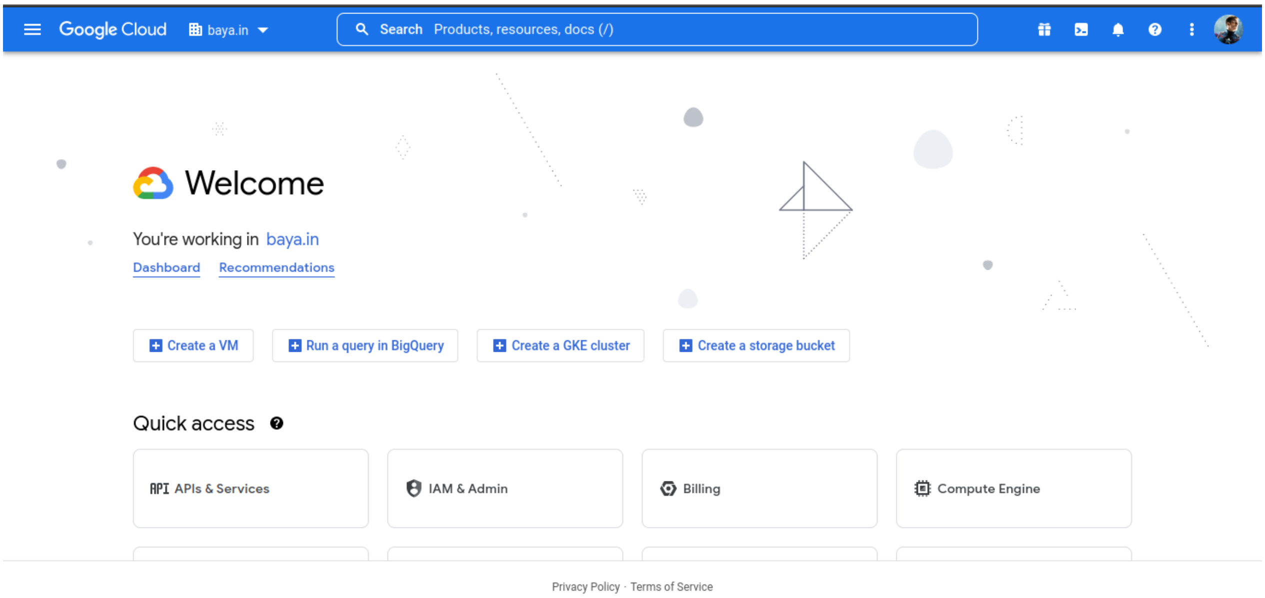
Preparation for Google Workspace by enabling domain-wide delegation using OAuth service

Table of Contents

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/)



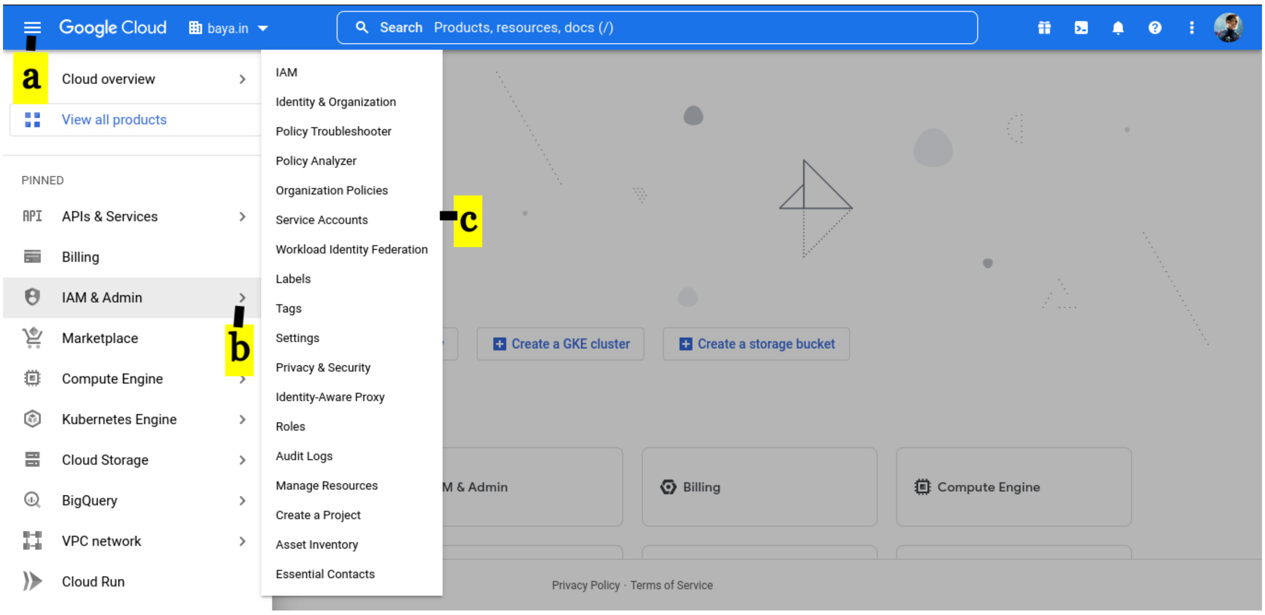
Welcome

You're working in baya.in

a. Select top left panel.

b. Select **IAM & Admin**.

c. Select **Service Accounts**.



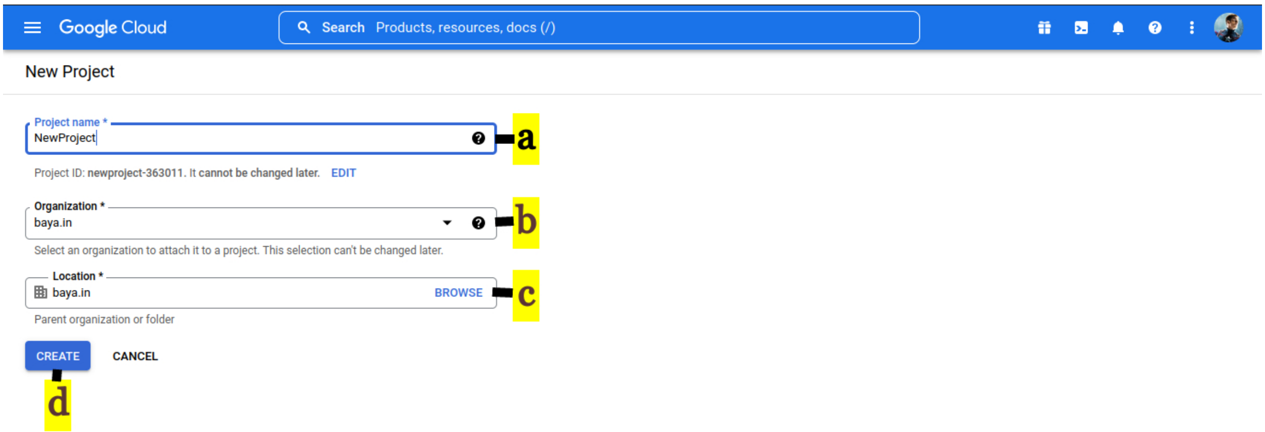
2. CREATE A PROJECT

a. Provide **Project name**.

b. Select the **Organization**.

c. Browse for the **Location**.

d. Click on **CREATE**.



New Project

Project name * NewProject

Project ID: newproject-363011. It cannot be changed later. EDIT

Organization * baya.in

Select an organization to attach it to a project. This selection can't be changed later.

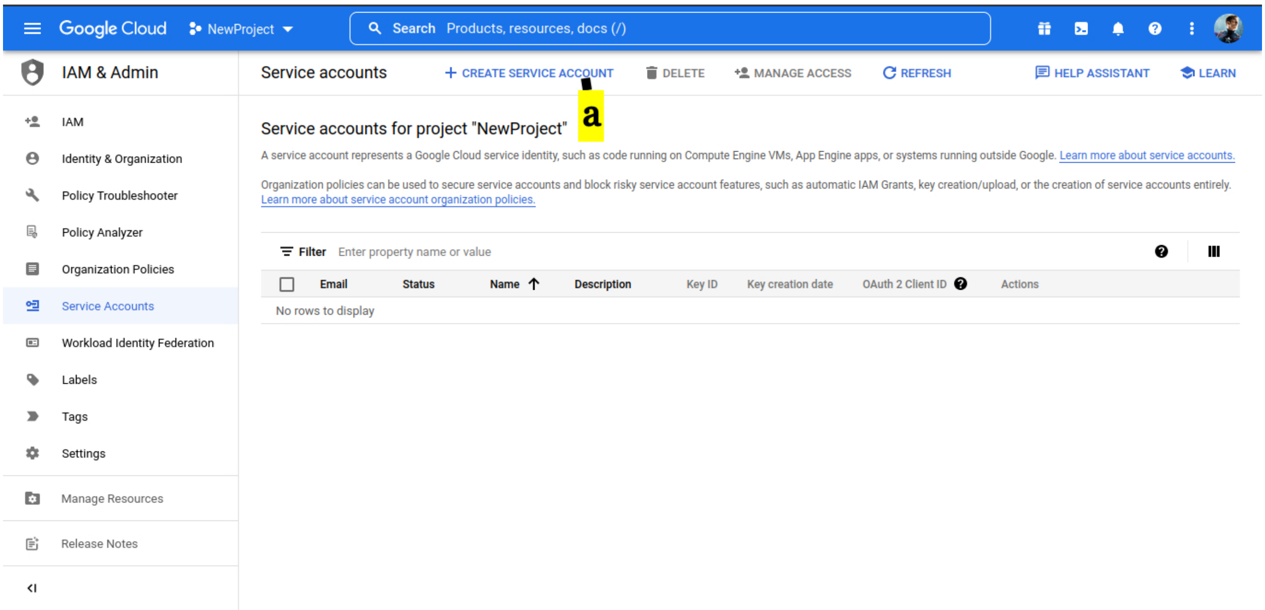
Location * baya.in BROWSE

Parent organization or folder

CREATE CANCEL

3. Create a service account

a. Click **CREATE SERVICE ACCOUNT.**



Service accounts for project "NewProject"

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 about service accounts.

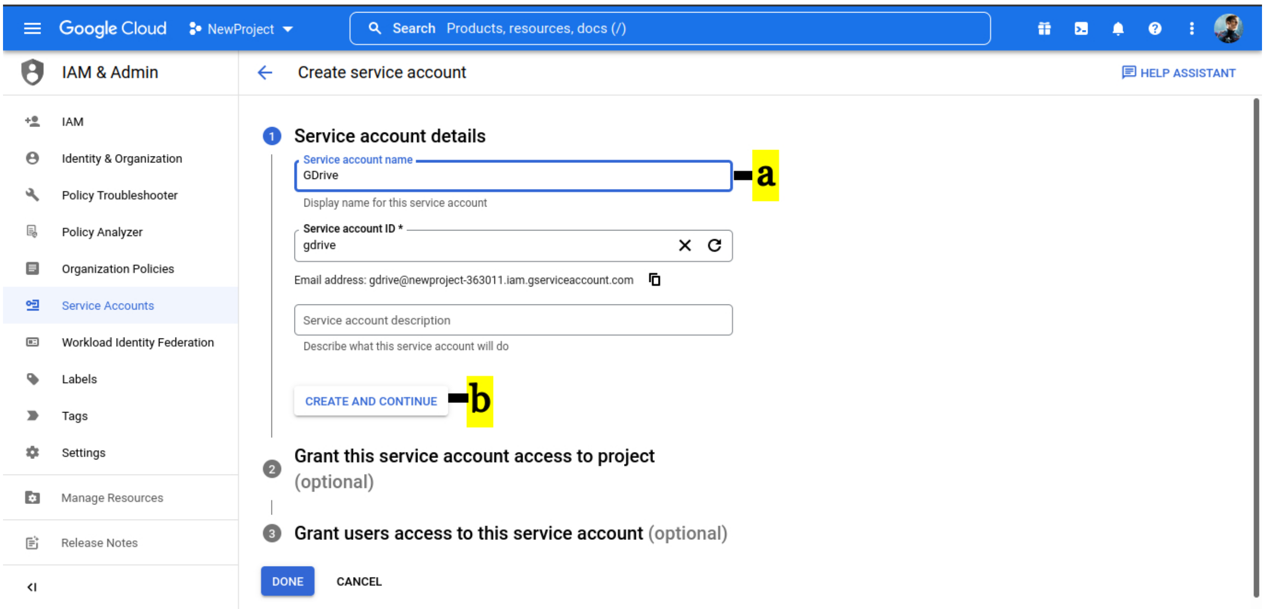
Organization policies can be used to secure service accounts and block risky service account features, such as automatic IAM Grants, key creation/upload, or the creation of service accounts entirely. Learn more about service account organization policies.

No rows to display

4. On the service account details window.

a. Provide **Service account name**.

b. Click on **CREATE AND CONTINUE**



Create service account

1 Service account details

Service account name: GDrive

Display name for this service account

Service account ID *: gdrive

Email address: gdrive@newproject-363011.iam.gserviceaccount.com

Service account description

Describe what this service account will do

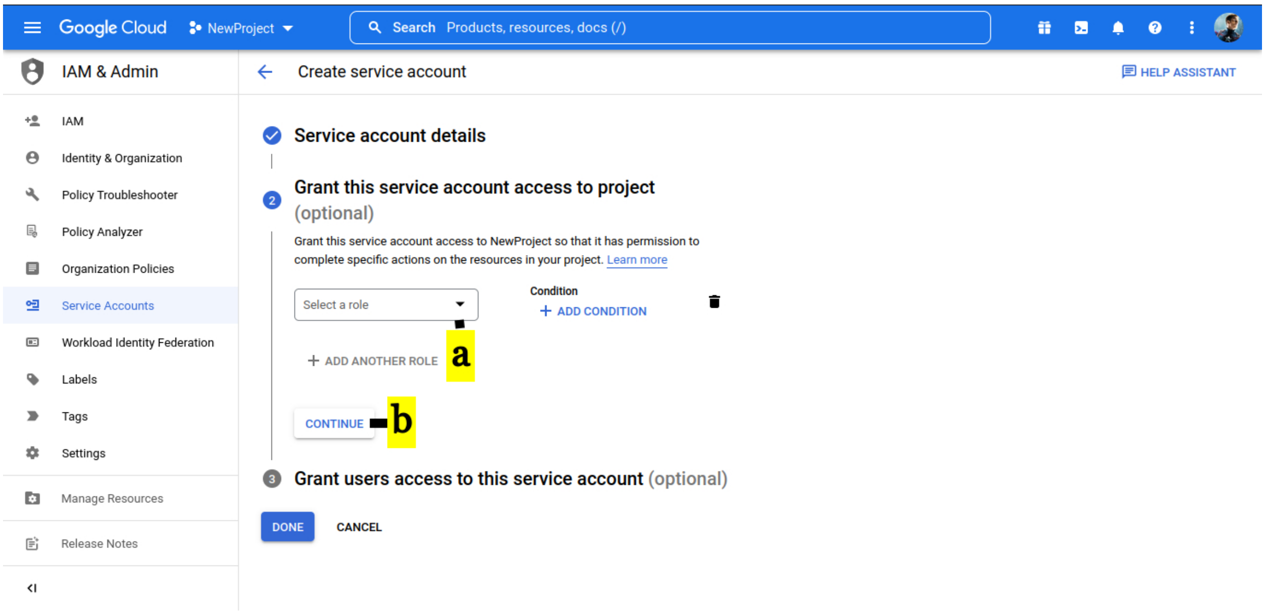
2 Grant this service account access to project (optional)

3 Grant users access to this service account (optional)

5. Grant this service account access to project.

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

b. Click on **CONTINUE**



Create service account

Service account details

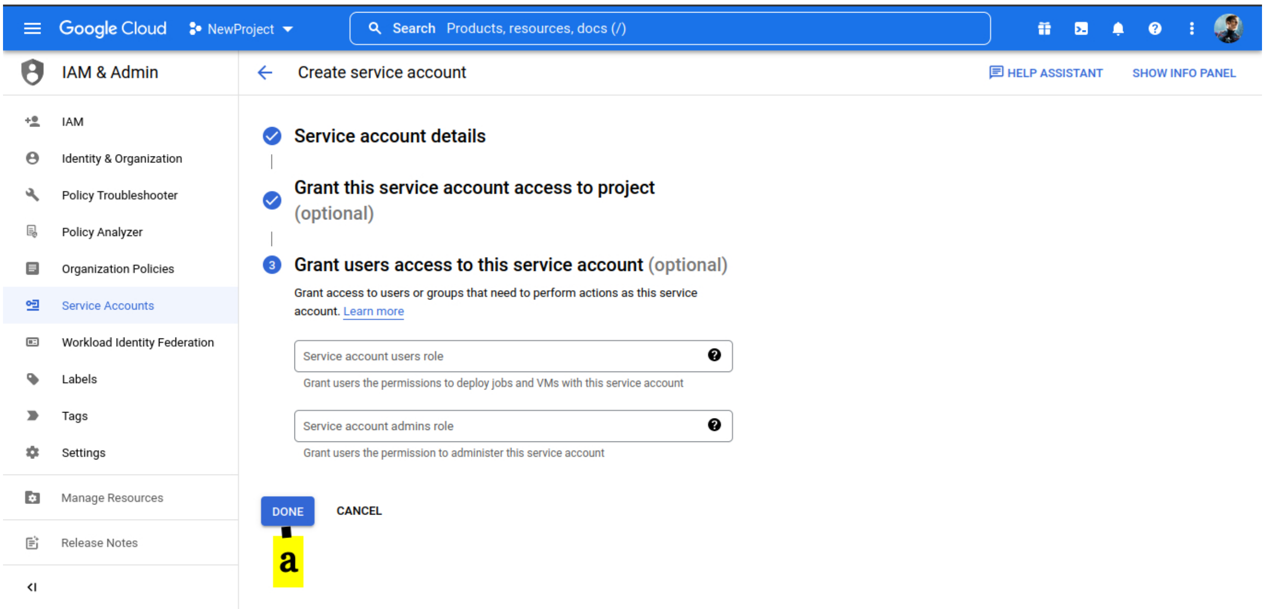
Grant this service account access to project (optional)

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

Grant users access to this service account (optional)

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

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



Create service account

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

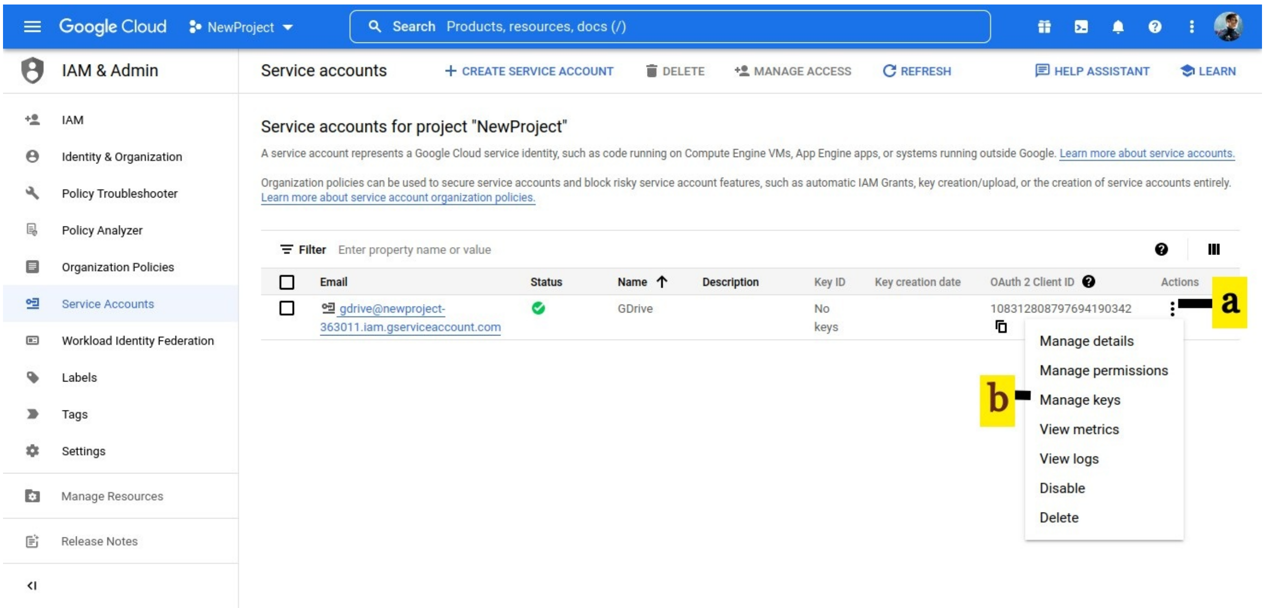
Grant users the permissions to deploy jobs and VMs with this service account

Grant users the permission to administer this service account

7. On service account window.

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

b. Select **Manage Keys**



Service accounts for project "NewProject"

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 about service accounts.

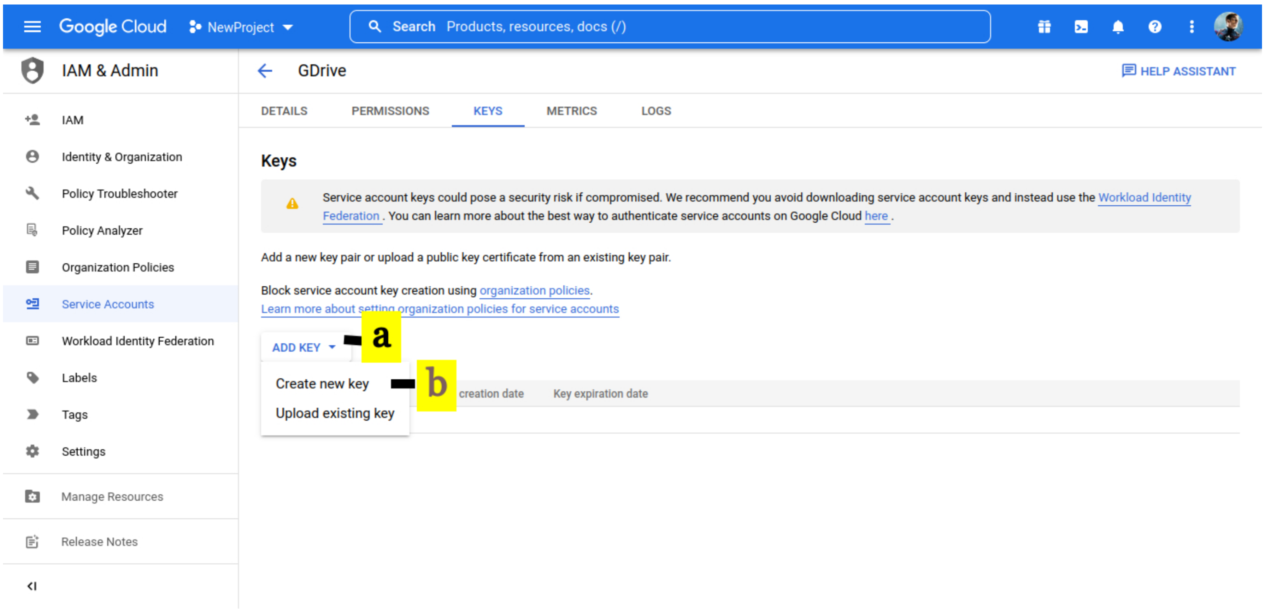
Organization policies can be used to secure service accounts and block risky service account features, such as automatic IAM Grants, key creation/upload, or the creation of service accounts entirely. Learn more about service account organization policies.

□	Email	Status	Name ↑	Description	Key ID	Key creation date	OAuth 2 Client ID	Actions
□	gdrive@newproject-363011.iam.gserviceaccount.com	✓	GDrive		No keys		108312808797694190342	⋮

8. Create a key

a. Drop down **ADD KEY**

b. Select **Create new key**



Keys

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 .

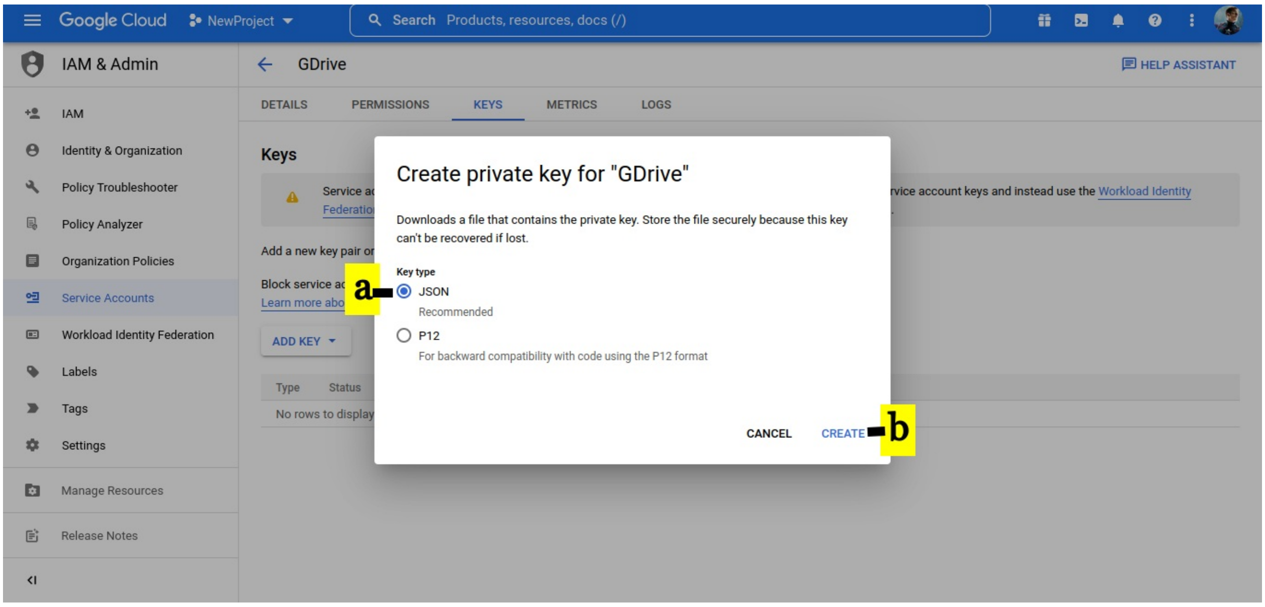
Add a new key pair or upload a public key certificate from an existing key pair.

Block service account key creation using organization policies.
Learn more about setting organization policies for service accounts

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**



Create private key for "GDrive"

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

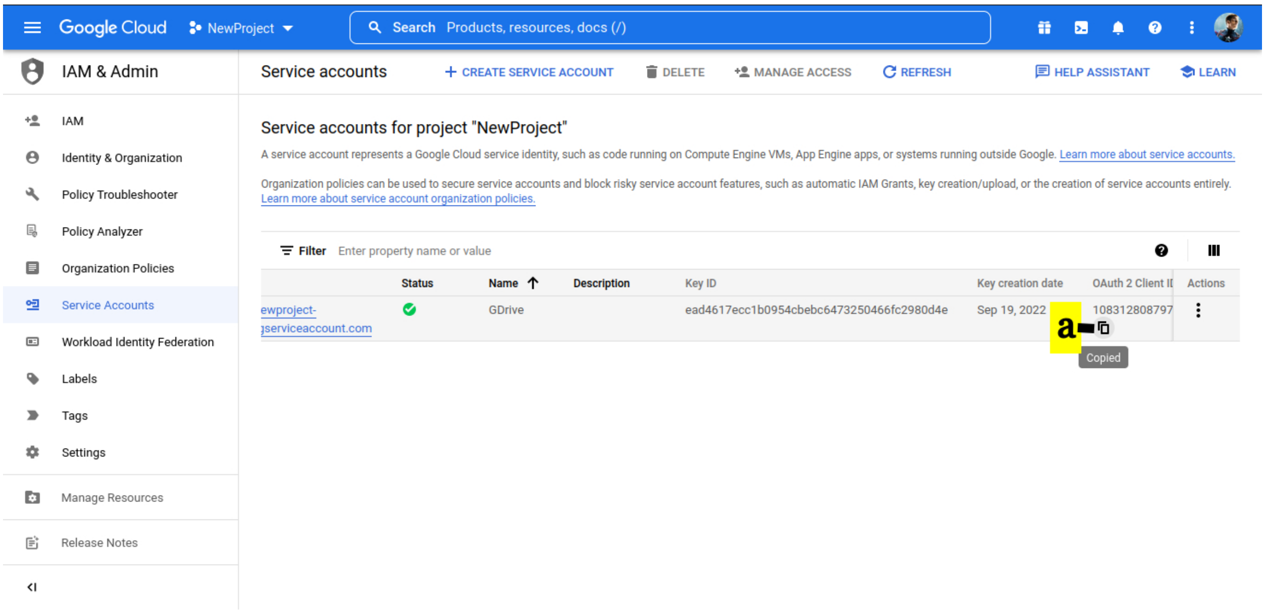
Key type

● JSON
Recommended

○ P12
For backward compatibility with code using the P12 format

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

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



Service accounts for project "NewProject"

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 about service accounts.

Organization policies can be used to secure service accounts and block risky service account features, such as automatic IAM Grants, key creation/upload, or the creation of service accounts entirely. Learn more about service account organization policies.

Email	Status	Name ↑	Description	Key ID	Key creation date	OAuth 2 Client I[D]	Actions
ewproject- jserviceaccount.com	✓	GDrive		ead4617ecc1b0954cbebc6473250466fc2980d4e	Sep 19, 2022	108312808797	⋮

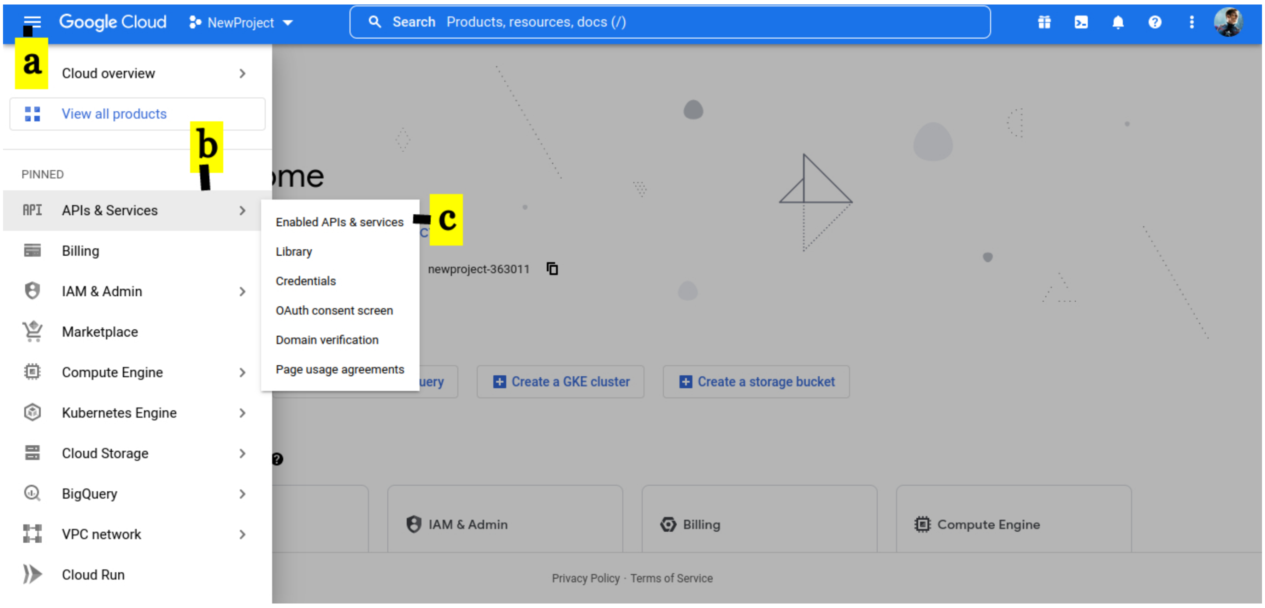
Step 2: Enable the API Services

1. Enable API Services

   a. Click on top left panel

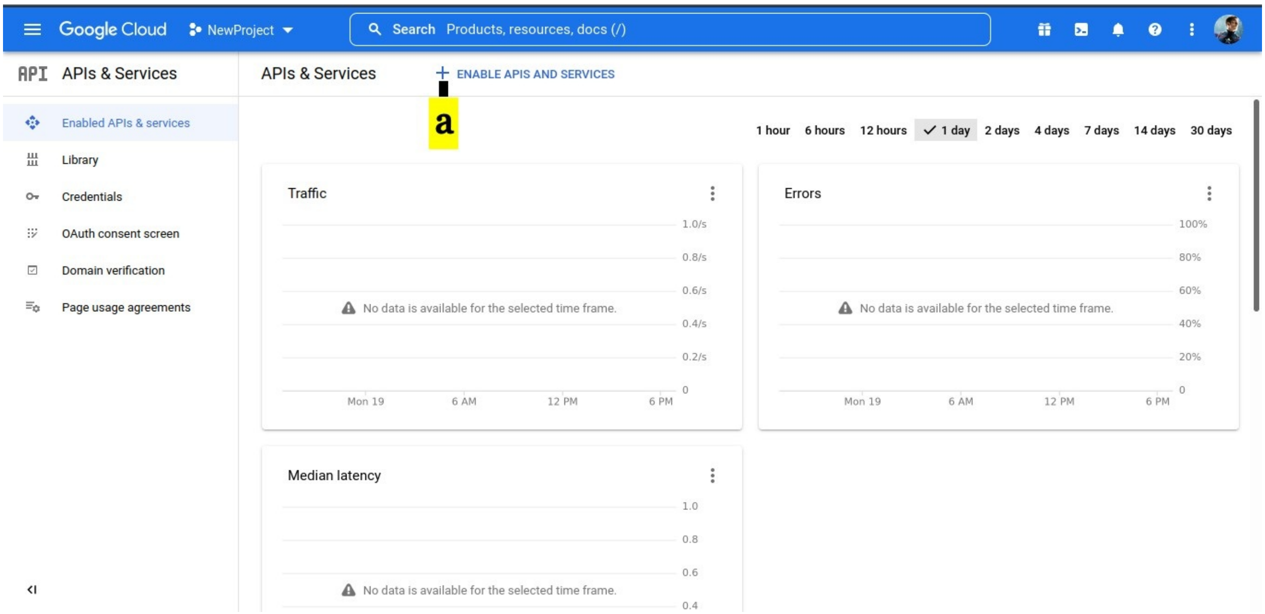
   b. Select **APIs & Services**

   c. Click on **Enabled APIs & services**



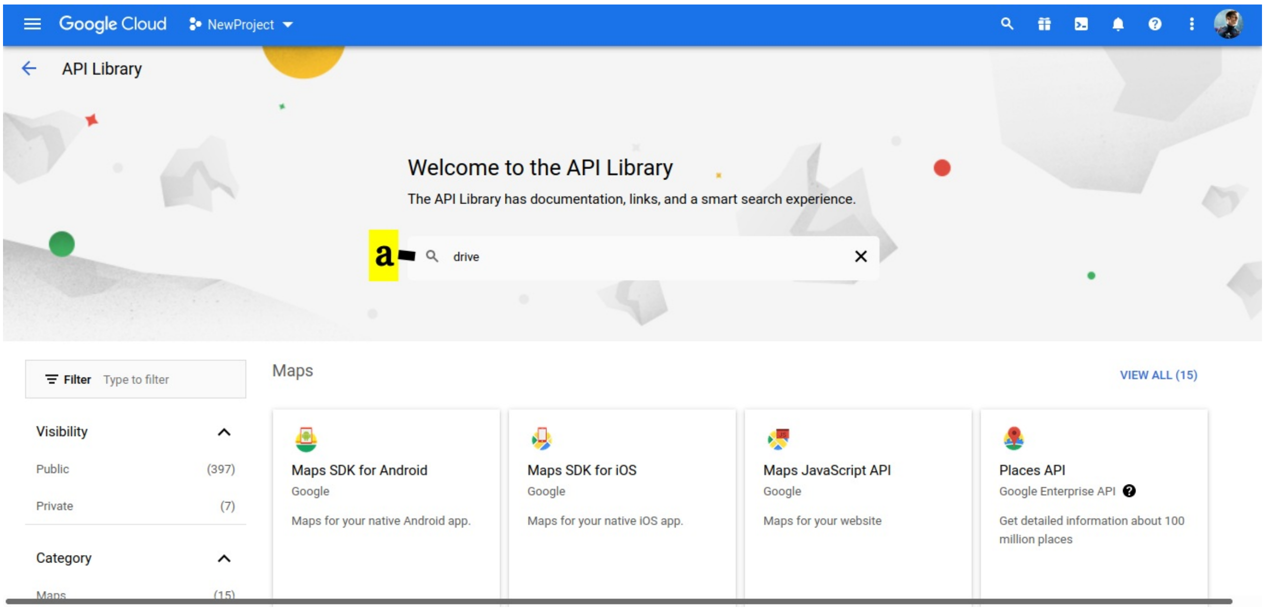
2. In the APIs & Services console

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



3. In the API Library

a. Search for the API. For mailbox access, seach for GMail. For drive access serach for GDrive



Welcome to the API Library

The API Library has documentation, links, and a smart search experience.

Visibility	
Public	(397)
Private	(7)
Category	
Maps	(15)

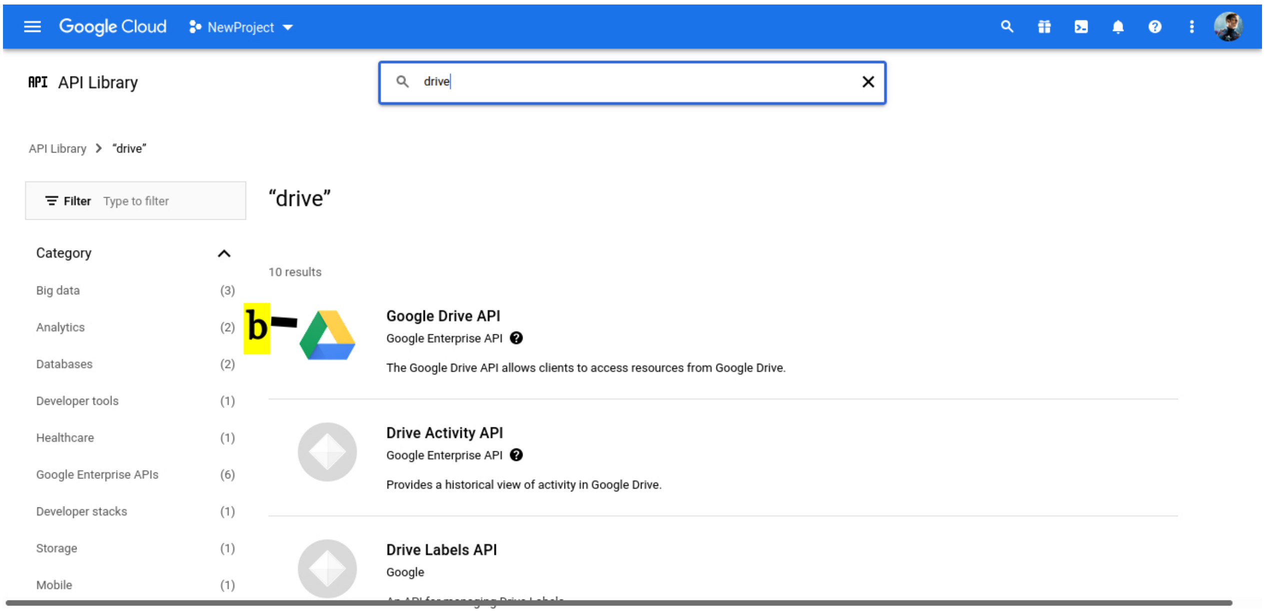
Maps SDK for Android
Google
Maps for your native Android app.

Maps SDK for iOS
Google
Maps for your native iOS app.

Maps JavaScript API
Google
Maps for your website

Places API
Google Enterprise API
Get detailed information about 100 million places

b. Select your API. Select Google Drive API for Drive and GMail API to migrate email



"drive"

10 results

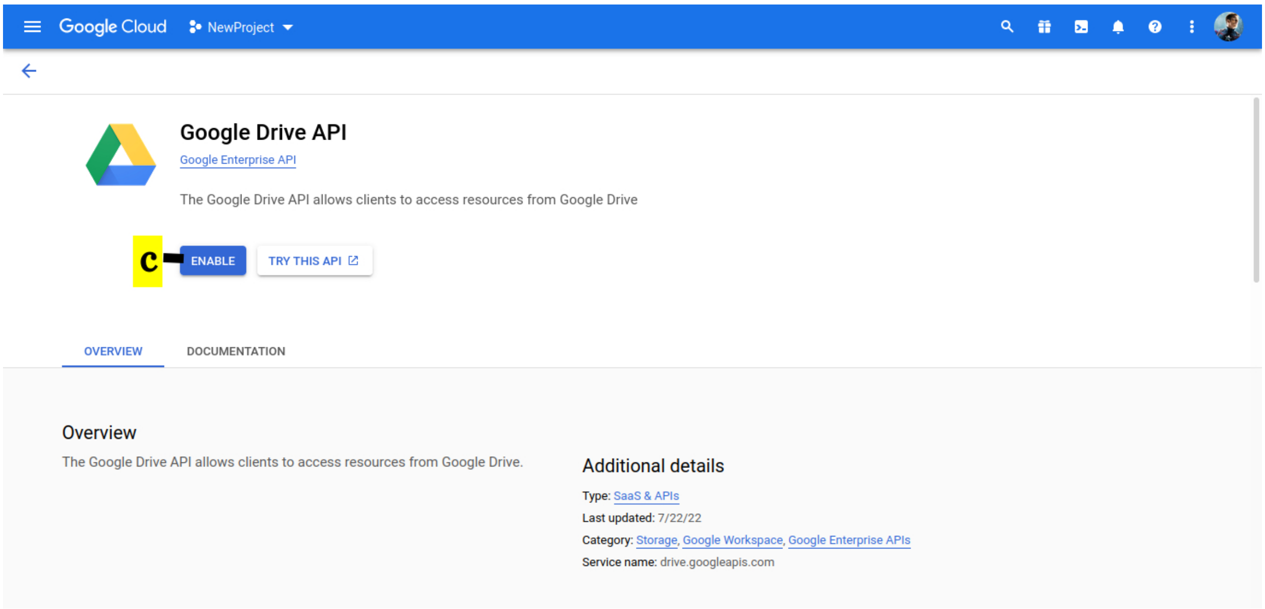
Category	
Big data	(3)
Analytics	(2)
Databases	(2)
Developer tools	(1)
Healthcare	(1)
Google Enterprise APIs	(6)
Developer stacks	(1)
Storage	(1)
Mobile	(1)

Google Drive API
Google Enterprise API
The Google Drive API allows clients to access resources from Google Drive.

Drive Activity API
Google Enterprise API
Provides a historical view of activity in Google Drive.

Drive Labels API
Google
An API for managing Drive Labels

c. Click on **ENABLE** button



The Google Drive API allows clients to access resources from Google Drive

Overview

The Google Drive API allows clients to access resources from Google Drive.

Additional details

Type: SaaS & APIs

Last updated: 7/22/22

Category: Storage, Google Workspace, Google Enterprise APIs

Service name: drive.googleapis.com

Step 3: Enable domain-wide delegation

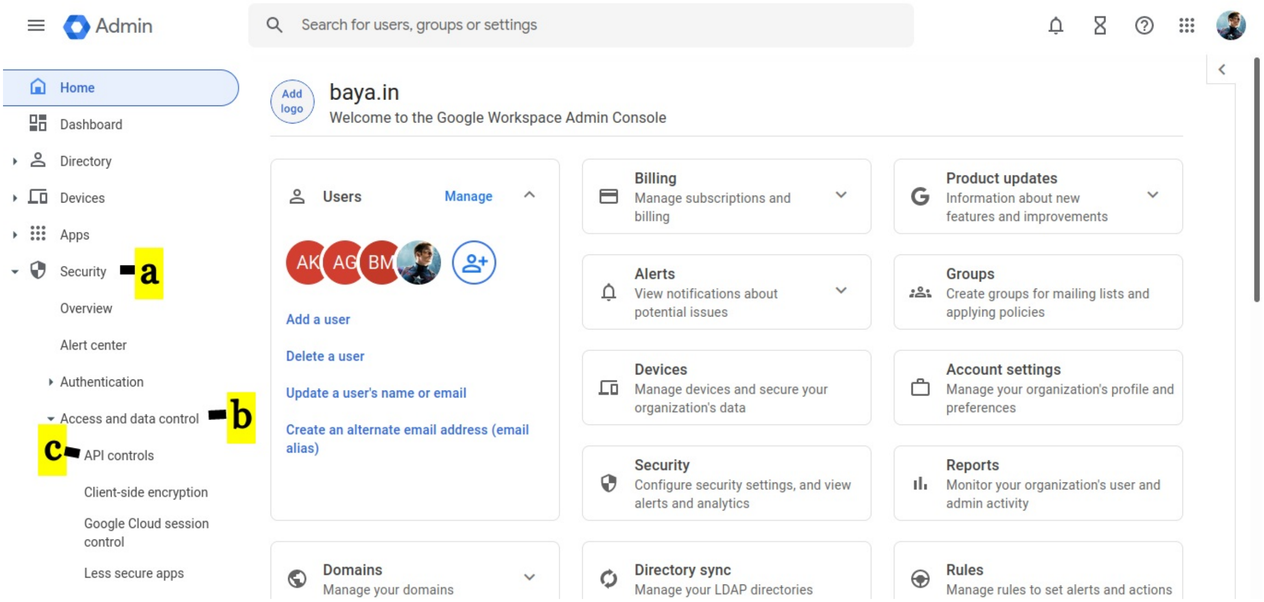
Login to G-suite Admin account and navigate to Google Admin (https://admin.google.com/).

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**



baya.in

Welcome to the Google Workspace Admin Console

Billing: Manage subscriptions and billing

Product updates: Information about new features and improvements

Alerts: View notifications about potential issues

Groups: Create groups for mailing lists and applying policies

Devices: Manage devices and secure your organization's data

Account settings: Manage your organization's profile and preferences

Security: Configure security settings, and view alerts and analytics

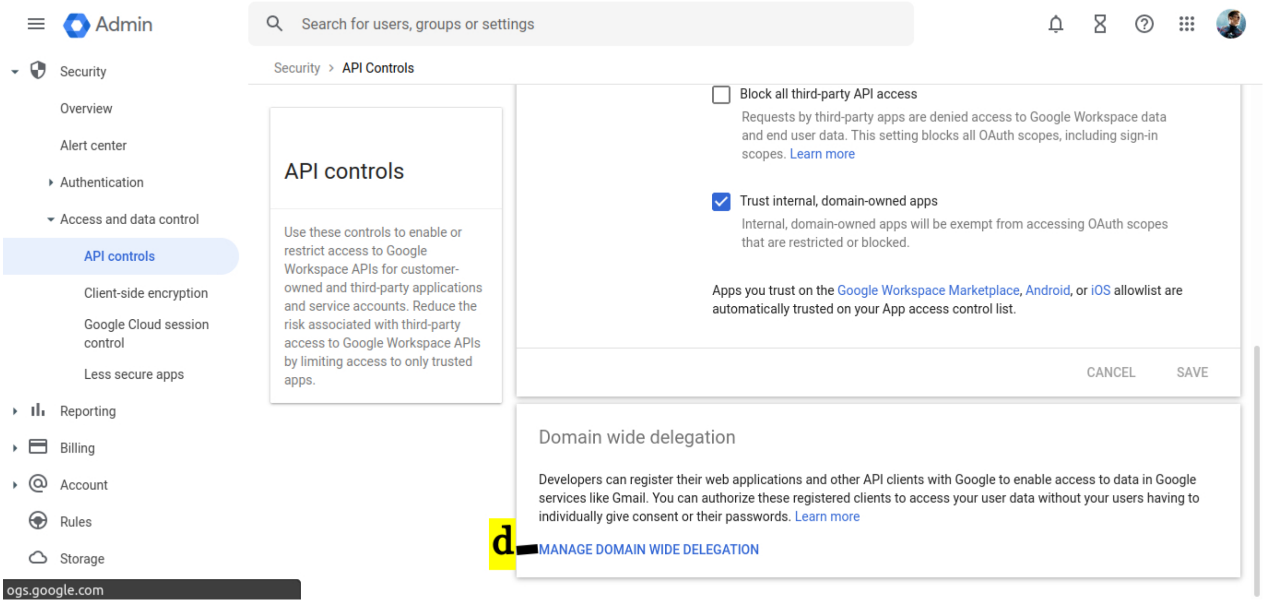
Reports: Monitor your organization's user and admin activity

Domains: Manage your domains

Directory sync: Manage your LDAP directories

Rules: Manage rules to set alerts and actions

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



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

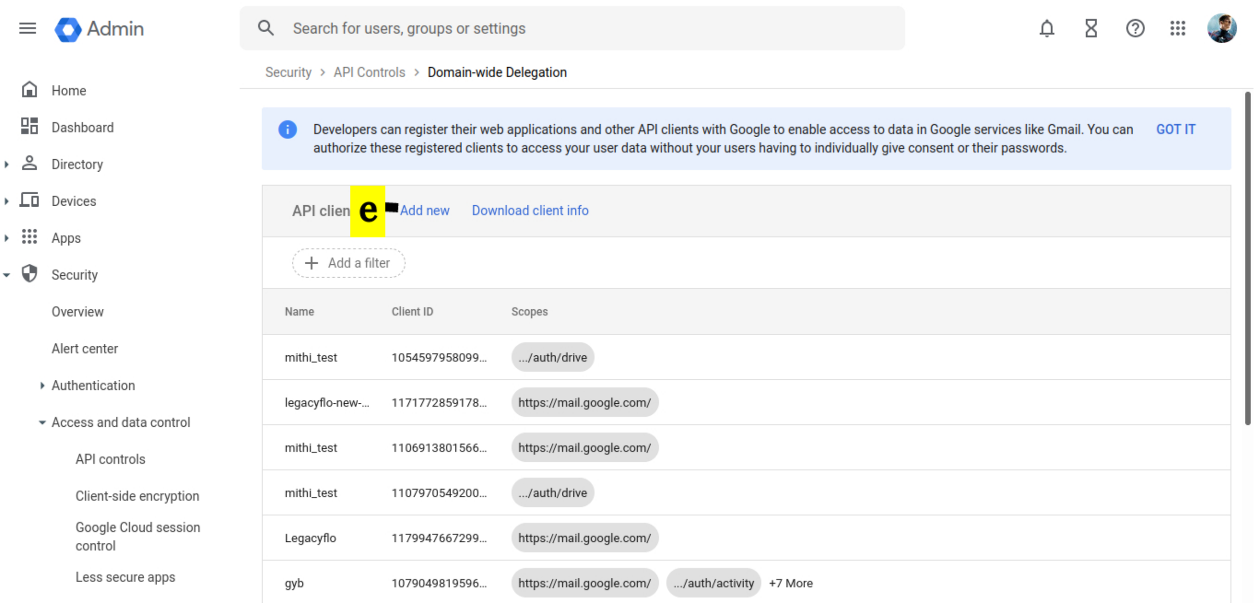
Internal, domain-owned apps will be exempt from accessing OAuth scopes that are restricted or blocked.

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

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

e. Click on **Add new**



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.

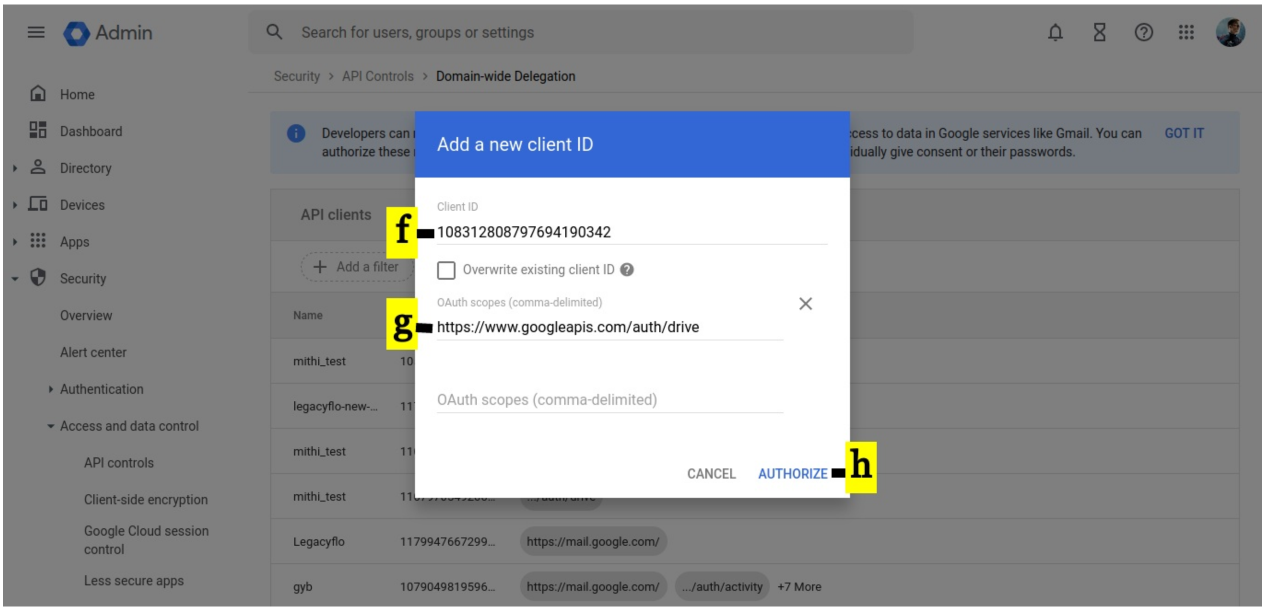
Name	Client ID	Scopes
mithi_test	1054597958099...	.../auth/drive
legacyflo-new-...	1171772859178...	https://mail.google.com/
mithi_test	1106913801566...	https://mail.google.com/
mithi_test	1107970549200...	.../auth/drive
Legacyflo	1179947667299...	https://mail.google.com/
gyb	1079049819596...	https://mail.google.com/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

GDrive	https://www.googleapis.com/auth/drive
GMail	https://mail.google.com/

h. Click the AUTHORIZE button



Add a new client ID

Client ID: 108312808797694190342

□ Overwrite existing client ID

OAuth scopes (comma-delimited): https://www.googleapis.com/auth/drive

OAuth scopes (comma-delimited)

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. **Choose the JSON file** which has been downloaded to your desktop.
    3. Click on **Save**
    4. **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