




Settings in Gmail

Setting Gmail for OAUTH2 for Business accounts



Table of Contents

Setting Gmail for OAUTH2 - Business accounts (OAUTH2.0 does not support free Gmail account)	3
Create a Gmail service account	3
1. Step 1: Create a new project.	3
1.1 From the main dashboard, click Create Project	3
1.2 Click New Project.....	3
1.3 Enter a Project name for example 'Gmail Service Account' and click Create.	4
2. Step 2: Enable APIs Sets.	4
2.1. Make sure your new project is selected in the projects list at the top of the screen and then click Enable APIs & Services.	4
2.2. In the API library, search for the following API sets; Gmail API, Google Calendar API & Contacts API . Click on each of them in turn and click Enable . This allows the adding of permission scopes later, but nothing has been granted yet. 5	5
3. Step 3: Create the service account user	6
3.1. Click the menu button  and select IAM & Admin > Service accounts	6
3.2. Click Create Service Account.	6
3.3. Fill in a name and description for the service account and click Create and Continue	7
3.4. Click 'Done' (ignore sections 2 & 3)	7
3.5. Open the menu in the Action column and click Manage Keys	8
3.6. Click Create New Key	8
3.7. Make sure JSON is selected and click ' Create '	9
3.8. The JSON file should be downloaded to your computer. You must store this securely as it provides access to your resources. Click ' Close '.	9
4. Step 4: Enable service accounts with Gmail	9
4.1. Login to GSuite Admin Console	9
4.2. Click Security	10
4.3. Scroll down and click API Controls	10
4.4. Click Manage Domain Wide Delegation.	11
4.5. Click Add New	11
4.6. Input the Client ID* of your service account and OAuth scopes.....	12
4.7. Your service account will now be displayed here.....	13
4.8. <i>Allow 5 mins for the change to go through the system on Gmail side.</i>	13

Setting Gmail for OAUTH2 - Business accounts (OAUTH2.0 does not support free Gmail account)

Create a Gmail service account

Go to the [Google Cloud Platform Console](#) and sign in as a super administrator. If this is your first time signing in to the console, you will be asked to agree to the Terms of Service.

1. Step 1: Create a new project.

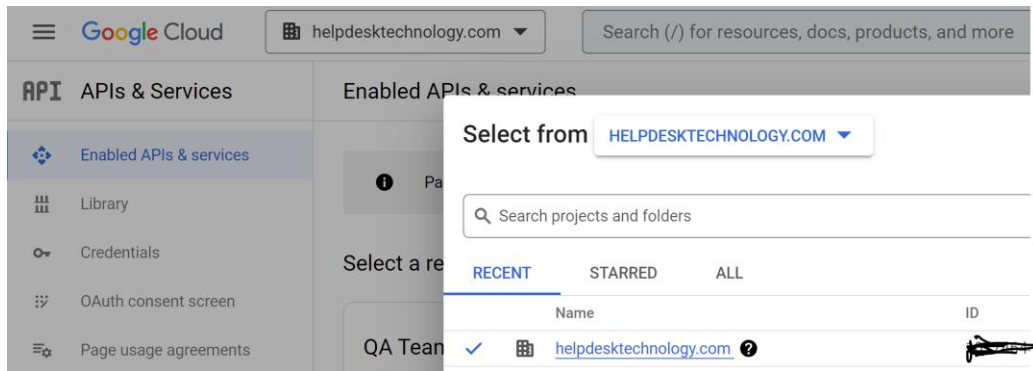
1.1 From the main dashboard, click **Create Project**.



If you have used the console before, you will need to click the down arrow to open your projects list.



1.2 Click New Project.



1.3 Enter a Project name for example 'Gmail Service Account' and click Create.

Google Cloud Search (/) for resources, do

New Project

Project name *
My Project 57658 ?
Project ID: fast-banner-398219. It cannot be changed later. [EDIT](#)

Organization *
helpdesktechnology.com ?
Select an organization to attach it to a project. This selection can't be changed later.

Location *
helpdesktechnology.com [BROWSE](#)
Parent organization or folder

[CREATE](#) [CANCEL](#)

2. Step 2: Enable APIs Sets.

2.1. Make sure your new project is selected in the projects list at the top of the screen and then click Enable APIs & Services.

Google APIs Gmail Service Account Search for APIs and Services

API APIs & Services APIs & Services [+ ENABLE APIS AND SERVICES](#)

i You don't have any APIs available to use yet. To get started, click "Enable APIs and services" or go to the [API library](#)

- Dashboard
- Library
- Credentials
- OAuth consent screen
- Domain verification
- Page usage agreements



2.2. In the API library, search for the following API sets; **Gmail API, Google Calendar API & Contacts API**. Click on each of them in turn and click **Enable**. This allows the adding of permission scopes later, but nothing has been granted yet.




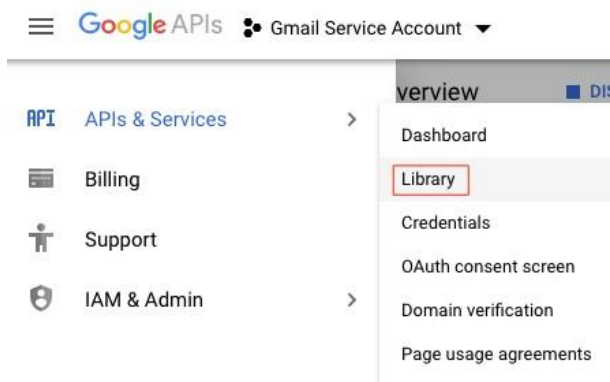
Gmail API

Google

Flexible, RESTful access to the user's inbox

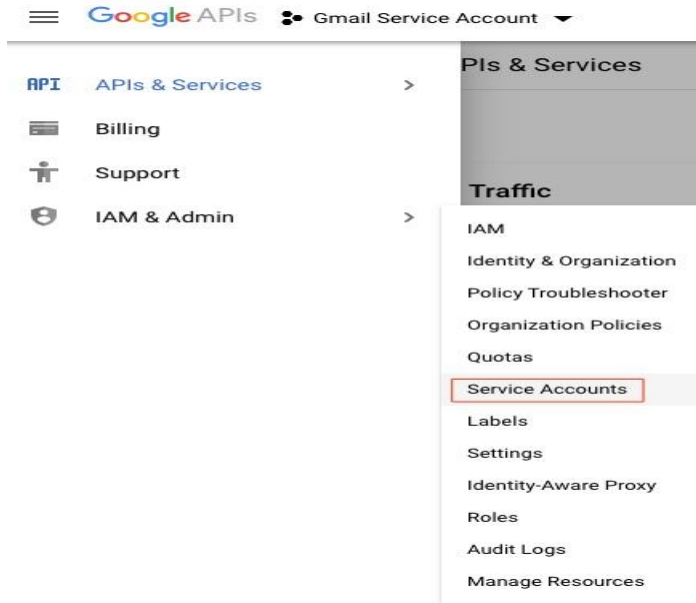


*Note: To get back to the API Library each time you will need to click the menu button  and select **APIs & Services > Library**.*

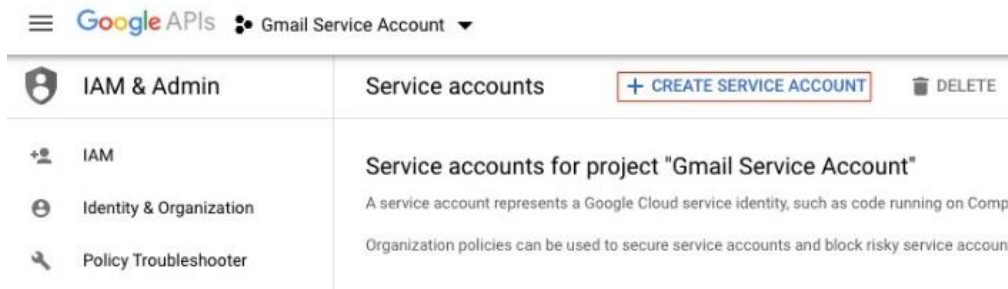


3. Step 3: Create the service account user

3.1. Click the menu button and select **IAM & Admin > Service accounts**.



3.2. Click Create Service Account.



3.3. Fill in a name and description for the service account and click **Create and Continue**.

IAM & Admin | Create service account

1 Service account details

Service account name
Gmail Service User
Display name for this service account

Service account ID *
gmail-service-user-110 X ↺
Email address: gmail-service-user-110@gmail-service-account-382212.iam.gserviceaccount.com

Service account description
Allow access to emails
Describe what this service account will do

CREATE AND CONTINUE

2 Grant this service account access to project (optional)

3 Grant users access to this service account (optional)

DONE CANCEL

3.4. Click 'Done' (ignore sections 2 & 3)

Google Cloud Platform | Gmail Service Account | Search Products, r

IAM & Admin | Create service account

1 Service account details

2 Grant this service account access to project (optional)

Grant this service account access to Gmail Service Account 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

CONTINUE

3 Grant users access to this service account (optional)

DONE CANCEL

3.5. Open the menu in the Action column and click **Manage Keys**.

Service accounts + CREATE SERVICE ACCOUNT DELETED MANAGE ACCESS REFRESH

Service accounts for project "Gmail Service Account"

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.](#)

Filter Enter property name or value

Email	Status	Name ↑	Description	Key ID	Key creation date	OAuth 2 Client ID	Actions
							<ul style="list-style-type: none">Manage detailsManage permissionsManage keysView metricsView logsDisableDelete

3.6. Click **Create New Key**.

DETAILS PERMISSIONS **KEYS** METRICS LOGS

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 Feder](#) [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 ▾

Create new key	Key creation date	Key expiration date
Upload existing key		

3.7. Make sure JSON is selected and click 'Create'

Create private key for "Gmail Service User"

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

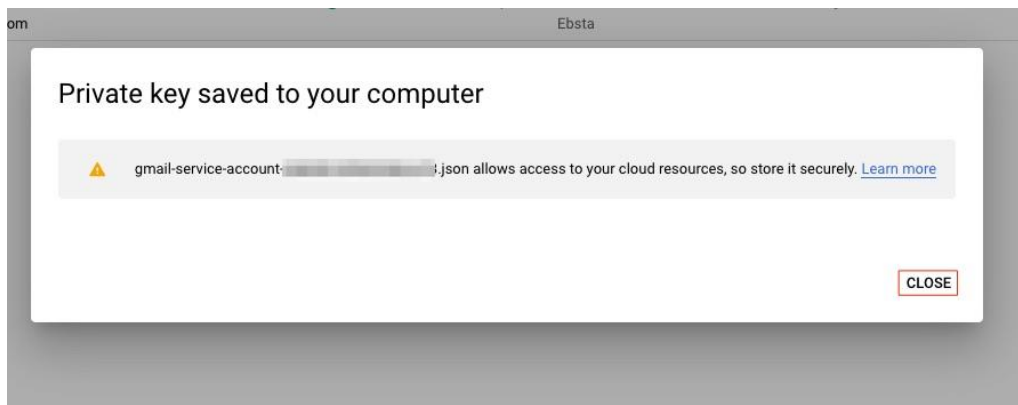
P12

For backward compatibility with code using the P12 format

CANCEL

CREATE

3.8. The JSON file should be downloaded to your computer. You must store this securely as it provides access to your resources. Click 'Close'.

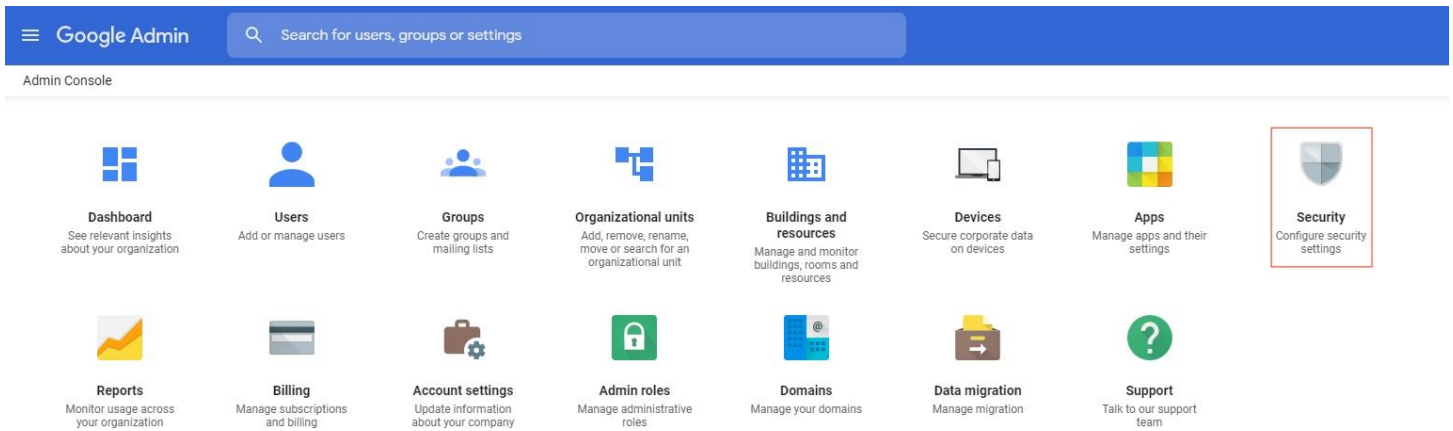


4. Step 4: Enable service accounts with Gmail

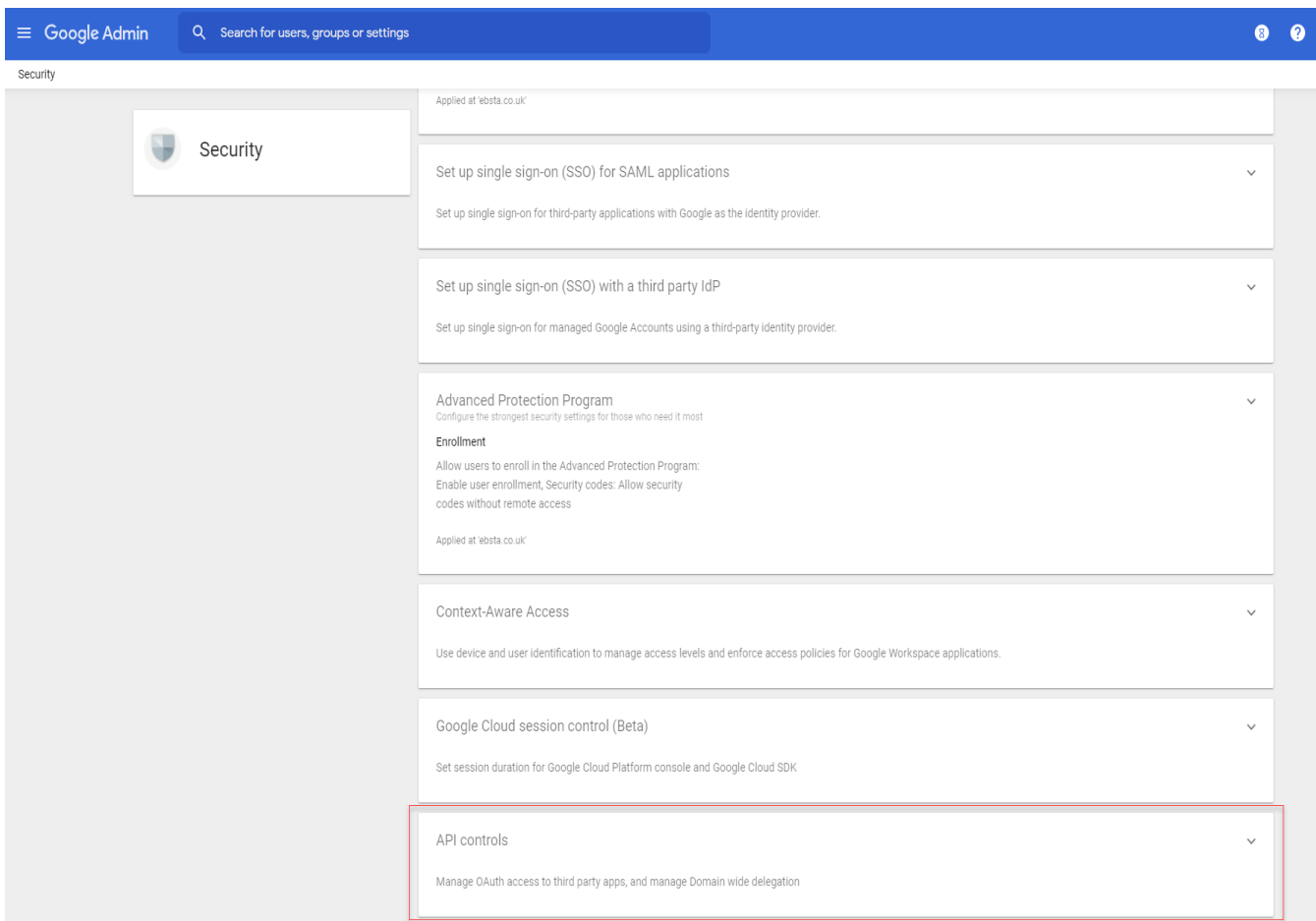
4.1. Login to G Suite Admin Console

Link to G Suite Admin Console - [G Suite Admin Console](#)

4.2. Click Security.



4.3. Scroll down and click API Controls.



4.4. Click Manage Domain Wide Delegation.

The screenshot shows the Google Admin console interface. At the top, there is a blue header with the Google Admin logo and a search bar. Below the header, the breadcrumb trail reads "Security > API Controls". The main content area is divided into two sections. The left section is titled "API controls" and contains a brief description: "Use these controls to enable or restrict access to G Suite APIs for customer-owned and third-party applications and service accounts. Reduce the risk associated with third-party access to G Suite APIs by limiting access to only trusted apps." The right section is titled "App access control" and contains the following information: "Manage app access to your Google services. Ensure that users can give access only to apps that your organisation trusts. Learn more". Below this is an "Overview" section with two columns of statistics: "0 restricted Google services" and "2 third-party apps configured", and "15 unrestricted Google services". There are two links: "MANAGE GOOGLE SERVICES" and "MANAGE THIRD-PARTY APP ACCESS". Below the overview is a "Settings" section with a checkbox labeled "Trust internal, domain-owned apps" which is checked. A message field is also present with a "Message (300 characters limit)" label. At the bottom right of the settings section are "CANCEL" and "SAVE" buttons. Below the app access control section is a "Domain wide delegation" section with a description: "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". A link "MANAGE DOMAIN WIDE DELEGATION" is highlighted with a red box.

4.5. Click Add New.

The screenshot shows the Google Admin console interface for "Domain-wide Delegation". At the top, there is a blue header with the Google Admin logo and a search bar. Below the header, the breadcrumb trail reads "Security > API Controls > Domain-wide Delegation". The main content area is titled "API clients" and features an "Add new" button highlighted with a red box. Below the title is a filter section with a "+ Add a filter" button. The main area contains an empty table with the following columns: "Name", "Client ID", and "Scopes". At the bottom left, there is a "Rows per page: 10" dropdown menu. At the bottom right, there is a pagination control showing "Page 1 of 1" with navigation arrows.

4.6. Input the Client ID* of your service account and OAuth scopes

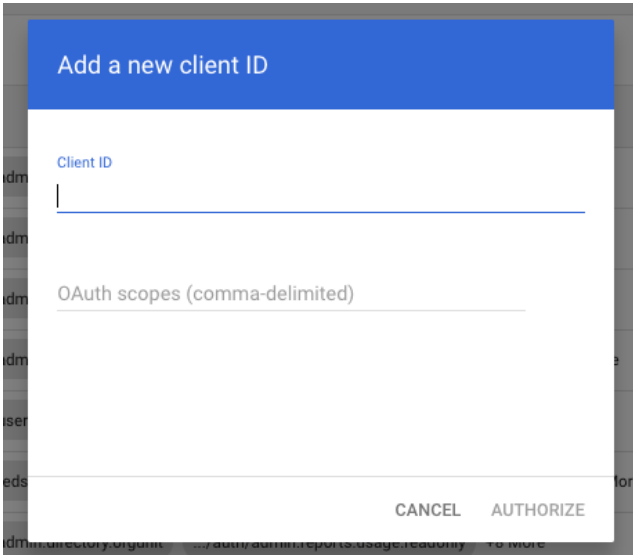
In OAuth scopes, input:

https://mail.google.com


https://www.googleapis.com/auth/gmail.send

https://www.googleapis.com/auth/gmail.modify

Then click **Authorize**.



Check below to know how you can find the Client ID of your service account

* **Client ID** is the unique ID of the Service account client (not the Key ID). It can be found by clicking the menu button  in the GCP console and selecting **IAM & Admin > Service accounts**. Click **View Client ID** and then copy it onto your clipboard.



Service accounts [+ CREATE SERVICE ACCOUNT](#) [DELETED](#) [MANAGE ACCESS](#) [REFRESH](#) [HELP ASSISTANT](#) [LEARN](#)

Service accounts for project "Gmail Service Account"

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.](#)

Filter Enter property name or value

mail	Status	Name ↑	Description	Key ID	Key creation date	OAuth 2 Client ID	Actions
gmail-service-user@gmail-service-account-92212.iam.gserviceaccount.com	Enabled	Gmail Service User	Allow to access emails	e9e8843b56f12ed81601355cb46077087f1ffbe6	Mar 30, 2023		

Client ID for service account

DELETE

i Service account clients are created when [domain-wide delegation](#) is enabled on a service account.

Client ID	[REDACTED]
Service account	ebstaexample ebstaexample@gmail-service-account- [REDACTED]gserviceaccount.com
Creation date	Aug 20, 2020
Display name	Client for ebstaexample

SAVE

CANCEL

4.7. Your service account will now be displayed here.

Admin

Search for users, groups or settings

Security > API Controls > Domain-wide Delegation

i Developers can register their web applications and other API clients with Google to enable access to data without your users having to individually give consent or their

API clients [Add new](#) [Download client info](#)

+ Add a filter

Name	Client ID	Scopes
gmail-service-user@...	[REDACTED]	.../auth/gmail.send .../auth/gmail.modify +1 More

4.8. Allow 5 mins for the change to go through the system on Gmail side.