Googify Google Cloud/Workspace Setup

The audience of this document is the company/organization Network/IT Admin who has control of its Google Workspace and Google Cloud Console. There are some configurations needed to be done before the Googify Sync application gains the authority to access Gmail API to sync messages from UC (e.g: Cisco Unity) to Gmail.

At the end of finishing the steps described in this document, what you'll achieve:

1. You'll download a key file in .json format that represents Google Service Account in which you'll put in the Googify Sync app folder so that Googify Sync can access your Gmail system.
2. You'll finish certain configurations on Google Workspace and Google Cloud backend to allow the application (e.g: Googify Sync) who can access the json key file to be authorized to access Gmail API to conduct the message sync.

Note: The process seems lengthy in writing, but it's not that hard after you successfully go through once. Pay attention to the **Bold Yellow highlighted section** since those are often overlooked and thus cause the message sync not working properly during initial installation and waste time to troubleshoot.

The Google document in this link is almost enough to guide you through preparing Service Account key generation (json file) and Domain delegation configuration on Google Workspace. https://developers.google.com/identity/protocols/oauth2/service-account

Our document below just adds some detailed screenshot in case the Google document link is not detailed enough for you.

Section 1 - Google Cloud Setup

We need to create a “Service Account " on Google Cloud console so that Googify Sync can use this “Service Account" key file (json format) to gain access to your organization GMail through Gmail API to fulfill the purpose of syncing messages.

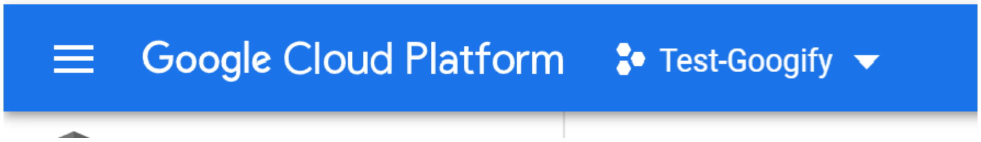
In order to create Google “Service Account”, we need to create a Google Cloud Project first (you may already have an existing Google Cloud project for other purposes such as for Avaya/Esna Cloudlink, you can choose that project as well).

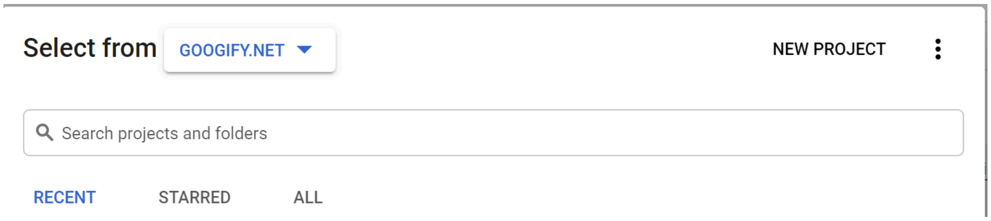
Sign into Google Cloud Console.

https://console.cloud.google.com/

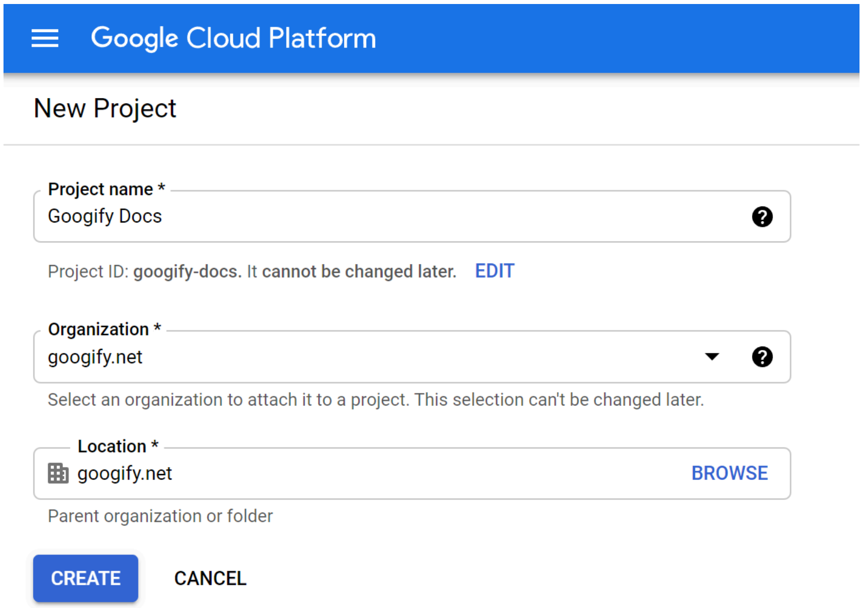
You may already have existing Google Cloud project that you can choose from or simply creat a new project like below:

Click on the dropdown and select New Project





Enter a name and click create.



Project name *
Googify Docs

Project ID: googify-docs. It cannot be changed later. EDIT

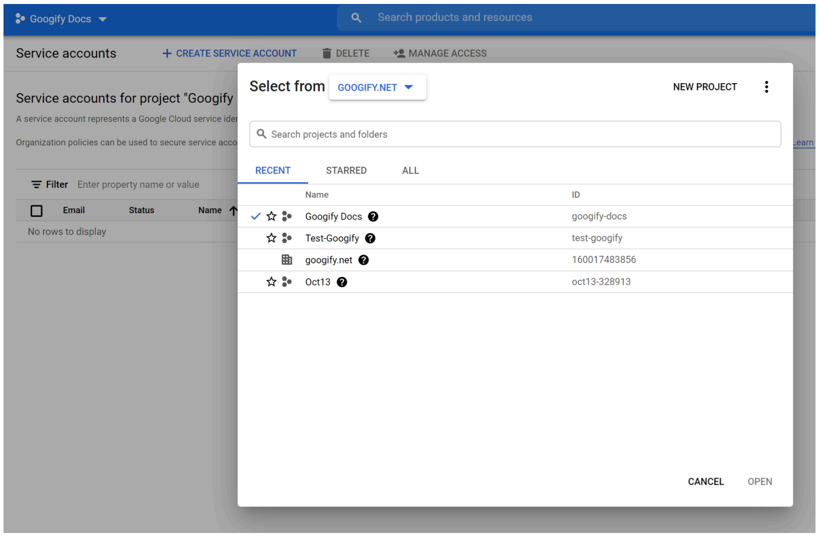
Organization *
googify.net

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

Location *
googify.net

Parent organization or folder

Make sure you are in the project and select open



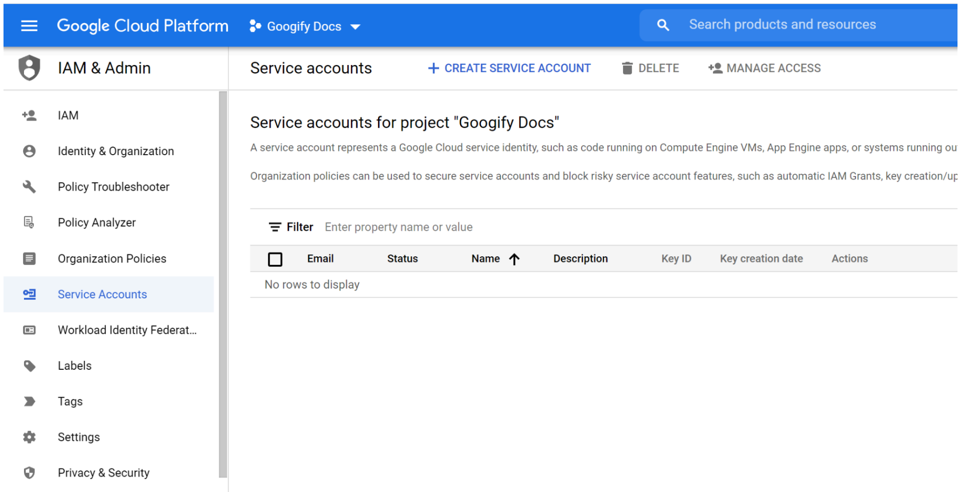
Service accounts for project "Googify

A service account represents a Google Cloud service ider

Organization policies can be used to secure service acco

Name	ID
Googify Docs	googify-docs
Test-Googify	test-googify
googify.net	160017483856
Oct13	oct13-328913

Goto Service Accounts page under the Menu "IAM & Admin=>Service Accounts" Under service accounts, click on the button "Create Service Account" on top section of the screen:



Service accounts for project "Googify Docs"

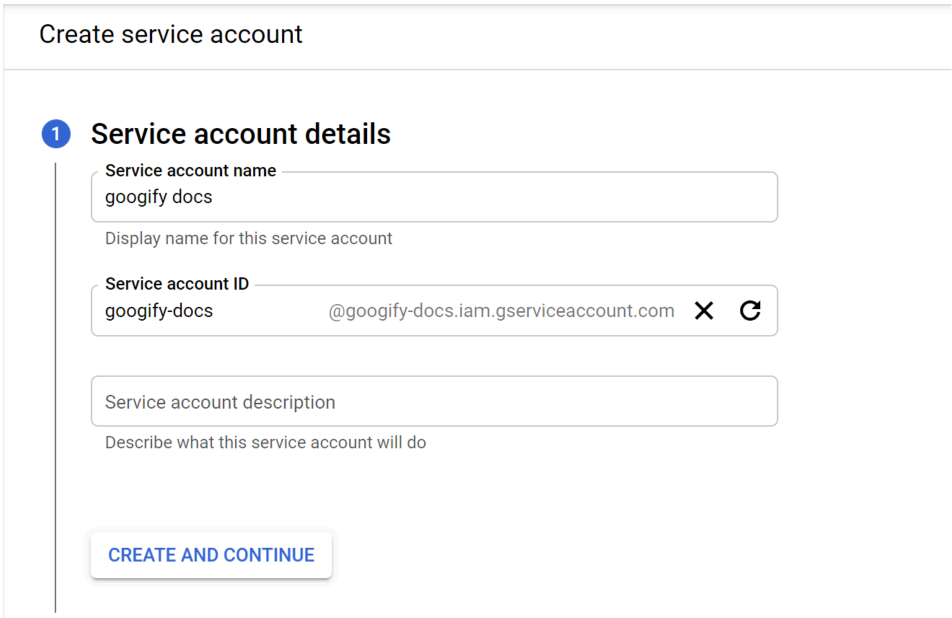
A service account represents a Google Cloud service identity, such as code running on Compute Engine VMs, App Engine apps, or systems running ou

Organization policies can be used to secure service accounts and block risky service account features, such as automatic IAM Grants, key creation/up

□	Email	Status	Name ↑	Description	Key ID	Key creation date	Actions

No rows to display

Give the service account a name and click on the button "Create and Continue"



Create service account

1 Service account details

Service account name: googify docs

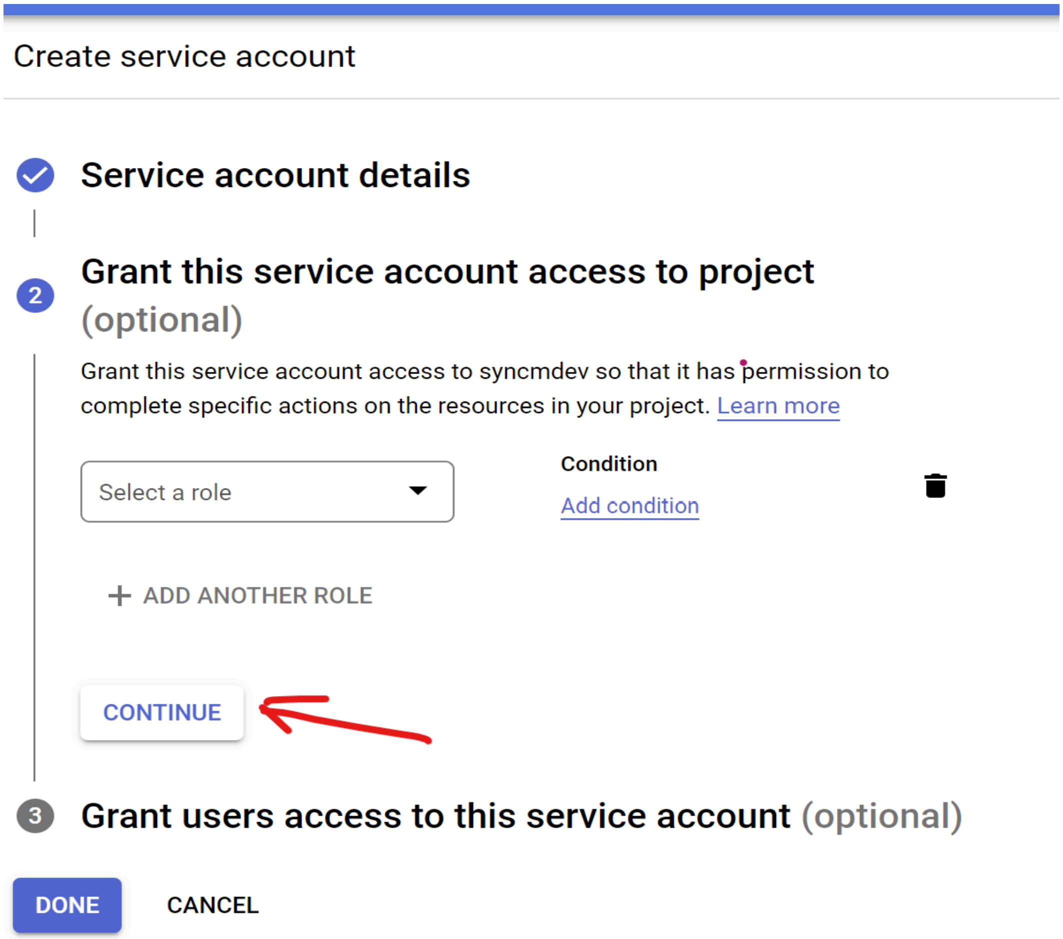
Display name for this service account

Service account ID: googify-docs @googify-docs.iam.gserviceaccount.com

Service account description

Describe what this service account will do

Then Skip the optional step “Grant this service account access to project” by clicking on button “CONTINUE”



Create service account

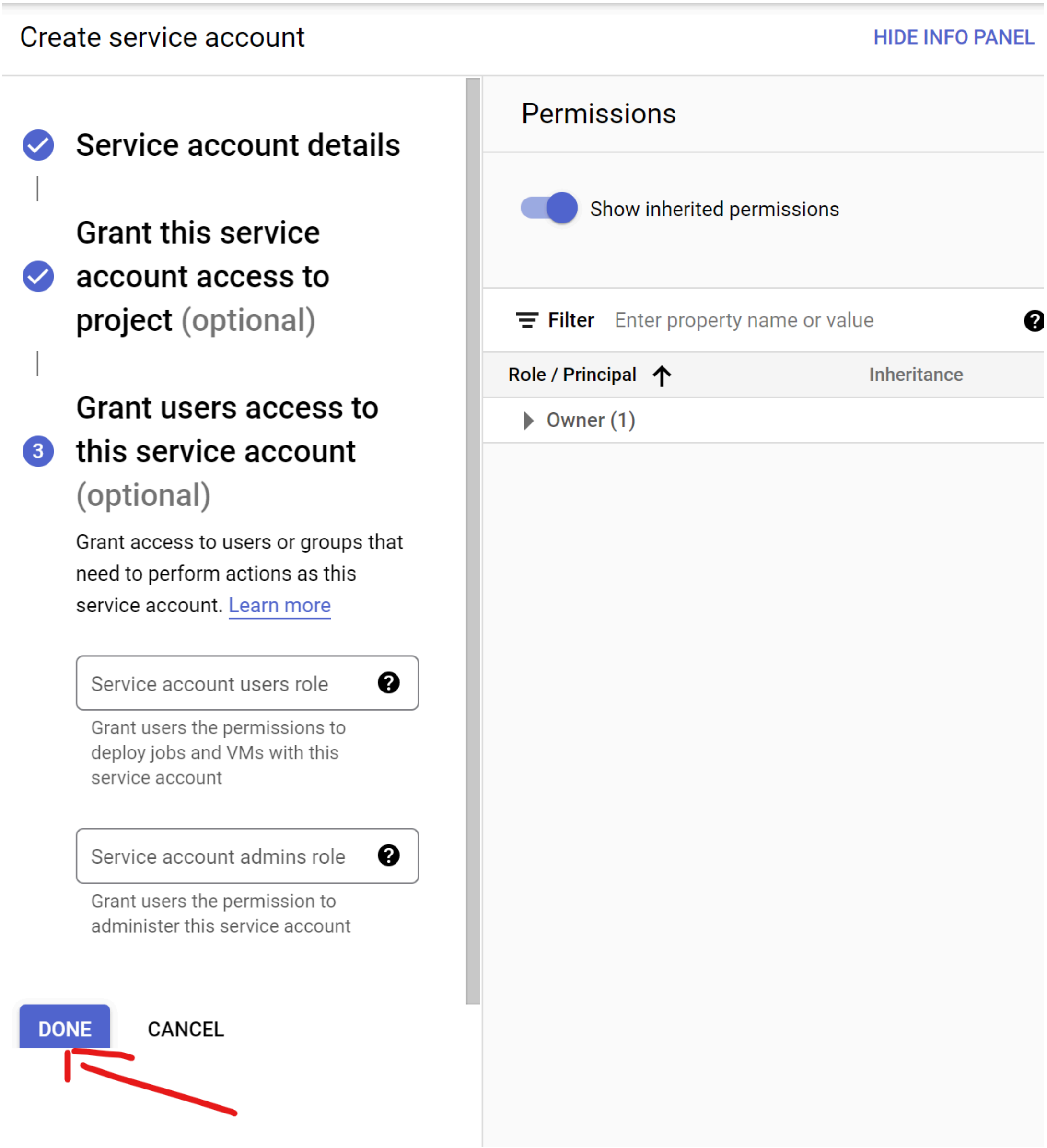
Service account details

2 Grant this service account access to project (optional)

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

3 Grant users access to this service account (optional)

And skip the “Grant users access to this service account” by just clicking on the button “DONE”:



Create service account

Service account details

Grant this service account access to project (optional)

3 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

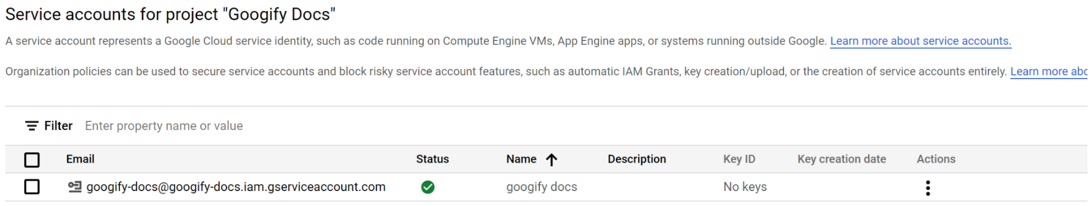
Permissions

Show inherited permissions

Filter Enter property name or value

Role / Principal ↑	Inheritance
▸ Owner (1)	

Click on the newly created service account to open it.



Service accounts for project "Googify Docs"

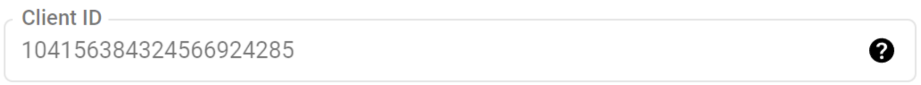
A service account represents a Google Cloud service identity, such as code running on Compute Engine VMs, App Engine apps, or systems running outside Google. Learn more about service accounts.

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 abc

Filter Enter property name or value

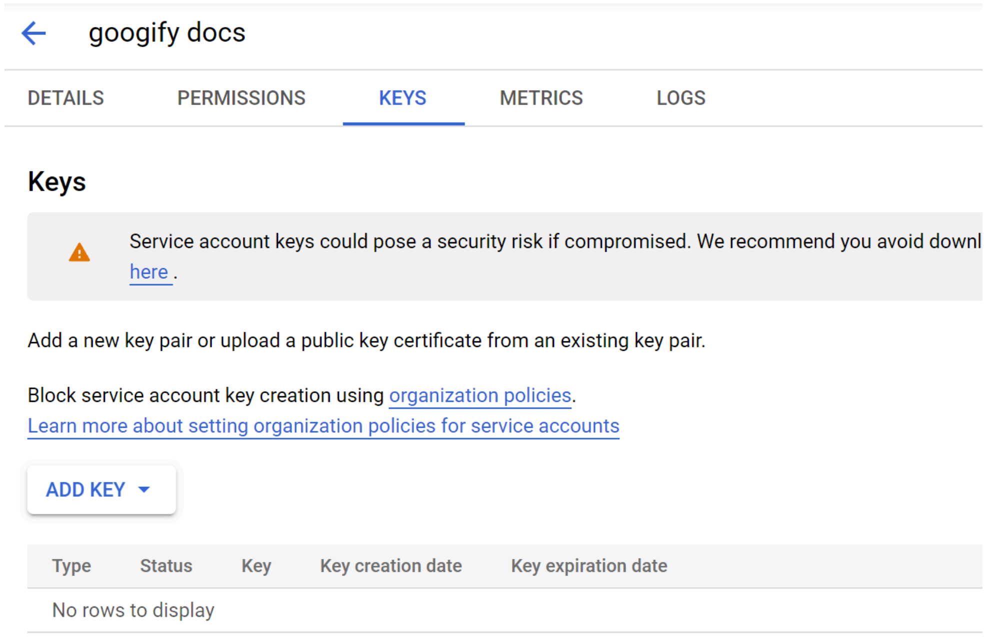
□	Email	Status	Name ↑	Description	Key ID	Key creation date	Actions
□	googify-docs@googify-docs.iam.gserviceaccount.com	✓	googify docs		No keys		⋮

On the “Details” tab, you’ll see some long digits called “UniqueID” or “ClientID” like “1041563….” (Google keeps changing the UI, so use your gut feeling). This is OAuth Client ID, please copy and paste somewhere. We’ll need this Client ID soon in another step.



Client ID
104156384324566924285

Click on the Keys tab.



googify docs

DETAILS PERMISSIONS KEYS METRICS LOGS

Keys

⚠ Service account keys could pose a security risk if compromised. We recommend you avoid downl
here .

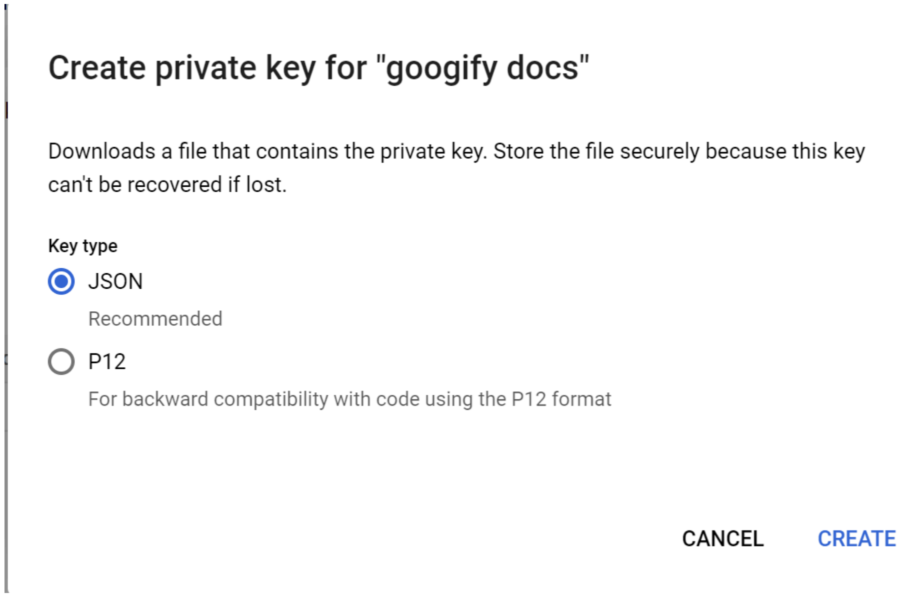
Add a new key pair or upload a public key certificate from an existing key pair.

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

ADD KEY ▾

Type	Status	Key	Key creation date	Key expiration date
No rows to display				

Select Add Key and create key. Key type should be JSON, then select create.



Create private key for "googify docs"

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

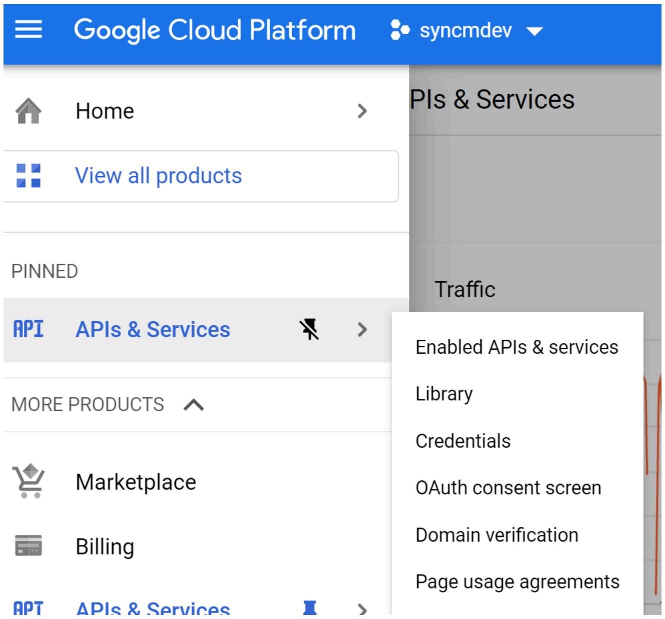
○ P12

For backward compatibility with code using the P12 format

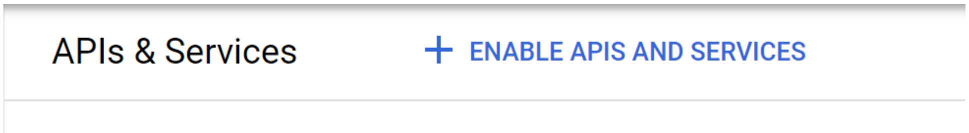
The key will be automatically downloaded to your PC in a file extension in .json. Save this key file and rename it to “**gcloud_serviceaccount.json**”. It should be eventually copied to the server where Googify Sync resides.

So far you have successfully created the Service Account and downloaded the json key file that will be copied to Googify Sync folder.   You can always come back to generate the json key as many times as you want as long as the Service Account still exists. So don’t worry that you may accidentally delete the json key file (but don’t share with other irrelevant people though since it has secret to access your Gmail messages)

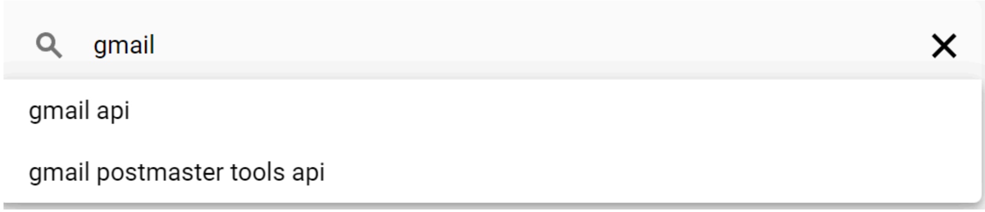
Next we’ll enable GMail API and this is also the last thing we need to do on Google Cloud console. Navigate the menu=>”APIs & Services=>Enabled APIs And services”:



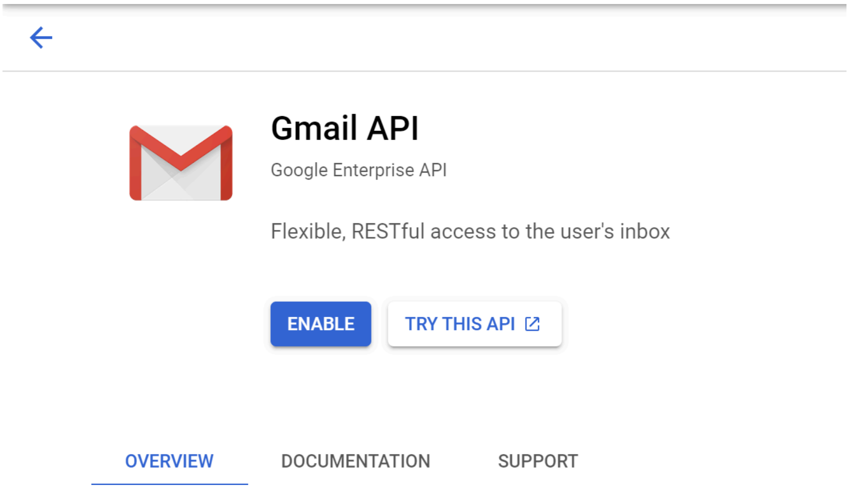
Click the button “Enable APIS and Services” on the top section of the screen:



Search for gmail and select gmail api.



Click “Enable”:



Gmail API

Google Enterprise API

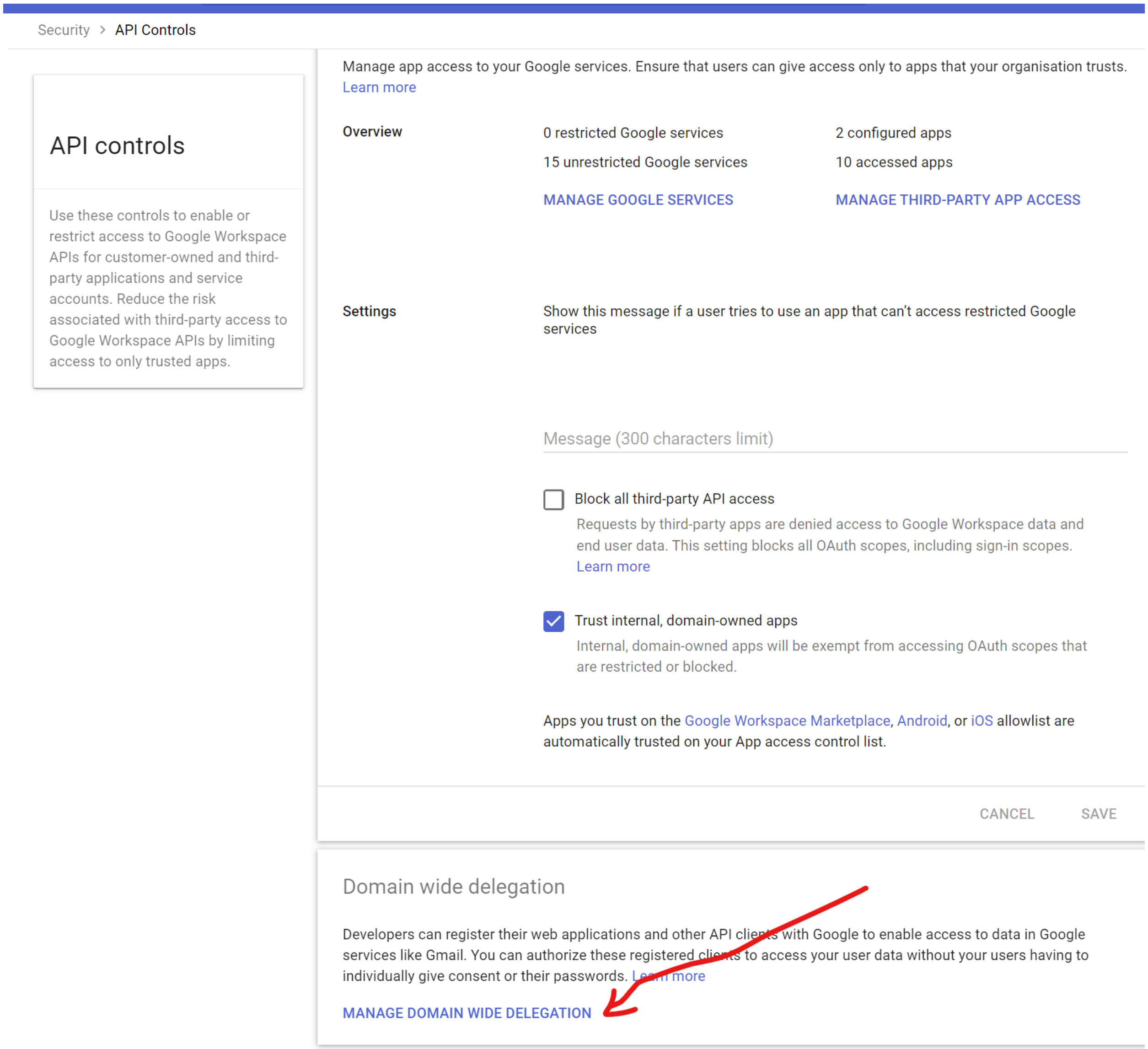
Flexible, RESTful access to the user's inbox

You may already have configured the above Service Account and enabled Gmail API previously (e.g: due to Esna/Avaya Cloudlink configuration), then you don’t need to do all the steps above, just simply open the existing service account and create the json key and rename properly to “gcloud_serviceaccount.json” and put into Googify folder.

Section 2 - Google Domain Setup

Next step is to add permissions to your Google Org in Google Workspace, please go to Manage This Organization.

Go to Security and API Controls and click “MANAGE DOMAIN WIDE DELEGATION” at the bottom:



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.

Manage app access to your Google services. Ensure that users can give access only to apps that your organisation trusts. Learn more

Overview		
	0 restricted Google services	2 configured apps
	15 unrestricted Google services	10 accessed apps
	MANAGE GOOGLE SERVICES	MANAGE THIRD-PARTY APP ACCESS

Settings

Show this message if a user tries to use an app that can’t access restricted Google services

Message (300 characters limit)

□ 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

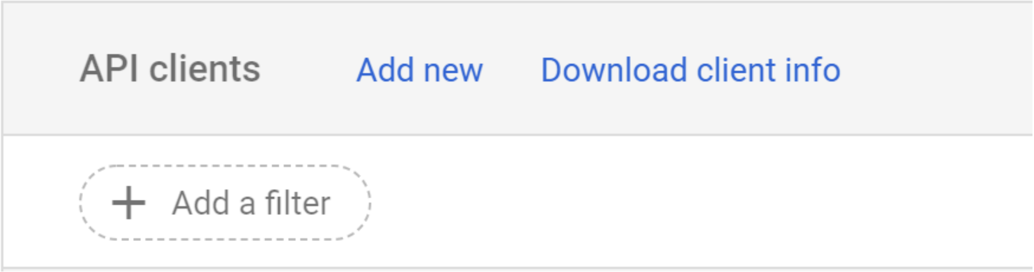
Internal, domain-owned apps will be exempt from accessing OAuth scopes that are restricted or blocked.

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

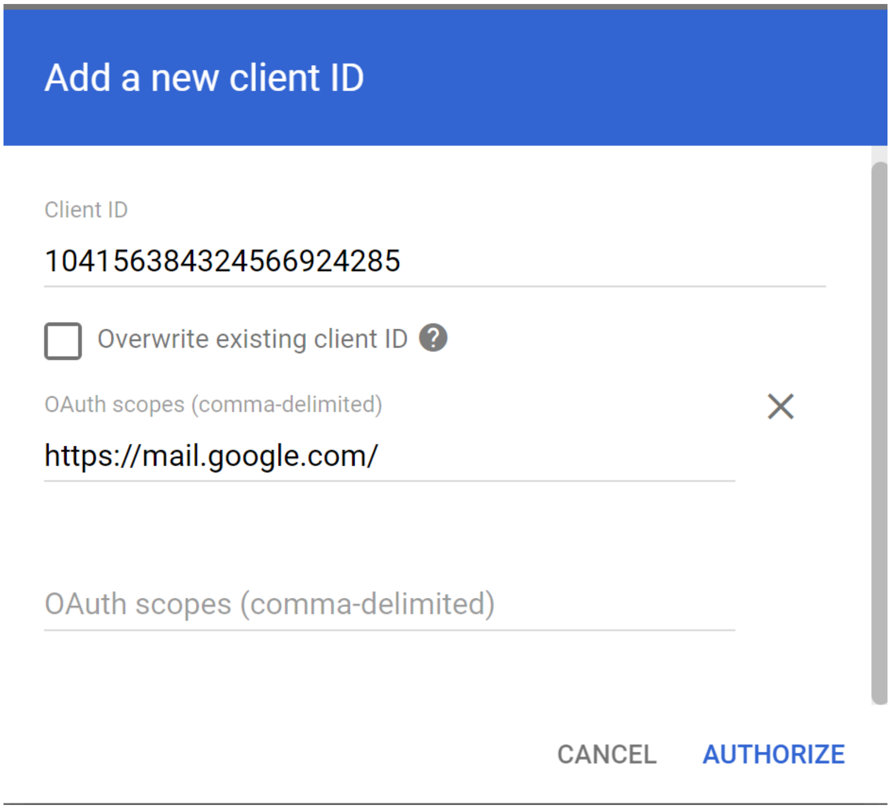
Domain wide delegation

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

Click on Add New.



Enter the client id from the previous steps and under OAuth Scopes enter, https://mail.google.com/ and click on Authorize:



Add a new client ID

Client ID

104156384324566924285

☐ Overwrite existing client ID

OAuth scopes (comma-delimited)

https://mail.google.com/

OAuth scopes (comma-delimited)