MoxiWorks

MoxiEngage Integration Process using Google Workspace

Overview

MoxiEngage integrates directly with your brokerage's Google Workspace (formerly G Suite) account to provide your agents and support staff with consistent and convenient access to their information, while eliminating any need to enter the same information multiple times.

MoxiEngage uses a service account as an API client to synchronize data and perform actions on behalf of individual users. Each MoxiEngage user account has an email address that corresponds to a mailbox on your Google Workspace account. All integration actions are performed within the context of a single given mailbox. MoxiEngage never requires administrative access to your Google Workspace account.

Contacts

Using the Google People API, MoxiEngage synchronizes a user's contacts and contact details with Google Workspace. Contacts created in Google Workspace will appear in MoxiEngage. Contacts created in MoxiEngage are synchronized back to the user's contacts in Google Workspace.

Calendar

Using the Google Calendar API, MoxiEngage displays the user's calendar events and appointments. Calendar events and appointments can also be added through MoxiEngage and are synchronized to the user's calendar in Google Workspace.

Email

Using the Gmail API, MoxiEngage sends certain email messages through user's mailbox. These email messages will appear in the Sent mail folder and will be delivered to the recipient from the mailbox just as if the user had sent the email from Gmail directly. MoxiEngage does not synchronize or inspect incoming email messages.

Service Account Setup

MoxiEngage is designed to utilize service account credentials for organizations that use Google Workspace (formerly G Suite) for administration of the company's email functions.

An email administrator in your company organization will need to perform steps to create a service account and obtain the necessary credentials for MoxiEngage to use.

Refer to Google Workspace Setup Instructions for Administrators and follow the provided step-by-step instructions to set up service account credentials with domainwide delegation, then enable the needed API endpoints and authorize the service account as an API client with appropriate OAuth scopes.

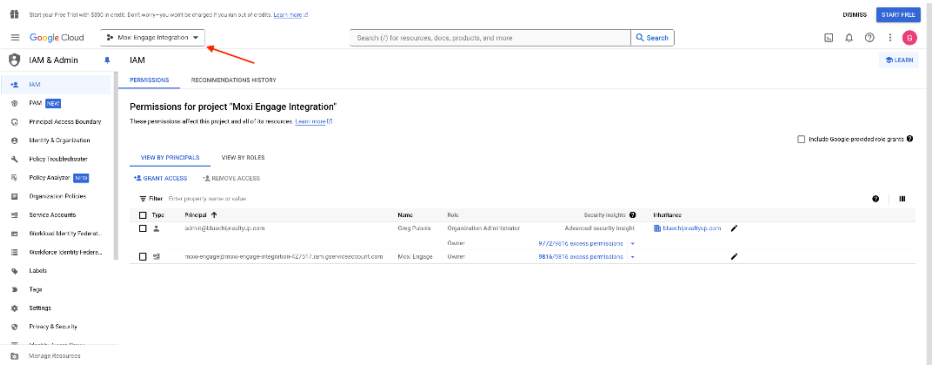
MoxiWorks

You will need to provide the service account key in JSON format, along with a regular user email address that we can use for testing. By default, Google has disabled the service account key function. Here is what you need to do to enable it.

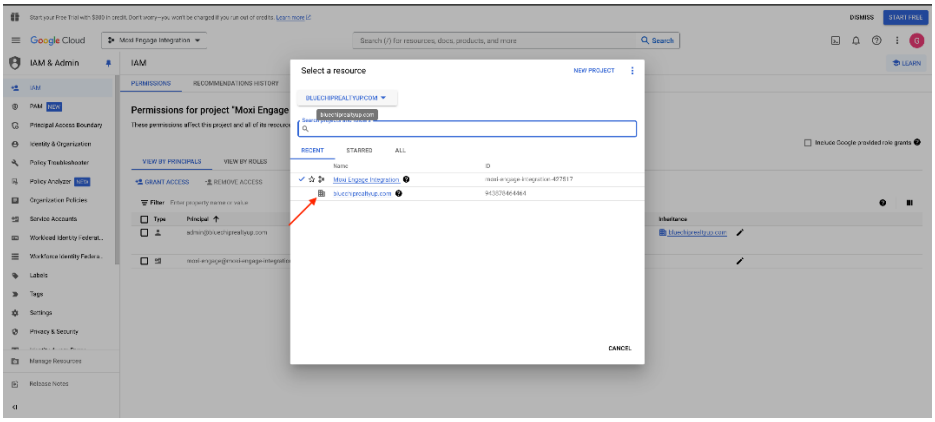
Enabling the Account Key Function

When you are logged in as the admin of the account, select this link: https://console.cloud.google.com/iam-admin/iam

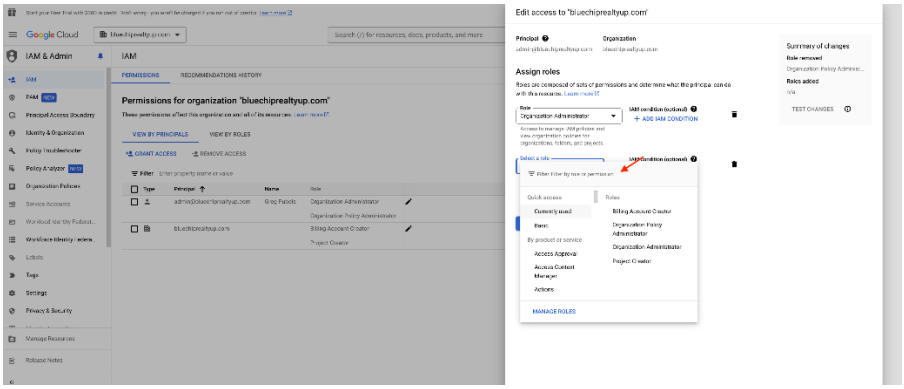
Click into dropdown. It will say Moxi Engage Integration



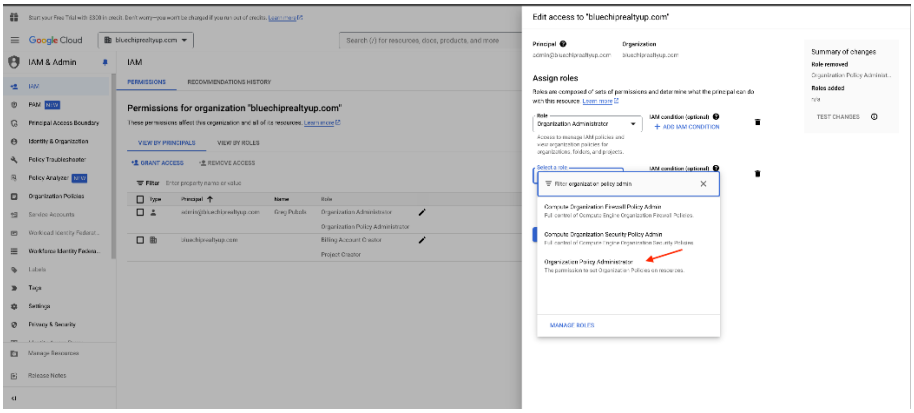
Select the Parent Organization. It will have a building icon next to it.



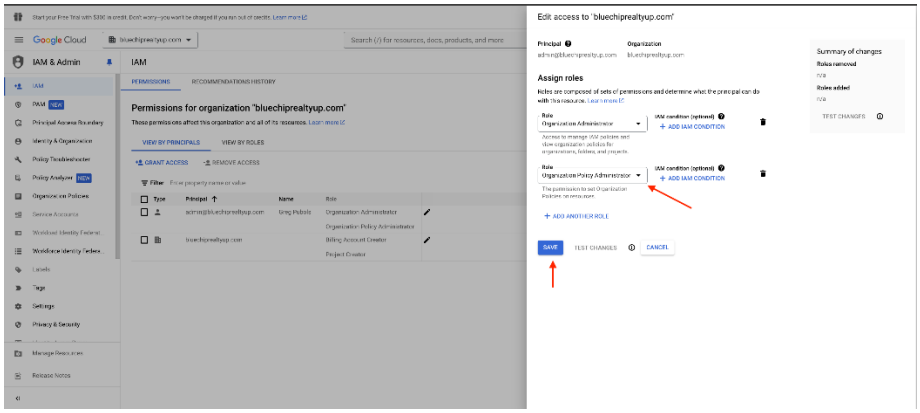
Select the pencil icon next to that record to edit the record. This will bring up the edit access screen.



Click in the box under Select a Role and add a new role. Select **Organization Policy Admin**.



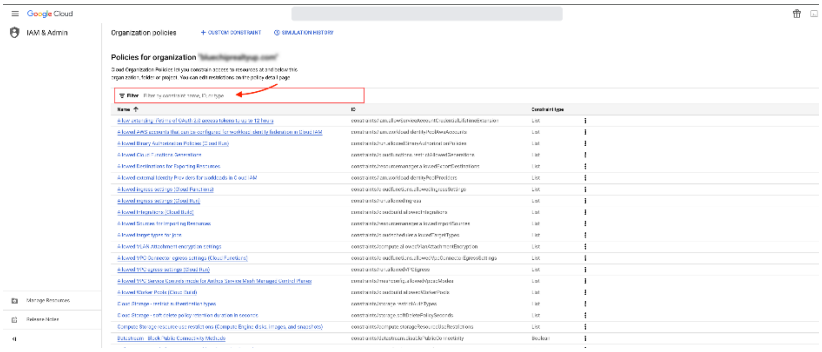
Once entered, select the **Save** button.



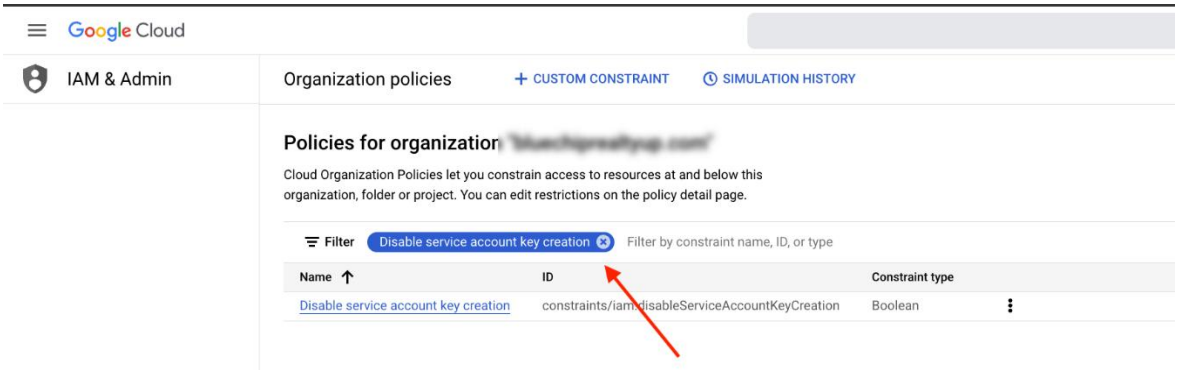
This role gives you the ability to enable the service account key function. Here are the steps to do that.

7. In your browser, go to this link: Go here https://console.cloud.google.com/iam-admin/orgpolicies/

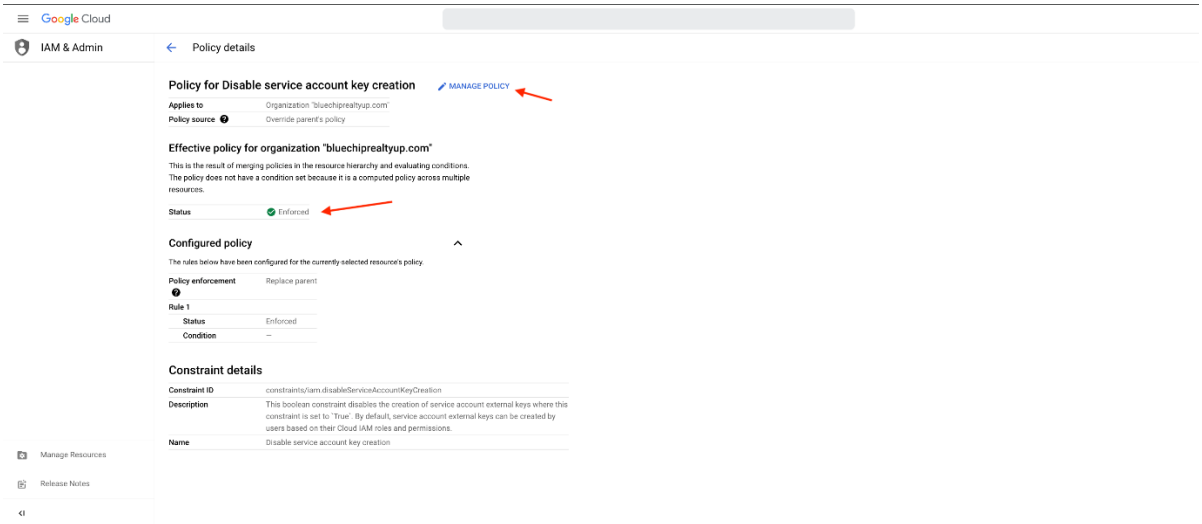
In the Filter by Constraint Name, ID, or Type box, enter **Disable Service Account Key Creation**



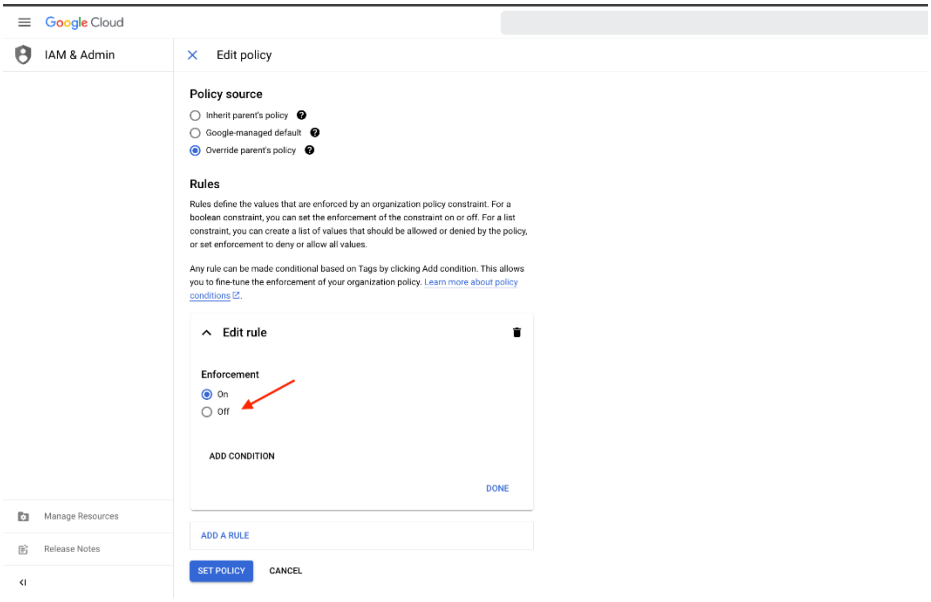
Once you have found that match, select the **Disable Service Account Key Creation** item.



Once in the Disable Service Account Key Creation item, select the **Manage Policy** link.



In the Manage Policy screen, under the **Enforcement** heading, select the ‘Off’ radio button and select the **Set Policy** button.



You can now proceed with the rest of the MoxiEngage integration steps.

Information Gathering

To enable configuration of the MoxiEngage integration, we will need to gather some key information from you, including the service account credentials created by following the steps in the Google Workspace Setup Instructions for Administrators section of this document.

Next Steps

Verification of Credentials

MoxiWorks staff will begin the next step of the integration process. We will test the credentials you provided to verify that the service account is able to connect to your email service and perform a synchronization for the test email address you supplied.

Outcome: Credentials Cannot be Verified

If your entered credentials cannot be verified, we will contact you. Your email administrator will need to resolve the issue and then you will provide us with the updated information.

Outcome: Credentials are Verified Successfully

If your credentials are verified successfully, we will store the credentials securely. Congratulations! This is a key milestone that enables us to continue the process of getting MoxiEngage enabled for your brokerage.

MoxiWorks

Security

MoxiWorks requires the use of a single service account in your Google Workspace, configured with domain-wide delegation. This service account must be authorized as a client to the Google API with the following OAuth scopes:

- https://www.google.com/m8/feeds
- https://www.googleapis.com/auth/calendar
- https://www.googleapis.com/auth/gmail.compose

All interactions between the MoxiWorks system and your user's account happens through this designated service account, authenticated by credentials (i.e., a JSON formatted key) generated and provided by your Google Workspace administrator. MoxiEngage never requires administrative access to your Google Workspace account.

Network Access

MoxiWorks systems communicate directly with the Google Workspace API over secure HTTPS/SSL connections.

Managing Shared Secrets and Credentials

For automated access, MoxiWorks makes use of methods native to our configuration management software. Credentials are stored in encrypted objects accessible only to servers with the relevant service role and environment. These credentials are pulled and decrypted during software deployment. Server identity is validated via pre-shared public/private key. Credentials are managed through a commercial password manager and any non-automated access is limited to the MoxiWorks Technical Operations team and, with customer approval, limited support personnel on an as-needed basis. See also:

https://docs.chef.io/secrets.html#encrypt-a-data-bag-item

https://www.lastpass.com/en/enterprise

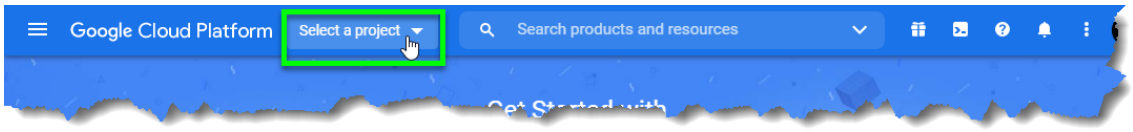
Communications Policy for Security Breaches

In the unlikely event of a security breach where client data such as account credentials for registrar management, impersonation credentials, and the like may have been compromised, MoxiWorks Technical Operations and/or Account Management staff will notify affected clients. If the client is aware of a potential security breach, they should notify MoxiWorks immediately so that we may contain and mitigate potential risk in a timely manner. In either case, a change to Impersonation account credentials will be coordinated between both parties.

Google Workspace Setup Instructions for Administrators

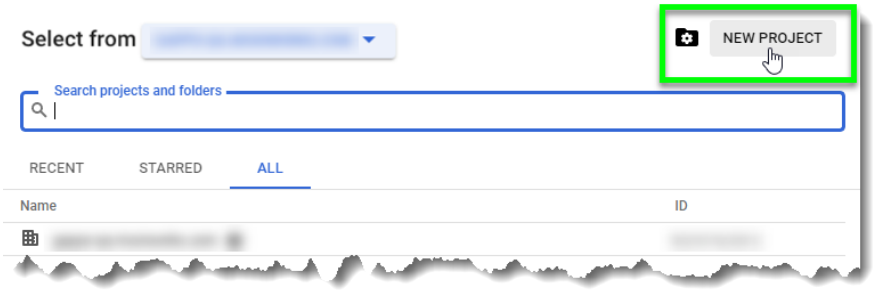
The following steps describe the recommended process for creating a service account in Google Workspace for use with your brokerage's MoxiWorks integration. ***Create Google Service Account Credentials with the "Owner" Role***

1. Login to your Google Cloud Platform.
2. Click on the "Select a project" dropdown button.

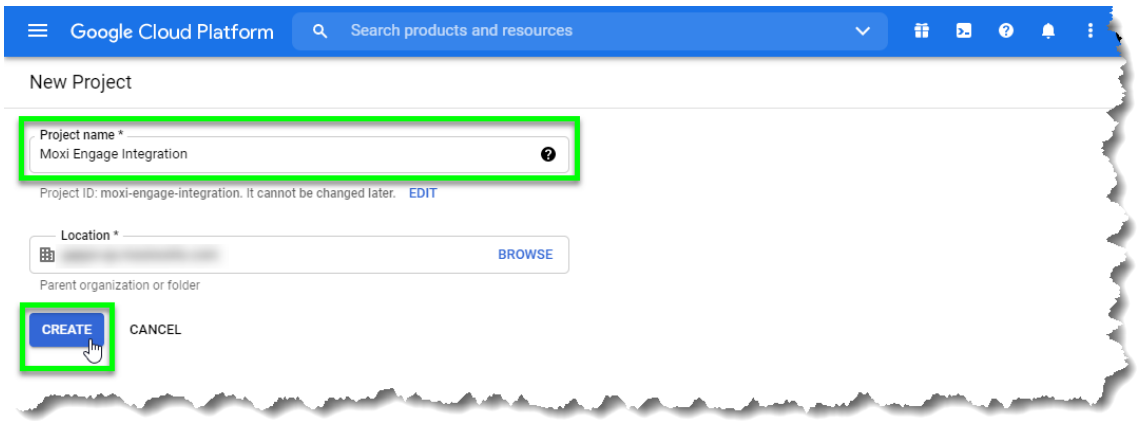


3. Choose your organization's Google Workspace identifier from the dropdown list.

4. Click on the "NEW PROJECT" button.



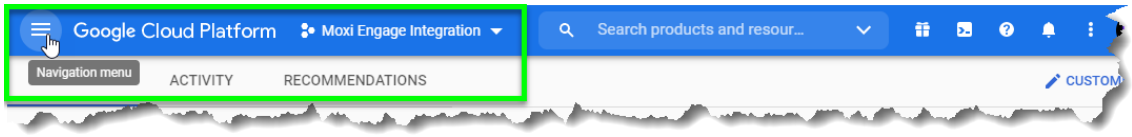
5. Enter a meaningful project name to represent MoxiEngage (e.g., "Moxi Engage Integration"), then click on the "CREATE" button.



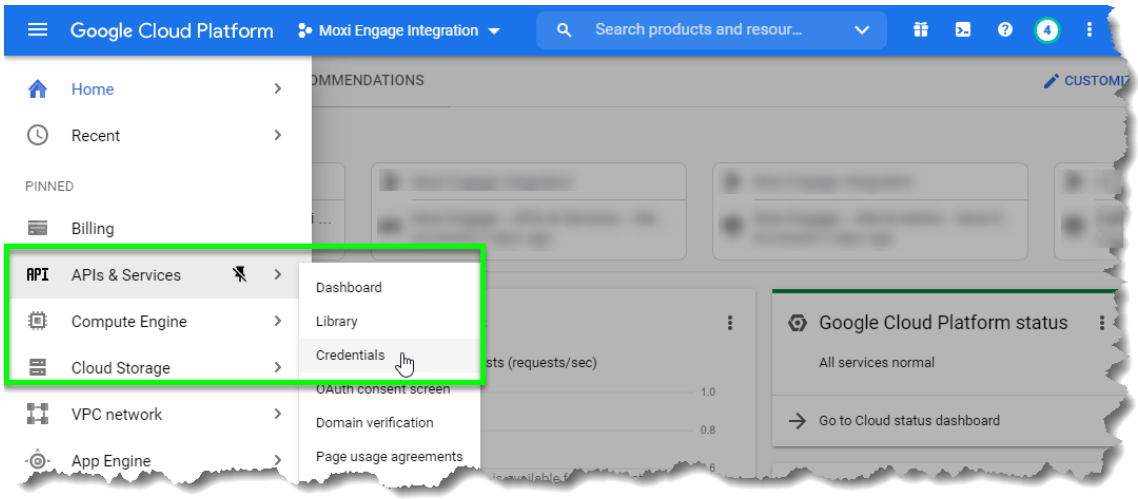
Note

Now that you have created a new project, you should see the name of the project displayed in the header area next to the "Google Cloud Platform" title.

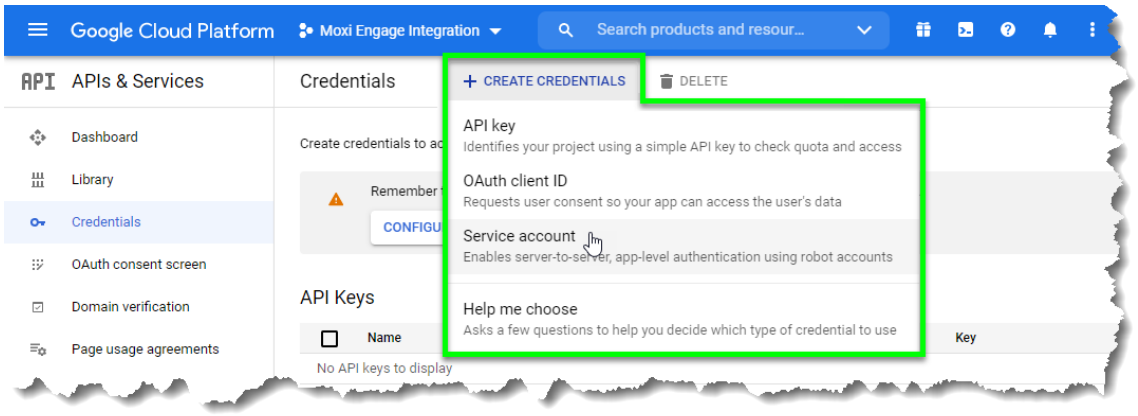
6. Click on the three horizontal lines next to the "Google Cloud Platform" label to access the navigation menu.



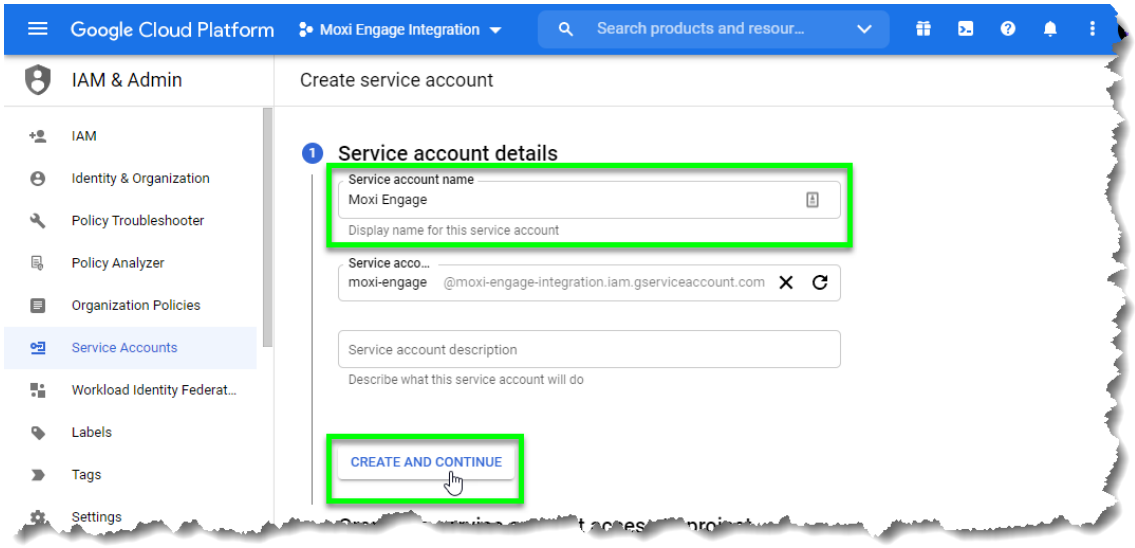
7. Using the Google Cloud Platform menu, navigate to the "APIs and Services" => "Credentials" option.



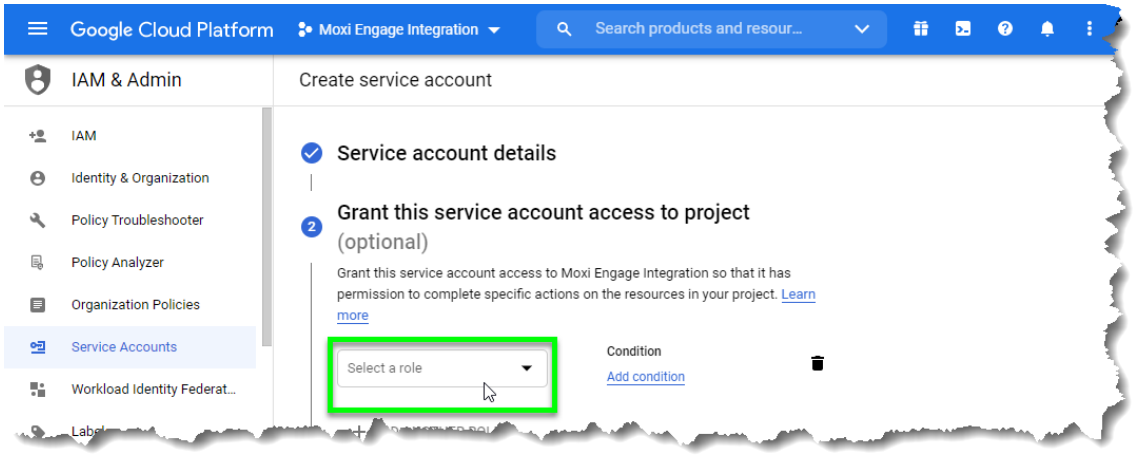
8. Click on the "Create Credentials" dropdown and select "Service account" from the available options.



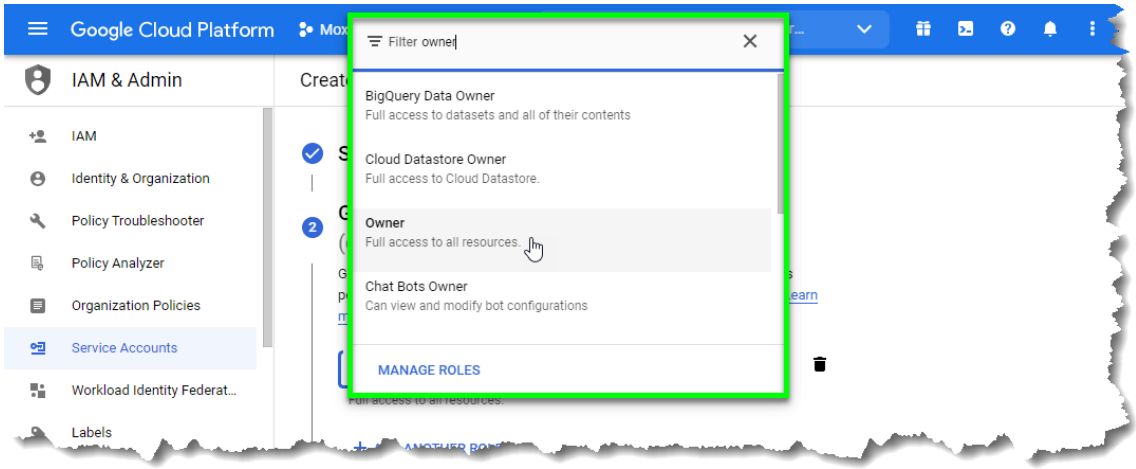
9. Enter "Moxi Engage" in the "Service account name" text box, then click on the "CREATE AND CONTINUE" button.



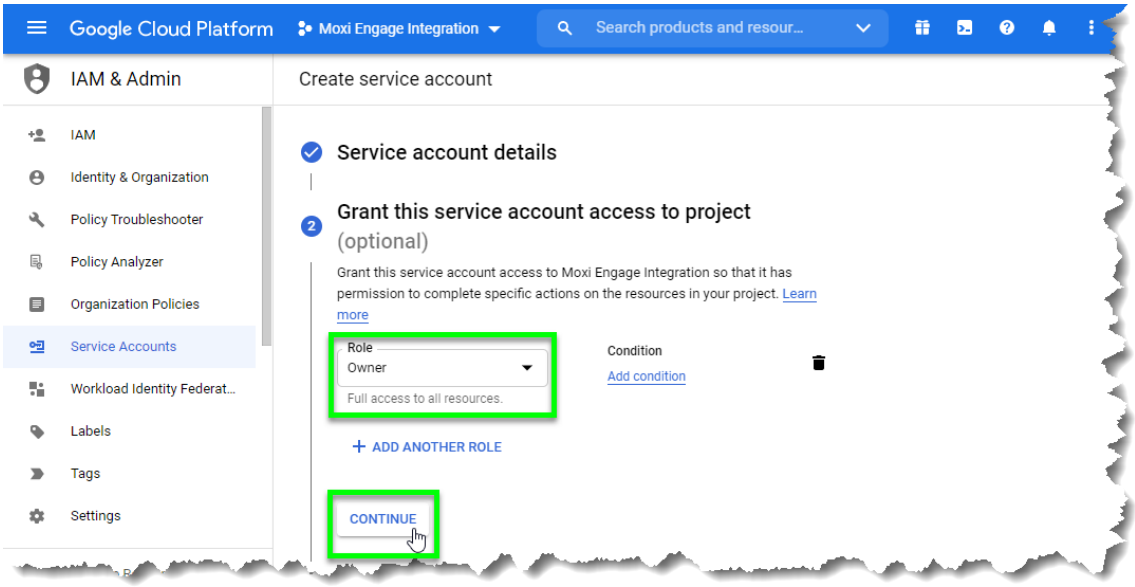
10. Click on the “Select a role” dropdown.



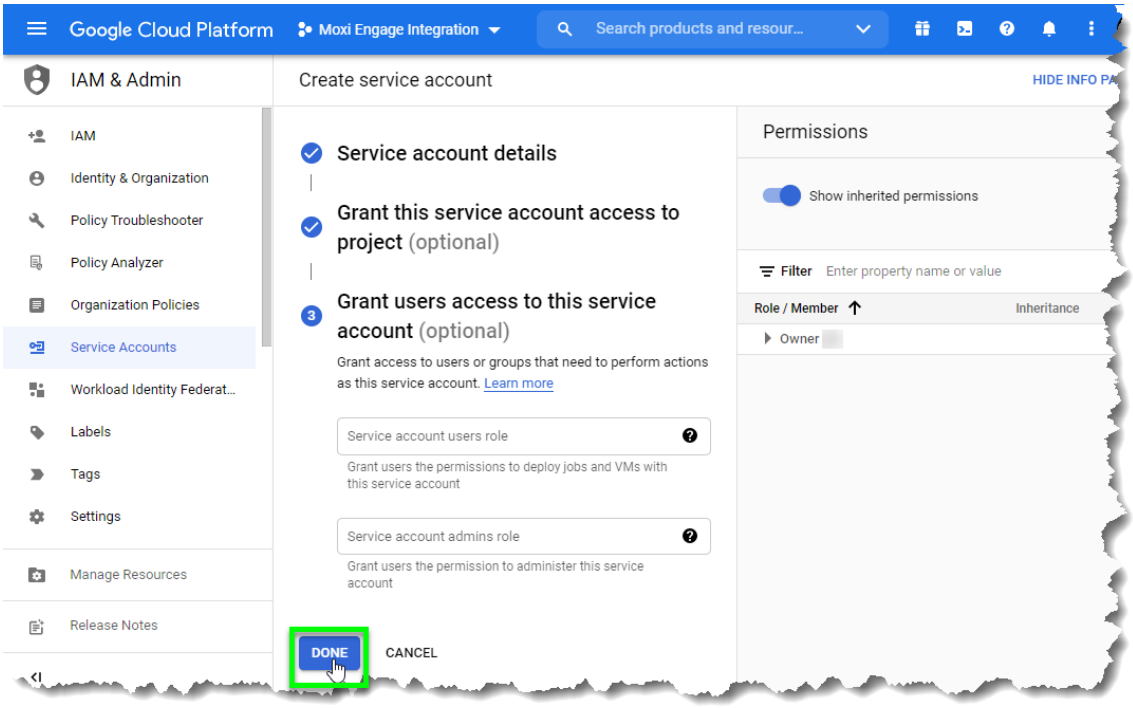
11. Enter “owner” in the search filter box, then select “Owner” from the list. (Alternatively, navigate the list to locate and select “Project” => “Owner” from the available roles.)



12. With “Owner” selected as the “Role” for the service account, click on the “CONTINUE” button.

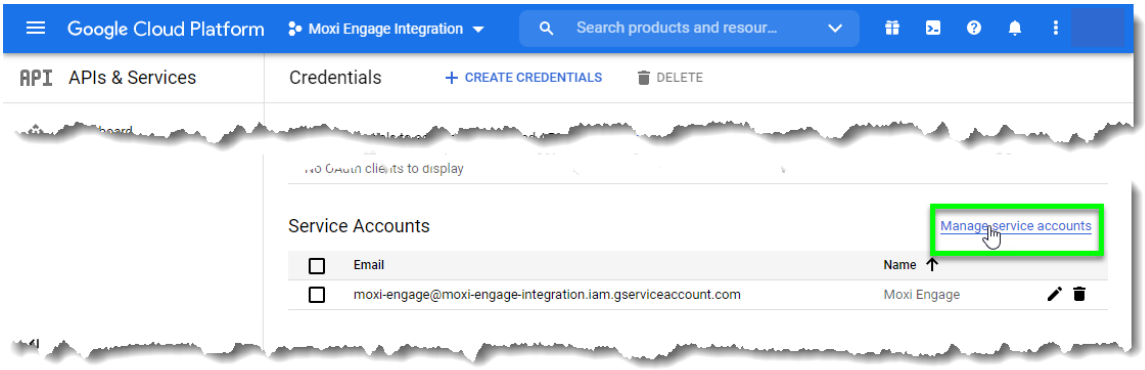


13. Click on the “DONE” button.

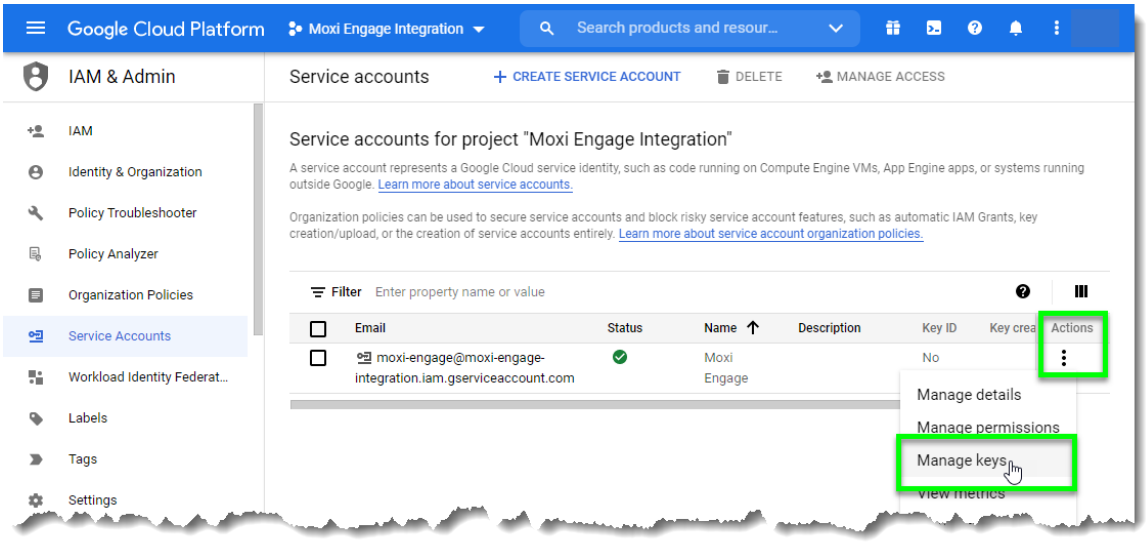


Create a Key for the MoxiEngage Service Account in JSON Format

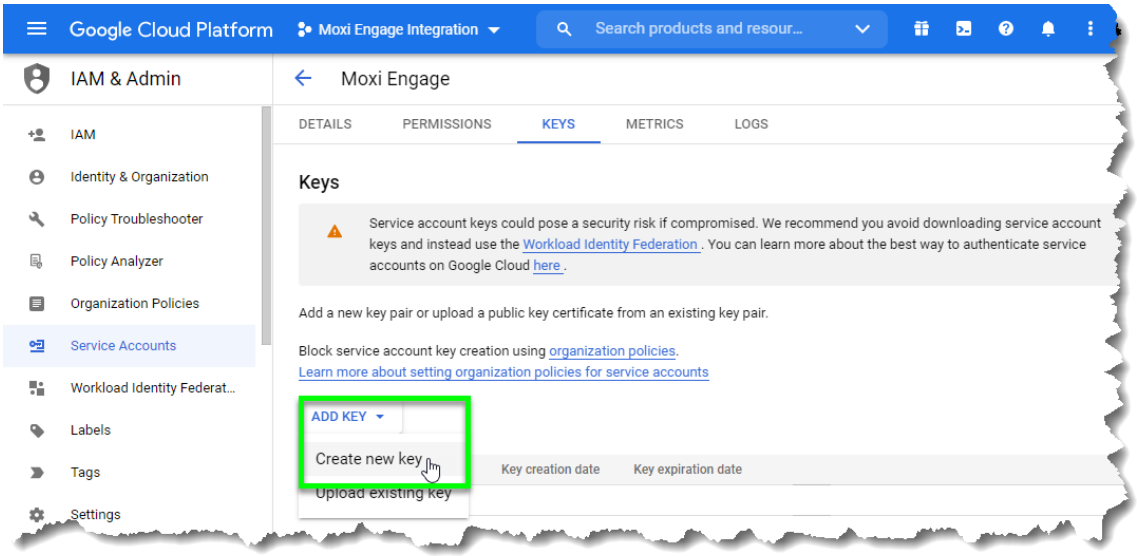
1. Click on the “Manage service accounts” link displayed on the righthand side of the “Credentials” list screen.



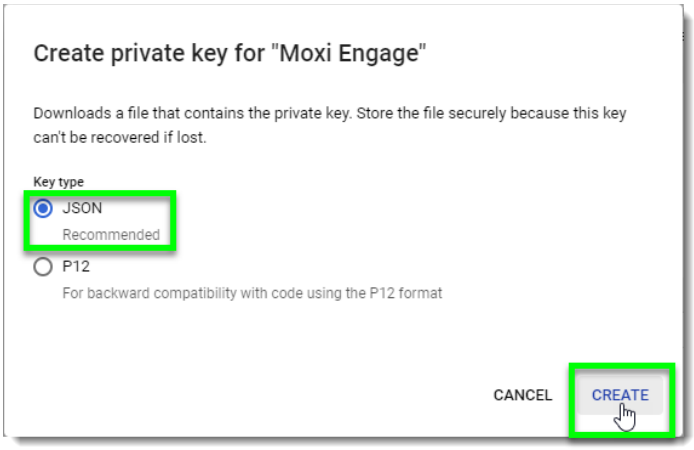
2. Click on the three dots in the “Actions” column next to the Moxi Engage service account, then select “Manage keys” from the list of options.



3. Click on the “ADD KEY” dropdown, then select the “Create new key” option.

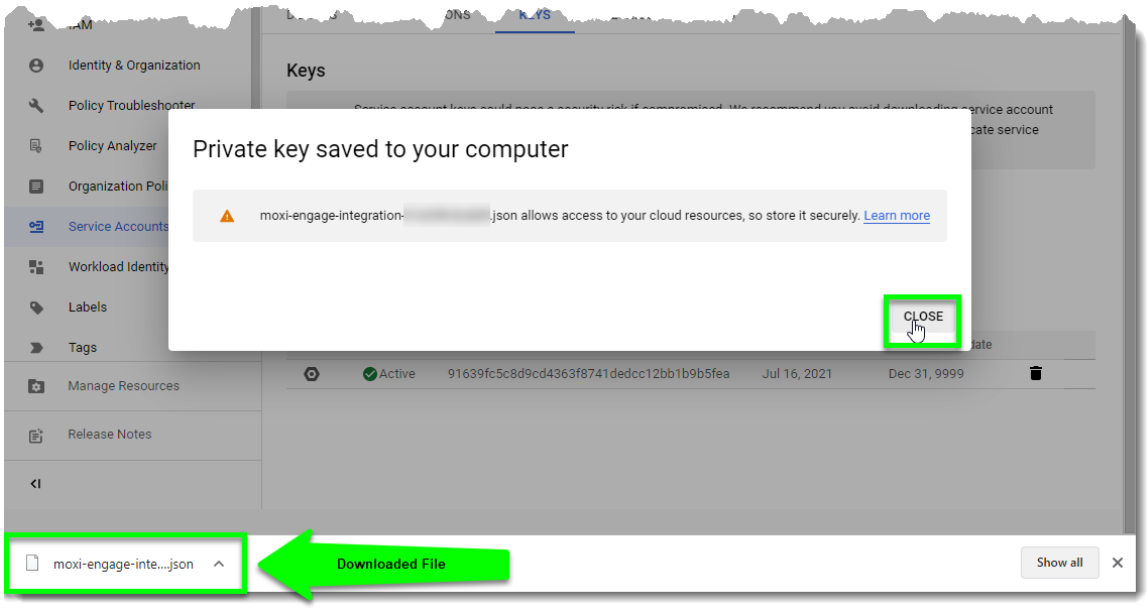


4. Ensure the “JSON” radio button is selected for the “Key type” option, then click on the “CREATE” button.



Note When you click on the “CREATE” button, a JSON file will be generated automatically and downloaded to your computer. Make a note of the location where the JSON file was downloaded and saved. You will need to locate this file later in the process.

5. A popup will let you know that a private key was saved to your computer. Click on the “CLOSE” button to acknowledge the message and continue.

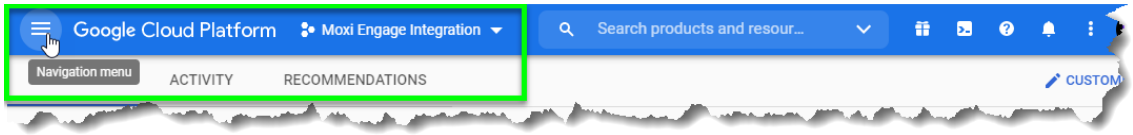


Enable Gmail API

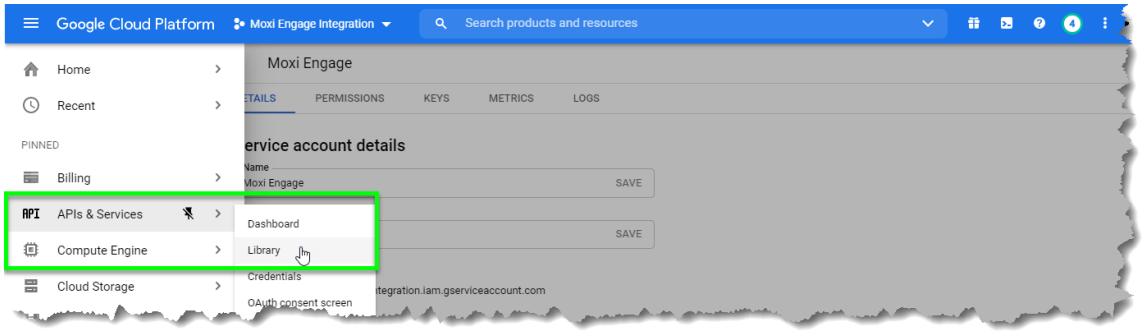
Note

You have already created the credentials necessary for MoxiEngage to use this API. Ignore any warnings or prompts that would lead you to create additional credentials.

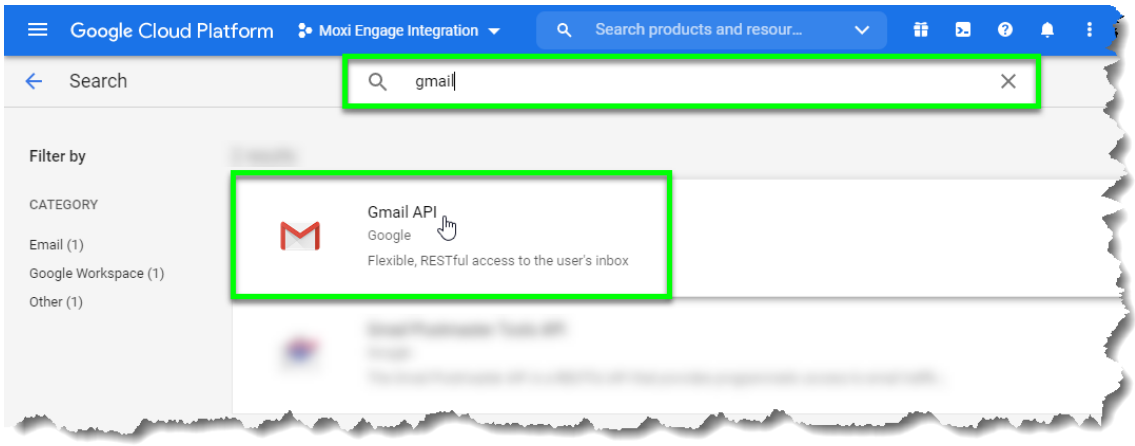
1. Click on the three horizontal lines next to the “Google Cloud Platform” label to access the navigation menu.



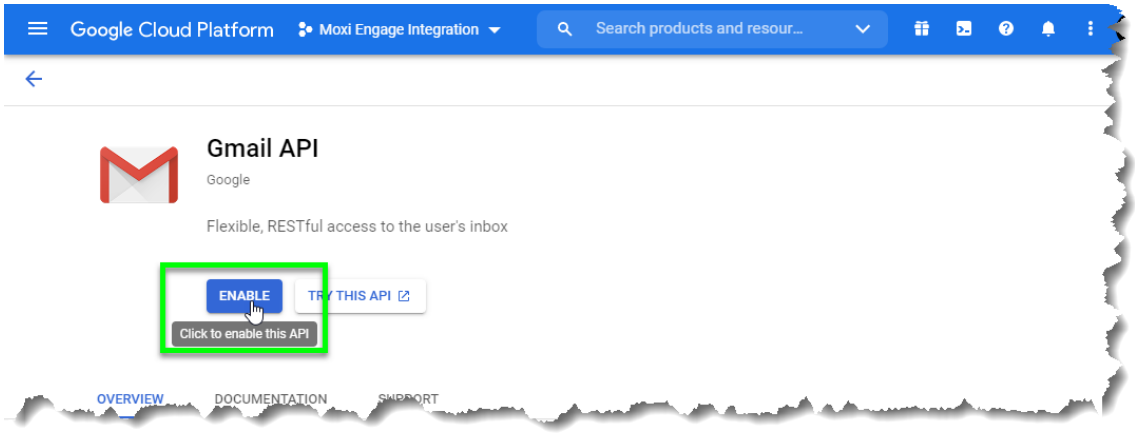
2. Using the Google Cloud Platform menu, navigate to the “APIs and Services” => “Library” option.



3. Click on the “Gmail API” card (use the search box to find this card if it is not readily visible to you).



4. Click on the “ENABLE” button.

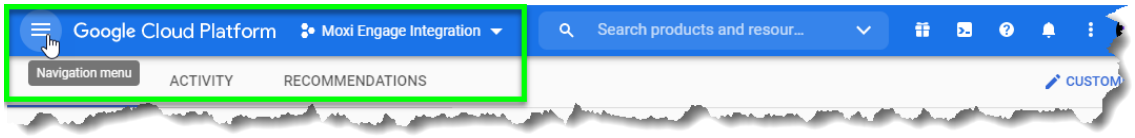


Enable Calendar API

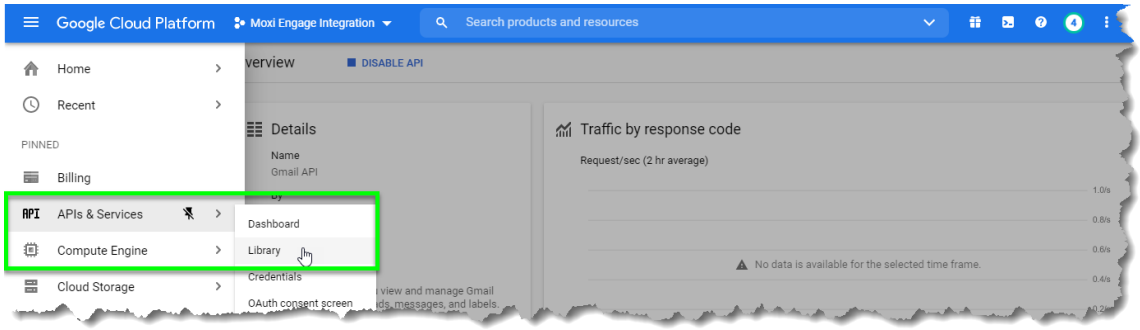
Note

You have already created the credentials necessary for MoxiEngage to use this API. Ignore any warnings or prompts that would lead you to create additional credentials.

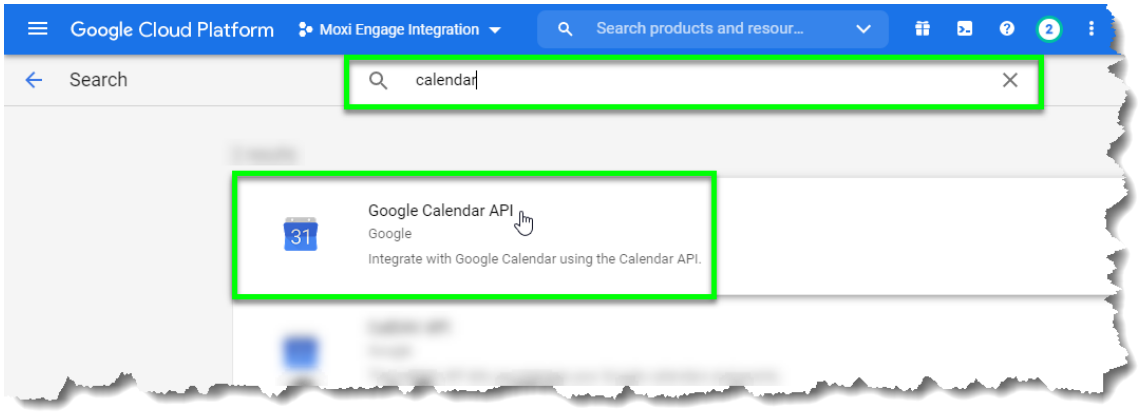
1. Click on the three horizontal lines next to the “Google Cloud Platform” label to access the navigation menu.



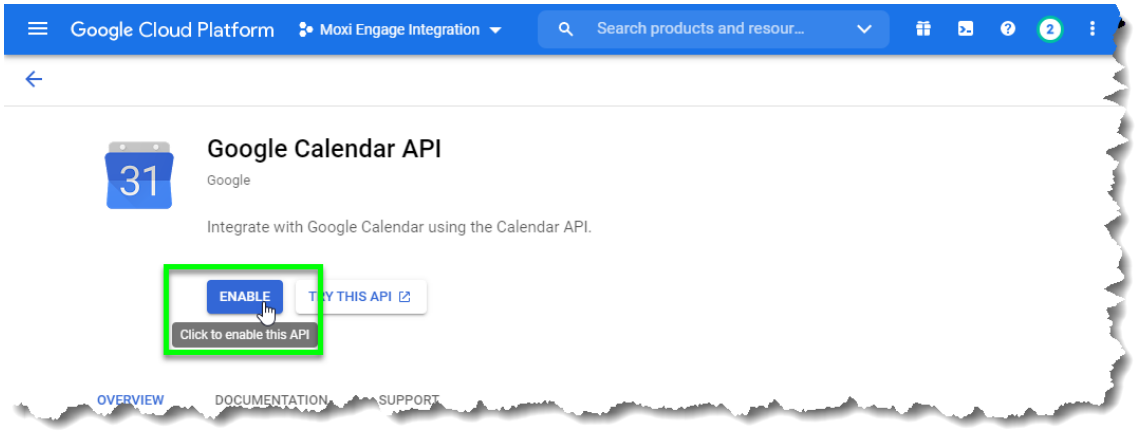
2. Using the Google Cloud Platform menu, navigate to the “APIs and Services” => “Library” option.



3. Click on the “Calendar API” card (use the search box to find this card if it is not readily visible to you).



4. Click on the “ENABLE” button.

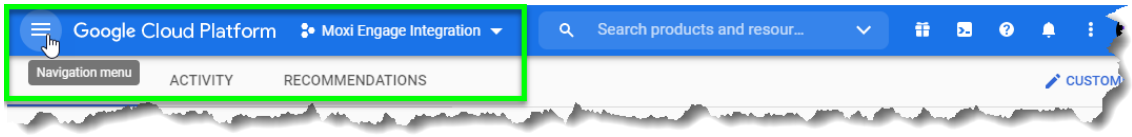


Enable People API

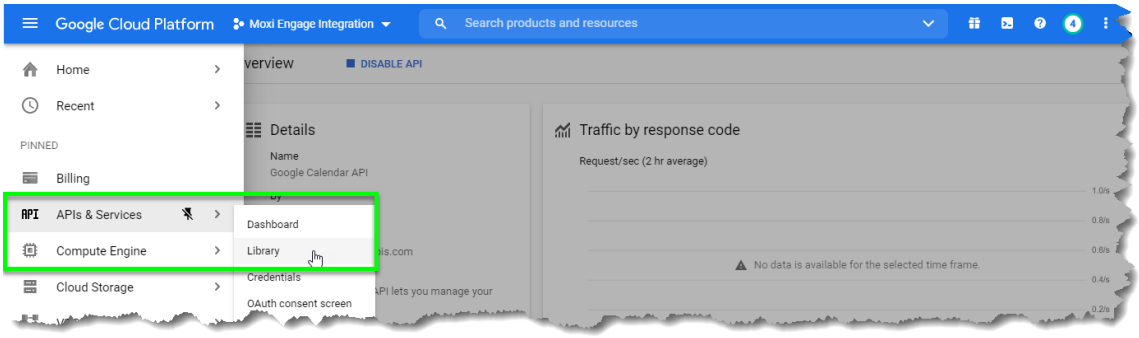
Note

You have already created the credentials necessary for MoxiEngage to use this API. Ignore any warnings or prompts that would lead you to create additional credentials.

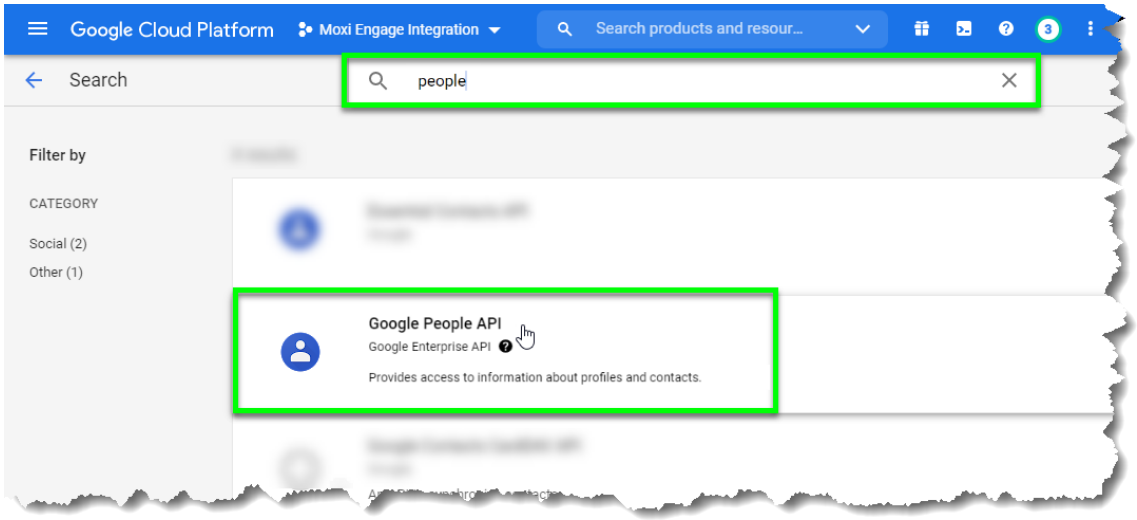
1. Click on the three horizontal lines next to the “Google Cloud Platform” label to access the navigation menu.



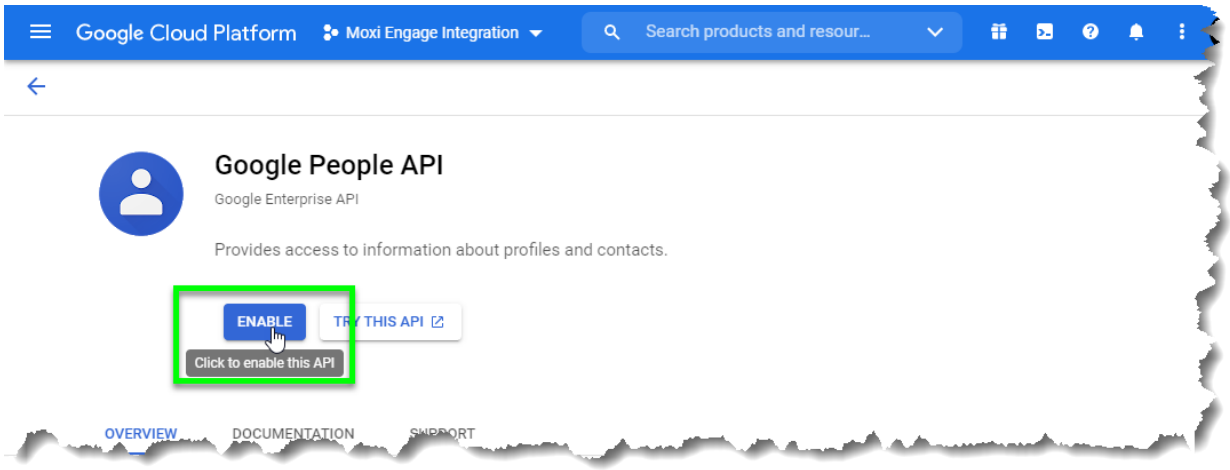
2. Using the Google Cloud Platform menu, navigate to the “APIs and Services” => “Library” option.



3. Click on the “Google People API” card (use the search box to find this card if it is not readily visible to you).



4. Click on the “ENABLE” button.

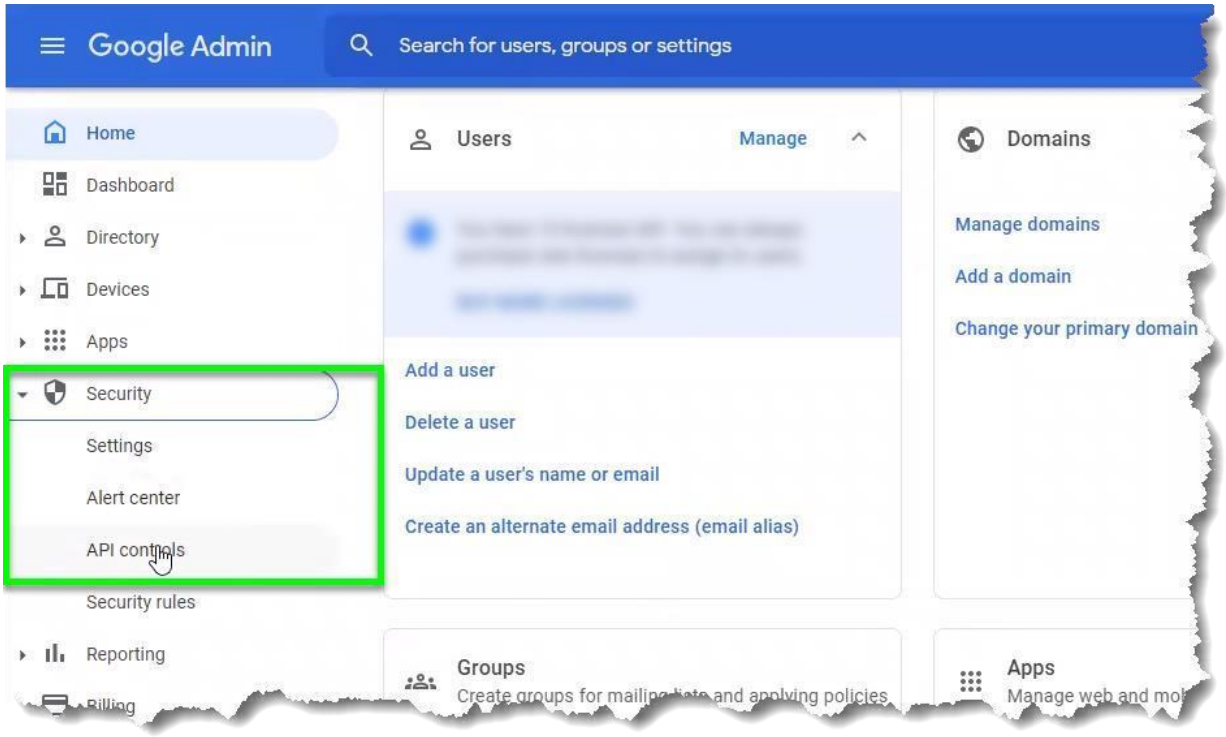


Authorize the MoxiEngage Service Account as an API Client

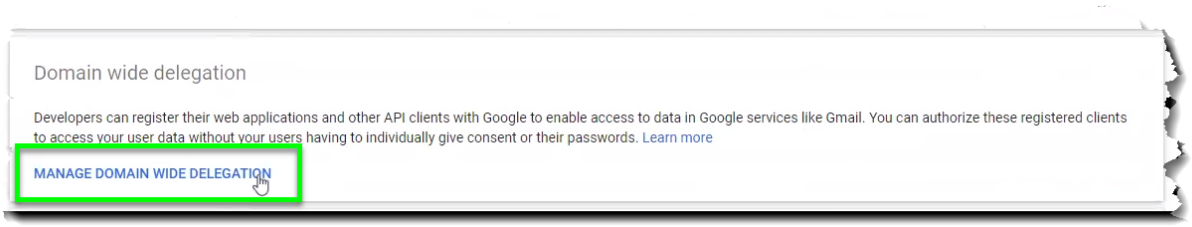
1. Login to your Google Admin Console.

2. Click on the three horizontal lines next to the “Google Admin” label to access the navigation menu.

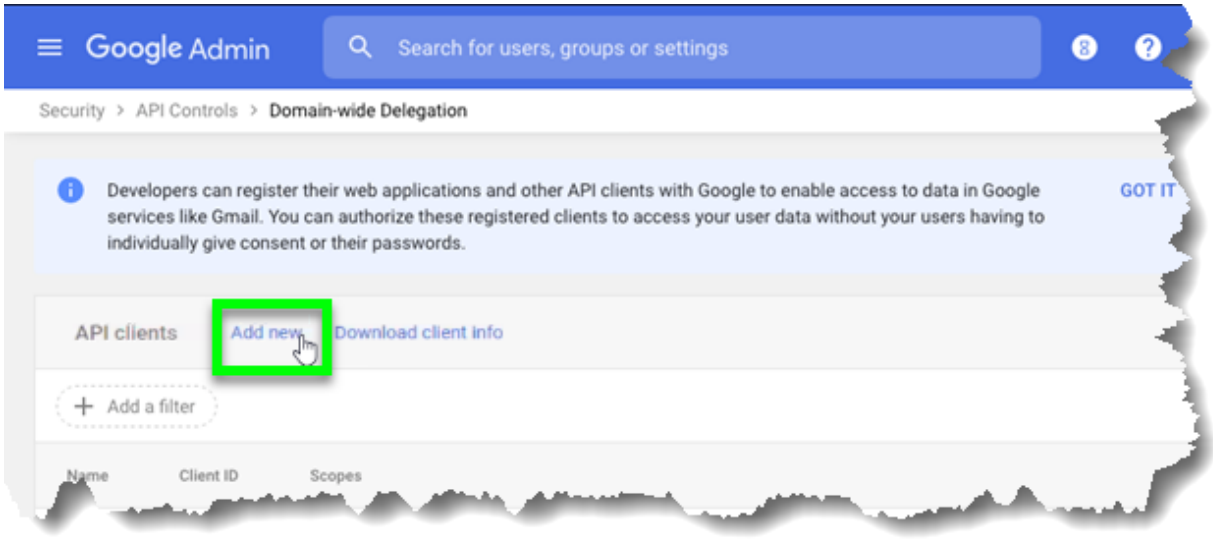
3. Using the Google Admin Console menu, navigate to the “Security” => “API controls” option.



4. From the API Controls page, locate the “Domain wide delegation” section and click on the “MANAGE DOMAIN WIDE DELEGATION” link.



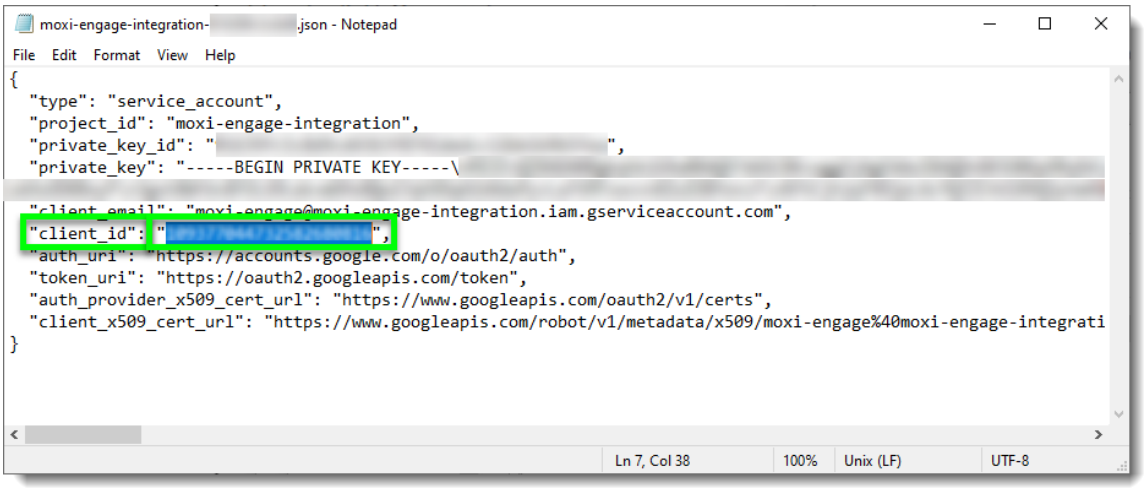
5. Click on the “Add new” link.



6. Locate the Moxi Engage service account client id in the JSON format credential file downloaded earlier:

   a. Open the JSON file in a text editor (e.g., *Notepad* if using Windows, *TextEdit* if using macOS).

   b. Find the “client_id” label in the text of the file.



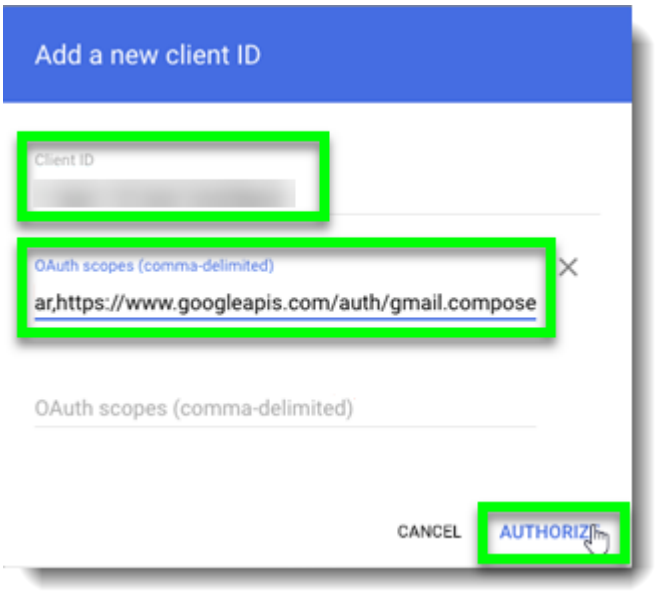
   c. Select the value for the “client_id” and copy it to your clipboard.

7. Paste the client-id obtained from the JSON file into the “Client ID” box.

8. Enter the following text exactly as it appears into the ”OAuth scopes (commadelimited)” field (you may copy and paste for accuracy):

```
https://www.google.com/m8/feeds,
https://www.googleapis.com/auth/calendar,
https://www.googleapis.com/auth/gmail.compose
```

9. Click on the “AUTHORIZE” button.



10. Verify that the Moxi Engage service account is displayed on the list of API clients.