

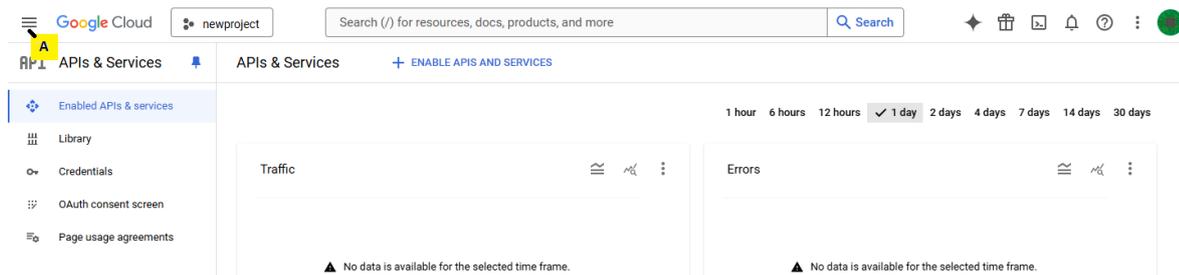
# Enable Service Account Key Creation

If you are unable to create a Google Cloud Service Account Key to be registered with LegacyFlo, the error message will have a statement similar to the one below

The organization policy constraint "iam.disableServiceAccountKeyCreation" is enforced on your organization.

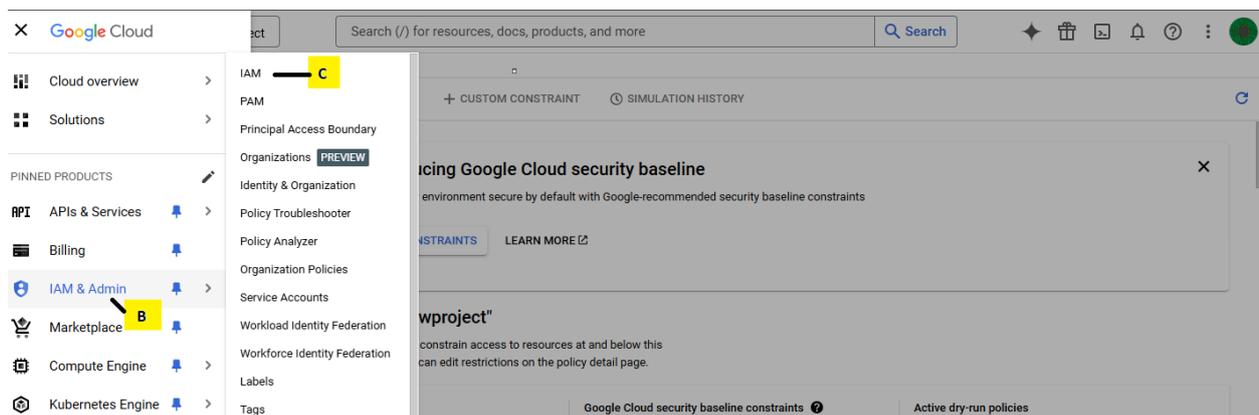
To enable Google Cloud Service Account Key creation, follow the steps below.

## A. From the top left corner of the Google Cloud interface, select the hamburger menu

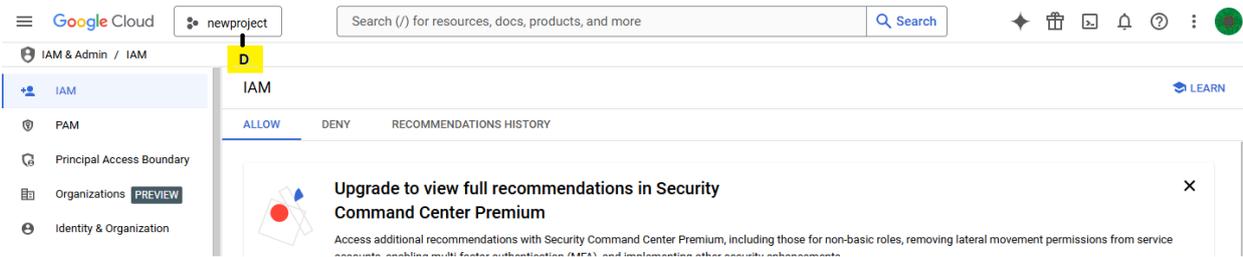


## B. Select IAM & Admin.

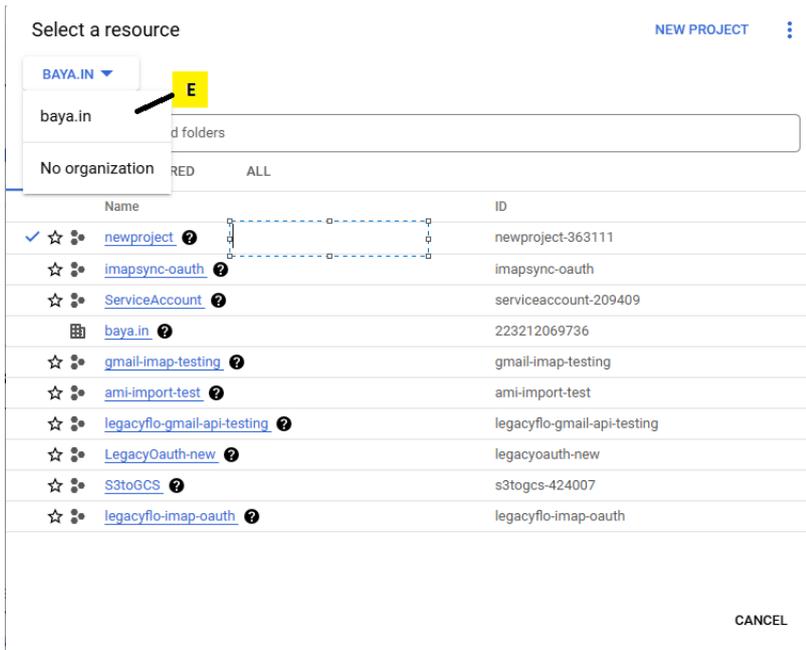
## C. Select IAM



## D. Navigate to project list . ( By default created while domain setup for primary domain)



### E. Select the Organization Unit for the domain



F. Confirm the organization administrator using whose email id you have logged in has the following Roles assigned:

- Organization Administrator
- Organization Policy Administrator
- Owner

G. If any of these Roles are missing, then click on GRANT ACCESS

Google Cloud | baya.in | Search (/) for resources, docs, products, and more

IAM & Admin / IAM

IAM | LEARN

ALLOW DENY RECOMMENDATIONS HISTORY

Permissions for organization "baya.in"  
These permissions affect this organization and all of its resources. [Learn more](#)

VIEW BY PRINCIPALS VIEW BY ROLES

GRANT ACCESS REMOVE ACCESS

Filter Enter property name or value

Type	Principal	Name	Role
<input type="checkbox"/>	baya.in	Billing Account Creator	
<input type="checkbox"/>		Project Creator	
<input type="checkbox"/>	mark@baya.in	Sunil Uttam	Organization Administrator

Add the necessary roles in the pop-up and Save the changes

Edit access to "baya.in"

Principal Organization

mark@baya.in baya.in

Assign roles

Roles are composed of sets of permissions and determine what the principal can do with this resource. [Learn more](#)

Role: Organization Administrator IAM condition (optional)   
 + ADD IAM CONDITION  
 Access to manage IAM policies and view organization policies for organizations, folders, and projects.

Role: Owner IAM condition (optional)   
 + ADD IAM CONDITION  
 Full access to most Google Cloud resources. See the list of included permissions.

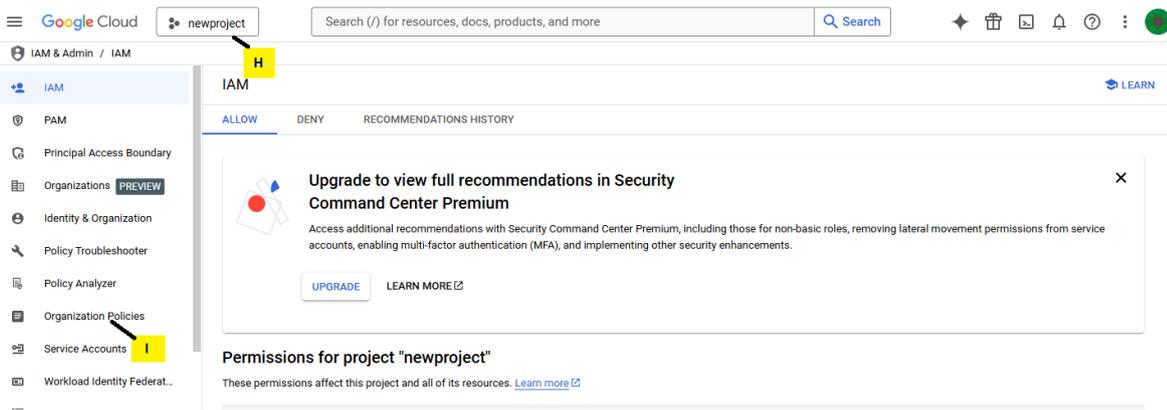
Role: Organization Policy Administrator IAM condition (optional)   
 + ADD IAM CONDITION  
 The permission to set Organization Policies on resources.

+ ADD ANOTHER ROLE

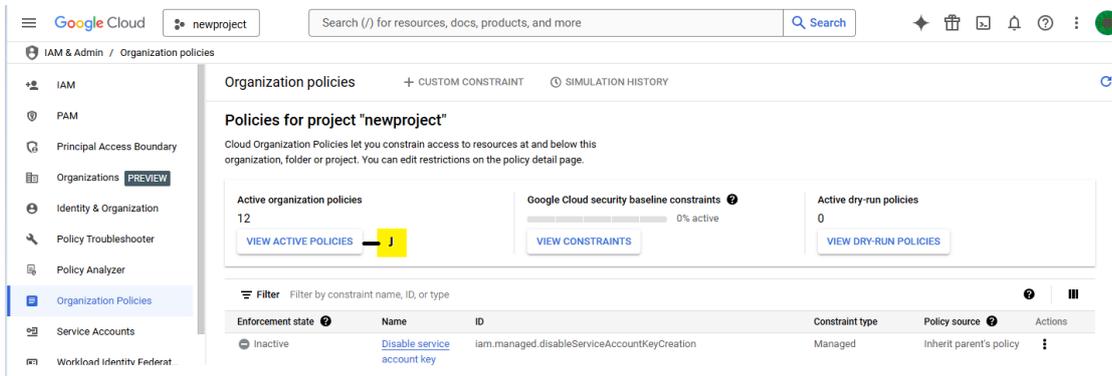
SAVE TEST CHANGES CANCEL

H. Now, navigate back to the project selected in the steps D and E.

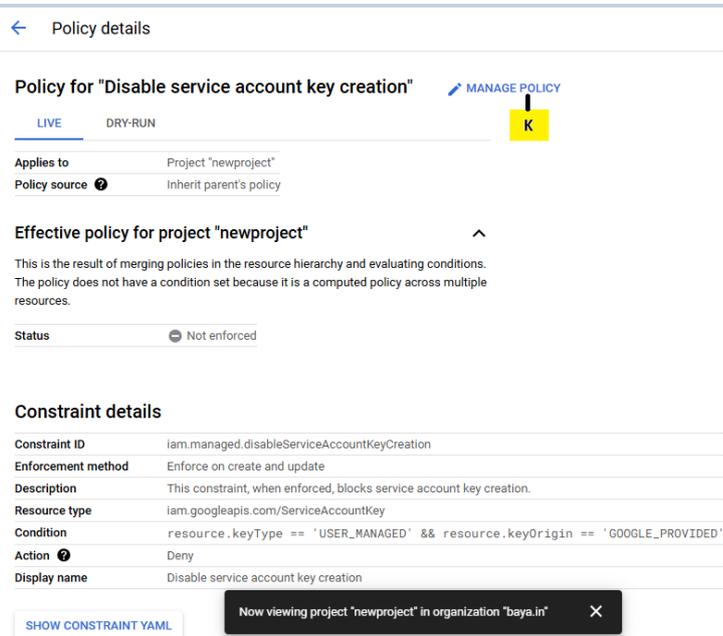
I. Select Organization Policies



J. Click on VIEW ACTIVE POLICIES and search for Disable service account key creation. Click on the link



K. Click MANAGE POLICY



I. In the Policy Source, select Override parent's policy and in the Enforcement section, select Off.

## Disable service account key creation

This constraint, when enforced, blocks service account key creation.

### Applies to

Project 'newproject'

### Policy source

- Inherit parent's policy ?
- Google-managed default ?
- Override parent's policy ?

### Rules

Rules define the values that are enforced by an organization policy constraint. For a boolean constraint, you can set the enforcement of the constraint on or off. For a list constraint, you can create a list of values that should be allowed or denied by the policy, or set enforcement to deny or allow all values.

Any rule can be made conditional based on Tags by clicking Add condition. This allows you to fine-tune the enforcement of your organization policy. [Learn more about policy conditions](#).

^ New rule 

Enforcement

On

Off

ADD CONDITION

DONE

ADD A RULE

TEST CHANGES ? SET POLICY CANCEL

Now viewing project "newproject" in organization "bays.i