Your Mission: Use F-Response Cloud Connector to access Google Apps for Business Drive Cloud Storage

Note: This guide assumes you have installed F-Response Consultant, Consultant + Covert, or Enterprise, your F-Response licensing dongle is plugged into your analyst machine, and the F-Response Cloud Connector (FCLDC) has been started. For more information, please reference the F-Response User Manual. **Note this is a Premium Service and only available for F-Response Consultant Edition and above.**

Step 1: 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 -> <u>https://console.developers.google.com</u>

Google Deve	lopers Console	
Projects	CREATE PROJECT	
Billing Account settings	PROJECT NAME	PROJECT ID
	API Project	

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 on your newly created project to access the API Project menu.





F-Response Mission Guide Using the F-Response Cloud Connector with Google Apps for Business Rev 3.0 2014 Email:support@f-response.com Website:www.f-response.com May 22, Phone: 1-800-317-5497

First you will need to select the APIs & auth menu option and create a new app. Just as before the name of the app is unimportant and all defaults can be accepted. Next you'll need to select the Credentials

OAuth	Create Client ID	
	APPLICATION TYPE	
OAuth 2.0 allows users to share specific data with you (for	 Web application Accessed by web browsers over a network. 	
example, contact lists) while keeping their usernames, passwords, and other	 Service account Calls Google APIs on behalf of your application instead of an end-user. Learn more 	
information private.	Installed application	
Learn more	Runs on a desktop computer or handheld device (like Android or iPhone).	
CREATE NEW CLIENT ID	Create Client ID Cancel	

option to generate a new Service Account. Select "Create New Client ID" and then in the following popup select "Service Account" and "Create Client ID". This will pop up a download for the newly generated p12 encryption key file. Save this file as it will be needed later.

Opening f3bbe15e3688156c27c0362a303eb89a877cfdf1-privatekey.p12
You have chosen to open:
f3bbe15e3688156c27c0362a303eb89a877cfdf1-privatekey.p12
which is: p12 File (1.7 KB)
from: https://console.developers.google.com
What should Firefox do with this file?
Open with Browse
Do this <u>a</u> utomatically for files like this from now on.
OK Cancel

Following the encryption key download you should see a newly created Service Account looking something like this:



Service Account

Support Need help with a task?

Client ID	733107590776-	.apps.googleusercontent.com
Email address	733107590776-	e6mb@developer.gserviceaccount.com
Public key fingerprints	f3bbe	
Generate new key Download J	SON Delete	

After the account has been created you will need to select the APIs option from the left hand menu and enable Drive API access.

Drive API	٥	ON

After the Drive API has been enabled you must open the Google Apps for Business Domain Administrator Console.

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

S A https://admin	n.google.com/AdminHome?chron	neless=1#Home:			<u></u> ☆ ▼
+You Search Images	Mail Drive Calendar	Sites Groups Contacts	⊨ More -		
Google				Q	
Admin console					
Nelcome to your new A	dmin console Take a tour	Watch a video			
2	\$	6			
Users 11 users, 0 invites sent	Company Profile F-Response	Billing View charges and manage subscriptions	Google Apps Manage the way Google Apps works for you	Groups Manage groups of users and mailing lists	Security Enable security features
\frown					

The Admin console provides options for administering the Google Apps for Business Domain. The option you will want to select is "Security".



F-Response Mission Guide Using the F-Response Cloud Connector with Google Apps for Business Rev 3.0 2014

Security •			? \$	
	Security	Advanced settings	×	
	Security Fresponse.com	Set up single sign-on (SSO)	Set up single sign-on (SSO) SAML-based Single Sign-On (SSO) senice allows you to authenticate user accounts for web based applications (like Gmail or Calendar). For desitop applications (like Google Talk	
	Basic settings Activate SSL for your users, set password strength policies, and enforce 2-step verification.		or POP access to Gmail, your users must continue to sign in directly with the username and password set up via the Google Admin Control Panel Learn more	
	Password monitoring Monitor the password strength of each user in your organization.	Authentication	Manage OAuth domain key Allows administrators in your domain to access all user data without requiring the user's login credentials. $\widehat{\odot}$	
	API reference Enable APIs to programmatically manage provisioning, reporting, or migration via custom-built or third-party applications.		Federated Login using OpenID Allows users to sign-in to 3rd party websites using their Fresponse.com account, without giving away their credentials.	
	Advanced settings Manage advanced security features such as Single Sign On, authentication, and integrating Google Apps with internal services.		Manage OAuth Client access Allows you to control access to user data by applications that use the OAuth protocol.	

Under Security you will need to press "Advanced Settings" and click on the "Manage OAuth Client Access" in the right hand panel.

Manage OAuth Client access

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

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 a

Authorized API clients The following API client domains are registered with Google	
Client Name	One or More API Scopes
Example: www.example.com	Example: http://www.google.com/calendar/feeds/ (comma-delimited)

Under Manage API Access you will want to paste in the Client ID (as Client Name) included in the JSON output that was downloaded earlier, and the following API Scope.

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

Press Authorize to complete the delegated account permissions.

Step 2: Open Google Apps for Business Drive Credential Configuration window

Before you can connect to Google using the new delegation account you must first input valid credentials.

In the F-Response Cloud Storage Connector go to File->Configure Credentials-> Google Apps for Business Credentials.



File Scan Connect Help Configure Credentials Amazon S3 Cloud Storage Credentials Clear Messages Rackspace Cloud Files Credentials Exit HP Public Cloud Storage Credentials OpenStack Cloud Files Credentials OpenStack Cloud Files Credentials Windows Azure Cloud Storage Credentials Dropbox Credentials
Clear Messages Rackspace Cloud Files Credentials Exit HP Public Cloud Storage Credentials OpenStack Cloud Files Credentials OpenStack Cloud Files Credentials Windows Azure Cloud Storage Credentials
Microsoft Skydrive Credentials Google Drive Credentials Google Apps for Business Credentials

Cloud Storage Connector

Step 3: Input account information and validate the credentials

Service account

Use service accounts to call Google APIs on behalf of your application instead of an end-user. Learn more

Client ID:	.apps.googleusercontent.com
Email address:	<pre>@developer.gserviceaccount.com</pre>
Public key fingerprints:	Bb56b264 - Delete

Sample Google Apps Console Service Account Details

In order to complete the credentials dialog you will need the following information:

- The delegation Service Account email address as provided by the Google Apps Console.
- The Public Key file as provided by the Google Apps Console.
- The target end user's email address.

Provided everything is accurate you can add the credential to your encrypted credential store, save, and move on to connecting to the Google Drive account.



Step 4: Scan and enumerate Google Drive Accounts

Use the Scan menu to enumerate Google Drive Cloud Storage Containers.

🐳 F-Response® Cloud Storage Connector - Premium Services					
File	Scan Connect Help				
F-Re	Scan All Scan Amazon S3 Cloud Storage Scan Rackspace Cloud Files Scan HP Public Cloud Storage Scan OpenStack Cloud Files Scan Windows Azure Cloud Storage Scan Dropbox Cloud Storage Scan Microsoft Skydrive Storage Scan Google Drive Storage	scription 16574			

Cloud Connector Scan menu

🍑 F-Response®	Cloud Storage C	onnector			
<u>F</u> ile Scan Conne	ct <u>H</u> elp				
Connect	Messages	1			
F-Response Cloud	Storage Target	Description	Provider	Connected	Local Volume
M Shannon-08	3674130311706	GDOCS24681	Google Docs	Inactive	
F Response-12	2884486562148	GDOCS21527	Google Docs	Inactive	
			HWID:155519963	Expires:4/27/2013	4.0.6 //

Cloud Connector scan results

Step 5: Login and mount one or more Google Drive Accounts

You can connect to a storage target by selecting the target, right clicking to open the context menu, and selecting "Login to F-Response Cloud Storage Volume". The newly attached volume will be assigned a drive letter and is now accessible read-only for evidence acquisition.



♣ F-Response® Cloud Storage Connector					
<u>File Scan Connect Help</u>					
Connect	Messages]			
F-Response Cloud Sto	orage Target	Description	Provider	Connected	Local Volume
M Shannon-0836			Google Docs	Connected	\\. \E:
			HWID:155519963 Ex	cpires:4/27/2013	4.0.6 //.

Logged in Cloud Storage target assigned the E:\ drive letter

Step 6: Fire up the tool of your choice!

F-Response is a vendor neutral product. Once F-Response presents the remote cloud storage target as a write blocked local network share, we step out of your way so that you can select the right tool to get your job done. At this point, you can reach into your toolbox and apply the tool of your choice to the newly attached network share.

