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

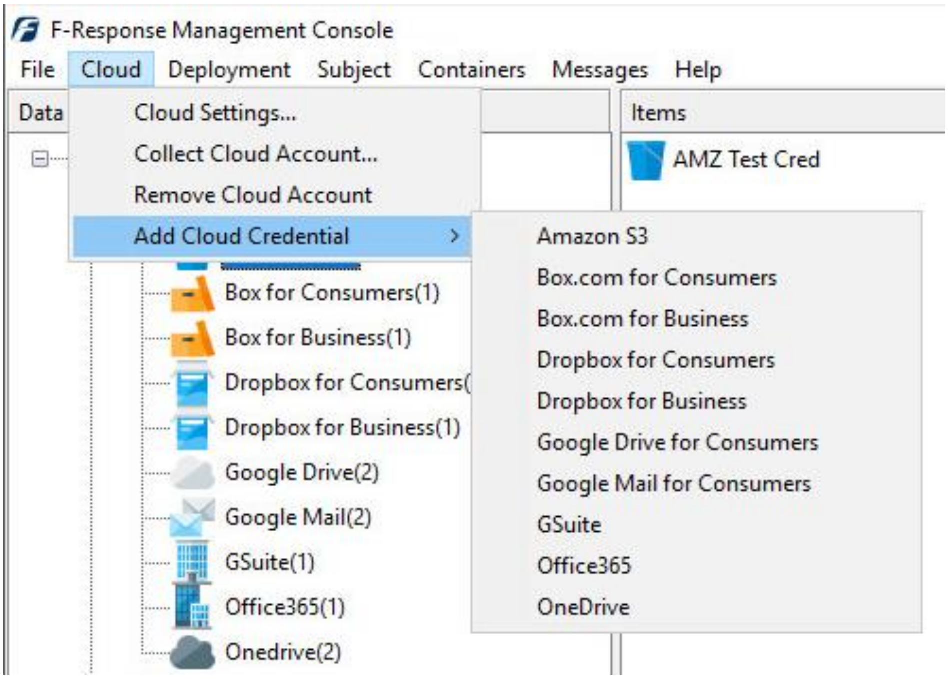
Important Note

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.

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.

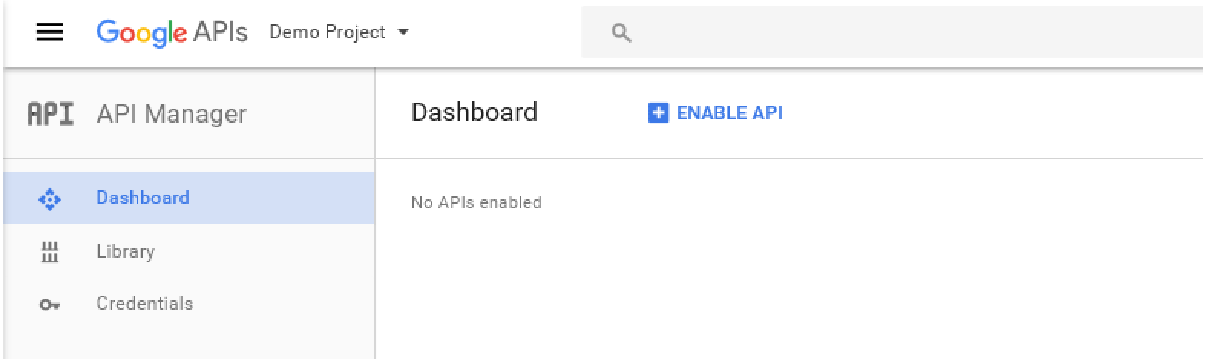


F-Response Management Console

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

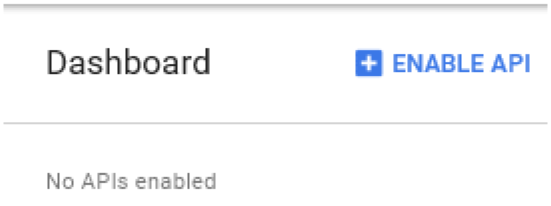
Before you can access Google Apps for Business Individual Google Drive accounts you must use the Google Developers Console to configure a Domain Wide Delegation account. The Developers Console is the latest refresh of what was the Google APIs console. This new console is located at:

Cloud Console -> https://console.developers.google.com



No APIs enabled

Google APIs Console



No APIs enabled

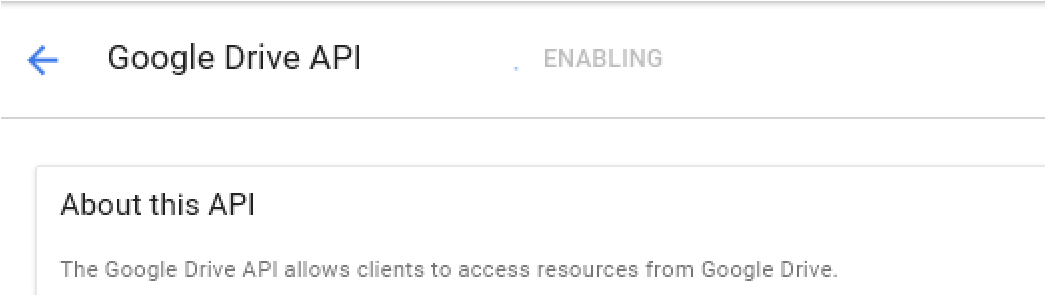
Enable API Button

Open a web browser and access the Google Cloud Console, you will need to login as the Administrative user of the Apps domain when prompted.

The first step is to create a project.

You can leave all the defaults for the project during creation. Next you will need to click “ENABLE API”.

Select the Drive API and press the Enable API link.



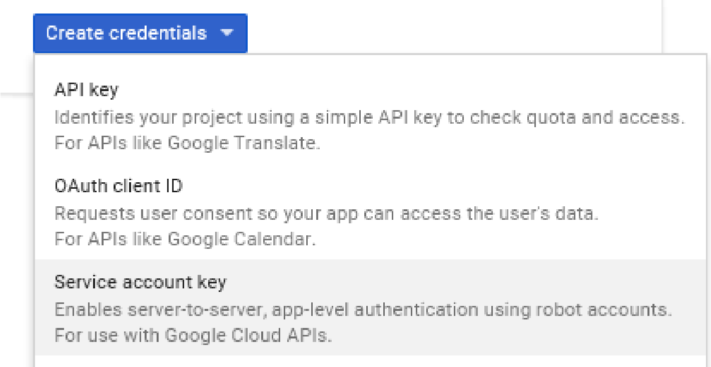
Google Drive API

About this API

The Google Drive API allows clients to access resources from Google Drive.

Enable Google Drive API

Next you'll need to select the Credentials option to generate a new Service Account. Select "Create Credentials" and then in the following pop-up select "Service account key".

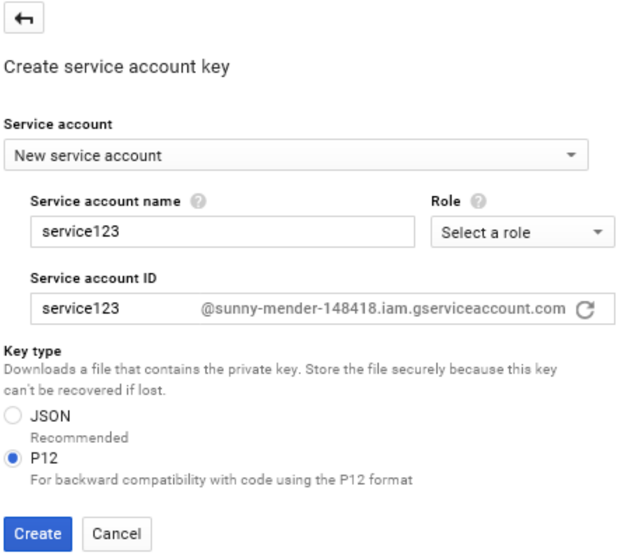


API key
Identifies your project using a simple API key to check quota and access.
For APIs like Google Translate.

OAuth client ID
Requests user consent so your app can access the user's data.
For APIs like Google Calendar.

Service account key
Enables server-to-server, app-level authentication using robot accounts.
For use with Google Cloud APIs.

Service account key



Create service account key

Service account: New service account

Service account name: service123

Role: Select a role

Service account ID: service123 @sunny-mender-148418.iam.gserviceaccount.com

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

○ JSON
Recommended

● P12
For backward compatibility with code using the P12 format

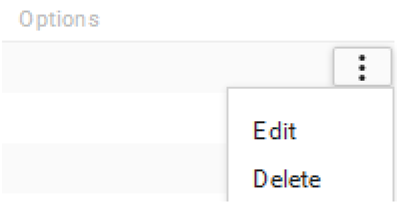
Service Account Creation

This will bring you to a dialog for creating the service account. Use “New service account” in the “Service Account” drop down, provide a name in the name field, this is purely for identification. Lastly be sure to select p12 as the Key type.

This will pop up a download for the newly generated p12 encryption key file. Save this file as it will be needed later.

Following the encryption key download 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 “Manage service accounts” link on the Credentials page and click it to edit the Service Account details.

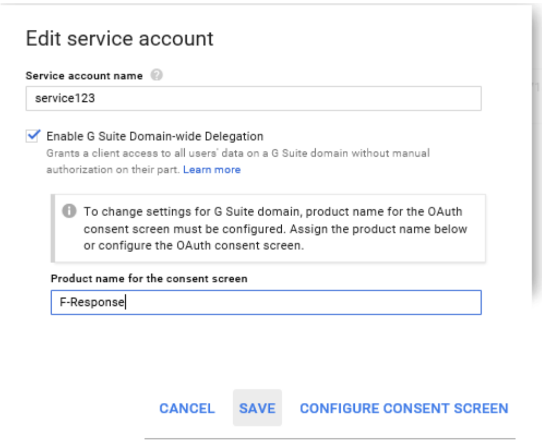
Locate the Service account in the presented list and look for the triple dots on the far right hand side. Clicking on these dots will give you the option to “Edit” the Service Account.



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

You may be asked about a consent screen, it appears you may input anything in this box.

In addition, you may be prompted that your service account has no role, you may select “Create without role” to continue.


Edit service account

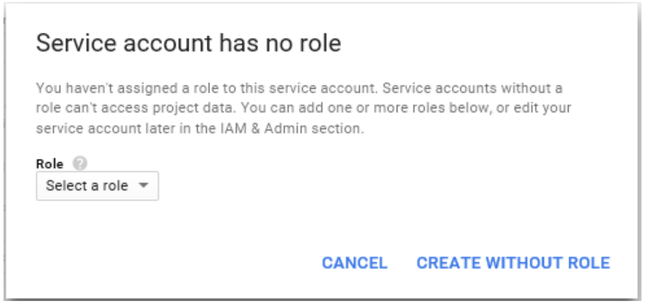
Service account name: service123

☑ Enable G Suite Domain-wide Delegation

Grants a client access to all users' data on a G Suite domain without manual authorization on their part. Learn more

To change settings for G Suite domain, product name for the OAuth consent screen must be configured. Assign the product name below or configure the OAuth consent screen.

Product name for the consent screen: F-Response

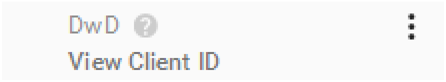

Service account has no role

You haven't assigned a role to this service account. Service accounts without a role can't access project data. You can add one or more roles below, or edit your service account later in the IAM & Admin section.

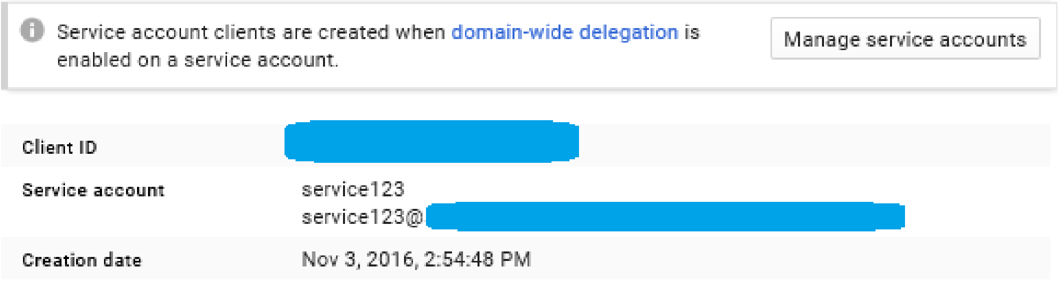
Role: Select a role

After you have enabled Domain-Wide Delegation you will see new options available under the Options column, including “View Client ID”. Click on View Client ID to get the client ID for the next step.

This popup will give you everything you need to complete access. 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 need in the F-Response Credentials Dialog.



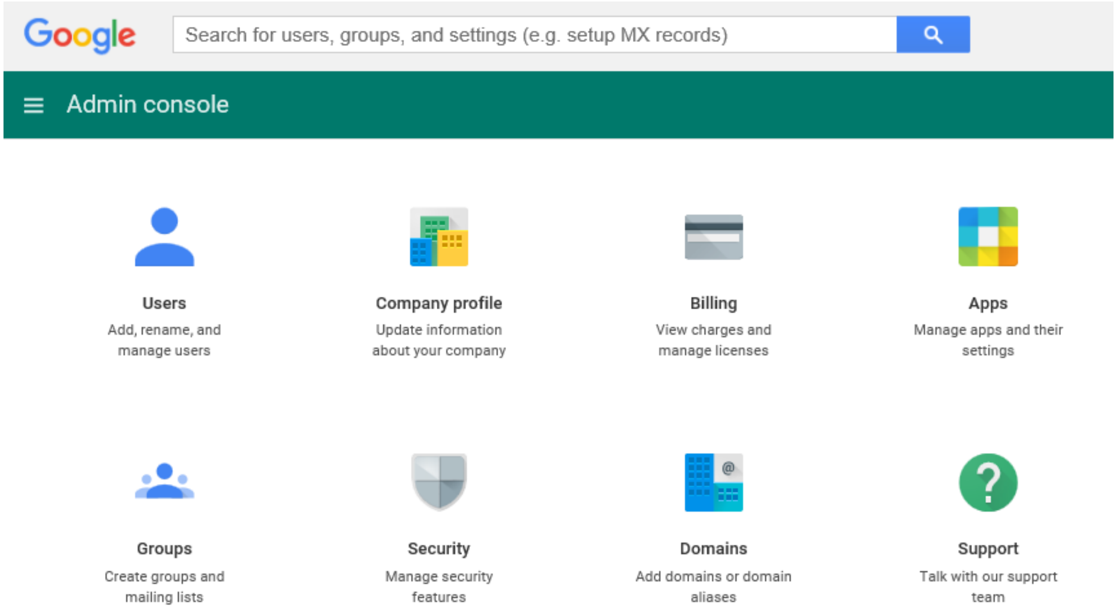
Service account clients are created when domain-wide delegation is enabled on a service account.

Client ID	[redacted]
Service account	service123 service123@[redacted]
Creation date	Nov 3, 2016, 2:54:48 PM

Client ID and Service Account

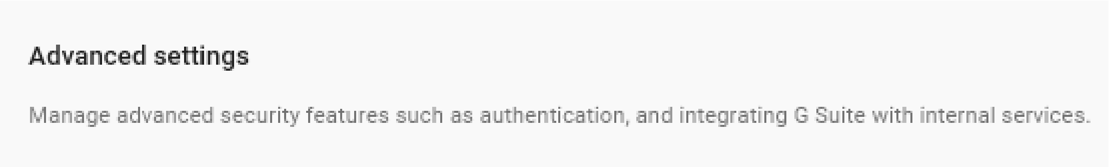
Now that we have created a service account and enabled Google Drive access we must give that service account access to the domain. We do this by logging in with an administrator account to the Google Admin Console.

Admin Console -> https://admin.google.com/


Google
Search for users, groups, and settings (e.g. setup MX records)
Admin console
Users
Add, rename, and manage users
Company profile
Update information about your company
Billing
View charges and manage licenses
Apps
Manage apps and their settings
Groups
Create groups and mailing lists
Security
Manage security features
Domains
Add domains or domain aliases
Support
Talk with our support team

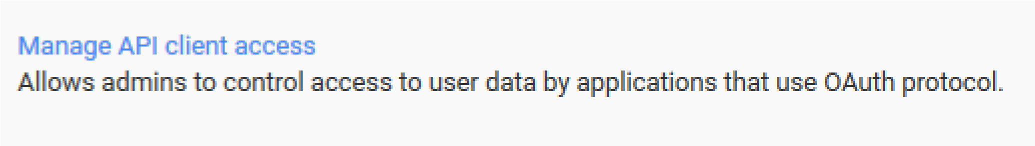
Google Admin Console

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



Advanced settings

Manage advanced security features such as authentication, and integrating G Suite with internal services.



Manage API client access

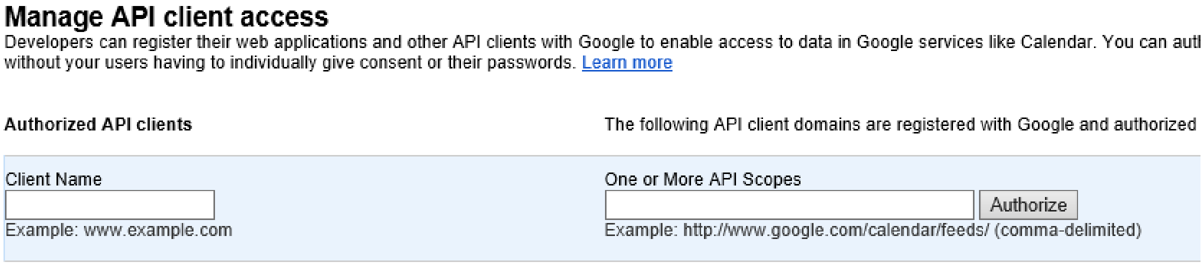
Allows admins to control access to user data by applications that use OAuth protocol.

Under Manage API Access you will want to paste in the Client ID included in the output that was shown earlier, 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



Manage API client access

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

Authorized API clients

The following API client domains are registered with Google and authorized

Client Name

Example: www.example.com

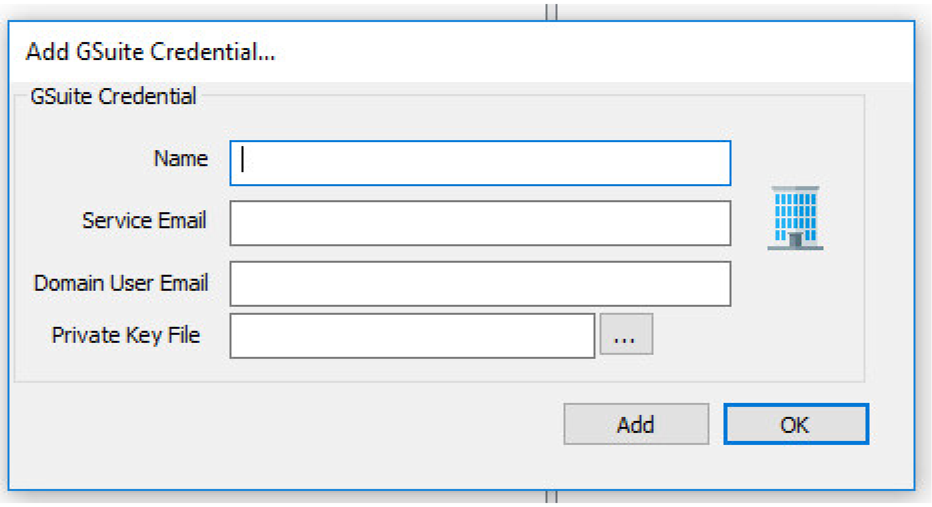
One or More API Scopes

Example: http://www.google.com/calendar/feeds/ (comma-delimited)

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, a Domain Admin Email Address, and the Private Key file downloaded earlier.


Add GSuite Credential...

GSuite Credential

Name

Service Email

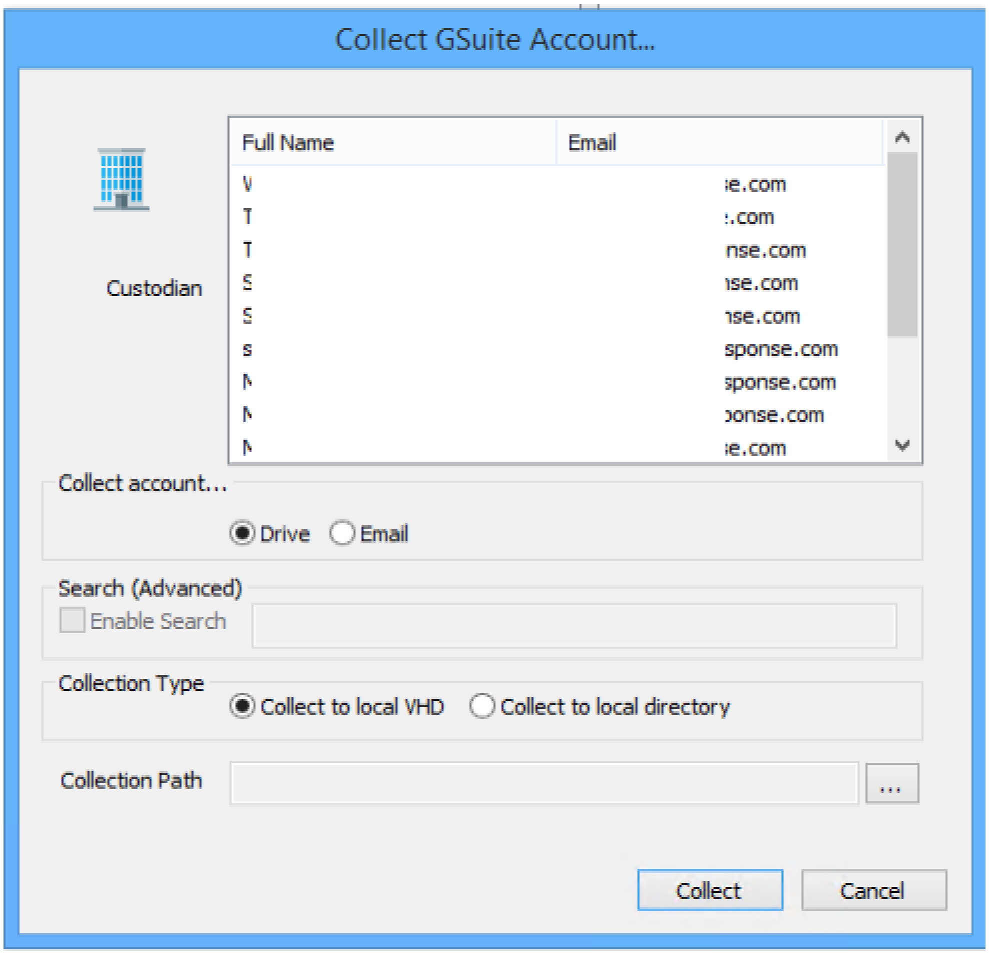
Domain User Email

Private Key File

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.



Collect GSuite Account...

Custodian

Full Name	Email
V	;e.com
T	:.com
T	nse.com
S	ıse.com
S	ıse.com
s	sponse.com
N	sponse.com
N	ɔonse.com
N	;e.com

Collect account...

● Drive ○ Email

Search (Advanced)

□ Enable Search

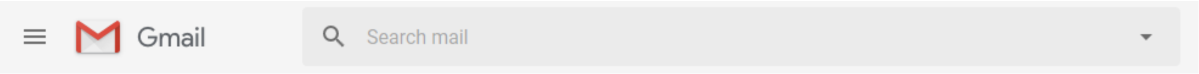
Collection Type

● Collect to local VHD ○ Collect to local directory

Collection Path

Starting a new collection…

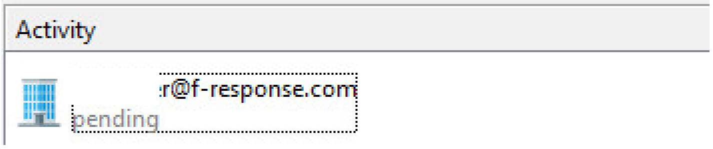
Use the optional Search feature to apply the same search mechanisms available in the Gmail web interface to your potential collection. This in an optional feature and may also be ignored to attempt a collection of the entire Google Mail account.



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

Step 4: Check the Activity Pane

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

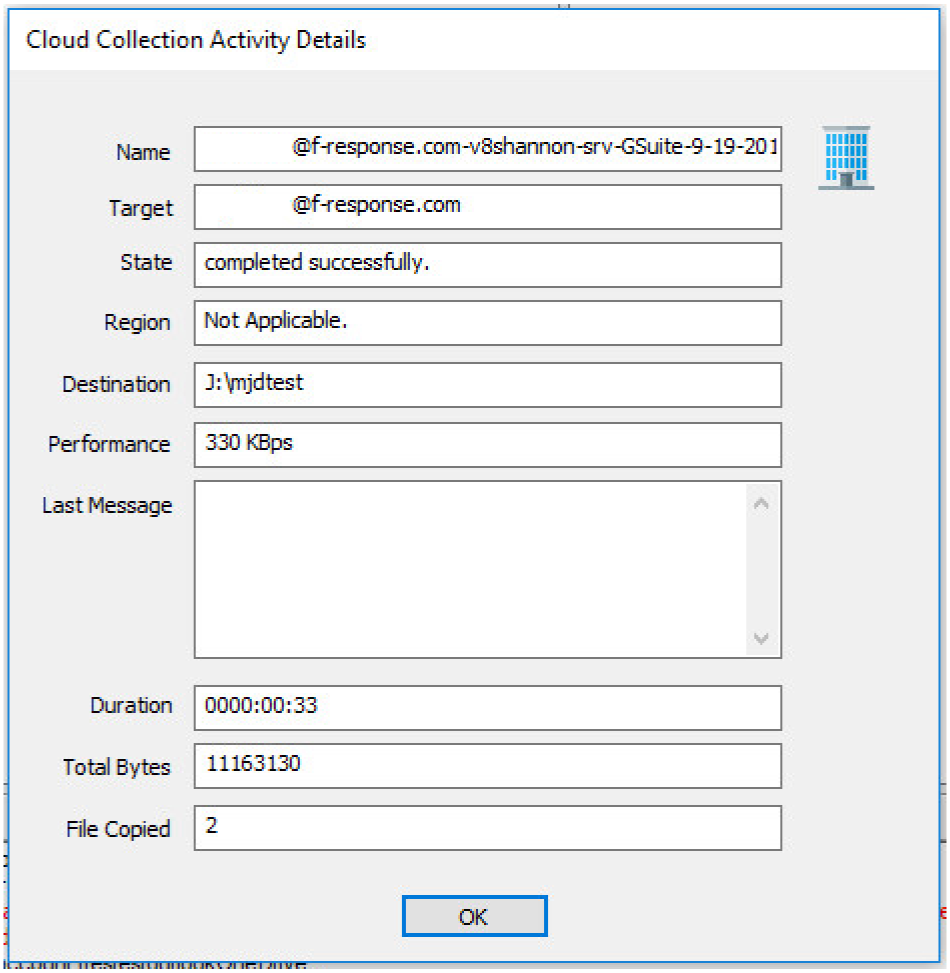


Activity

r@f-response.com

pending

Activity



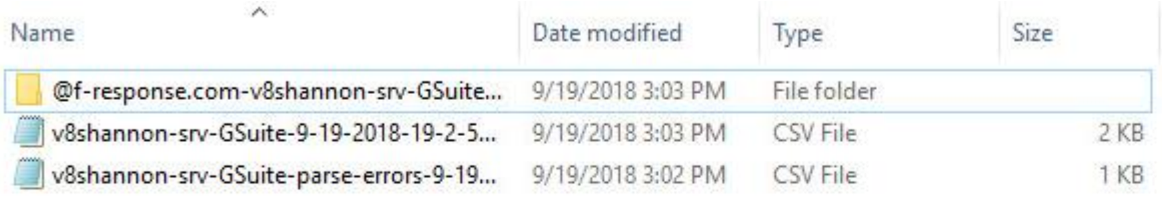
Cloud Collection Activity Details

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 5: 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.



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

Additional Details

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

Troubleshooting