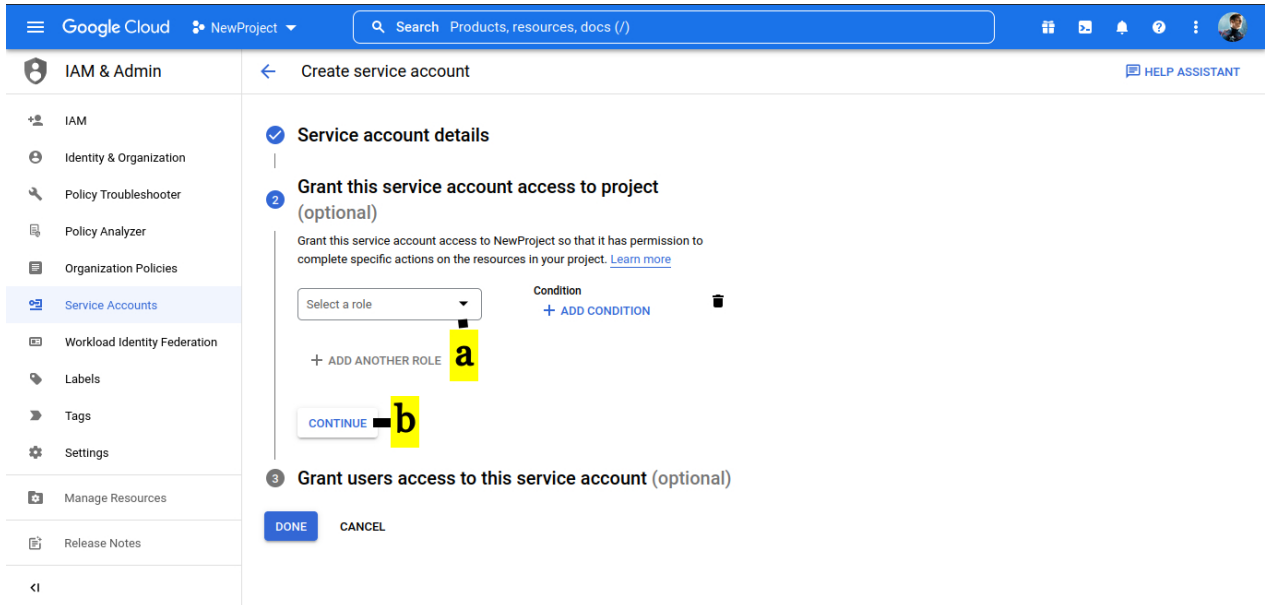
b. Click on **CREATE AND CONTINUE**



### 5. Grant this service account access to project.

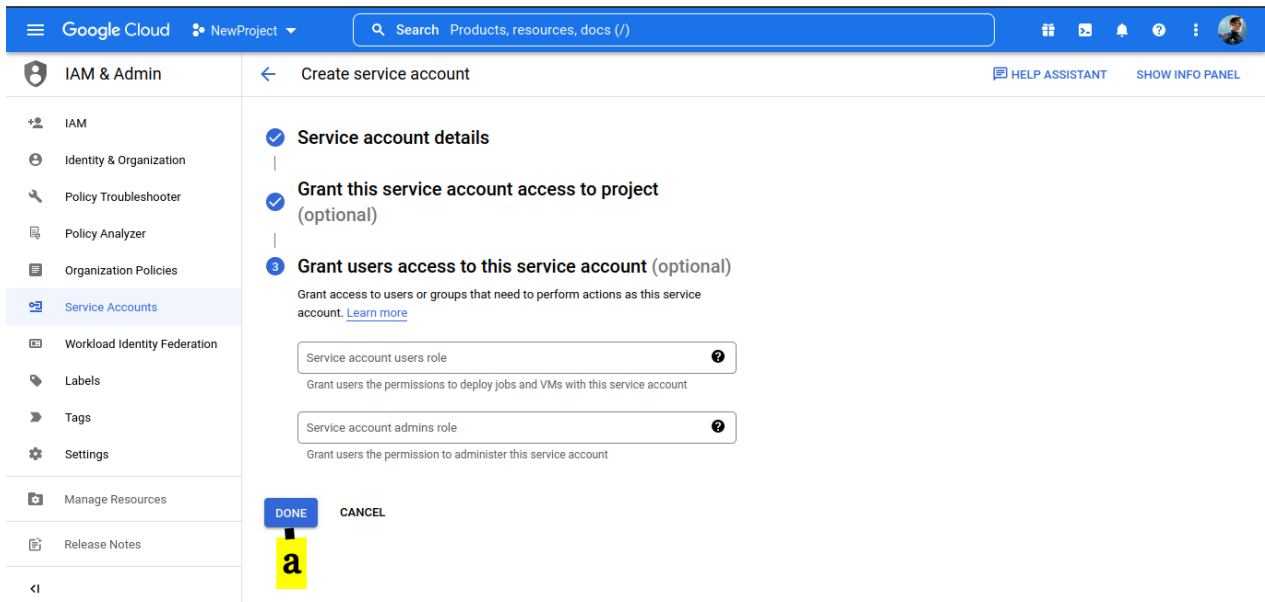
a. Select a role (**Basic -> Owner**)

b. Click on **CONTINUE**



6. Grant users access to this service account (optional)

a. Keep the defaults and click on **DONE**



7. On service account window.

a. Click on Action button **denoted by the three vertical dots**

## b. Select **Manage Keys**

The screenshot shows the Google Cloud IAM & Admin console for project "NewProject". The left sidebar lists various IAM & Admin tools, with "Service Accounts" selected. The main content area displays "Service accounts for project 'NewProject'", including a description and a table of service accounts. The table has columns for Email, Status, Name, Description, Key ID, Key creation date, OAuth 2 Client ID, and Actions. One service account is listed: "gdrive@newproject-363011.lam.gserviceaccount.com" with a status of "Active" and a description of "GDrive". A context menu is open over the "Actions" column for this service account, with "Manage keys" highlighted. A yellow box labeled "a" is next to the "Actions" column header, and another yellow box labeled "b" is next to the "Manage keys" option in the menu.

Email	Status	Name	Description	Key ID	Key creation date	OAuth 2 Client ID	Actions
<a href="mailto:gdrive@newproject-363011.lam.gserviceaccount.com">gdrive@newproject-363011.lam.gserviceaccount.com</a>	Active	GDrive		No keys		108312808797694190342	Manage details Manage permissions Manage keys View metrics View logs Disable Delete

## 8. Create a key

### a. Drop down **ADD KEY**

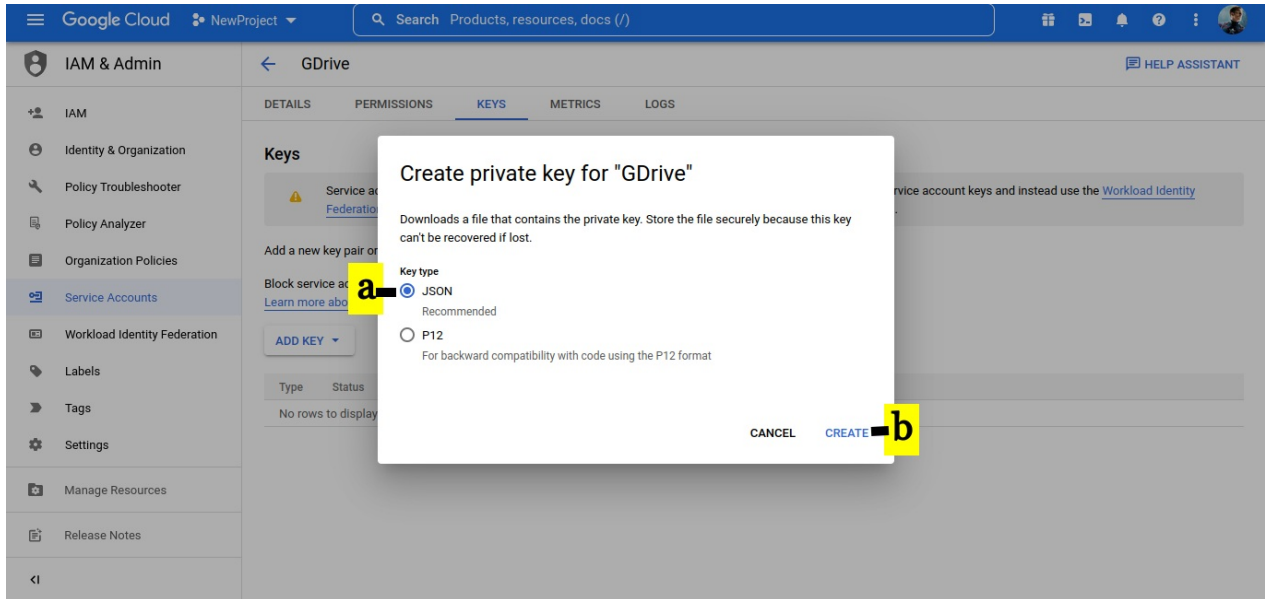
### b. Select **Create new key**

The screenshot shows the Google Cloud IAM & Admin console for project "NewProject", specifically the "Keys" page for the "GDrive" service account. The page has tabs for DETAILS, PERMISSIONS, KEYS, METRICS, and LOGS. A warning message is displayed at the top. Below the warning, there are instructions on how to add a new key pair or upload a public key certificate. The "ADD KEY" dropdown menu is open, showing two options: "Create new key" and "Upload existing key". The "Create new key" option is selected. A yellow box labeled "a" is next to the "ADD KEY" dropdown, and another yellow box labeled "b" is next to the "Create new key" option.

## 9. In Create private key.

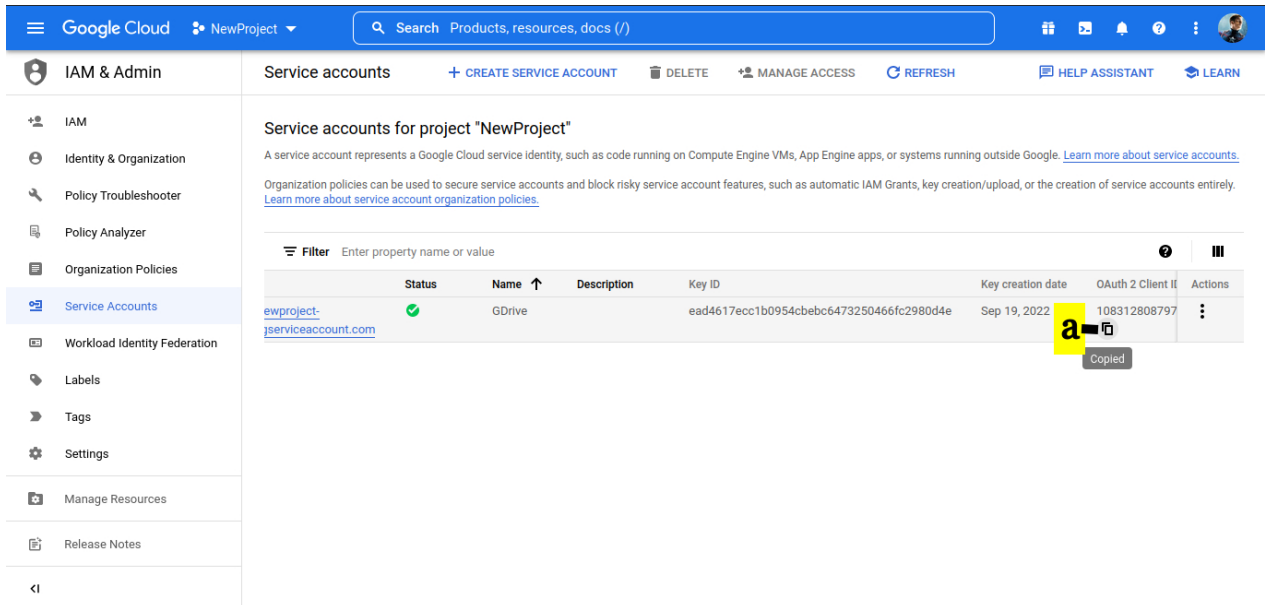
### a. Select **JSON**

b. Click on **CREATE**. On creation, the key will be downloaded to your desktop. This will be required in Step 4



10. Copy OAuth 2 Client ID - this will be required in step 3

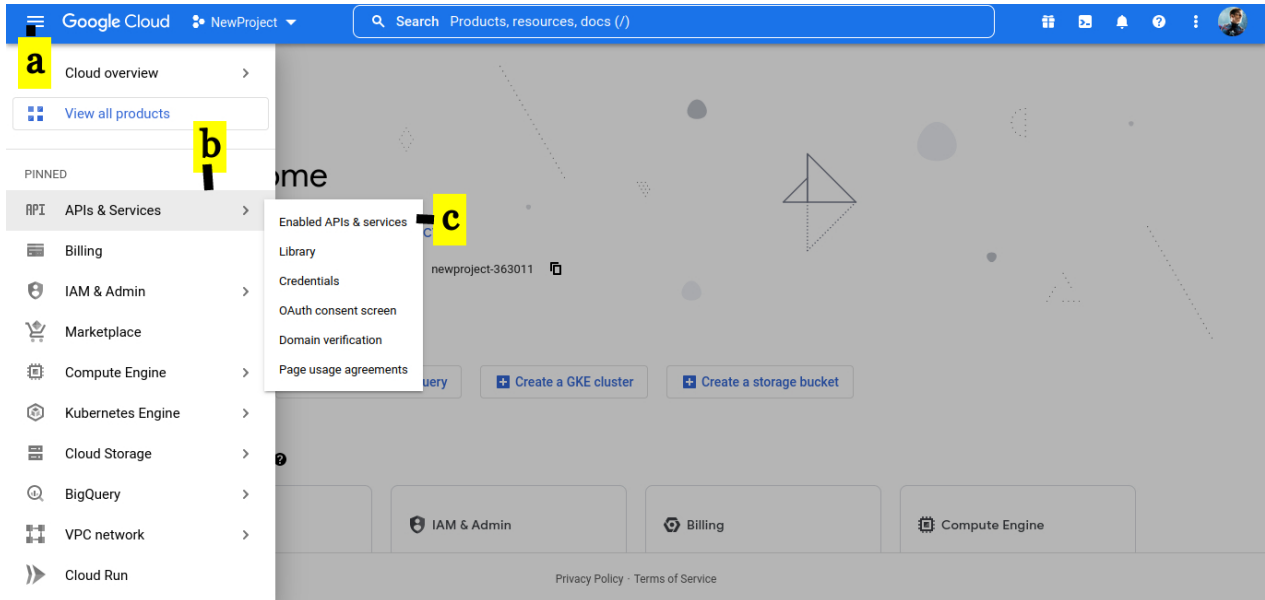
a. On copying the key, you will see the message **Copied**



## Step 2: Enable the API Services

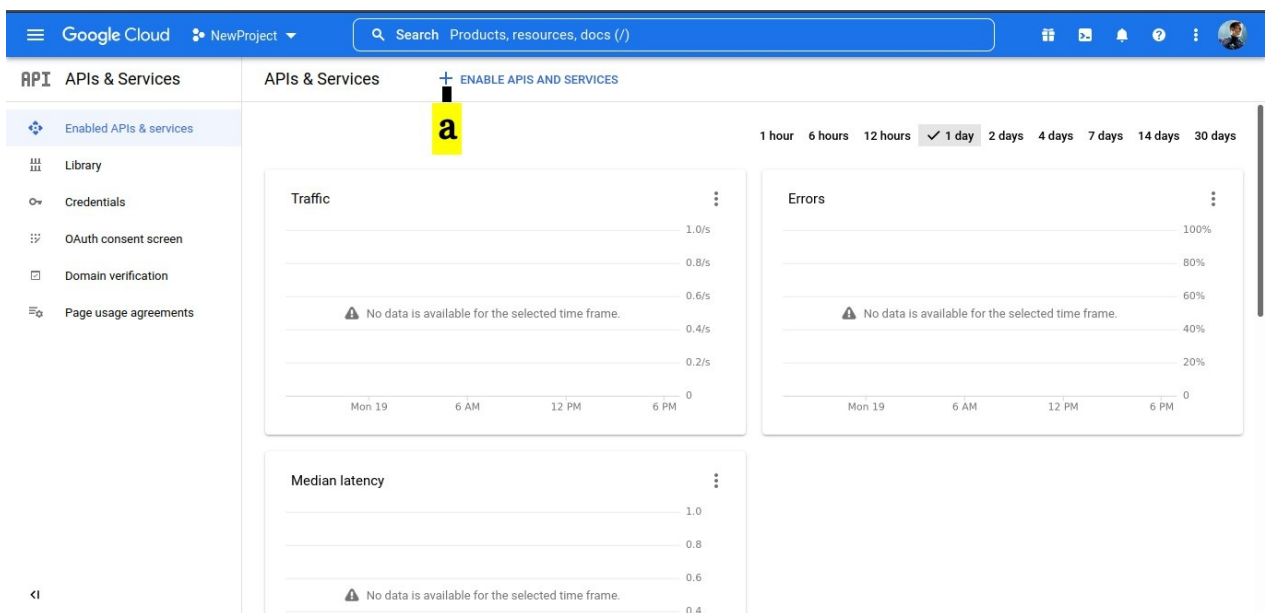
## 1. Enable API Services

- a. Click on top left panel
- b. Select **APIs & Services**
- c. Click on **Enabled APIs & services**



## 2. In the APIs & Services console

- a. Click on **ENABLE APIS AND SERVICES**

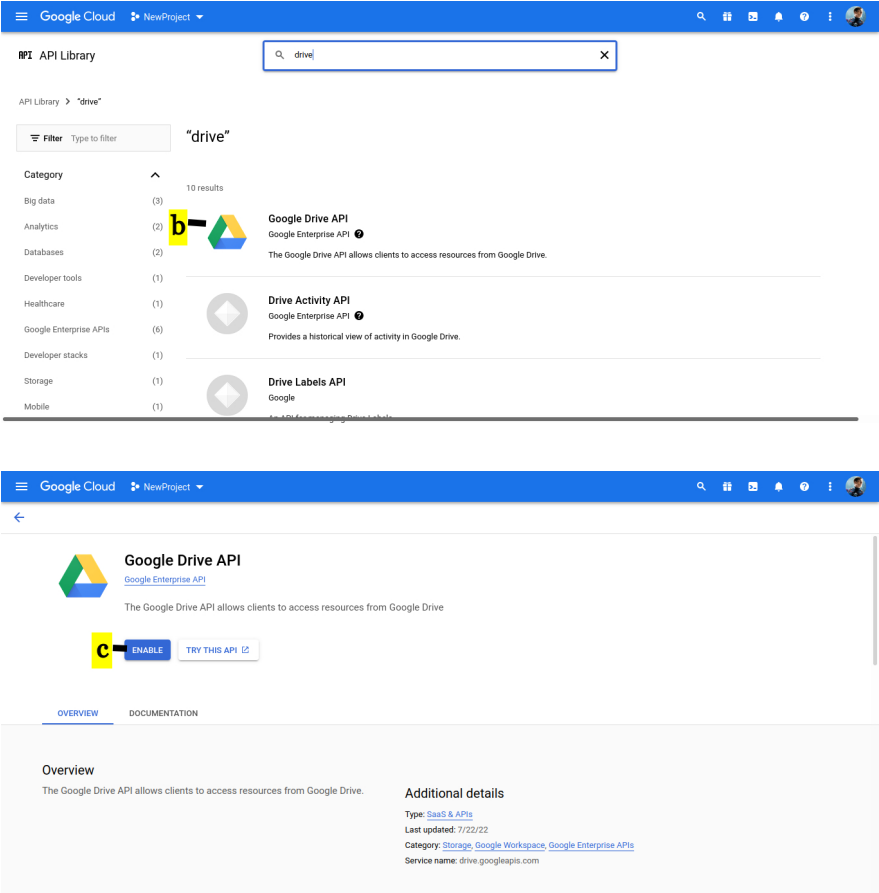


3. In the API Library,

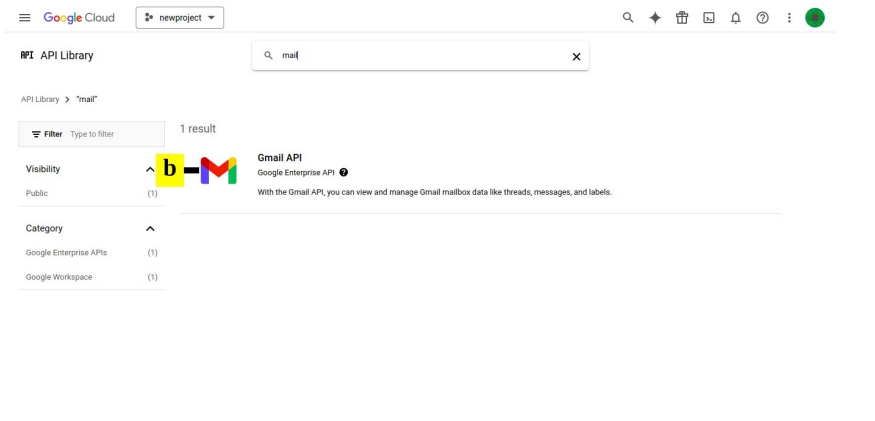
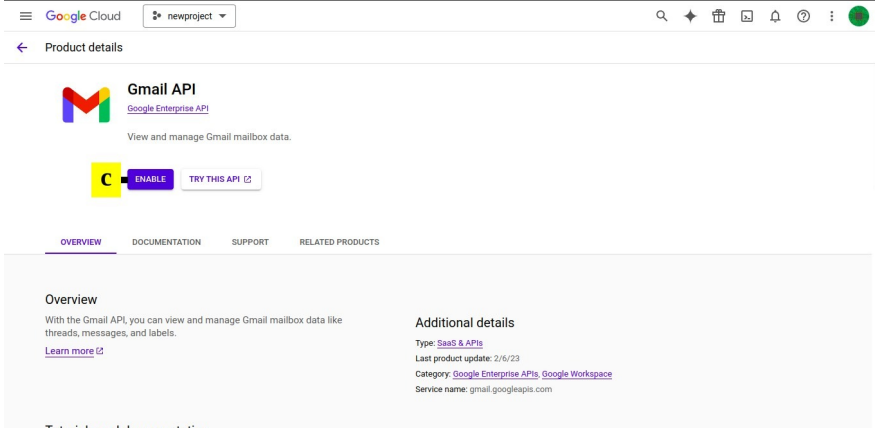
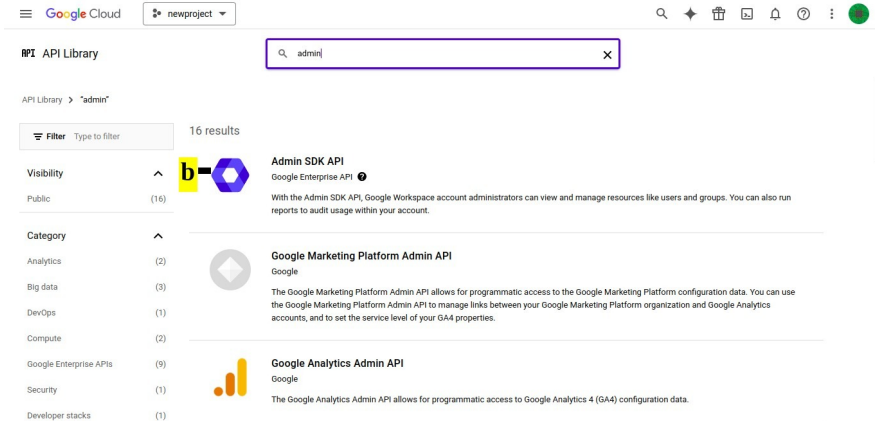
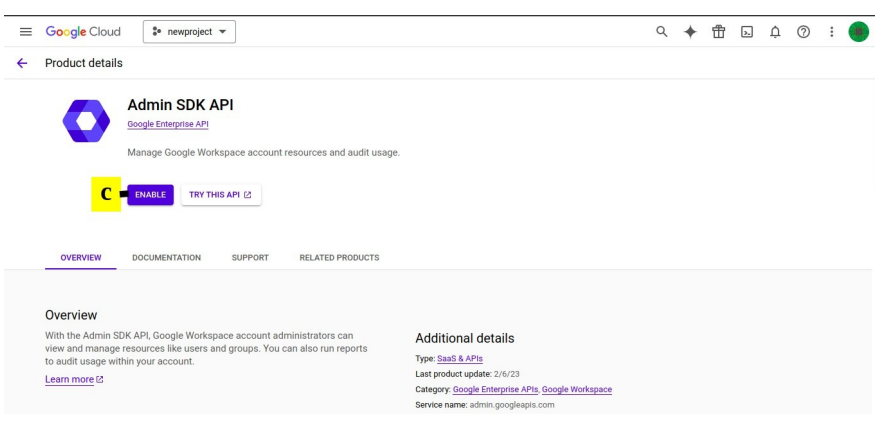
**b. search for the required APIs**

**c. Enable the API.**

The table below gives the list of API required to be enabled for different data source

Data source	API	Screenshots
<p><b>Drive Data</b> Required if you want to access data in any user's drive</p>	<p><b>Google Drive API</b></p>	 <p>The screenshot shows the Google Cloud API Library interface. The top navigation bar includes 'Google Cloud' and 'NewProject'. A search bar contains the text 'drive'. Below the search bar, the API Library is filtered to show results for 'drive'. A list of categories is shown on the left, including Big data (3), Analytics (2), Databases (2), Developer tools (1), Healthcare (1), Google Enterprise APIs (6), Developer stacks (1), Storage (1), and Mobile (1). The search results list includes 'Google Drive API' (Google Enterprise API), 'Drive Activity API' (Google Enterprise API), and 'Drive Labels API' (Google). The second screenshot shows the 'Google Drive API' detail page, which includes the Google Drive logo, the text 'The Google Drive API allows clients to access resources from Google Drive', and an 'ENABLE' button. Below the button are tabs for 'OVERVIEW' and 'DOCUMENTATION'. The 'OVERVIEW' tab is selected, showing the text 'The Google Drive API allows clients to access resources from Google Drive.' and 'Additional details' such as 'Type: SaaS &amp; APIs', 'Last updated: 7/22/22', 'Category: Storage, Google Workspace, Google Enterprise APIs', and 'Service name: drive.googleapis.com'.</p>



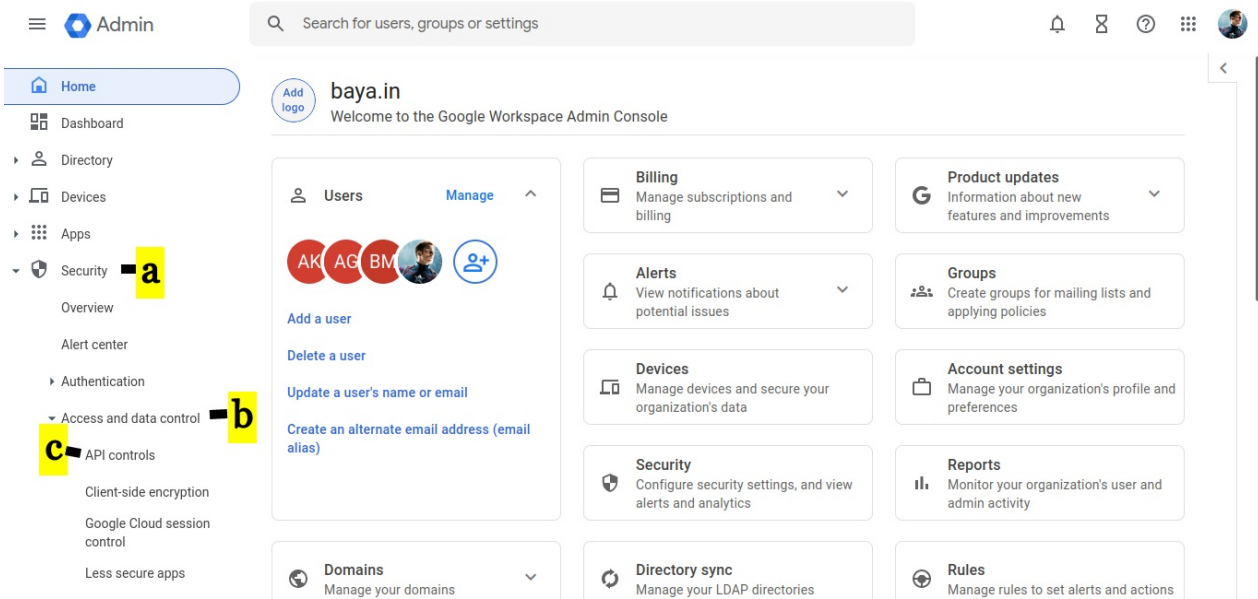
Data source	API	Screenshots
<p><b>Mailbox data</b></p> <p>Required if you want to access data from any user's mailbox</p>	<p><b>GMail API</b></p>	 
<p><b>Distribution List members</b></p> <p>Required if you want to automatically schedule requests for members of any DL</p>	<p><b>Admin SDK API</b></p>	 

### Step 3: Enable domain-wide delegation

Login to G-suite Admin account and navigate to [Google Admin](https://admin.google.com/) (<https://admin.google.com/>).

Http link: [https://admin.google.com](https://admin.google.com/) (<https://admin.google.com/>)

- a. Click on **Security**
- b. Select on **Access and data control**
- c. Click on **API controls**



- d. Click On **MANAGE DOMAIN WIDE DELEGATION**

Admin

Search for users, groups or settings

Security > API Controls

### API controls

Use these controls to enable or restrict access to Google Workspace APIs for customer-owned and third-party applications and service accounts. Reduce the risk associated with third-party access to Google Workspace APIs by limiting access to only trusted apps.

- Block all third-party API access  
Requests by third-party apps are denied access to Google Workspace data and end user data. This setting blocks all OAuth scopes, including sign-in scopes. [Learn more](#)
- Trust internal, domain-owned apps  
Internal, domain-owned apps will be exempt from accessing OAuth scopes that are restricted or blocked.

Apps you trust on the [Google Workspace Marketplace](#), [Android](#), or [iOS](#) allowlist are automatically trusted on your App access control list.

CANCEL SAVE

### Domain wide delegation

Developers can register their web applications and other API clients with Google to enable access to data in Google services like Gmail. You can authorize these registered clients to access your user data without your users having to individually give consent or their passwords. [Learn more](#)

**d** [MANAGE DOMAIN WIDE DELEGATION](#)

ogs.google.com

e. Click on **Add new**

Admin

Search for users, groups or settings

Security > API Controls > Domain-wide Delegation

Developers can register their web applications and other API clients with Google to enable access to data in Google services like Gmail. You can authorize these registered clients to access your user data without your users having to individually give consent or their passwords. [GOT IT](#)

API client **e** [Add new](#) [Download client info](#)

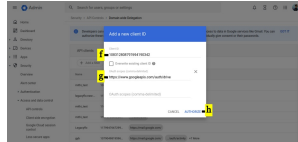
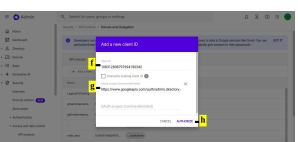
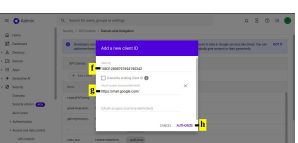
+ Add a filter

Name	Client ID	Scopes
mithi_test	1054597958099...	.../auth/drive
legacyflo-new...	1171772859178...	https://mail.google.com/
mithi_test	1106913801566...	https://mail.google.com/
mithi_test	1107970549200...	.../auth/drive
Legacyflo	1179947667299...	https://mail.google.com/
gyb	1079049819596...	https://mail.google.com/ .../auth/activity +7 More

f. Paste the Client ID which you copied earlier

g. In OAuth scopes (comma-delimited), provide the string for the relevant API

h. Click the AUTHORIZE button

GDrive API	<a href="https://www.googleapis.com/auth/drive">https://www.googleapis.com/auth/drive</a> (Required if you want to access data in any user's drive)	
Admin SDK API	<a href="https://www.googleapis.com/auth/admin.directory.group.readonly">https://www.googleapis.com/auth/admin.directory.group.readonly</a> (Required if you want to use Distribution List ID in the LegacyFlo Scheduler)	
Gmail API	<a href="https://mail.google.com/">https://mail.google.com/</a> (Required if you want to access data in any user's mailbox )	

This completes the process of enabling the domain-wide delegation for GSuite for the required API

## Step 4: Register with LegacyFlo

When you generated the key, it was downloaded to your desktop as a JSON file. This key has to be registered with LegacyFlo.

1. **Login** into LegacyFlo
2. From the menu on the left side, click on the **Profile icon at the bottom**
3. On the pop-up menu, select **Google Workspace integrations**
4. If you have an access key for **GMail**, select **Gmail**. If you have an access key for **GDrive**, select **GDrive**
5. To register the access key for a new domain, click on the **+ sign next to Register Key for the domain**
  1. Your user id, Client App, and Resource Owner fields will be pre-filled. **Enter the domain name** for which the key is to be registered
  2. Enter the **Google Workspace Admin ID** for which the key was registered.
  3. **Choose the JSON file** which has been downloaded to your desktop.
  4. Click on **Save**
  5. **Close** the dialog box.
6. To update the key for a domain, click on the edit icon next to the domain name and chose the new JSON file