Mission Guide: Google Workspace

Your Mission: Use F-Response to collect Google Workspace account data

Using F-Response to connect to Google Workspace custodian accounts and collect their contents

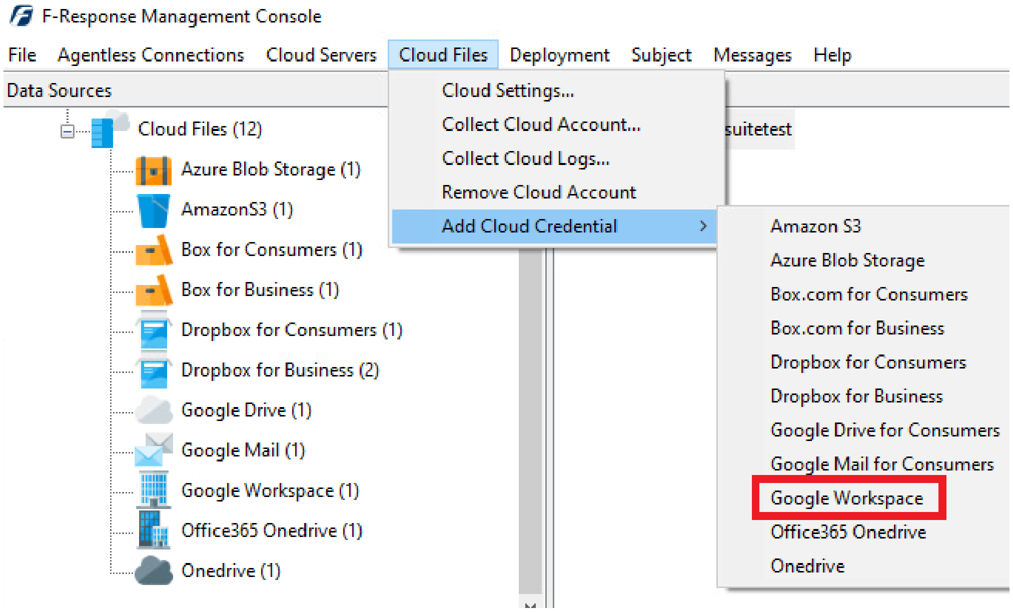
Important Note

Disclaimer: F-Response provides access to 3rd party data sources via Application Programming Interfaces (APIs) and internal structures presented by the provider. 3rd party provided data sources by their very nature are volatile. The afore mentioned F-Response products provide "best effort" for accessing and interacting with those 3rd party data sources however service disruptions, API changes, provider errors, network errors, as well as other communications issues may result in errors or incomplete data access. F-Response always recommends secondary validation of any 3rd party data collection.

F-Response Cloud Collector Options Supported		
Revision History	Not supported.	Google Drive provides revision history, but it is not supported at this time. Enabling Revision History in F-Response will have no effect on the collection.
Hash Verification	Available and supported.	Google Drive provides md5 hashes of items which will be automatically checked in F-Response if Verify Hashes is enabled.
Rerun Collection	Available and supported.	F-Response can retry to collect specific items that have errored out.

Step 1: Open the Google Workspace Credential Configuration Window

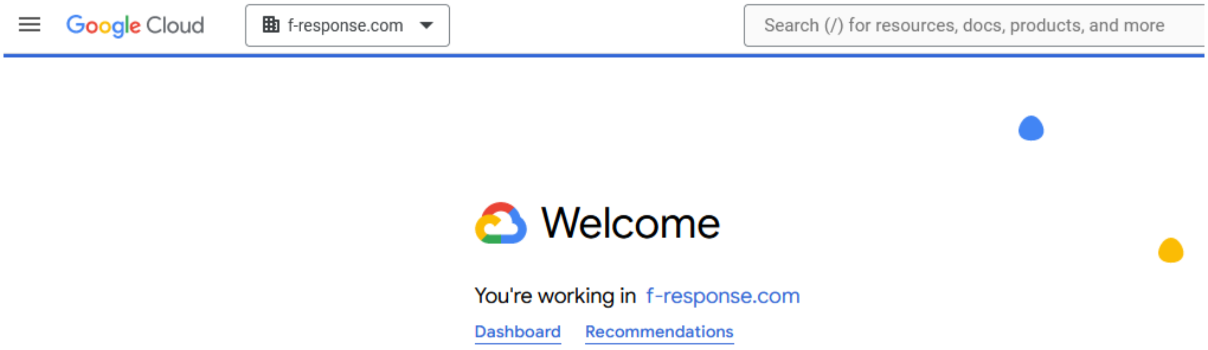
Open the F-Response Management Console and navigate to Providers->Provider Credentials->Google Workspace, or double click on the appropriate icon in the Data Sources pane.



F-Response Management Console

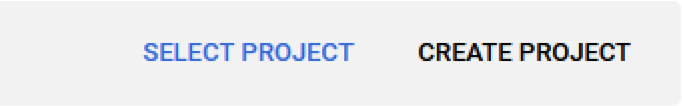
Step 2: Configure a Domain Wide Delegation account for the Google Workspace Domain

Before you can access Google Workspace accounts you must use the Google Developers Console to configure a Domain Wide Delegation account. This can no longer be done with an administrator account and must be done using the super admin account. The Developers Console is located at: https://console.cloud.google.com

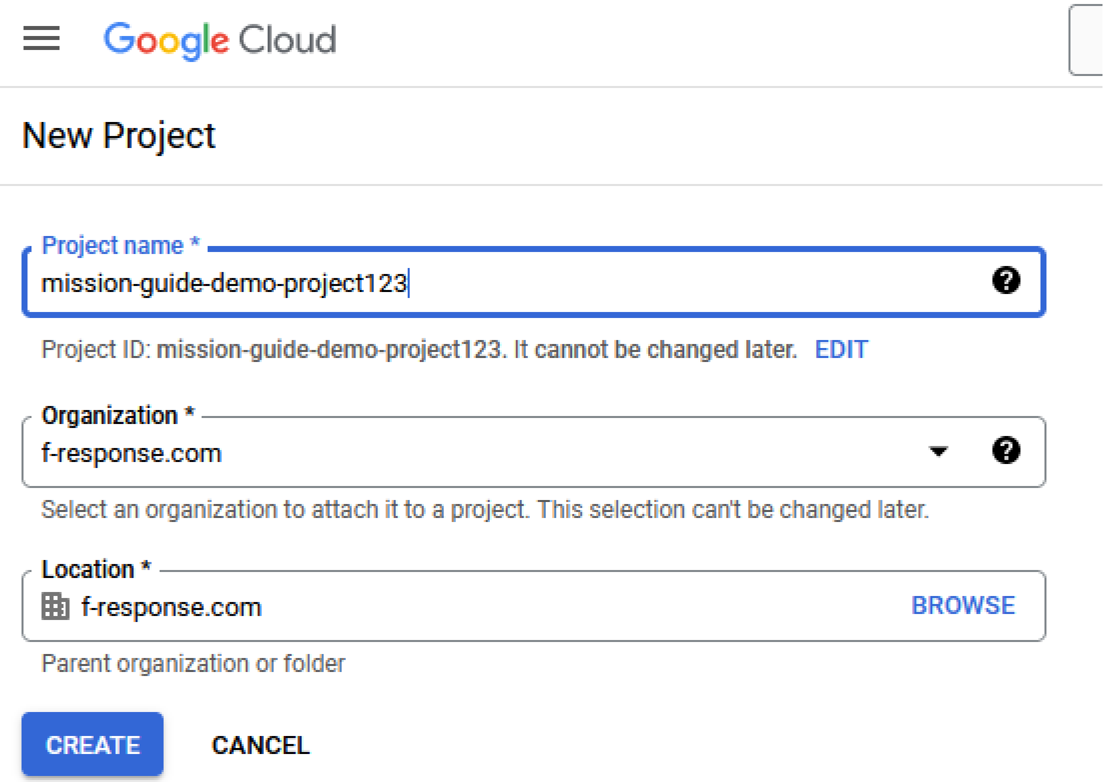

Google Cloud
f-response.com
Search (/) for resources, docs, products, and more
Welcome
You're working in f-response.com
Dashboard
Recommendations

Google APIs Console

Open a web browser and access the Google Console; the first step is to create a project. Select the "dashboard" and click on the "Create Project" button.



Give the project a name or accept the defaults.



New Project

Project name * mission-guide-demo-project123

Project ID: mission-guide-demo-project123. It cannot be changed later. EDIT

Organization * f-response.com

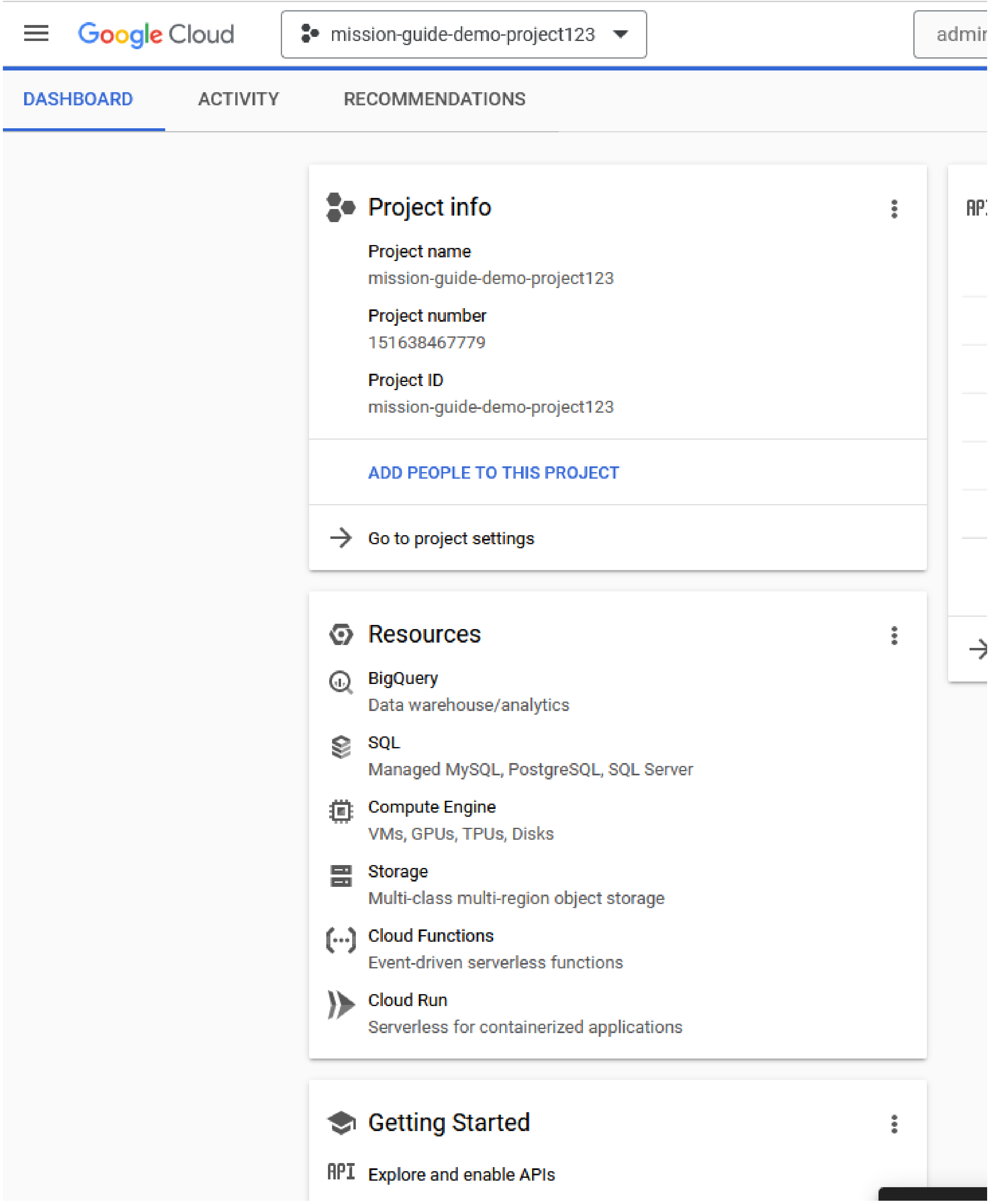
Select an organization to attach it to a project. This selection can't be changed later.

Location * f-response.com

Parent organization or folder

Press "Create" when done.

Next you will need to click "Explore and enable APIs" under "Getting Started." There are three options to enable here: Admin SDK, Google Drive API, and the Gmail API.



Project info

Project name
mission-guide-demo-project123

Project number
151638467779

Project ID
mission-guide-demo-project123

Resources

BigQuery
Data warehouse/analytics

SQL
Managed MySQL, PostgreSQL, SQL Server

Compute Engine
VMs, GPUs, TPUs, Disks

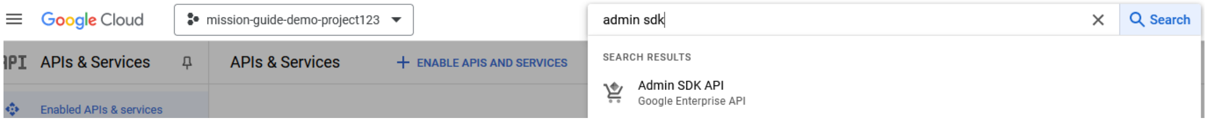
Storage
Multi-class multi-region object storage

Cloud Functions
Event-driven serverless functions

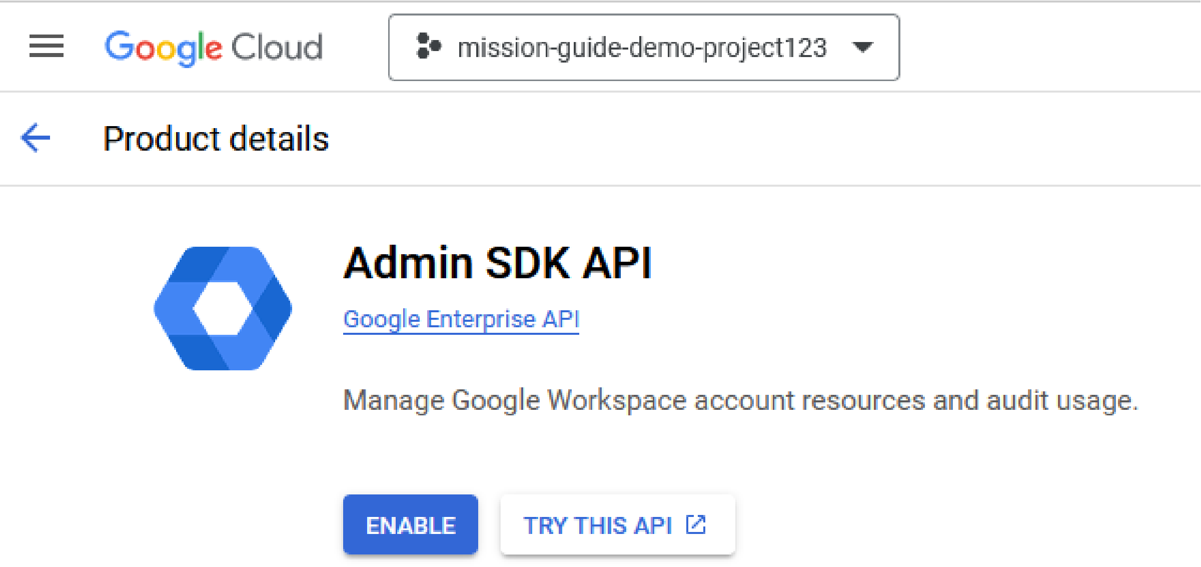
Cloud Run
Serverless for containerized applications

Getting Started

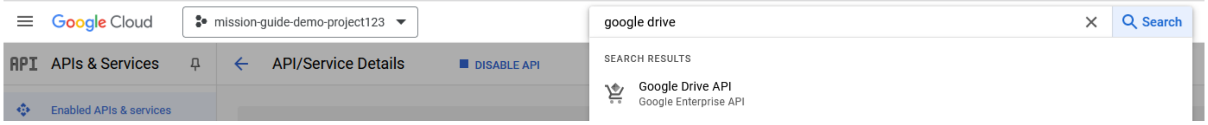
Use the search bar at the top to search for each API listed before and select them. Then press "Enable."



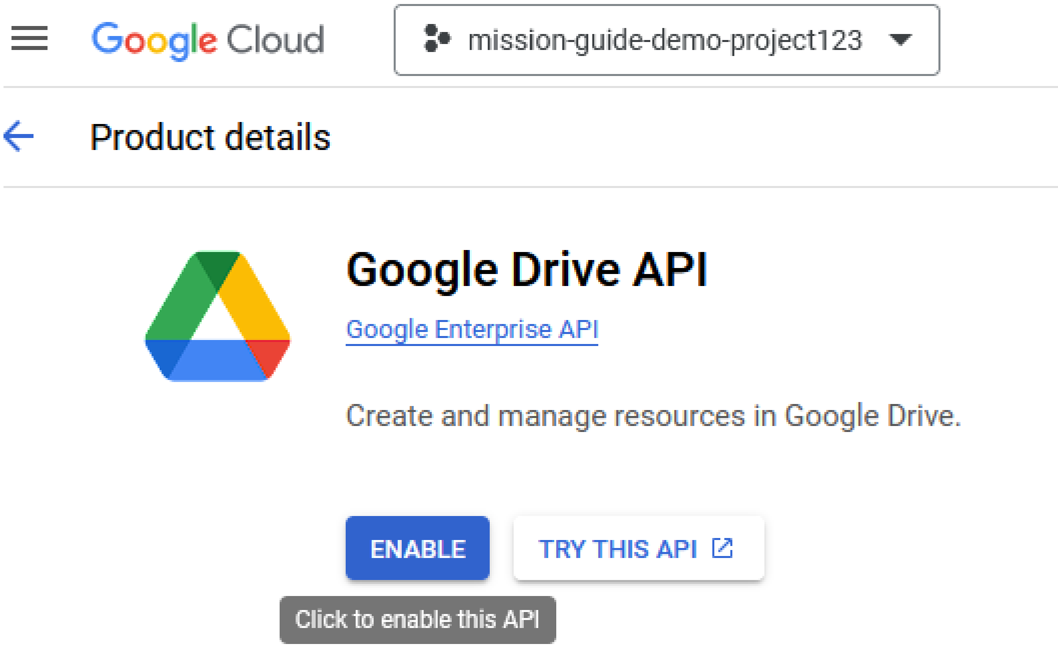
admin sdk



Manage Google Workspace account resources and audit usage.



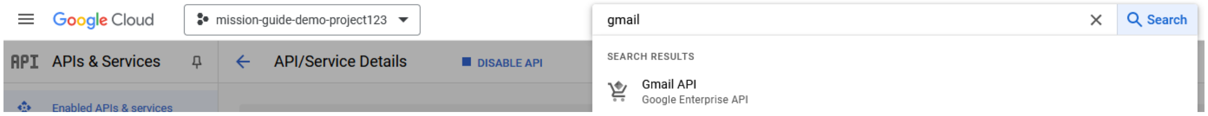
google drive

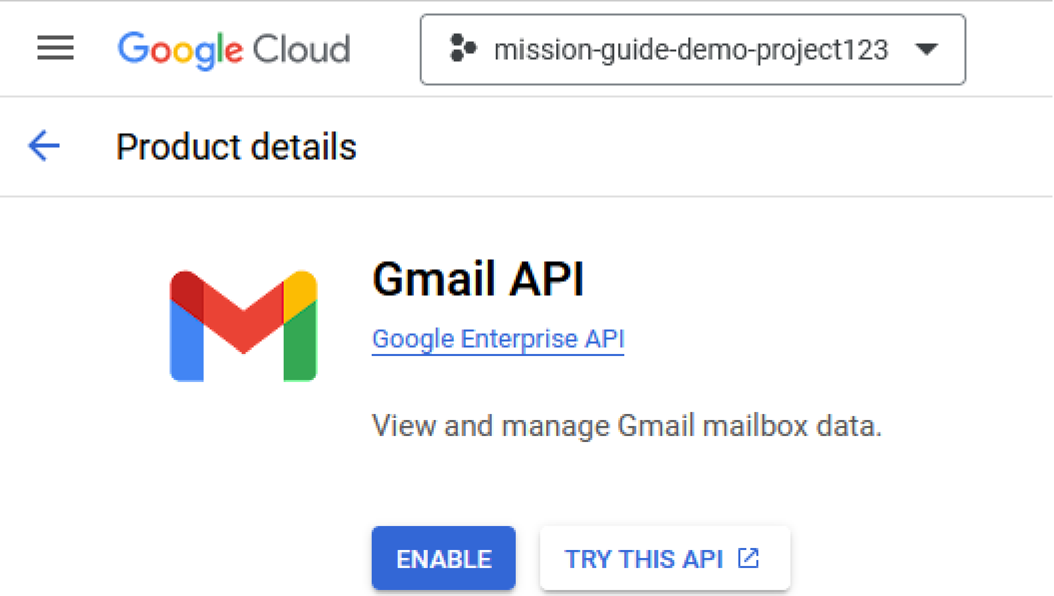


Google Drive API

Google Enterprise API

Create and manage resources in Google Drive.



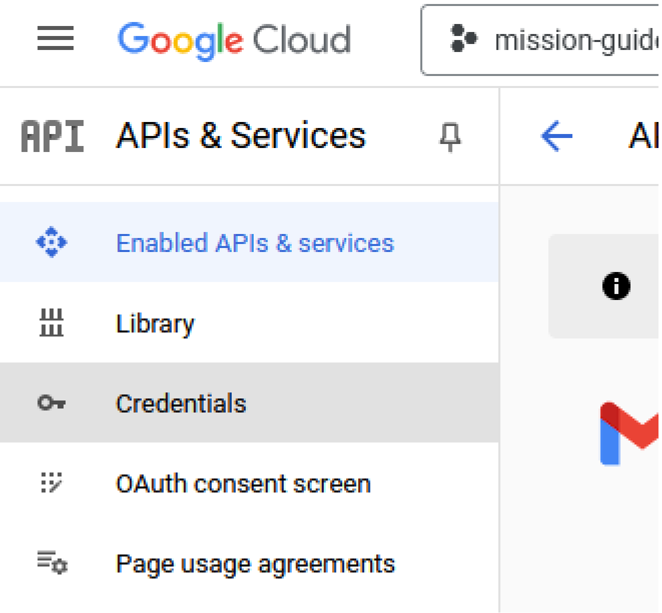


Gmail API

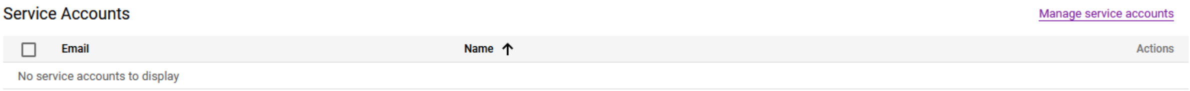
Google Enterprise API

View and manage Gmail mailbox data.

Now you will need to configure a service account. Press the "Credentials" icon on the left hand side of the screen.



Select "Manage service accounts."

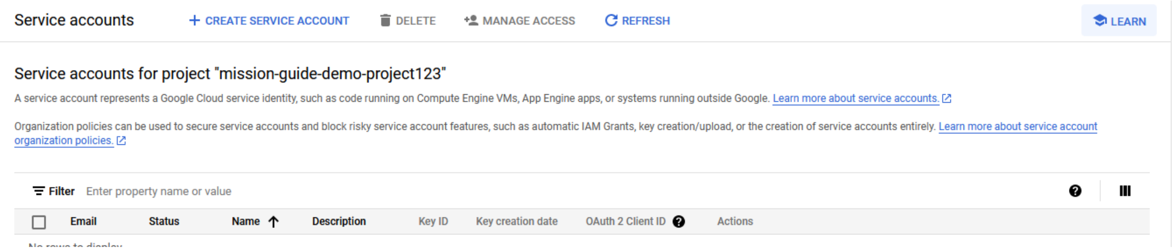


Service Accounts

Manage service accounts

□	Email	Name ↑	Actions
No service accounts to display			

Press the "+ Create Service Account" link at the top of the page.



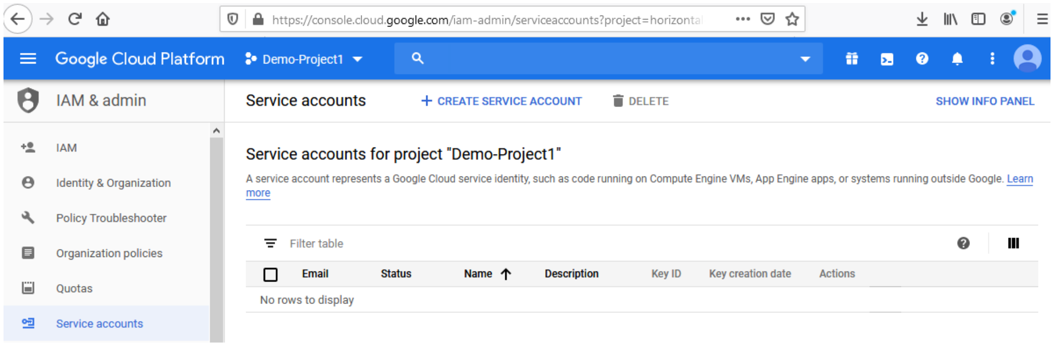
Service accounts for project "mission-guide-demo-project123"

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
No rows to display								

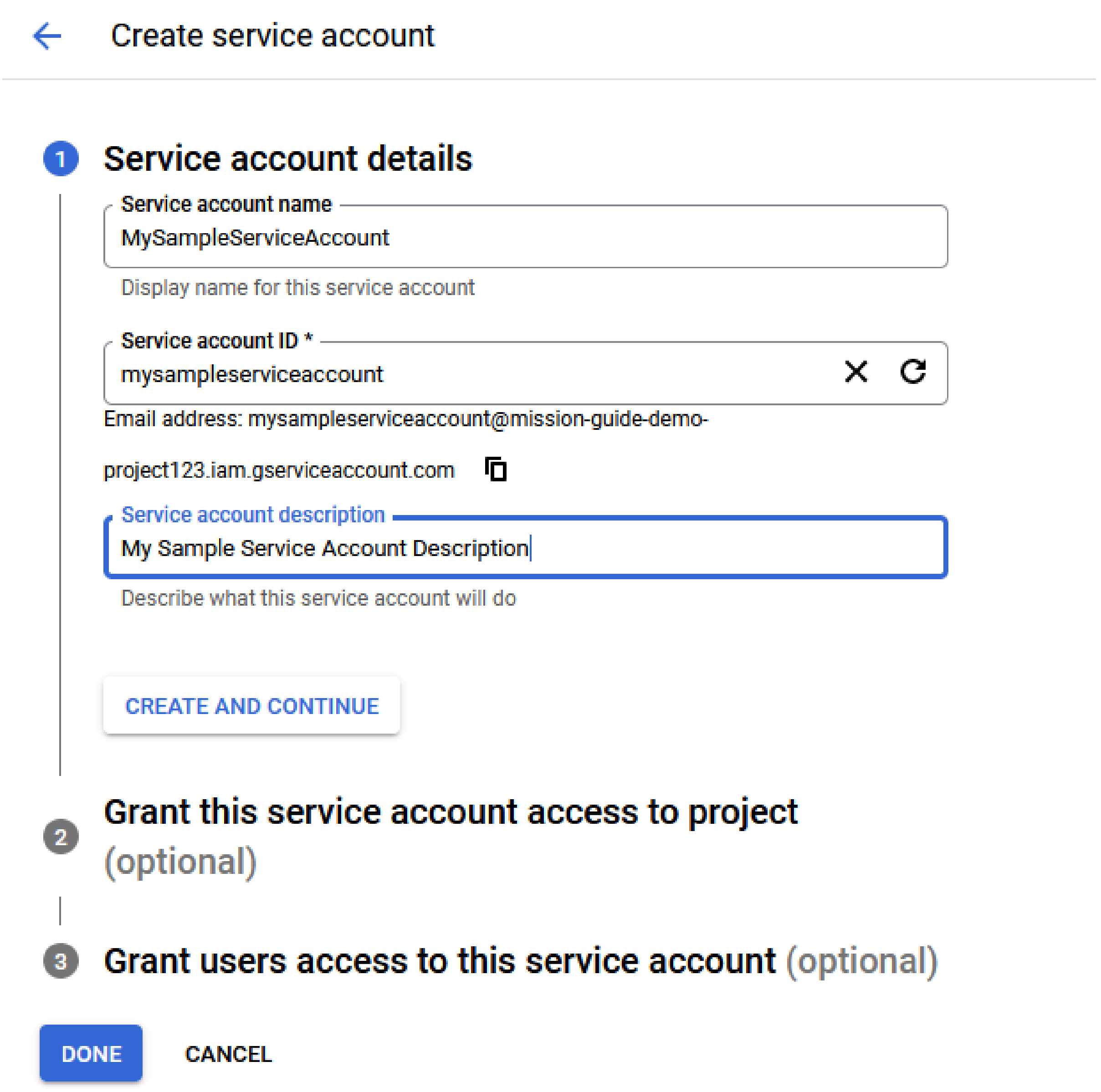


Service accounts for project "Demo-Project1"

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

□	Email	Status	Name ↑	Description	Key ID	Key creation date	Actions
No rows to display							

Here you can click on "+ CREATE SERVICE ACCOUNT"



Create service account

1 Service account details

Service account name: MySampleServiceAccount

Display name for this service account

Service account ID *: mysampleserviceaccount

Email address: mysampleserviceaccount@mission-guide-demo-project123.iam.gserviceaccount.com

Service account description: My Sample Service Account Description

Describe what this service account will do

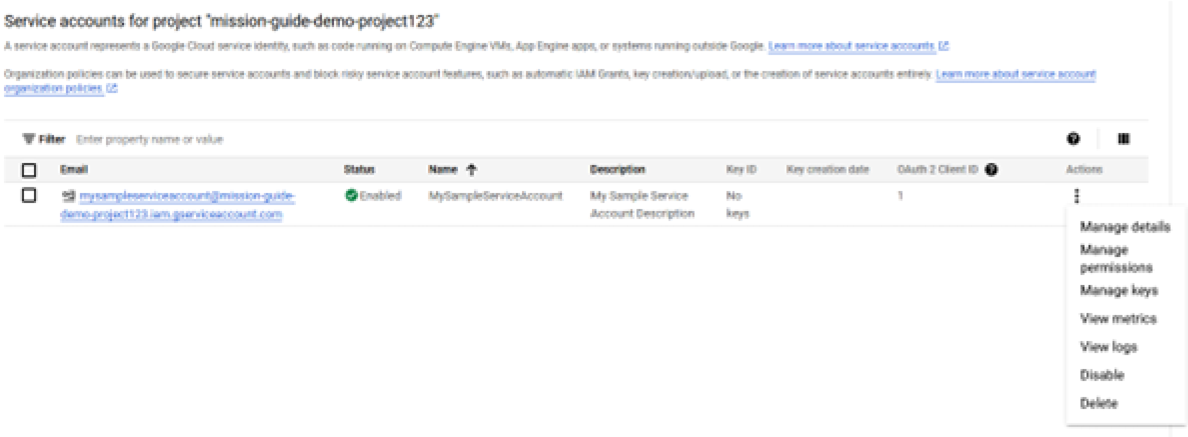
2 Grant this service account access to project (optional)

3 Grant users access to this service account (optional)

Service Account Creation

This will bring you to a dialog for creating the service account. Create a name in the ”Service account name” field, this is purely for identification. Click “Done.”

You will be returned to the service account listing, use the triple dots to select “Manage Keys.”



Service accounts for project "mission-guide-demo-project123"

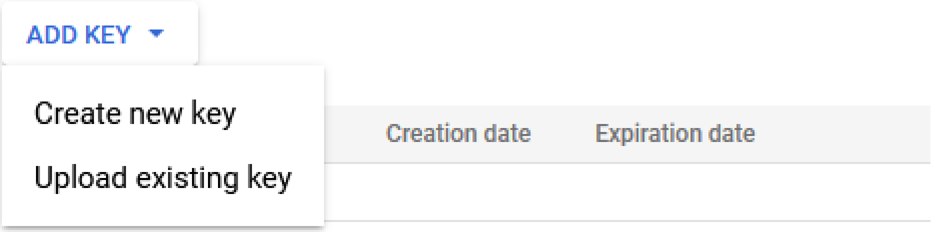
A service account represents a Google Cloud service identity, such as code running on Compute Engine VMs, App Engine apps, or systems running outside Google. Learn more about service accounts

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

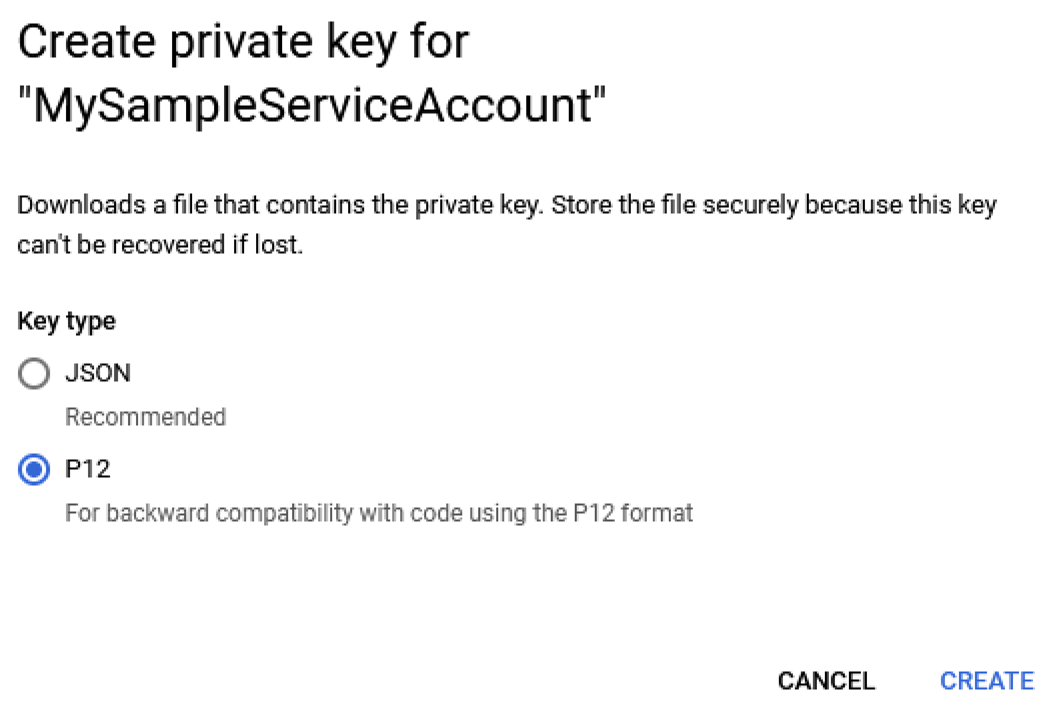
Filter Enter property name or value

□	Email	Status	Name ↑	Description	Key ID	Key creation date	OAuth 2 Client ID	Actions
□	mysampleserviceaccount@mission-guide-demo-project123.iam.gserviceaccount.com	Enabled	MySampleServiceAccount	My Sample Service Account Description	No keys		1	⋮

Select “Add Key” and “Create new key.”



Select the P12 format.



Create private key for "MySampleServiceAccount"

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

Key type

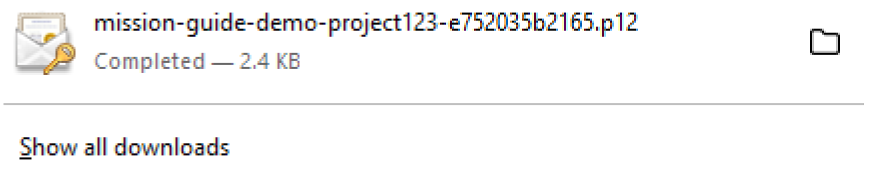
○ JSON

Recommended

● P12

For backward compatibility with code using the P12 format

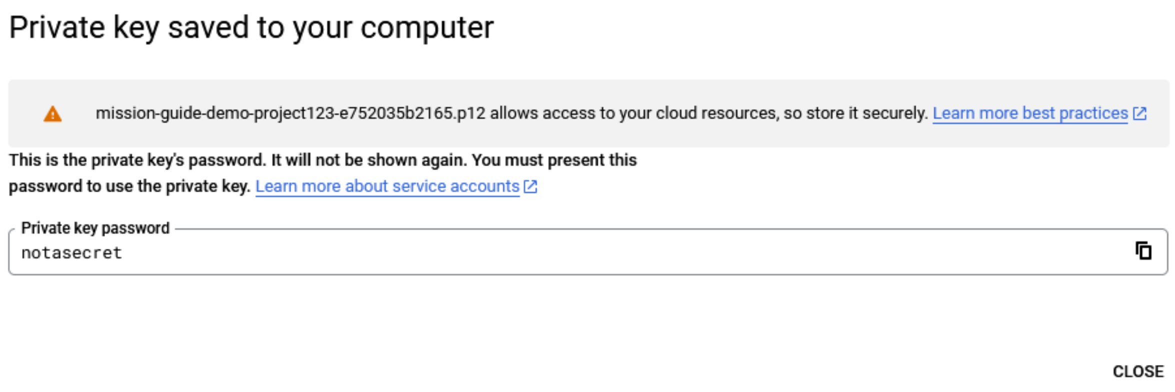
And press "Create."



mission-guide-demo-project123-e752035b2165.p12

Completed — 2.4 KB

The private P12 key will be downloaded, do not change the "notasecret" value in the displayed window.



Private key saved to your computer

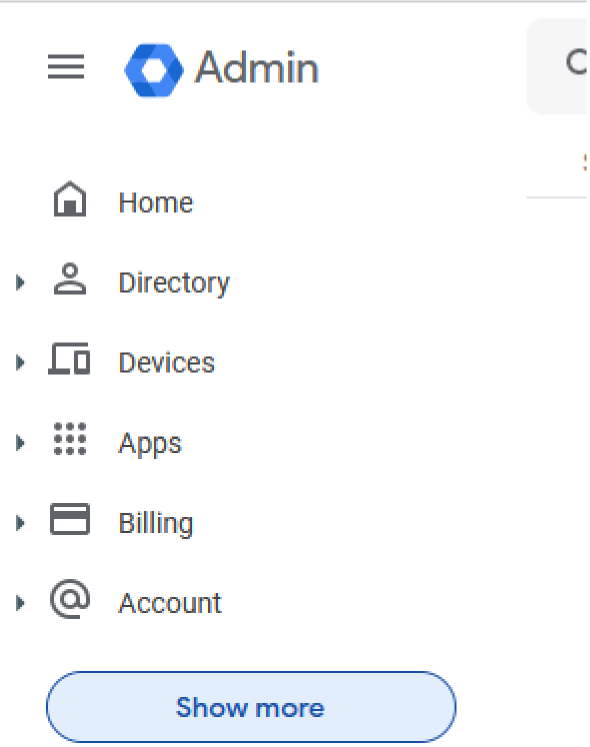
mission-guide-demo-project123-e752035b2165.p12 allows access to your cloud resources, so store it securely. Learn more best practices

This is the private key's password. It will not be shown again. You must present this password to use the private key. Learn more about service accounts

Private key password: notasecret

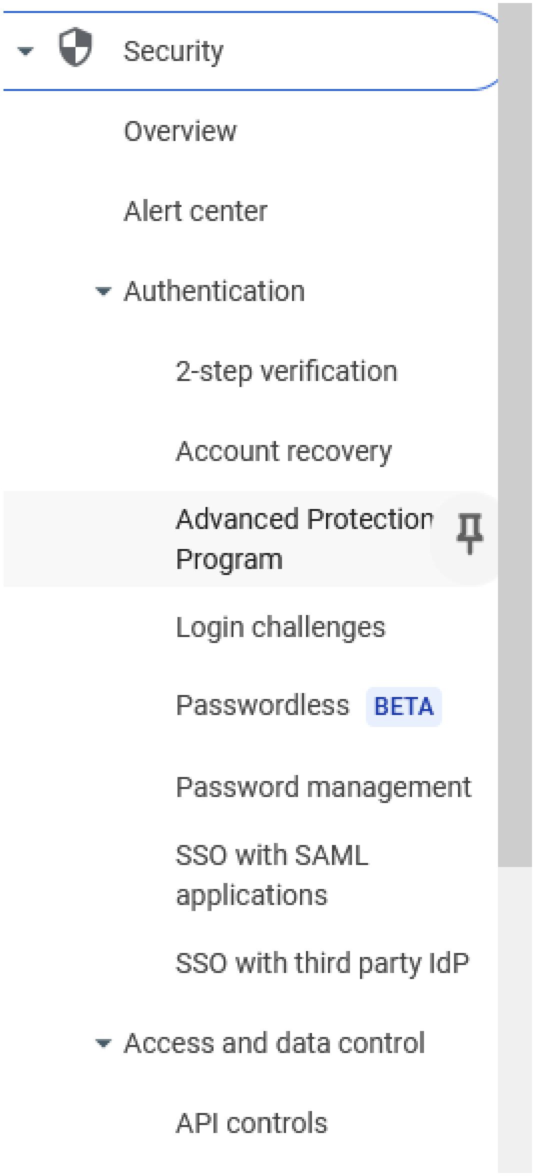
Following the encryption key download click DONE. You should see a newly created Service Account. Make note of the OAuth 2 Client ID and the Email value as they will both be needed in the next steps.

Now that we have created a service account and enabled API access we must give that service account access to the domain. We do this by logging in with the super administrator account in the Google Admin Console -> https://admin.google.com/



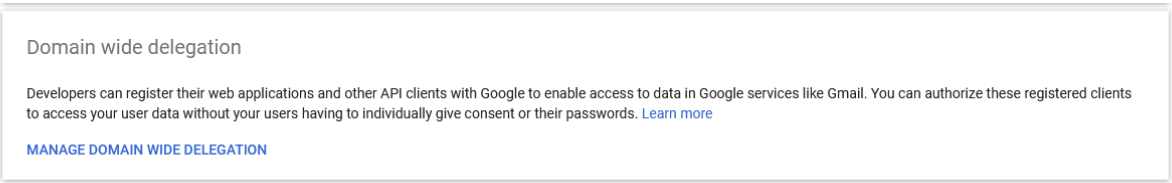
Google Admin Console

The Admin console provides options for administering the Google Workspace Domain. On the left hand side you will need to press "Show more" to see the Security options. Under Security you will need to expand "Access and data controls" then click on "API controls."



API controls

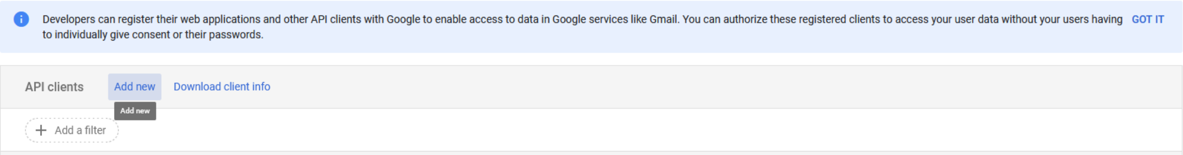
Next you will need to press on "Manage Domain Wide Delegation," to input the client id and scopes.



Domain wide delegation

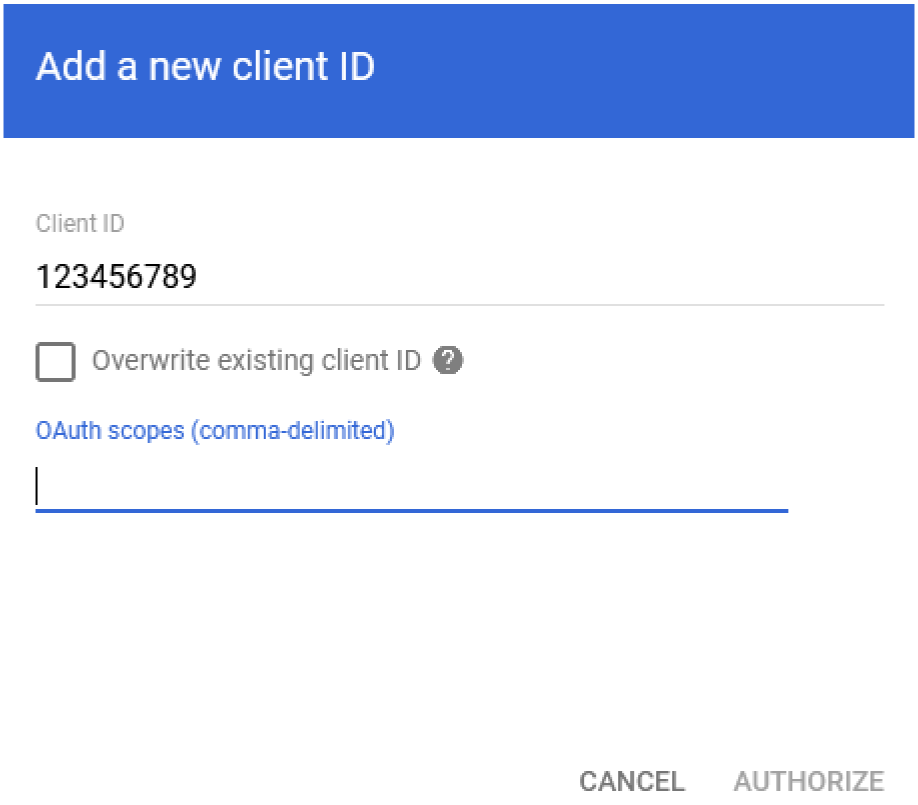
Developers can register their web applications and other API clients with Google to enable access to data in Google services like Gmail. You can authorize these registered clients to access your user data without your users having to individually give consent or their passwords. Learn more

MANAGE 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.

Press the “Add new” button to open the panel for inputting the details.



Add a new client ID

Client ID: 123456789

□ Overwrite existing client ID

OAuth scopes (comma-delimited)

Under “Add a new client ID” you will want to paste the Client ID that was recorded earlier into the Client ID field, and the following API Scope (please note the API scopes **must be comma separated**).

https://www.googleapis.com/auth/drive.readonly

https://www.googleapis.com/auth/admin.directory.user.readonly

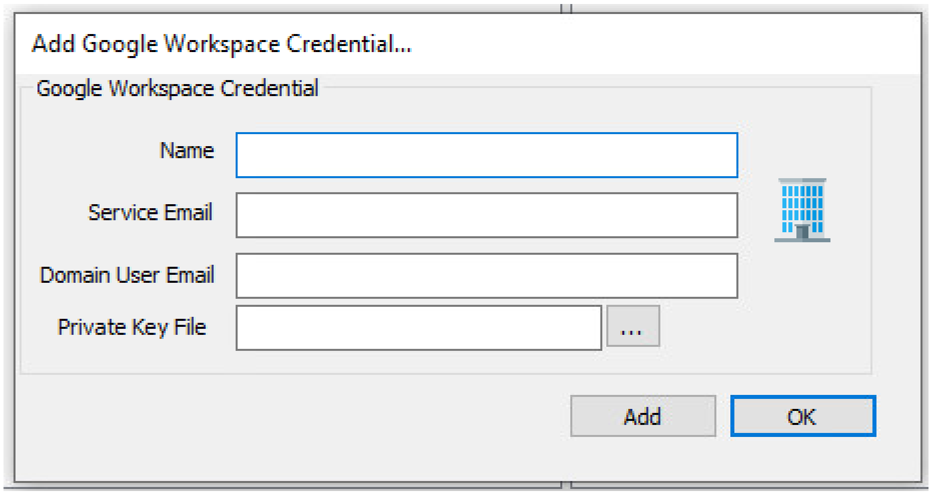
https://www.googleapis.com/auth/gmail.readonly https://www.googleapis.com/auth/admin.reports.usage.readonly

https://www.googleapis.com/auth/admin.reports.audit.readonly

Press Authorize to complete the delegated account permissions.

Step 3: Provide the newly obtained Google Workspace Credentials

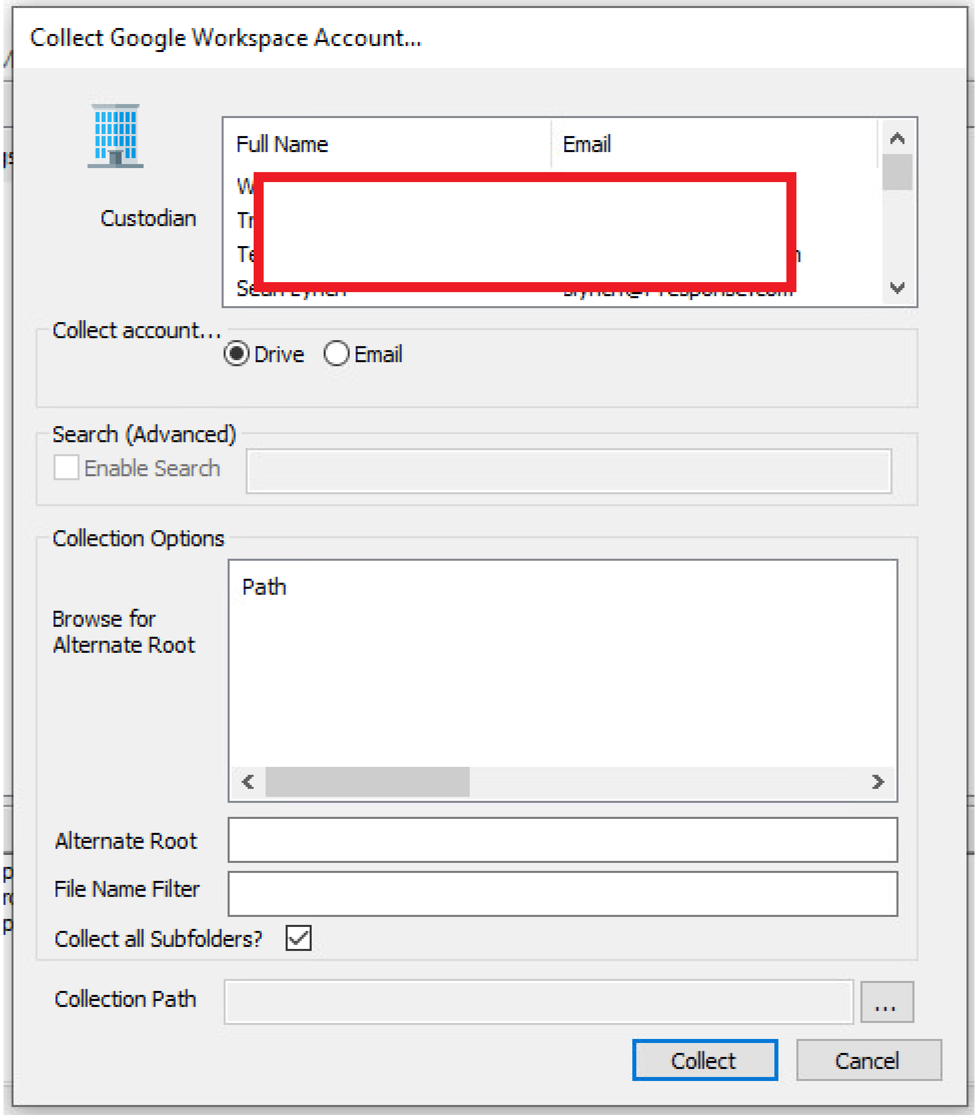
To configure Google Workspace access you will need the Service Email recorded earlier, the Super Admin Email Address (Domain User Email field), and the Private Key file downloaded earlier.


Add Google Workspace Credential...
Google Workspace Credential
Name
Service Email
Domain User Email
Private Key File
...
Add
OK

Configure Google Workspace Credentials

Step 4: Start a collection

Select the Google Workspace icon under Data Sources and then double click on the newly added Google Workspace account under Items. This will prepare a new dialog for collecting the account's contents.



Collect Google Workspace Account...

Custodian

Full Name	Email
[redacted]	[redacted]

Collect account... ● Drive ○ Email

Search (Advanced)

□ Enable Search

Collection Options

Browse for Alternate Root

Path

Alternate Root:

File Name Filter:

Collect all Subfolders? ☑

Collection Path:

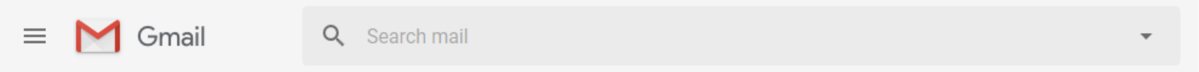
Starting a new collection...

Let's walk through the options here starting from the top of the window. First, locate the custodian you wish to collect and highlight.

Next, specify the type of data you wish to collect under from the respective options under **Collect Account…** To collect all the selected data type from the account, simply select the **Collection Type,** enter a location to save the data in the **Collection Path**, and click the Collect button. For more targeted collection options see below.

Email options

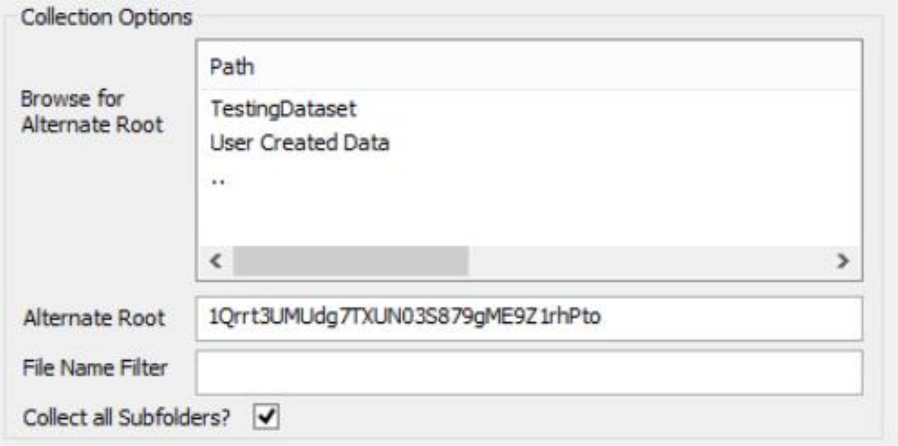
Use the optional **Search (Advanced)** feature to apply the same search mechanisms available in the Gmail web interface to your potential collection. This is an optional feature and may also be ignored to attempt a collection of the entire Google Mail account.



More information about Google Mail search options is available on the Google Mail API website. (https://support.google.com/mail/answer/7190?hl=en)

Drive Options

F-Response now has the option to target specific data in Google Drive. Some, or all, of the **Collection Options** can be invoked to reduce the size of the data set to be collected. The options are as follows:



Collection Options

Browse for Alternate Root

Path
TestingDataset
User Created Data
..

Alternate Root: 1Qrrt3UMUdg7TXUN03S879gME9Z1rhPto

File Name Filter:

Collect all Subfolders? ☑

Browse for Alternate Root: This option will allow you to select a different starting location to pull data from. Click on an item and wait a moment for the subdirectories to parse. Continue to click and drill as far down the path as you need to narrow the scope of the collection accordingly (the 'double dot' option will take you back). The Alternate Root field below will populate with the correct information.

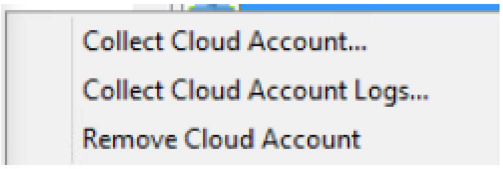
File Name Filter: Will check the string entered here against files as presented by the provider. There is no need to enter wildcards (*.*) and it does not use regular expressions. For example, to collect only Excel files in the account, just type **.xls** in the box.

Collect all Subfolders? If checked, it will collect the content of all subfolders, if unchecked, it will only collect that folder’s file contents.

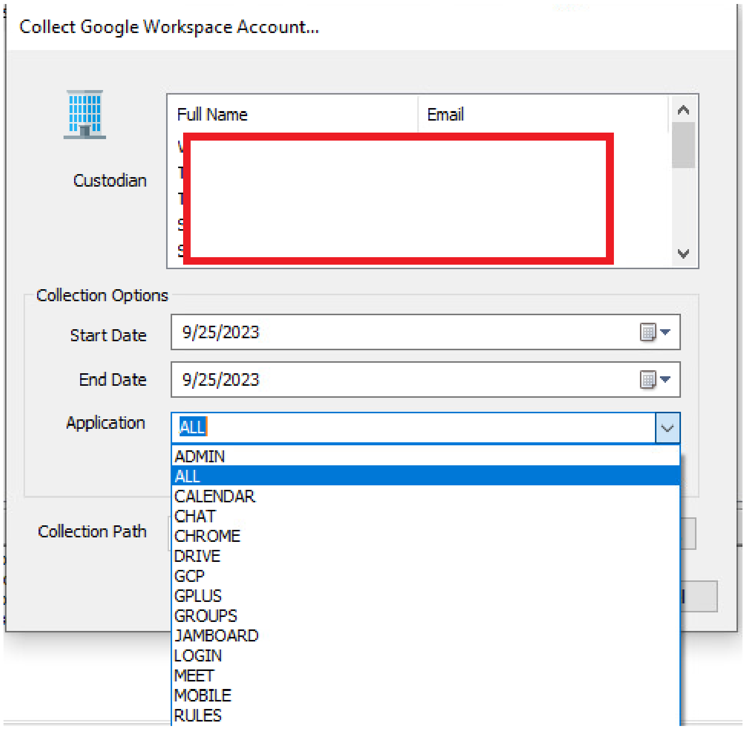
Step 4a (optional): Collect Google Log Information

F-Response has added Google Workspace log file collection capabilities. Note this is a separate process from data collection. Please find the details on what specific logs are available from Google here. All log files are collected in JSON format which can be parsed using your own tools for further review.

To initiate a log collection, highlight the account in the Items column and choose **Collect Cloud Account Logs..** from the drop-down menu or simply right click to bring up the same menu.



This will bring up the Collection configuration window:



Collect Google Workspace Account...

Custodian

Full Name	Email
[redacted]	

Collection Options

Start Date 9/25/2023

End Date 9/25/2023

Application ALL

Collection Path

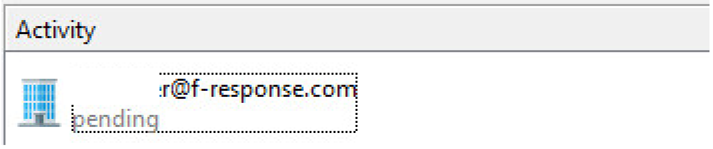
Here we can walk through the options starting from the top of the window. First, locate the custodian you wish to collect logs for and highlight.

Under **Collection Options** choose a start and end date for the scope of log collection. **Note: Google does not offer logs outside of the previous six months**. Then choose the log type you wish to collect from the Application drop down list.

Lastly, enter a location to save the data in the **Collection Path**, and click the Collect button.

Step 5: Check the Activity Pane

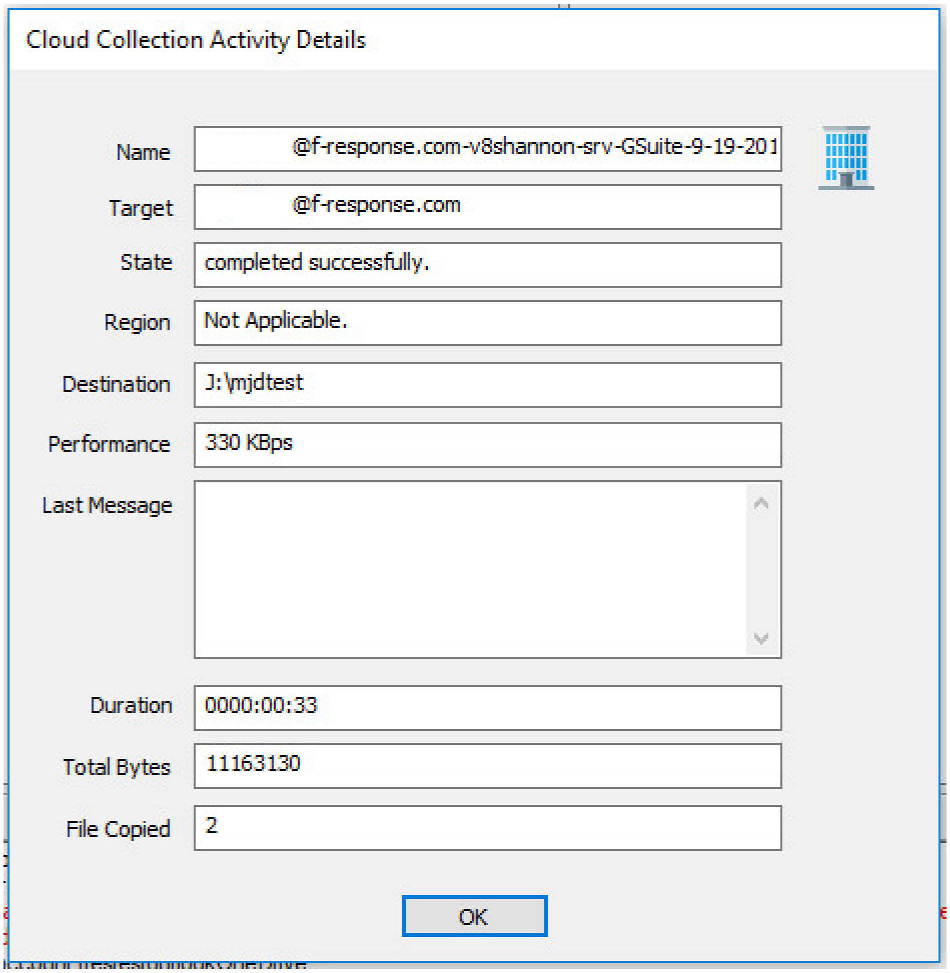
The Activity Pane shows the active collection. Double clicking on the collection will provide additional details.



Activity

r@f-response.com
pending

Activity



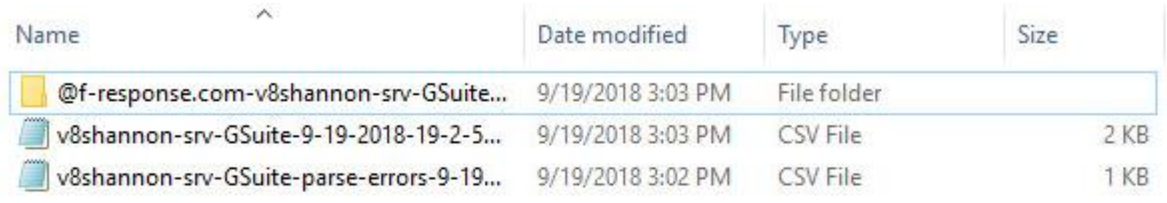
Cloud Collection Activity Details

Name	@f-response.com-v8shannon-srv-GSuite-9-19-201
Target	@f-response.com
State	completed successfully.
Region	Not Applicable.
Destination	J:\mjdtest
Performance	330 KBps
Last Message	
Duration	0000:00:33
Total Bytes	11163130
File Copied	2

Collection Details…

Step 6: Review the collection

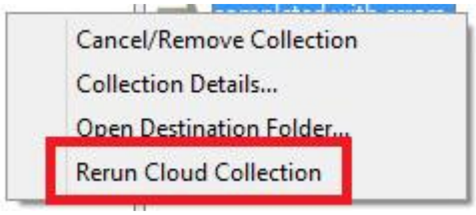
Navigate to the destination folder at the completion of the collection to review the individual files collected along with any log or error reports.



Name	Date modified	Type	Size
@f-response.com-v8shannon-srv-GSuite...	9/19/2018 3:03 PM	File folder	
v8shannon-srv-GSuite-9-19-2018-19-2-5...	9/19/2018 3:03 PM	CSV File	2 KB
v8shannon-srv-GSuite-parse-errors-9-19...	9/19/2018 3:02 PM	CSV File	1 KB

Collected items

Rerunning a collection



If your cloud collection completes with errors, F-Response can be used to rerun the collection and target only those files/folders it was unable to collect. This operation can be performed multiple times until a collection completes successfully. Not all providers offer rerunning options, and not all errors can be reattempted. To rerun a cloud collection, right click on the completed collection in the Activity column and choose **Rerun Cloud Collection**.

Additional Details

Date/Time Values

The following file datetime values are used by F-Response during the collection *(Any missing dates are set to 1601-01-01T00:00:01Z)*:

GOOGLE DRIVE WINDOWS TIME	PROVIDER VALUE
MODIFIED	modifiedTime
ACCESSED	viewedByMeTime
CREATED	createdTime

GOOGLE MAIL WINDOWS TIME	PROVIDER VALUE
MODIFIED	
ACCESSED	

CREATED	Raw Email Datetime

Available Google Log Files (Data provided by Google)

All the log details are here: https://developers.google.com/admin-sdk/reports/reference/rest/v1/activities/list#ApplicationName

`ADMIN` The Admin console application's activity reports return account information about different types of administrator activity events.

`CALENDAR` The Google Calendar application's activity reports return information about various Calendar activity events.

`CHAT` The Chat activity reports return information about various Chat activity events.

`DRIVE` The Google Drive application's activity reports return information about various Google Drive activity events. The Drive activity report is only available for Google Workspace Business and Enterprise customers.

`GCP` The Google Cloud Platform application's activity reports return information about various GCP activity events.

`GPLUS` The Google+ application's activity reports return information about various Google+ activity events.

`GROUPS` The Google Groups application's activity reports return information about various Groups activity events.

`JAMBOARD` The Jamboard activity reports return information about various Jamboard activity events.

`LOGIN` The Login application's activity reports return account information about different types of Login activity events.

`MEET` The Meet Audit activity report return information about different types of Meet Audit activity events.

`MOBILE` The Mobile Audit activity report return information about different types of Mobile Audit activity events.

`RULES` The Rules activity report return information about different types of Rules activity events.

`SAML` The SAML activity report return information about different types of SAML activity events.

`TOKEN` The Token application's activity reports return account information about different types of Token activity events.

`CHROME` The Chrome activity reports return information about unsafe events reported in the context of the WebProtect features of BeyondCorp.