

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](#)

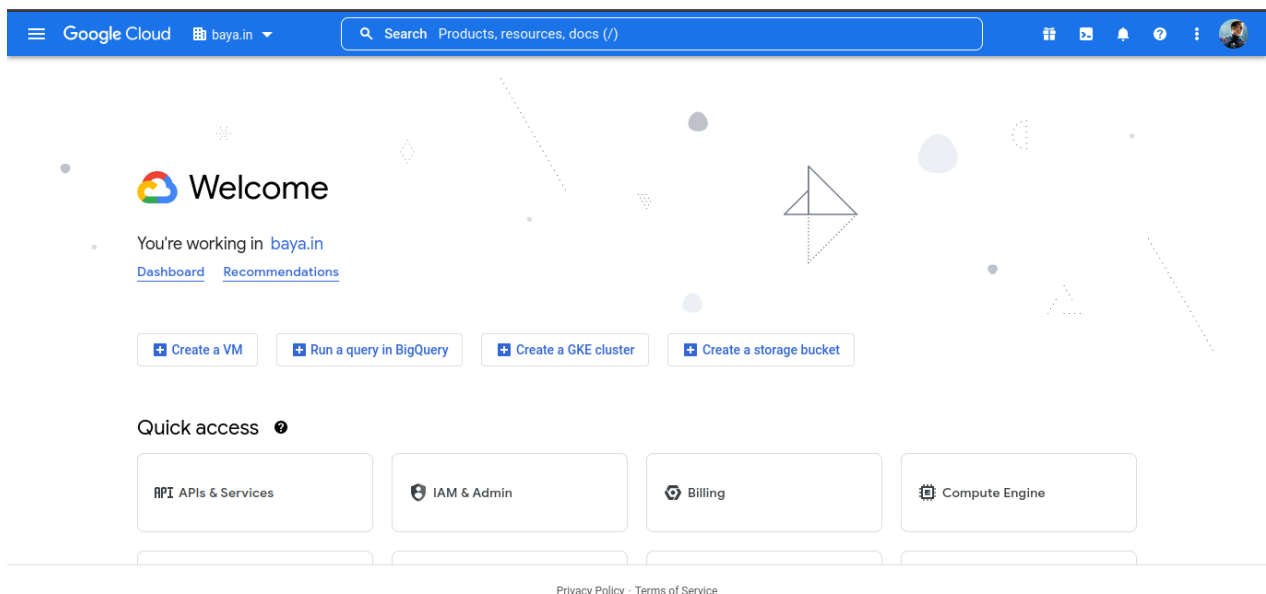
[Step 4: Register with LegacyFlo](#)

Step 1: Create the access key

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

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

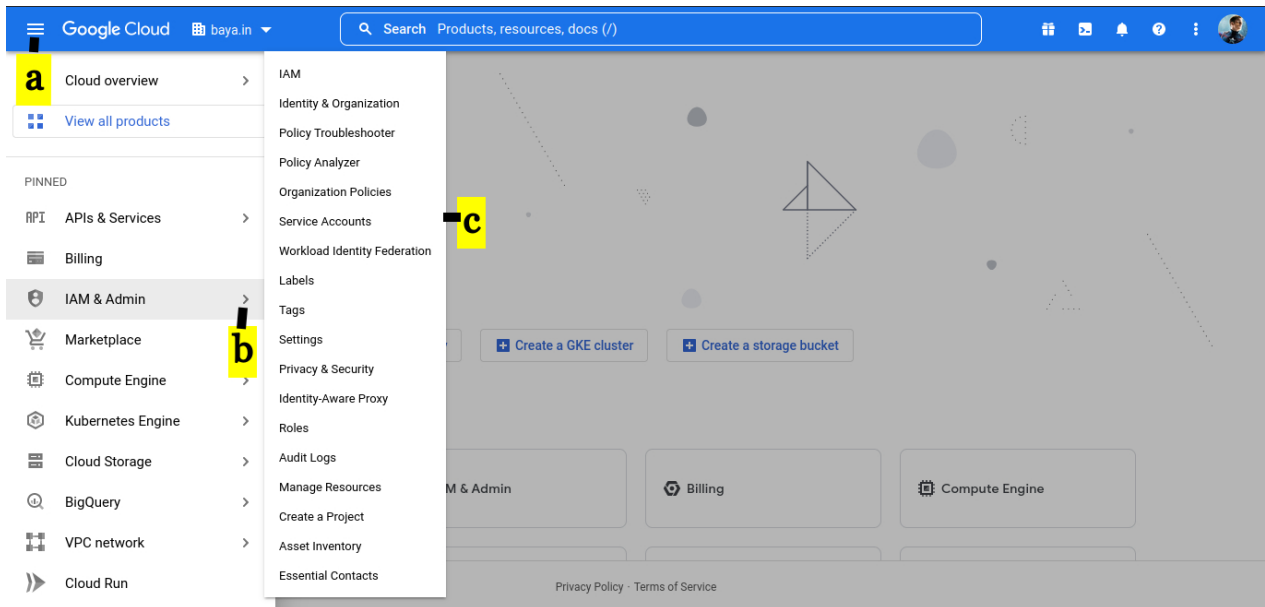
Http link: <https://console.developers.google.com> (<https://console.developers.google.com/>)



a. Select top left panel.

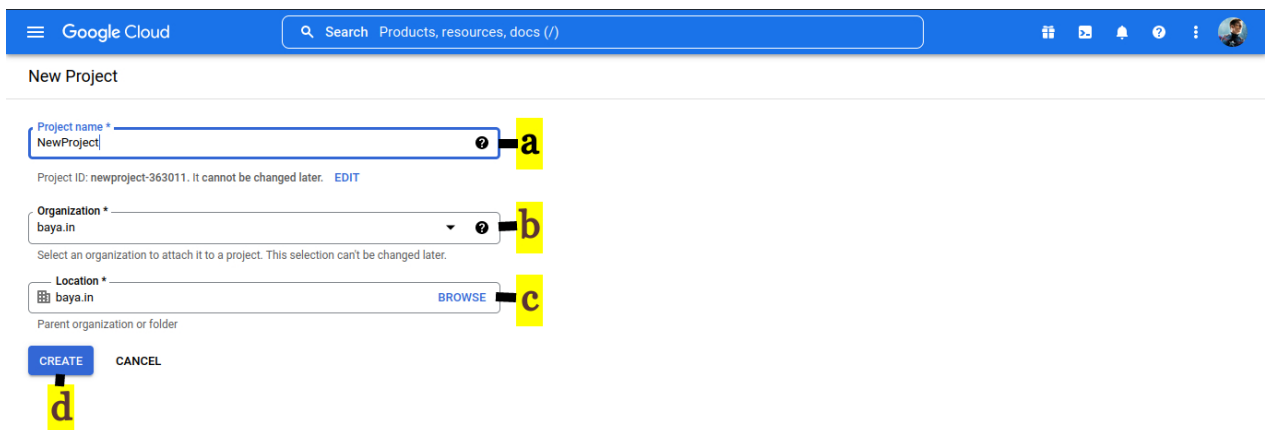
b. Select **IAM & Admin**.

c. Select Service Accounts.



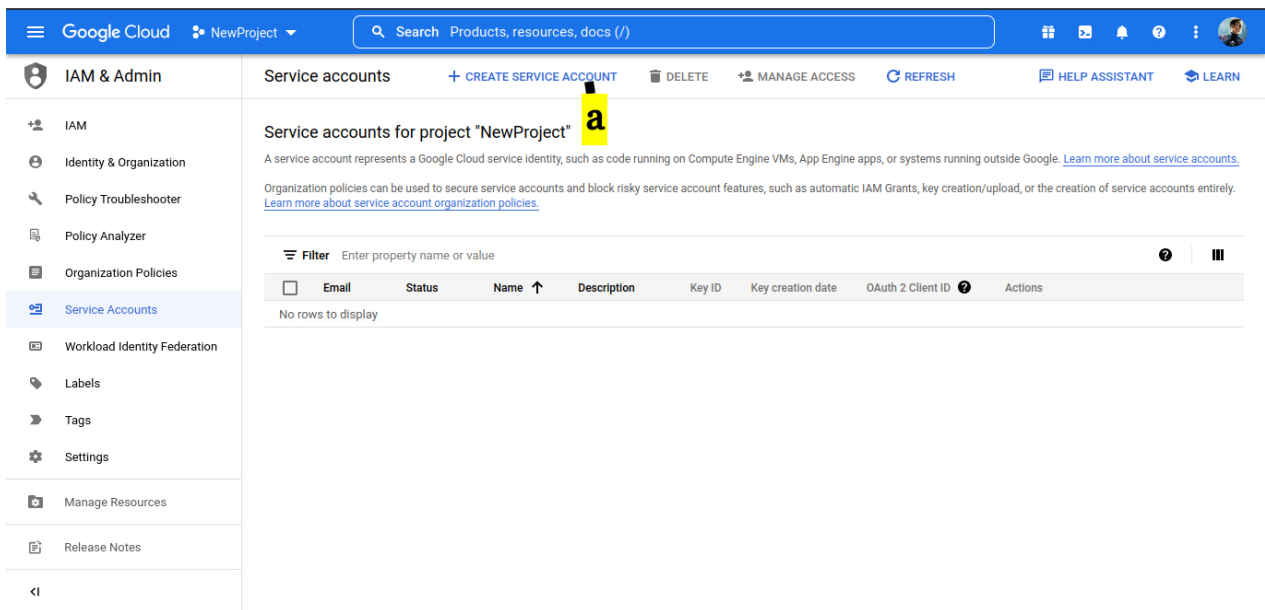
2. CREATE A PROJECT

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



3. Create a service account

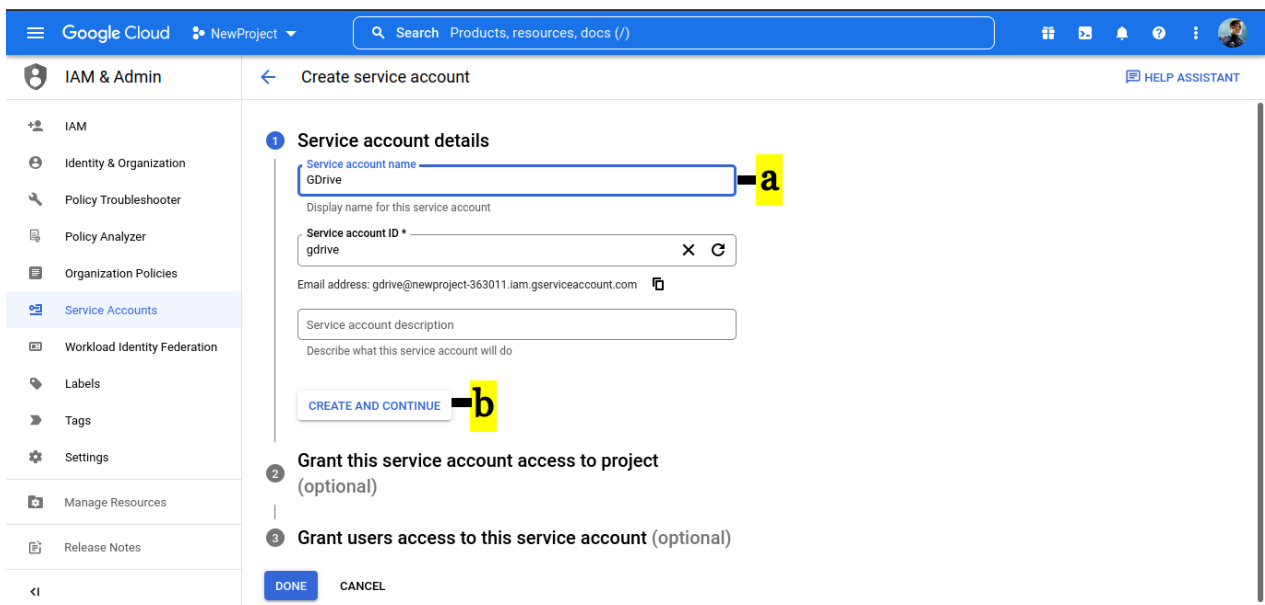
a. Click CREATE SERVICE ACCOUNT.



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

Google Cloud NewProject Search Products, resources, docs (/)

IAM & Admin Create service account HELP ASSISTANT

Service account details

Grant this service account access to project (optional)

Grant this service account access to NewProject so that it has permission to complete specific actions on the resources in your project. [Learn more](#)

Select a role Condition + ADD CONDITION

+ ADD ANOTHER ROLE a

CONTINUE b

Grant users access to this service account (optional)

DONE CANCEL

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

a. Keep the defaults and click on DONE

Google Cloud NewProject Search Products, resources, docs (/)

IAM & Admin Create service account HELP ASSISTANT SHOW INFO PANEL

Service account details

Grant this service account access to project (optional)

Grant users access to this service account (optional)

Grant access to users or groups that need to perform actions as this service account. [Learn more](#)

Service account users role ?
Grant users the permissions to deploy jobs and VMs with this service account

Service account admins role ?
Grant users the permission to administer this service account

DONE a CANCEL

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, "GDrive", is listed with a status of "Active" and "No keys". A context menu is open over the "GDrive" service account, showing options: "Manage details", "Manage permissions", "Manage keys", "View metrics", "View logs", "Disable", and "Delete". The "Manage keys" option is highlighted with a yellow box labeled "b".

Email	Status	Name	Description	Key ID	Key creation date	OAuth 2 Client ID	Actions
gdrive@newproject-363011.lam.gserviceaccount.com	Active	GDrive		No keys		108312808797694190342	a

8. Create a key

a. Drop down ADD KEY

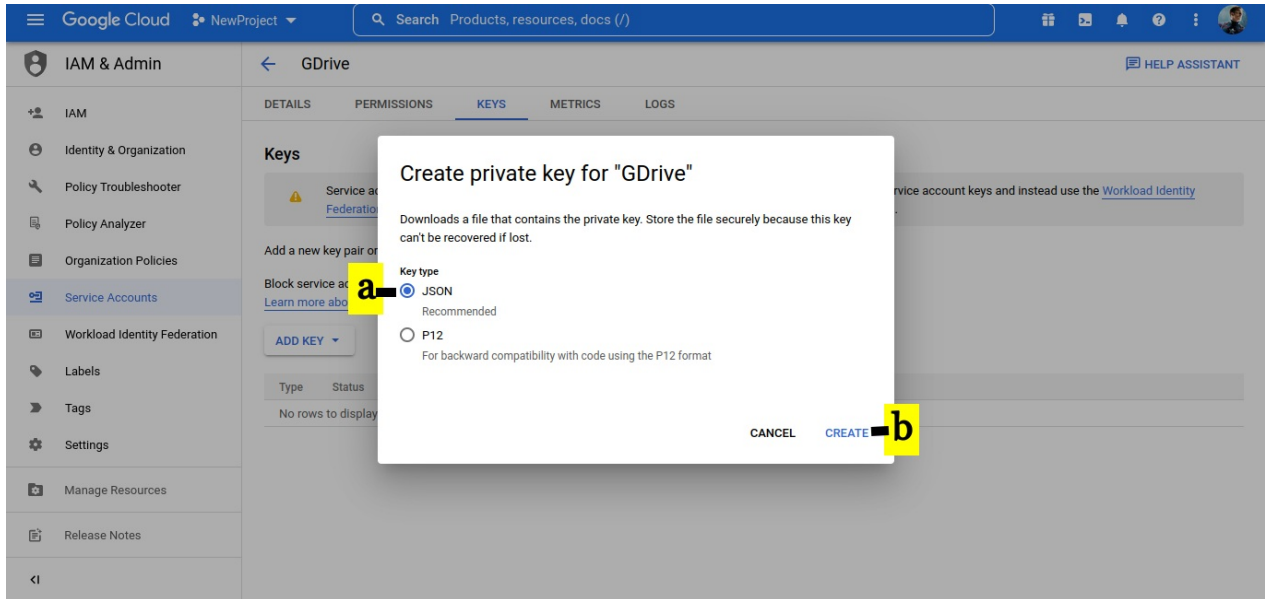
b. Select Create new key

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: "Service account keys could pose a security risk if compromised. We recommend you avoid downloading service account keys and instead use the Workload Identity Federation. You can learn more about the best way to authenticate service accounts on Google Cloud here." Below the warning, there are instructions to "Add a new key pair or upload a public key certificate from an existing key pair." and "Block service account key creation using organization policies." The "ADD KEY" dropdown menu is open, showing options: "Create new key" and "Upload existing key". The "Create new key" option is highlighted with a yellow box labeled "b".

9. In Create private key.

a. Select JSON

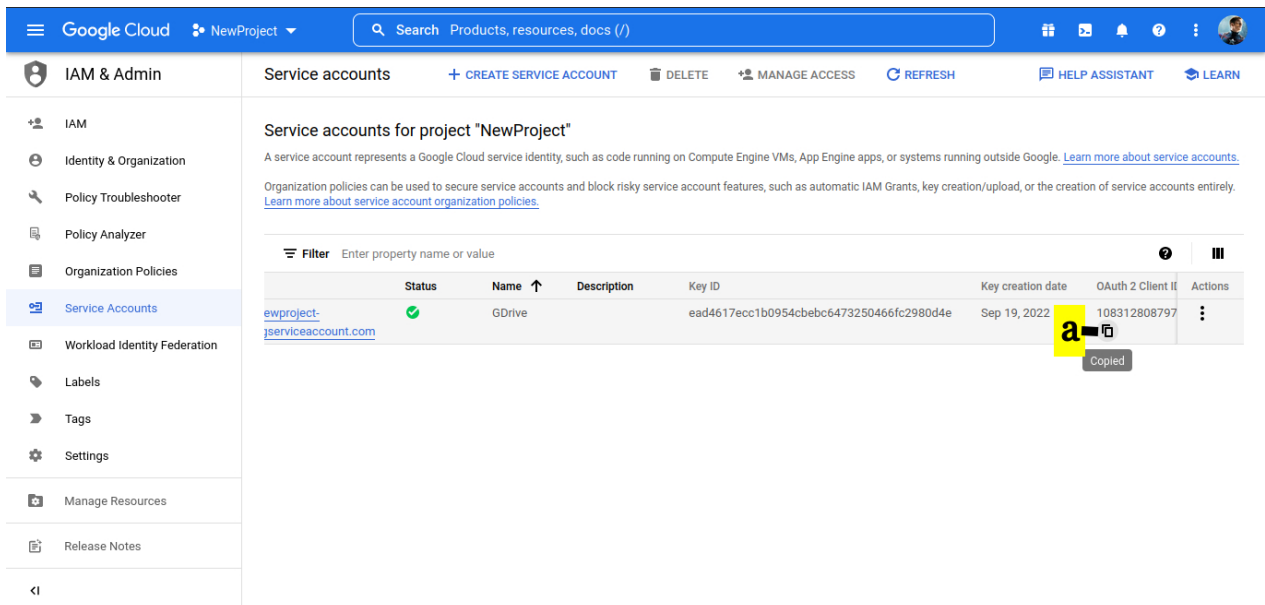
b. Click on CREATE. On creation, the key will be downloaded to your desktop. This will be required in Step 4



1. **IMPORTANT NOTE:** If you are unable to generate a key, then [follow the steps given here](https://docs.mithi.com/home/enable-service-account-key-creation) (<https://docs.mithi.com/home/enable-service-account-key-creation>).

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

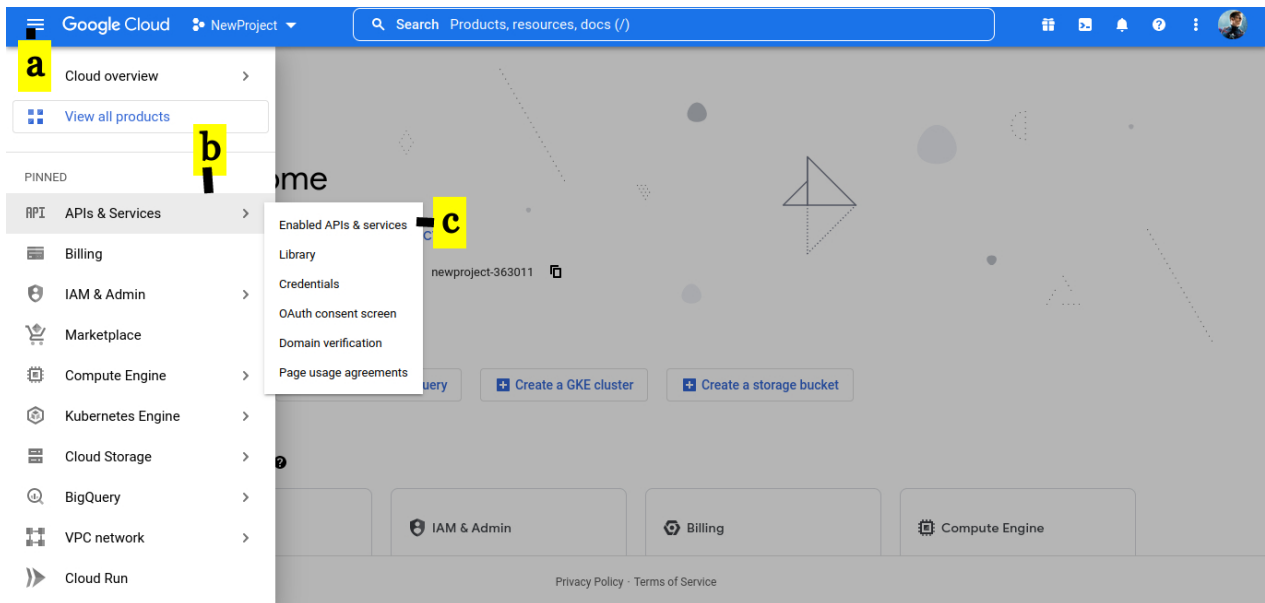
a. On copying the key, you will see the message Copied



Step 2: Enable the API Services

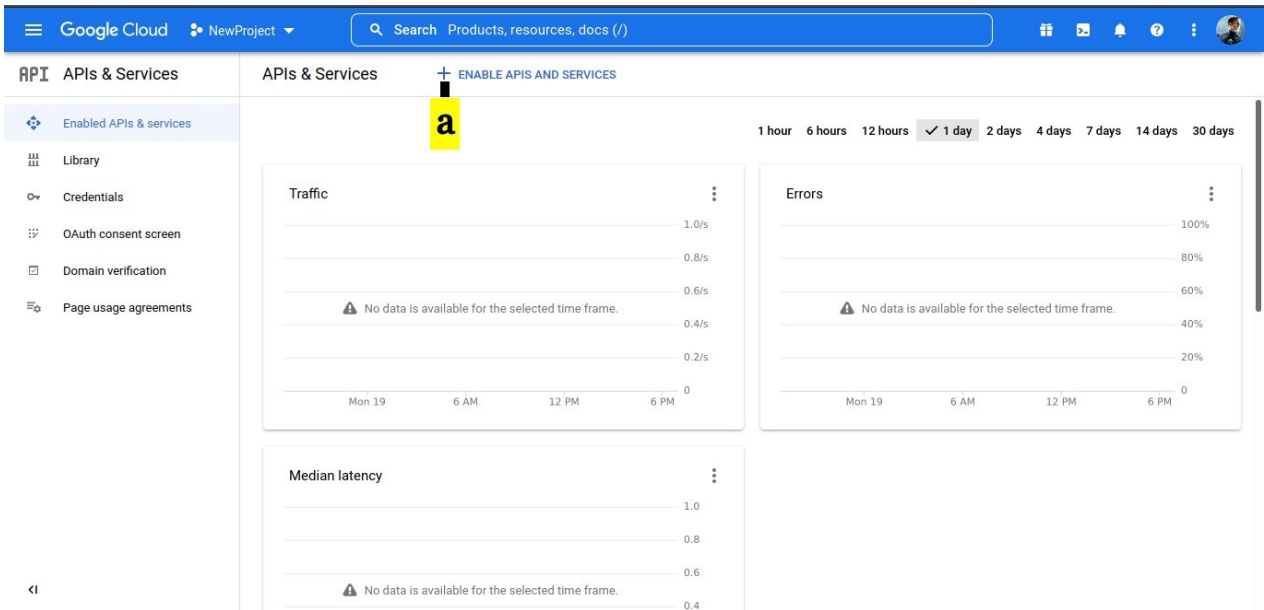
1. Enable API Services

- 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**



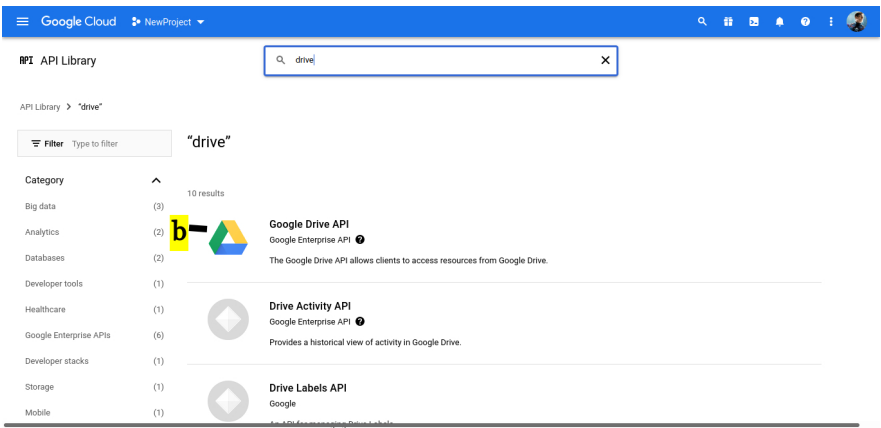
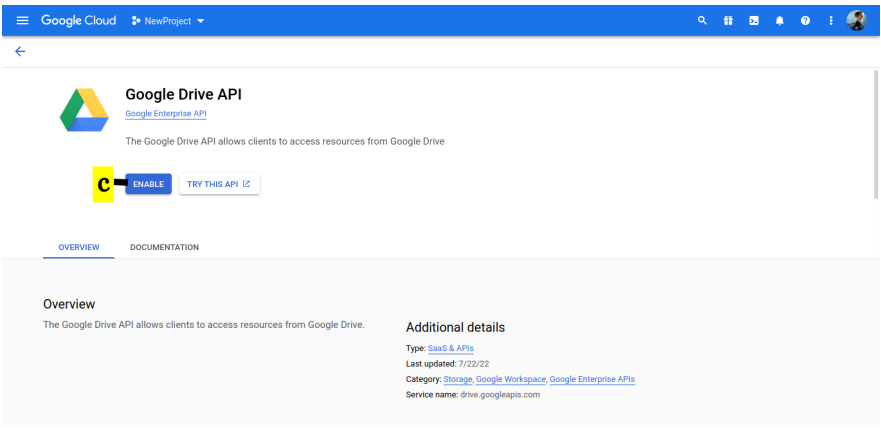
3. In the API Library,

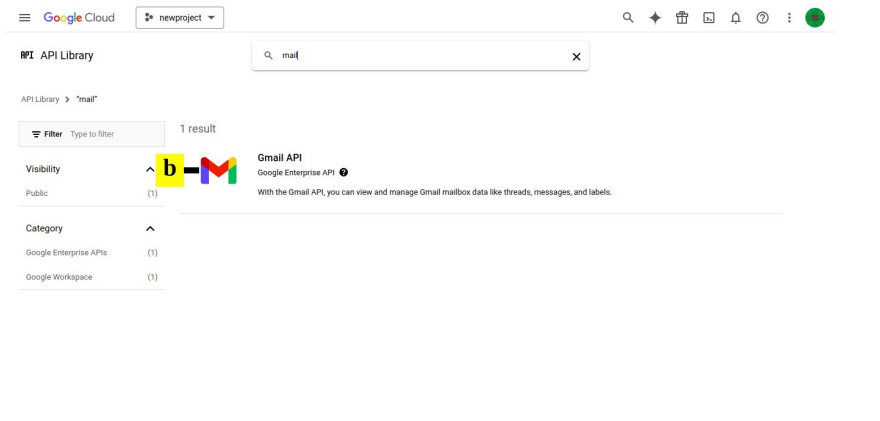
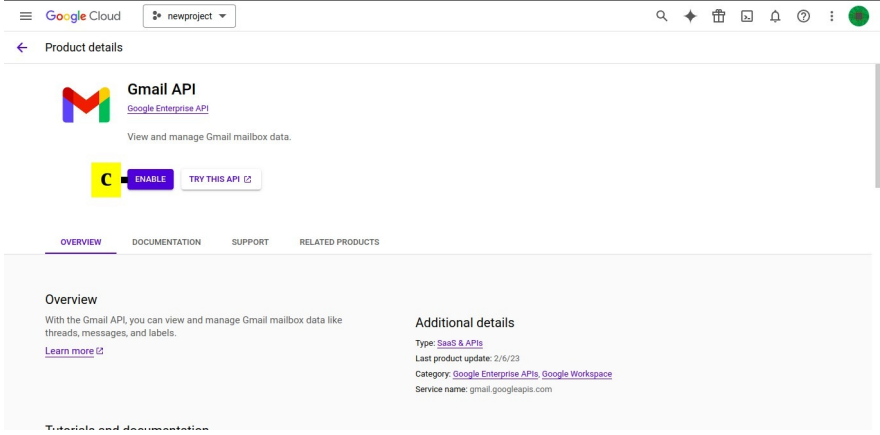
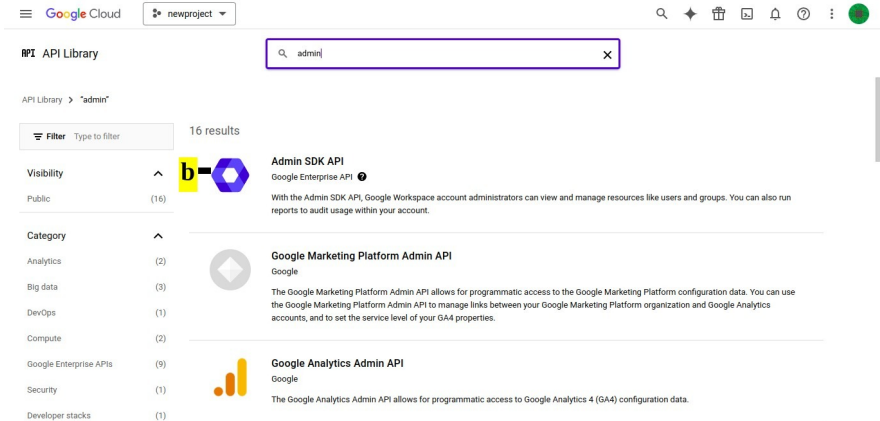
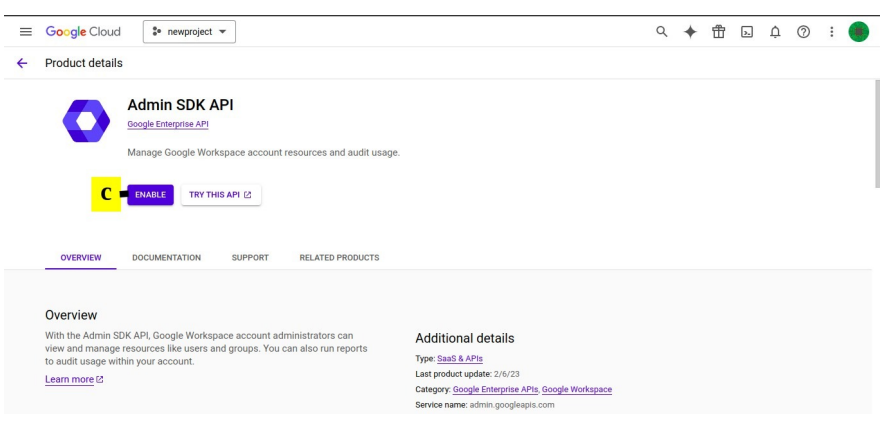
b. search for the required APIs

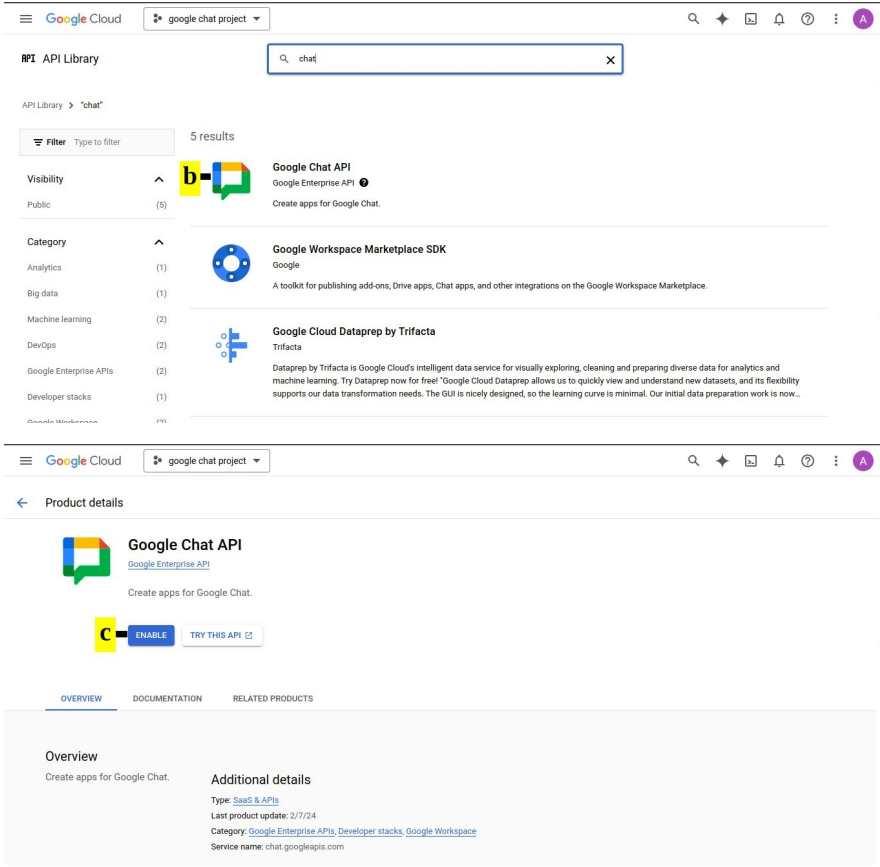
c. Enable the API.

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

Data source	API	Screenshots
-------------	-----	-------------

Data source	API	Screenshots
<p>Drive Data</p> <p>For:</p> <ol style="list-style-type: none"> 1. User's data in drive 2. Google Chat data 	<p>Google Drive API</p>	 <p>The first screenshot shows the Google Cloud API Library search interface. The search bar contains 'drive', and the results list includes 'Google Drive API', 'Drive Activity API', and 'Drive Labels API'. The 'Google Drive API' is highlighted with a yellow 'b' icon.</p>  <p>The second screenshot shows the detail page for the Google Drive API. It includes the API logo, a description: 'The Google Drive API allows clients to access resources from Google Drive', and buttons for 'ENABLE' and 'TRY THIS API ID'. Below this, there are tabs for 'OVERVIEW' and 'DOCUMENTATION', and an 'Overview' section with additional details like 'Type: SaaS & 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>Mailbox data</p> <p>For user's mailbox</p>	<p>GMail API</p>	 <p>The screenshot shows the Google Cloud API Library search results for 'mail'. It displays one result: the Gmail API, which is a Google Enterprise API. The API description states: 'With the Gmail API, you can view and manage Gmail mailbox data like threads, messages, and labels.' The API is categorized under Google Enterprise APIs and Google Workspace.</p>  <p>The screenshot shows the product details page for the Gmail API. It includes the Gmail logo, the API name 'Gmail API', and the description 'View and manage Gmail mailbox data.' There are buttons for 'ENABLE' and 'TRY THIS API'. The page also has tabs for 'OVERVIEW', 'DOCUMENTATION', 'SUPPORT', and 'RELATED PRODUCTS'. The 'Overview' section provides more details about the API's capabilities.</p>
<p>Directory Data</p> <p>For</p> <ol style="list-style-type: none"> 1. Distrubution 2. Google Chat 3. Mailbox size <p>List members Required for scheduler</p> <p>Data</p> <p>Mailbox size</p>	<p>Admin SDK API</p>	 <p>The screenshot shows the Google Cloud API Library search results for 'admin'. It displays 16 results. The top result is the Admin SDK API, which is a Google Enterprise API. The API description states: 'With the Admin SDK API, Google Workspace account administrators can view and manage resources like users and groups. You can also run reports to audit usage within your account.' The API is categorized under Google Enterprise APIs and Google Workspace.</p>  <p>The screenshot shows the product details page for the Admin SDK API. It includes the Admin SDK logo, the API name 'Admin SDK API', and the description 'Manage Google Workspace account resources and audit usage.' There are buttons for 'ENABLE' and 'TRY THIS API'. The page also has tabs for 'OVERVIEW', 'DOCUMENTATION', 'SUPPORT', and 'RELATED PRODUCTS'. The 'Overview' section provides more details about the API's capabilities.</p>

Data source	API	Screenshots
<p>Google Chat Data</p>	<p>Google Chat API</p>	 <p>The top screenshot shows the Google Cloud API Library search results for 'chat'. It lists five results, including Google Chat API, Google Workspace Marketplace SDK, and Google Cloud Dataprep by Trifacta. The bottom screenshot shows the product details for the Google Chat API, including an 'ENABLE' button and an 'OVERVIEW' section.</p> <p>IMPORTANT NOTE: In addition to Enabling the Google Chat API, you have to update the configuration as given here (https://docs.mithi.com/home/google-chat-api-configuration).</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/>)

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

Admin | Search for users, groups or settings

Home | Dashboard | Directory | Devices | Apps | Security **a** | Authentication | Access and data control **b** | API controls | Client-side encryption | Google Cloud session control | Less secure apps | Reporting | Billing | Account | Rules | Storage

baya.in
Welcome to the Google Workspace Admin Console

Users Manage

Add a user
Delete a user
Update a user's name or email
Create an alternate email address (email alias)

Billing Manage subscriptions and billing

Alerts View notifications about potential issues

Devices Manage devices and secure your organization's data

Security Configure security settings, and view alerts and analytics

Domains Manage your domains

Directory sync Manage your LDAP directories

Product updates Information about new features and improvements

Groups Create groups for mailing lists and applying policies

Account settings Manage your organization's profile and preferences

Reports Monitor your organization's user and admin activity

Rules Manage rules to set alerts and actions

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

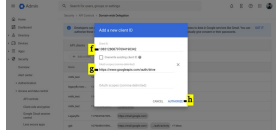
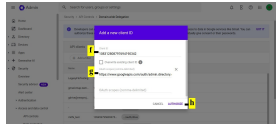
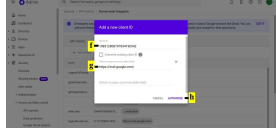
+ Add a filter

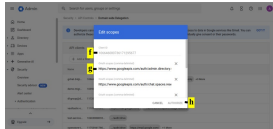
Name	Client ID	Scopes
mithi_test	1054597958099...	.../auth/drive
legacyflo-new...	1171772859178...	https://mail.google.com/
mithi_test	1106913801566...	https://mail.google.com/
mithi_test	1107970549200...	.../auth/drive
Legacyflo	1179947667299...	https://mail.google.com/
gyb	1079049819596...	https://mail.google.com/ .../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	https://www.googleapis.com/auth/drive (Required if you want to access data in any user's drive AND if you want to archive Google Chat transcripts)	
Admin SDK API	https://www.googleapis.com/auth/admin.directory.group.readonly (Required if you want to use Distribution List ID in the LegacyFlo Scheduler) https://www.googleapis.com/auth/admin.directory.user.readonly (Required if you want to archive Google Chat transcripts) https://www.googleapis.com/auth/admin.reports.usage.readonly (Required to calculate mailbox size for mailbox data migration)	
Gmail API	https://mail.google.com/ (Required if you want to access data in any user's mailbox)	

Google Chat API	https://www.googleapis.com/auth/chat.spaces.readonly https://www.googleapis.com/auth/chat.messages.readonly https://www.googleapis.com/auth/chat.memberships.readonly (Required if you want to access Google Chat transcripts)	
--------------------	---	---

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