Mission Guide: Google Apps

Your Mission: Use F-Response to collect GSuite account data

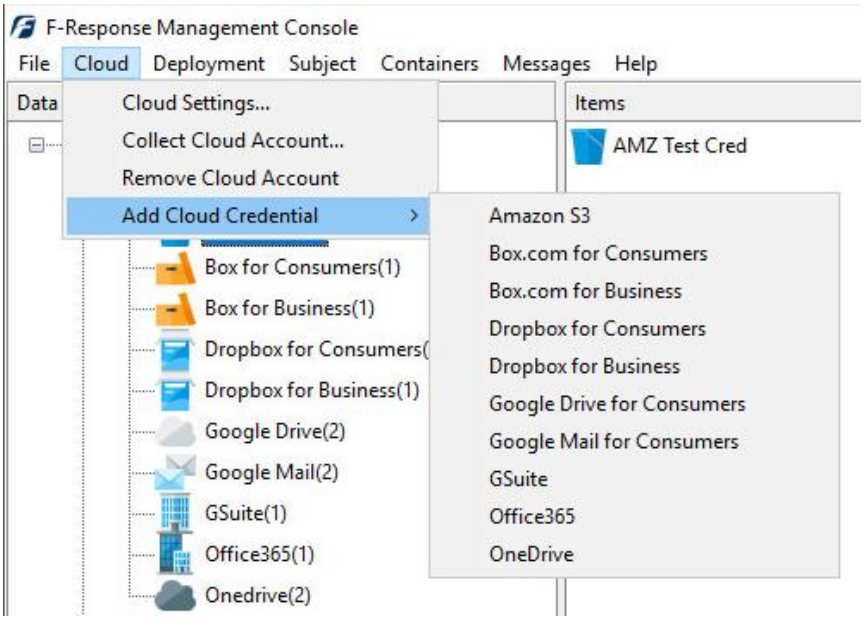
Using F-Response to connect to GSuite custodian accounts and collect their contents

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. This option is only available when collecting to a local directory.

Step 1: Open the GSuite Credential Configuration Window

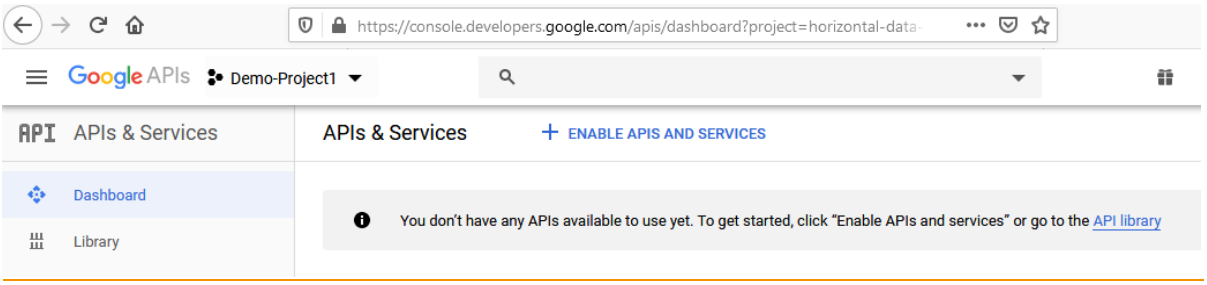
Open the F-Response Management Console and navigate to Providers->Provider Credentials->GSuite, or double click on the appropriate icon in the Data Sources pane.



F-Response Management Console

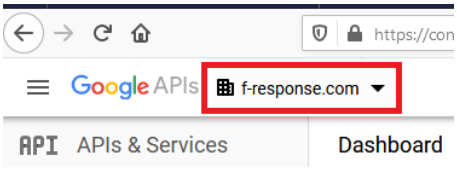
Step 2: Configure a Domain Wide Delegation account for the Google Apps for Business Domain

Before you can access Google Apps for Business Individual Google Drive 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.developers.google.com



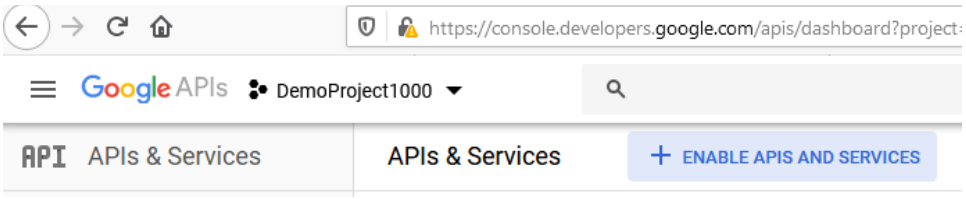
Google APIs Console

Open a web browser and access the Google Console; the first step is to create a project. Select the dropdown next to GoogleAPIs

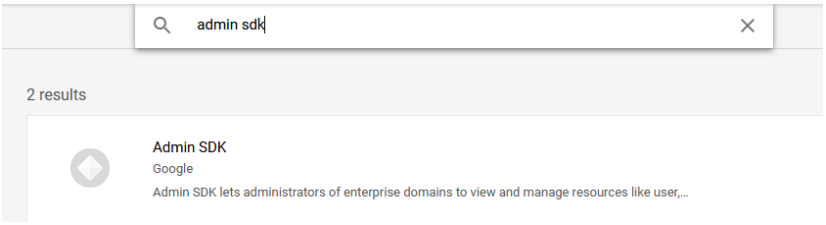


Then select NEW PROJECT, you can leave all the defaults for the project during creation.

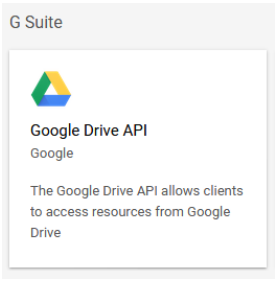
Next you will need to click "ENABLE APIS AND SERVICES" for the project. There are three options to enable here: The Admin SDK, Google Drive API, and the Gmail API.



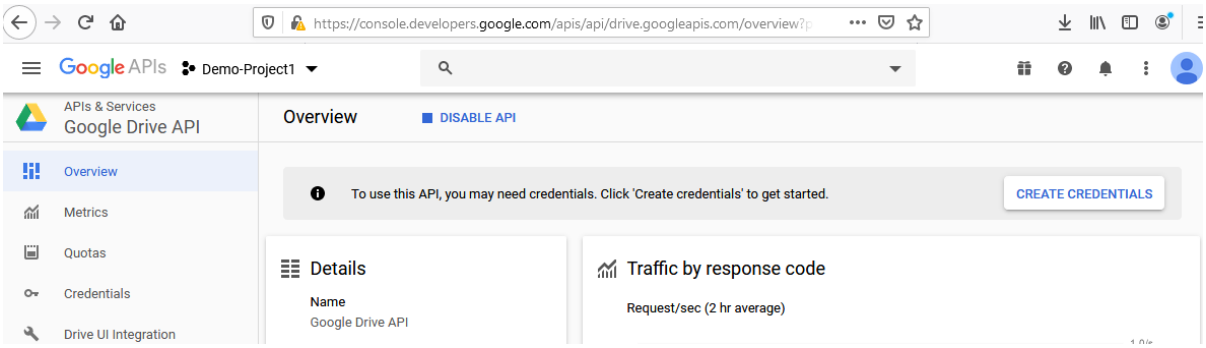
Type Admin SDK in the search box to locate it:



Scroll down to select the Google Drive API and press the Enable API button to activate.

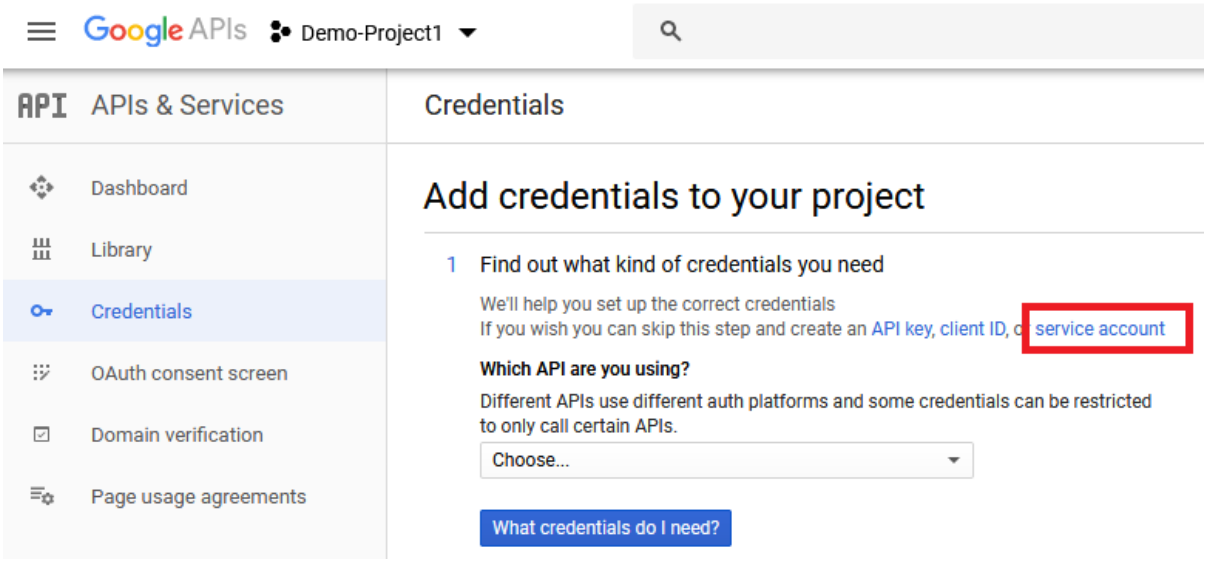


Repeat the same process for the Gmail API.

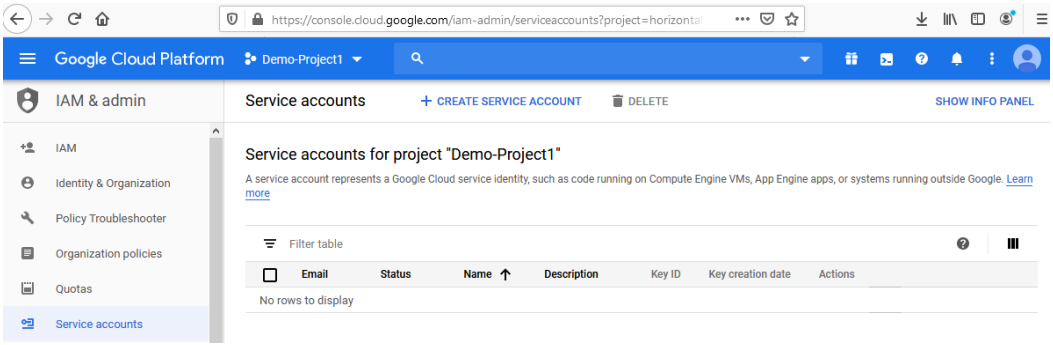


Enabled Google Drive API

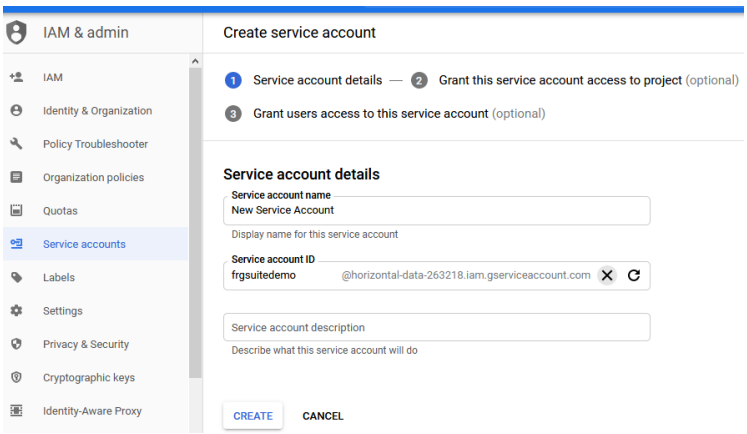
Now you will need to configure a service account.



Select "Create Credentials" and then click the hyperlink for "service account".

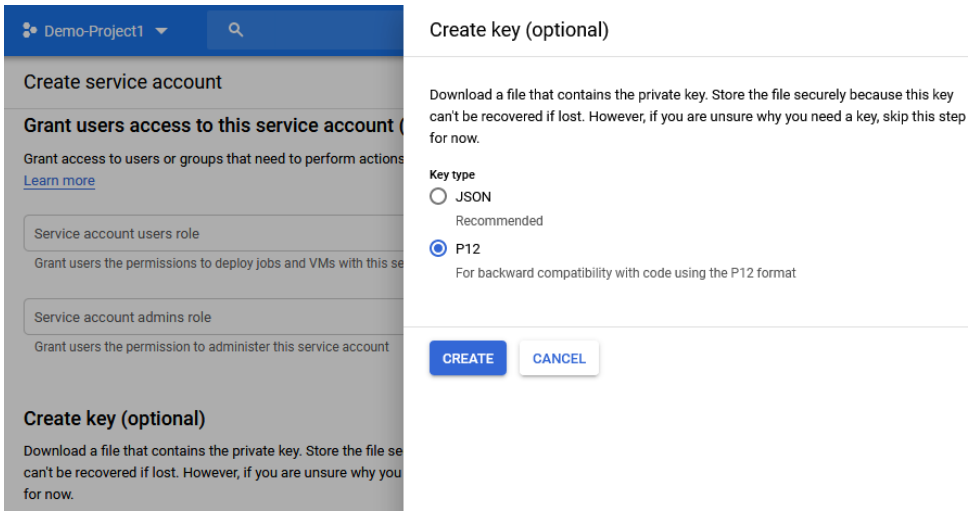


Here you can click on "+ CREATE SERVICE ACCOUNT"



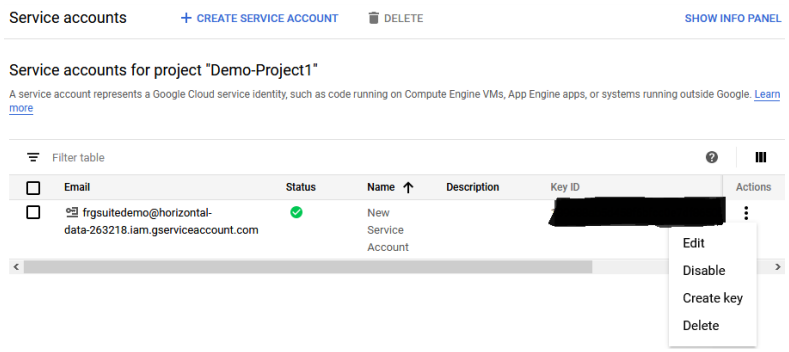
Service Account Creation

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 create and skip step 2 (Grant this service account access to a project). For the third and last step in the process, click create key and select p12 as the Key type.



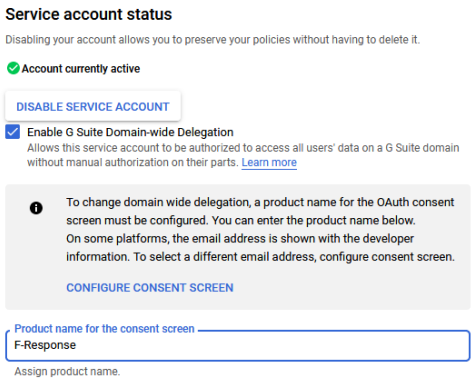
Click CREATE to download the newly generated p12 encryption key file. Save this file as it will be needed later.

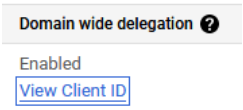
Following the encryption key download click DONE. You should see a newly created Service Account, however at this point your account is not sufficient for accessing Google services. You will need to locate the “Actions” column on the Service Accounts page to edit the Service Account details.



Locate the Service account in the presented list and look for the triple dots on the far-right hand side in the Actions column. Clicking on these dots will give you the option to "Edit" the Service Account.

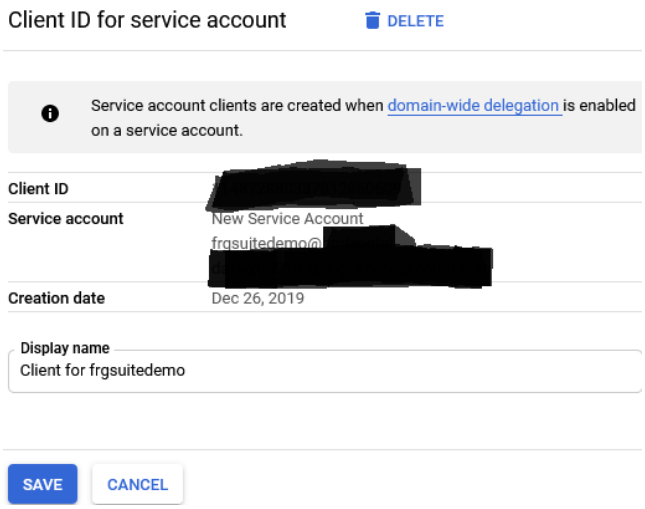
The Edit dialog that appears should present the option to "Enable G Suite Domain-wide Delegation", press this check box and Save.





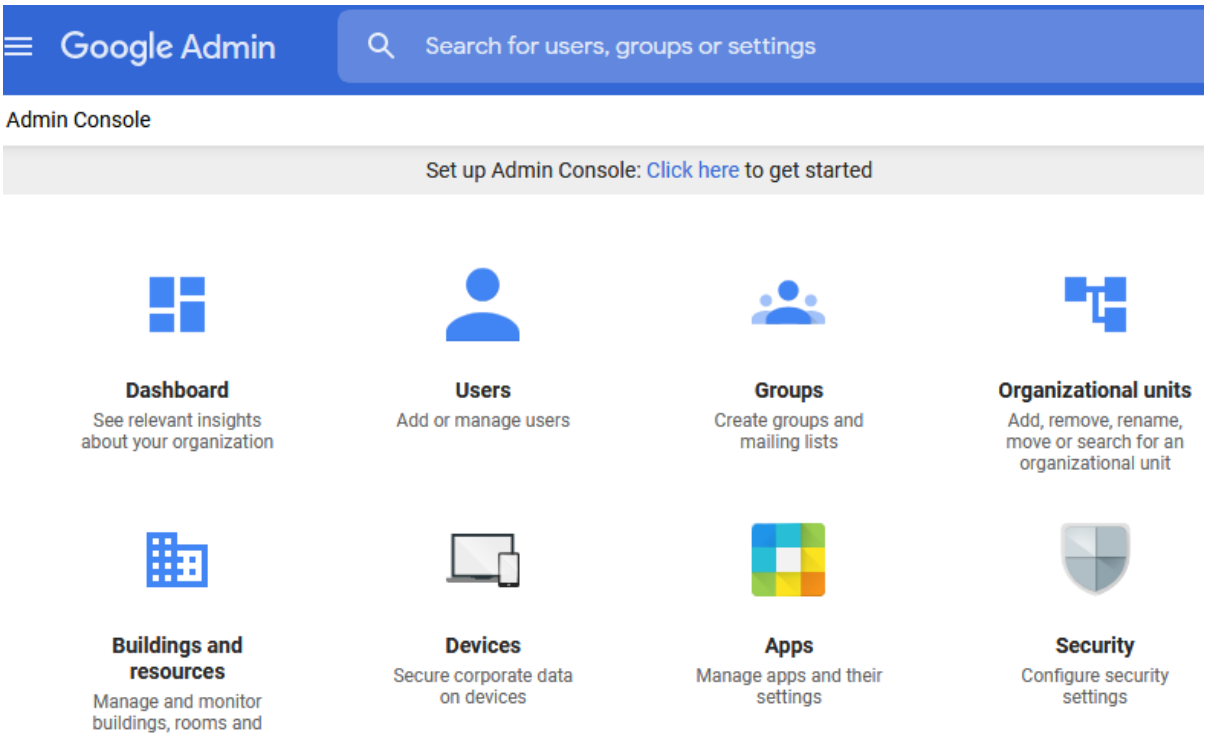
After you have enabled Domain-Wide Delegation scroll over to the new Domain-Wide Delegations column, where you can click on "View Client ID" to record the client ID for the next step.

This popup will give you everything you need to complete access so please take note. It will contain the Client ID necessary to enable Security in the following section, and it will give you the Service account email address, which is needed in the F-Response Credentials Dialog.



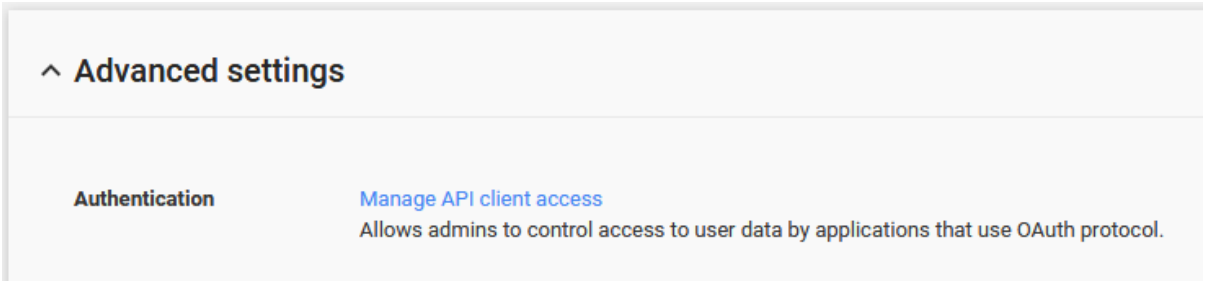
Client ID and Service Account

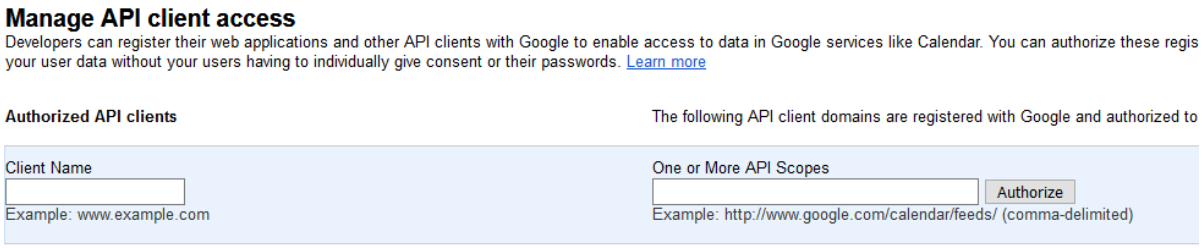
Now that we have created a service account and enabled Google Drive access we must give that service account access to the domain. We do this by logging in with the super administrator account in the Google Admin Console -> https://admin.google.com/



Google Admin Console

The Admin console provides options for administering the Google Apps for Business Domain. Under Security you will need to press "Advanced Settings" and click on the "Manage API Client Access" in the panel.





Under Manage API Access you will want to paste the Client ID that was recorded earlier into the Client Name 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

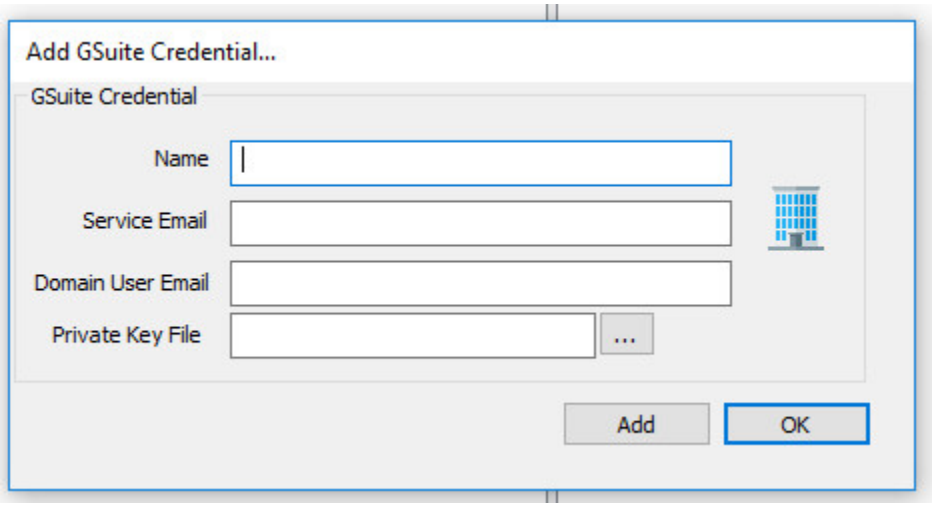
https://www.googleapis.com/auth/admin.reports.usage.readonly

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

Press Authorize to complete the delegated account permissions.

Step 3: Provide the newly obtained Google Drive for Business Credentials

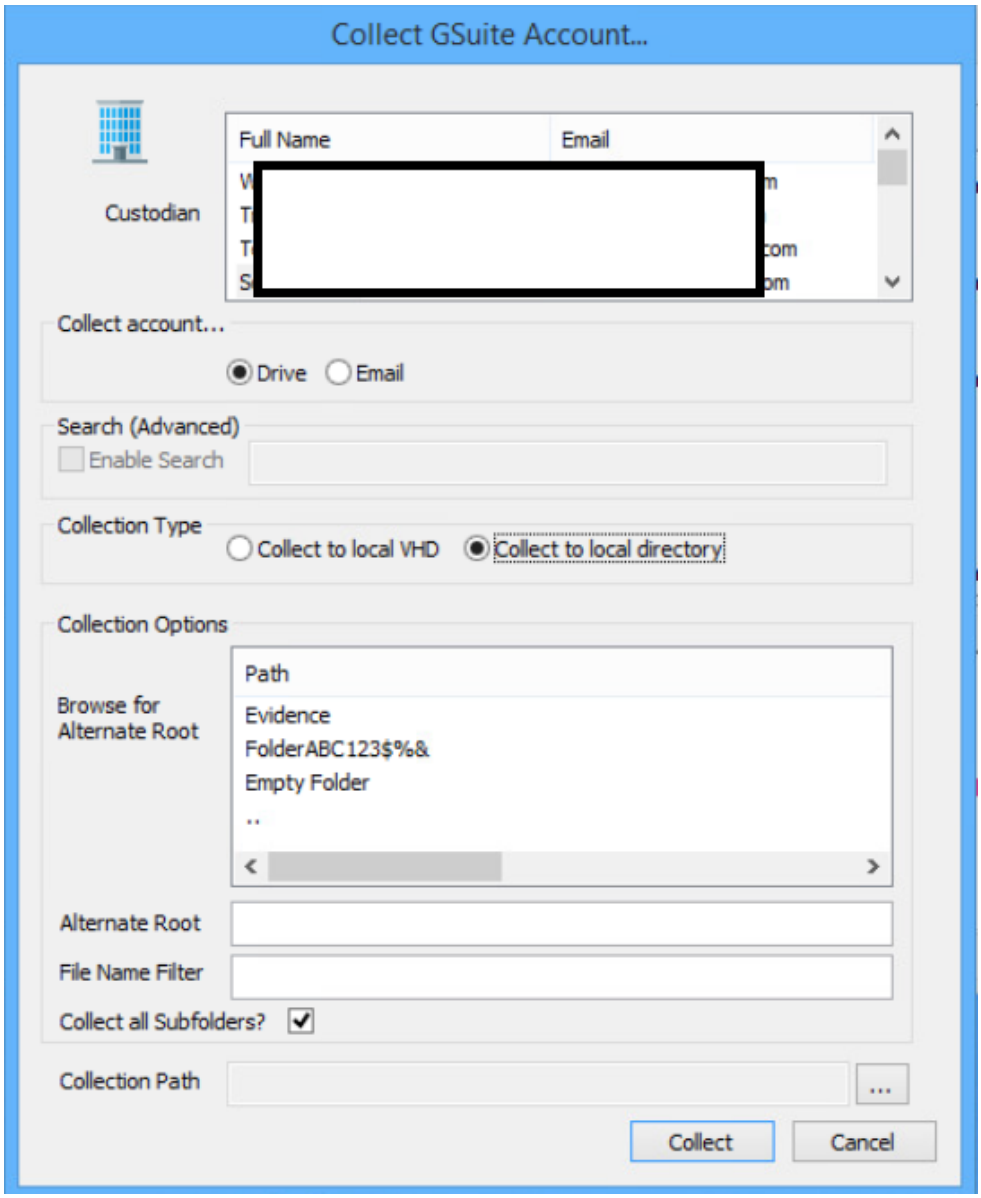
To configure Google Drive for Business access you will need the Service Email recorded earlier, the Super Admin Email Address (Domain User Email field), and the Private Key file downloaded earlier.



Configure GSuite Credentials

Step 4: Start a collection

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



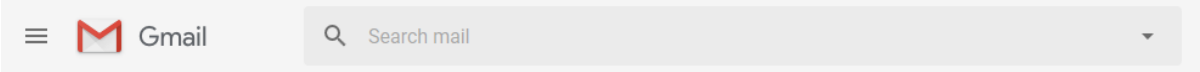
Starting a new collection…

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

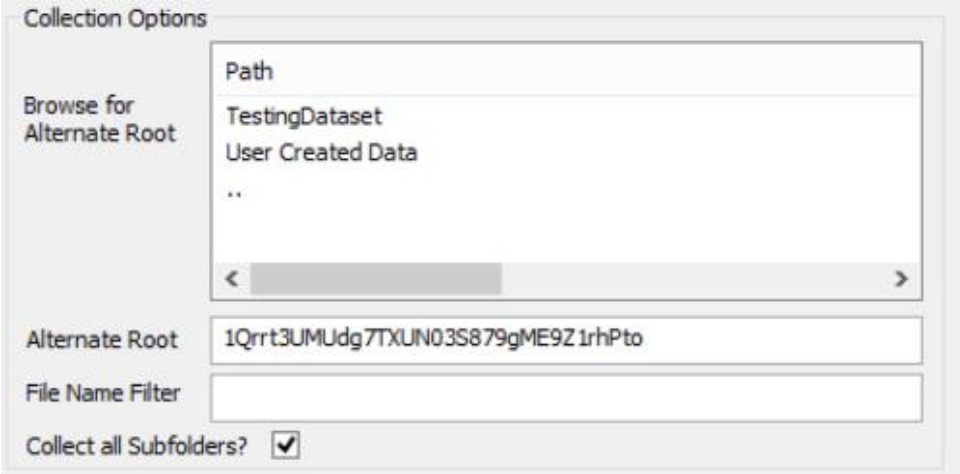
Use the optional **Search (Advanced)** feature to apply the same search mechanisms available in the Gmail web interface to your potential collection. This in an optional feature and may also be ignored to attempt a collection of the entire Google Mail account.



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:



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.

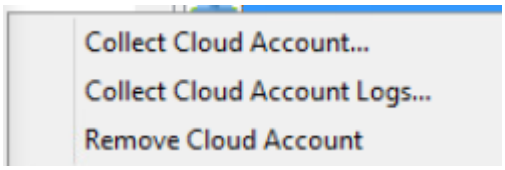
File Name Filter: Will check the string entered here against files as presented by the provider. There is no need to enter wildcards (*.*) and it does not use regular expressions. For example, to collect only Excel files in the account, just type **.xls** in the box.

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

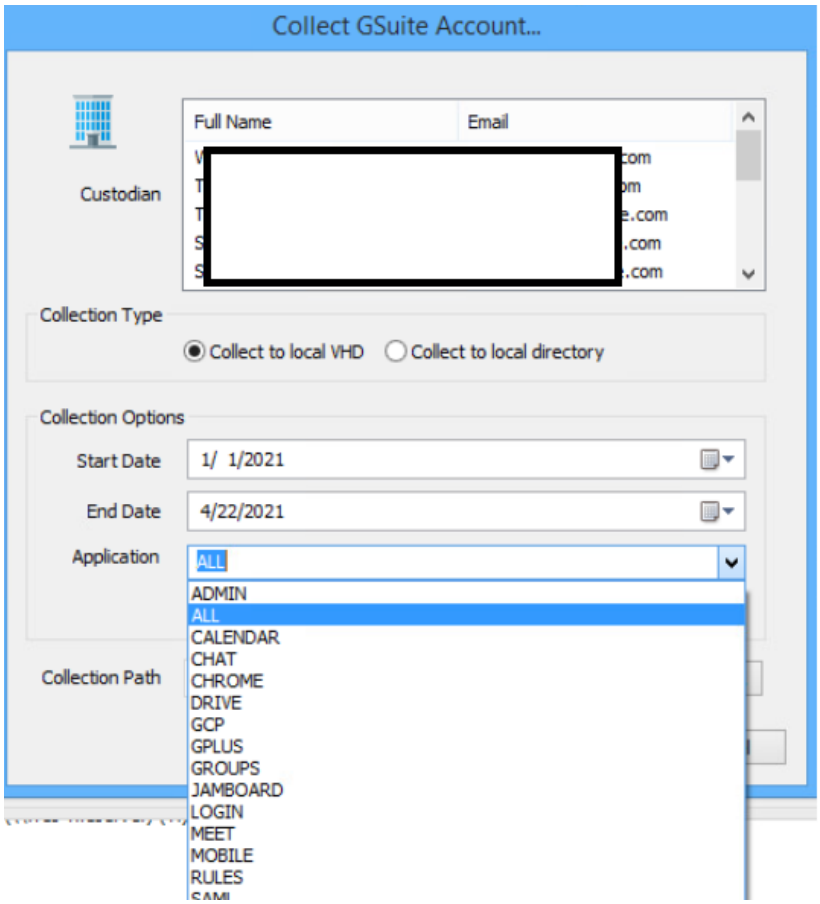
Step 4a (optional): Collect Google Log Information

F-Response has added GSuite 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:



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.

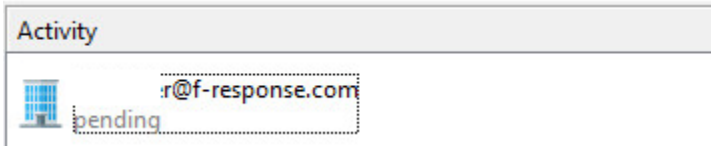
Under **Collection Type** select the option to collect into a **VHD container** or a **local directory** on your examiner computer.

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.

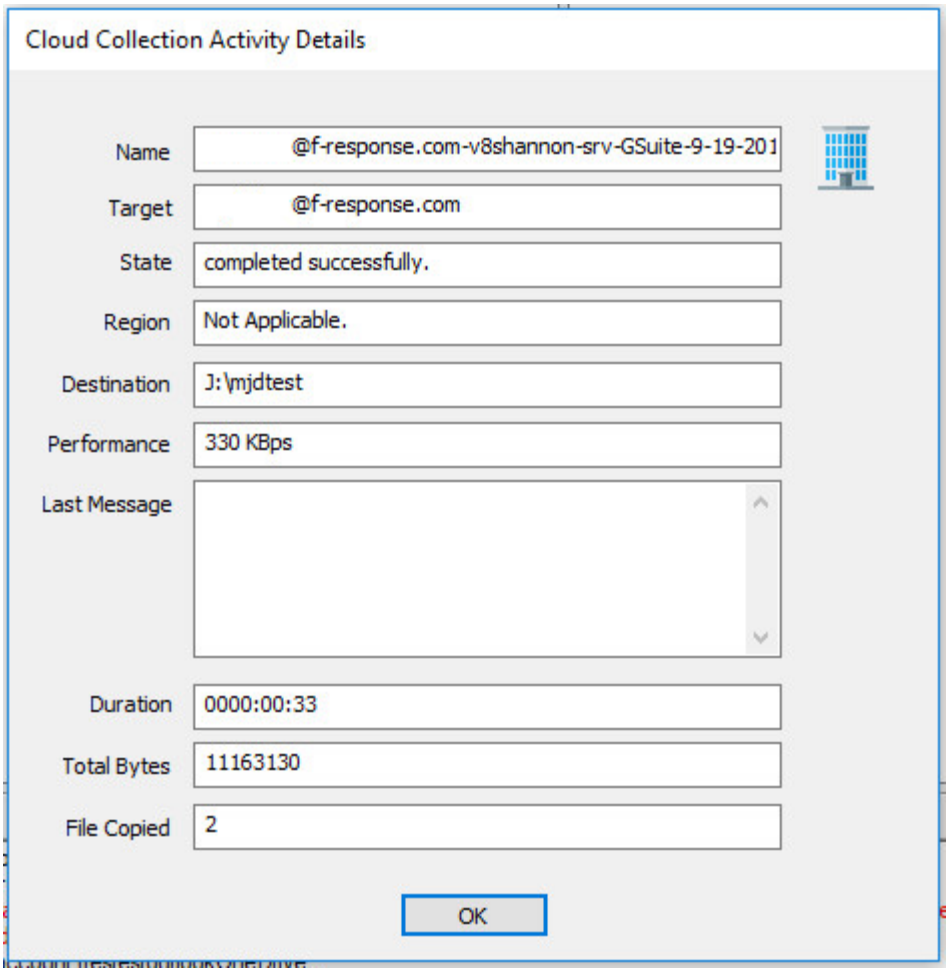
Lastly, enter a location to save the data in the **Collection Path**, and click the Collect button.

Step 5: Check the Activity Pane

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



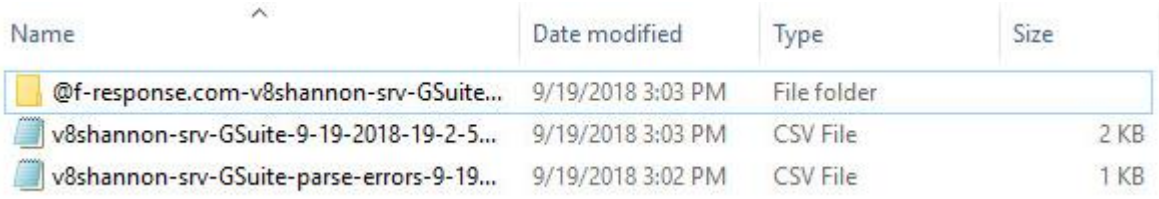
Activity



Collection Details…

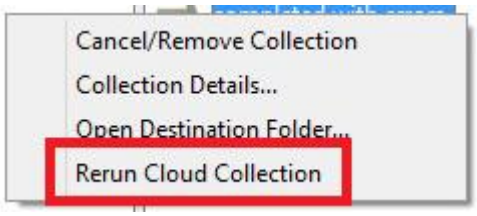
Step 6: Review the collection

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



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**.

***Note**: Rerunning a collection is only available when collecting to a local directory, this not an option when collecting in VHD format.

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.