Mission Guide: Google Apps

Your Mission: Use F-Response to access Google Drive Apps for Business (G Suite)

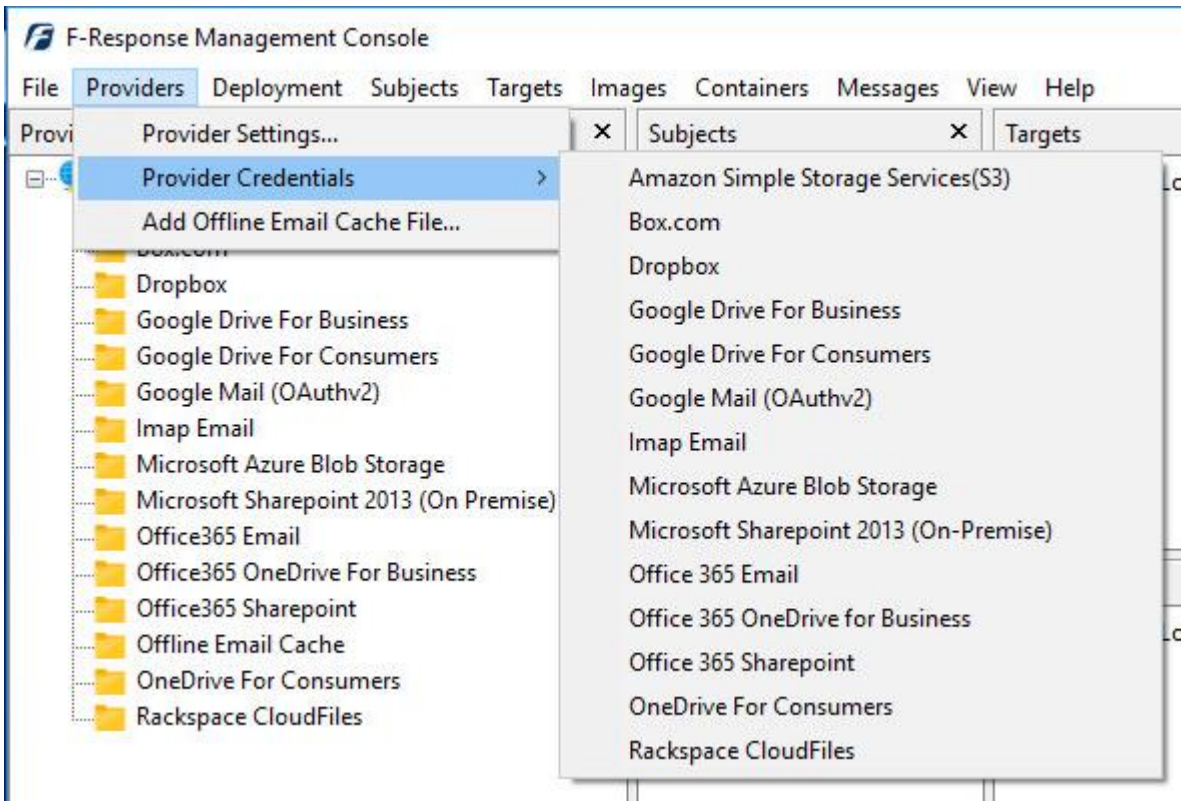
Using F-Response to connect to Google Drive Apps for Business and collect their contents

Important Note

Disclaimer: The F-Response Connector and legacy Connector products (F-Response Email Connector, Cloud Connector, and Database Object Connector) provide 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.

Step 1: Open the Google Drive for Business Credential Configuration Window

Open the F-Response Management Console and navigate to the Providers->Provider Credentials->Google Drive for Business menu item.

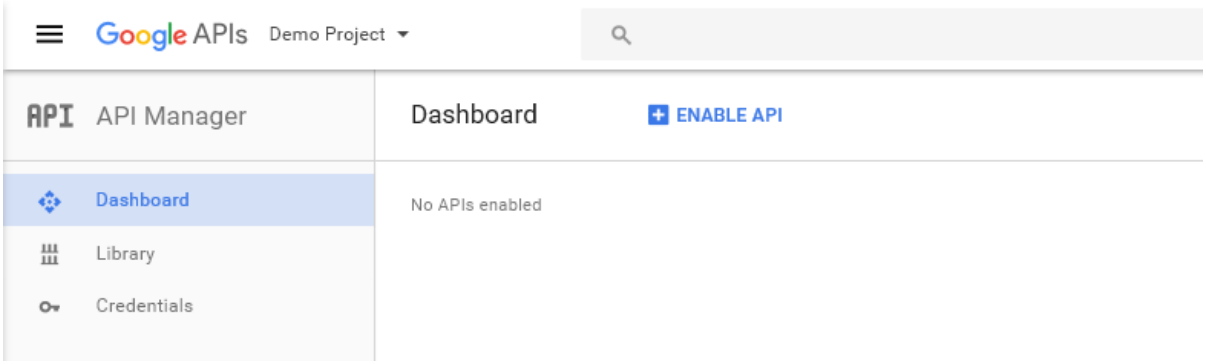


F-Response Management Console

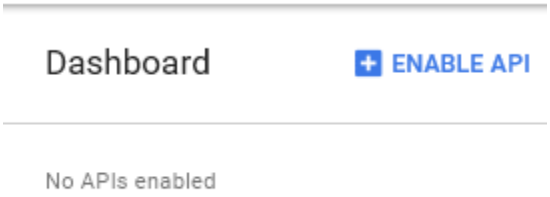
Step 2: Configure a Domain Wide Delegation account for the Google Apps for Business Domain

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



Google APIs Console



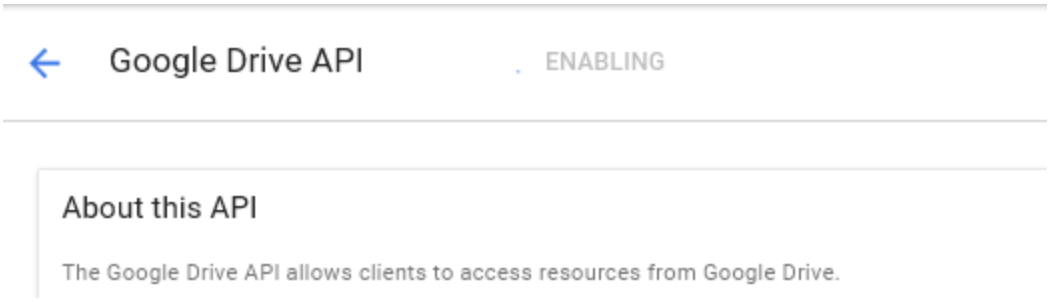
Enable API Button

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.

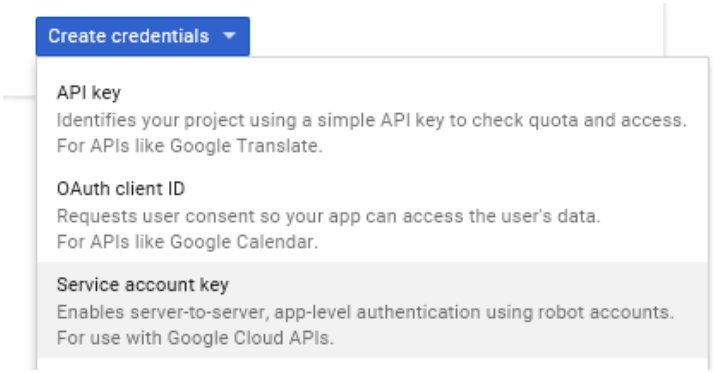
You can leave all the defaults for the project during creation. Next you will need to click "ENABLE API".

Select the Drive API and press the Enable API link.

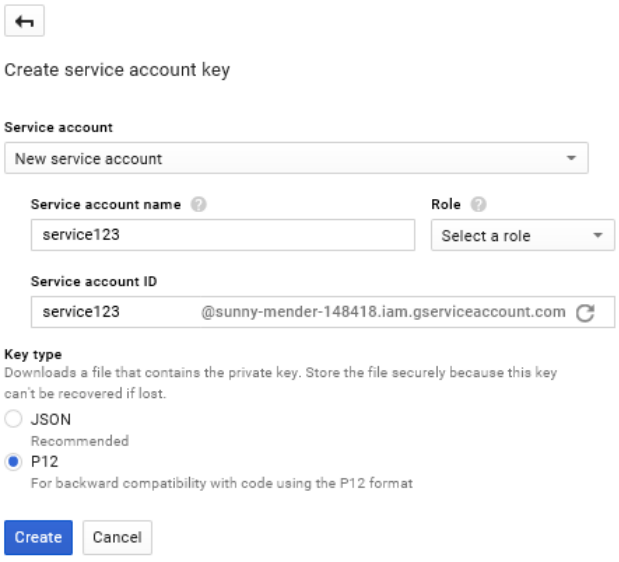


Enable Google Drive API

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".



Service account key



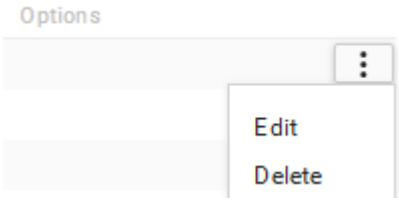
Service Account Creation

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.

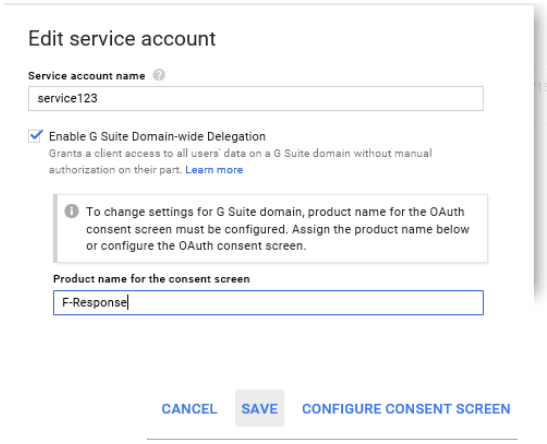
Locate the Service account in the presented list and look for the triple dots on the far right hand side. Clicking on these dots will give you the option to "Edit" the Service Account.

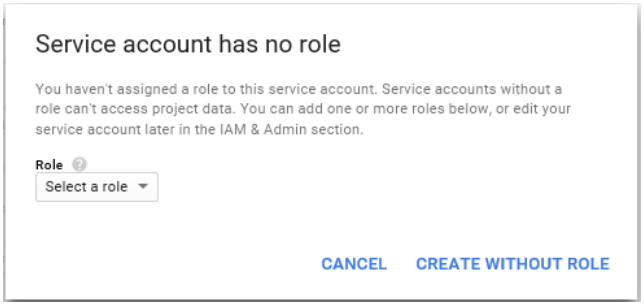


The Edit dialog that appears should present the option to "Enable G Suite Domain-wide Delegation", press this check box and Save.

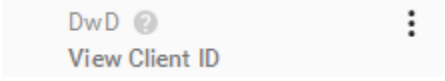
You may be asked about a consent screen, it appears you may input anything in this box.

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



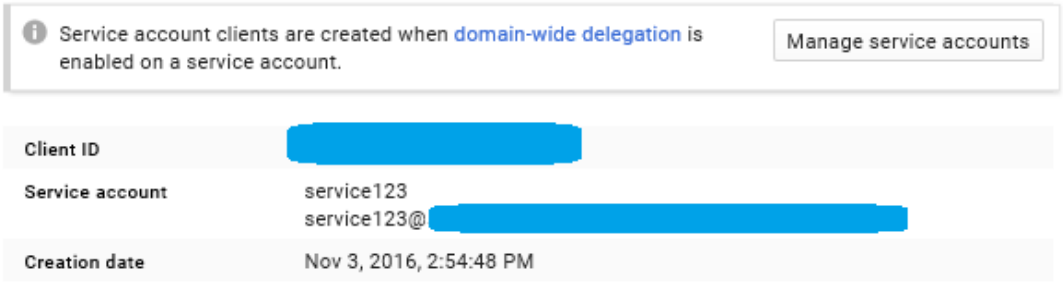


After you have enabled Domain-Wide Delegation you will see new options available under the Options column, including "View Client ID". Click on View Client ID to get the client ID for the next step.



This popup will give you everything you need to complete access. It will contain the Client ID necessary to enable

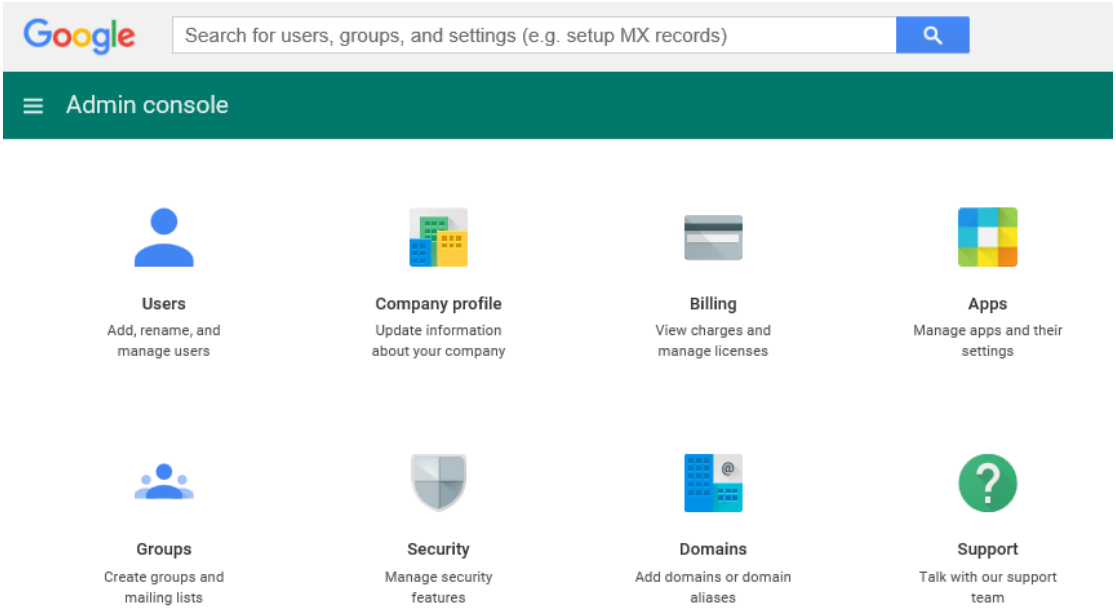
Security in the following section, and it will give you the Service account email address, which is need in the F-Response Credentials Dialog.



Client ID and Service Account

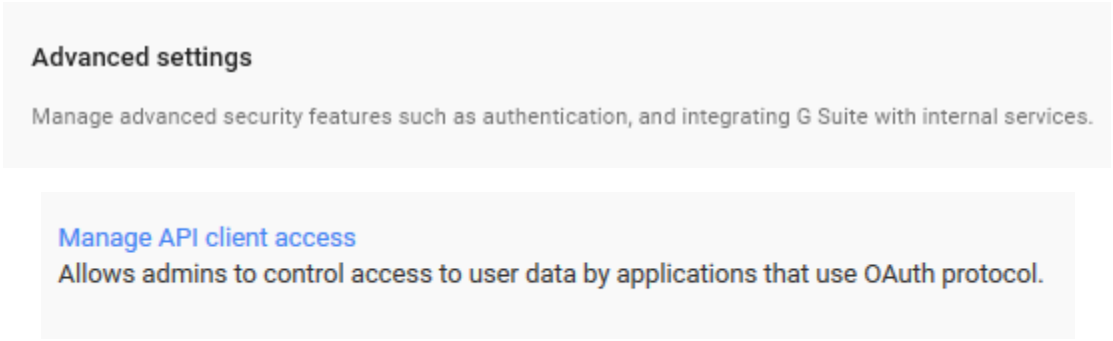
Now that we have created a service account and enabled Google Drive access we must give that service account access to the domain. We do this by logging in with an administrator account to the Google Admin Console.

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



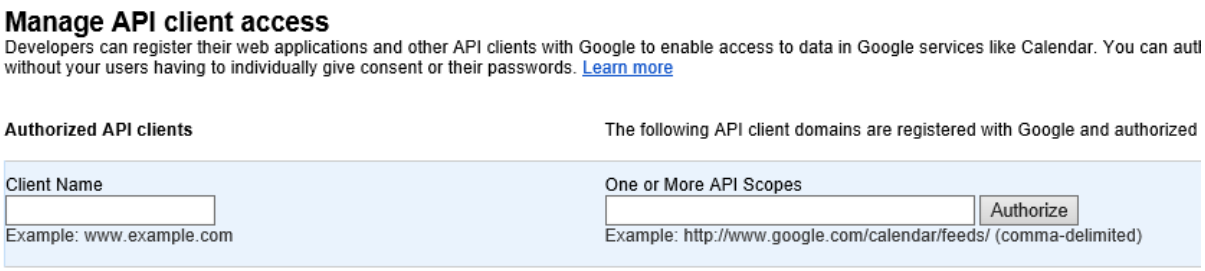
Google Admin Console

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.



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.

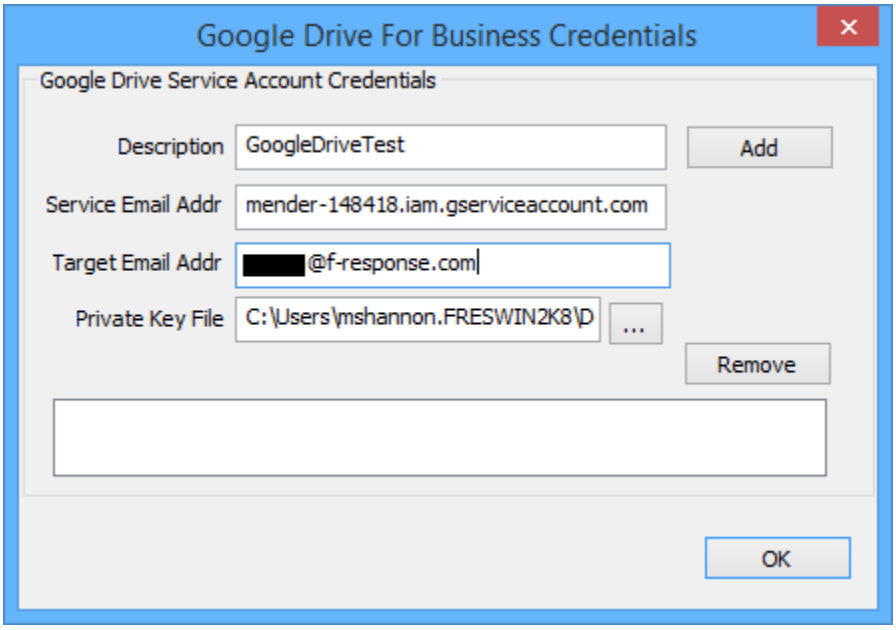
API Scope -> https://www.googleapis.com/auth/drive.readonly



Press Authorize to complete the delegated account permissions.

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

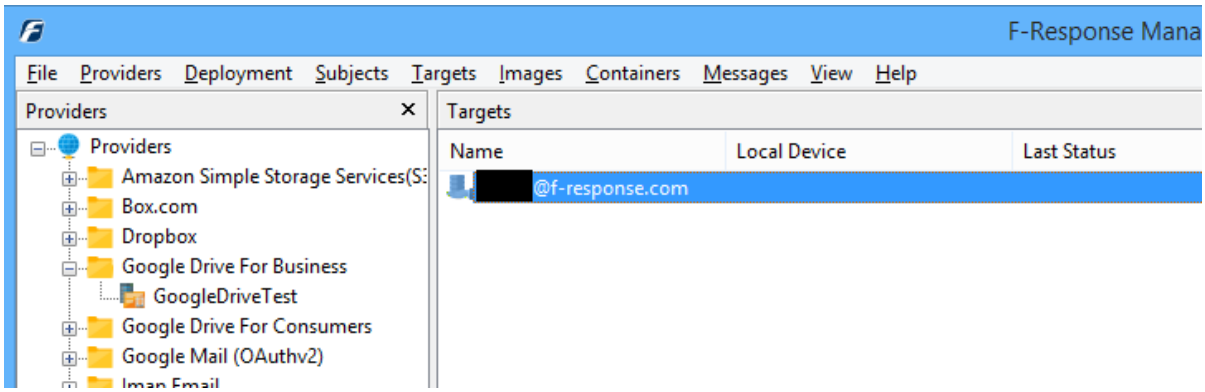
To configure Google Drive for Business access you will need the Service Email Address, the Target User Email Address, and the Private Key file downloaded earlier.



Configure Google Drive for Business Credentials

Step 3: Scan and Enumerate Google Drive for Business Targets

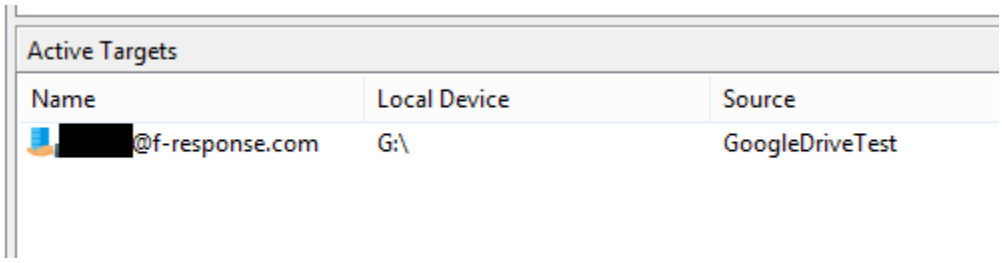
Double click on the newly added Google Drive account under the Providers tree. This will scan the provider and result in a listing of available targets in the Targets window.



Listing Targets

Step 4: Login and Mount one or more Google Drive for Business Targets

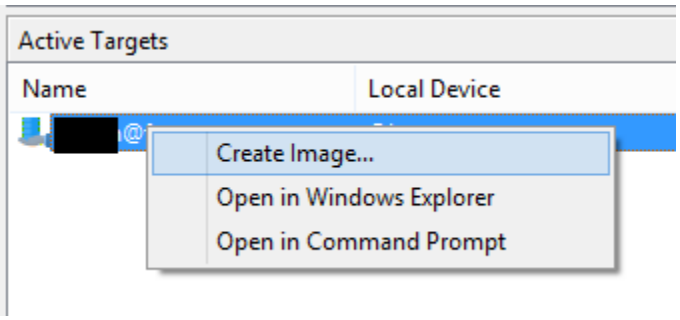
Double click on an individual target in the Targets window to begin the mounting process. Once attached the share will present a drive letter.



Attached Volume

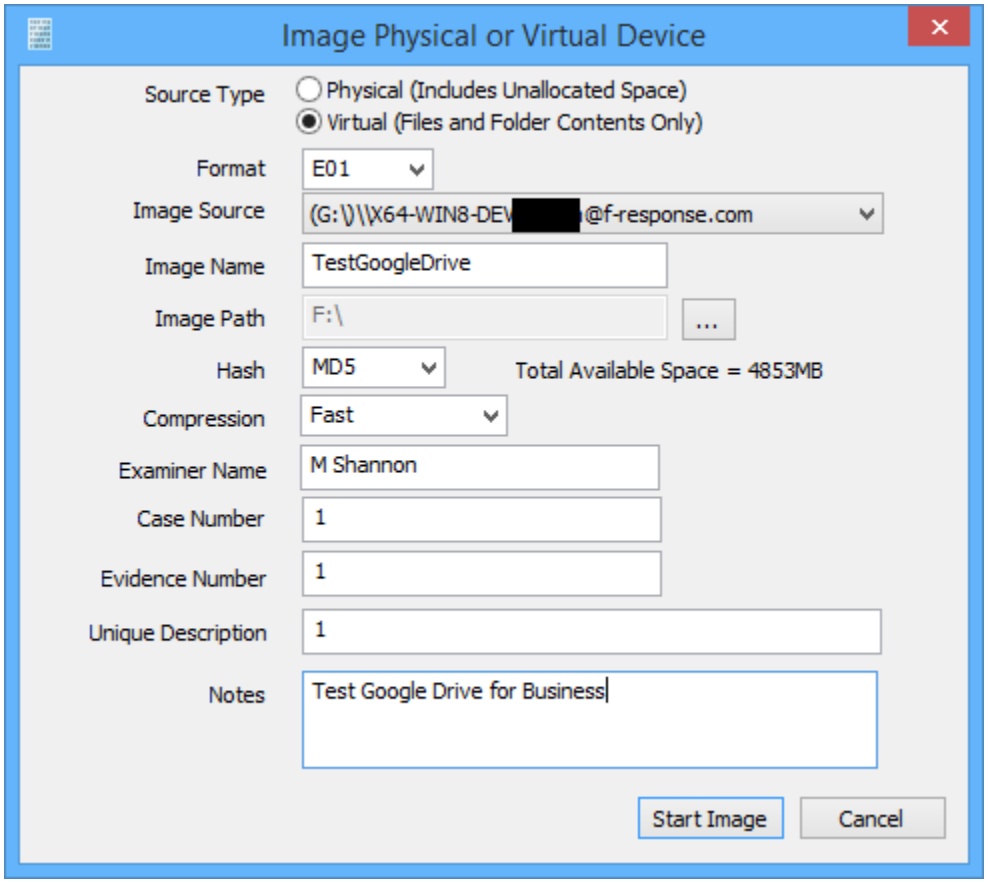
Step 5: Create Image of attached volume

Select the newly attached target and right click on it in the Local Device column. Use the "Create Image…" option to open the "Image" dialog to begin imaging the device.



Start Imaging Process…

Step 6: Complete Imaging Options…



We'll work through this window from the top down. First, the **Source Type** is set to **Virtual** (by default) to be able to create an image of the connected virtual device data.

Next you can select the image **Format**—you have a choice between **E01** (Expert Witness), **VHD** (Virtual Hard Disk), or **Both**. This option determines what the Imager will provide at the end of the collection.

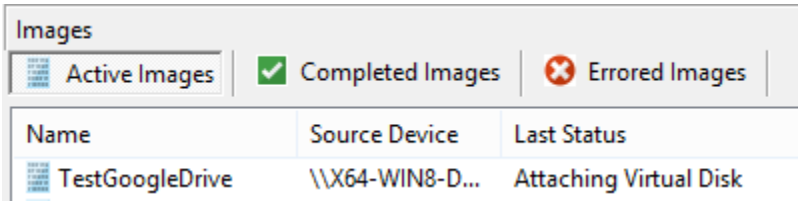
Image Source should be populated if we opened this window from Windows Explorer, just verify that the drive letter is correct from Step 1. For **Image Path** we need to choose our destination drive—this must be a physical drive attached to our examiner machine (we cannot image to a network share).

Next we can choose a **Hash** format and the **Compression** level if you wish to compress the resulting image file. The remaining fields are specific to your case and can be filled out accordingly. These fields will be included in the resulting log file for the image.

Once you have all your information entered simply click the **Start Image** button to begin the process.

Step 7: Review the Image

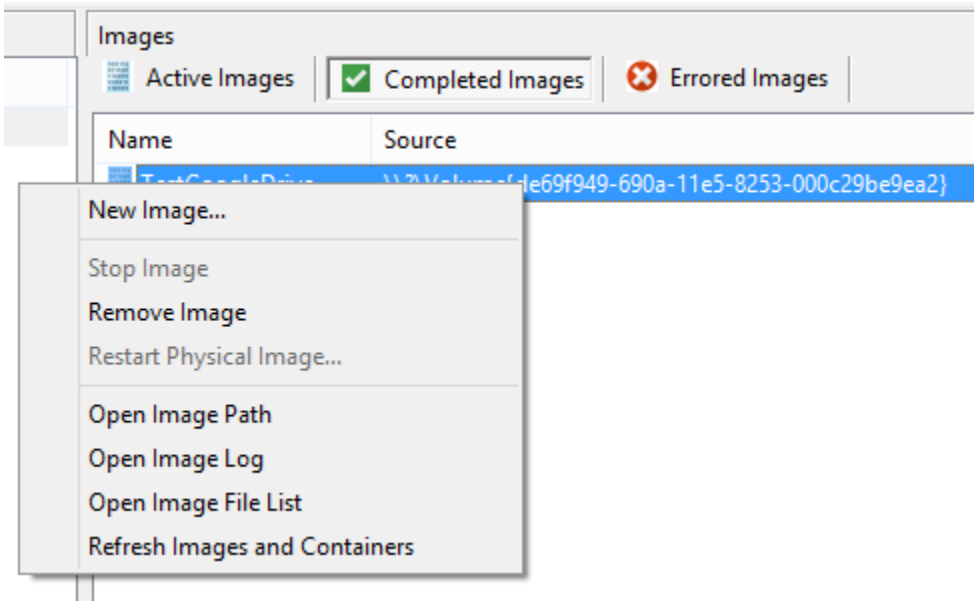
Once started the dialog will close and you'll be able to monitor the image using the Active Images. When the Image completes you will see it move to Completed Images.



Imaging started and running…

Step 8: Review the Completed Image

Right click on the completed image to access the Image Path, Log, and File List. These logs and listings contain details about the image, the image itself, and a file listing of files collected.



Reviewing the completed image.

Troubleshooting

I don't see an option to search and select the custodian accounts?

Correct, F-Response does not provide an enumerated listed of user accounts. You will need to use your account with domain wide delegation to add each user as per the instruction in this guide.

The files appear to have an alphanumeric string in the name?

Yes, this is the Google Drive file id appended to the name to prevent collisions.

Does F-Response show the previous versions of documents?

No, F-Response does not present file revision history for Google.

Does F-Response "get all the metadata"?

Providers vary widely in the type of metadata provided, if you wish to obtain additional metadata for each file, you can enable the option under Providers – Provider Settings… General Options, check the box for "Include provider specific metadata as .FRES_METADATA*files". This will present individual metadata files (in the original format from the provider) along with the data in the attached volume.