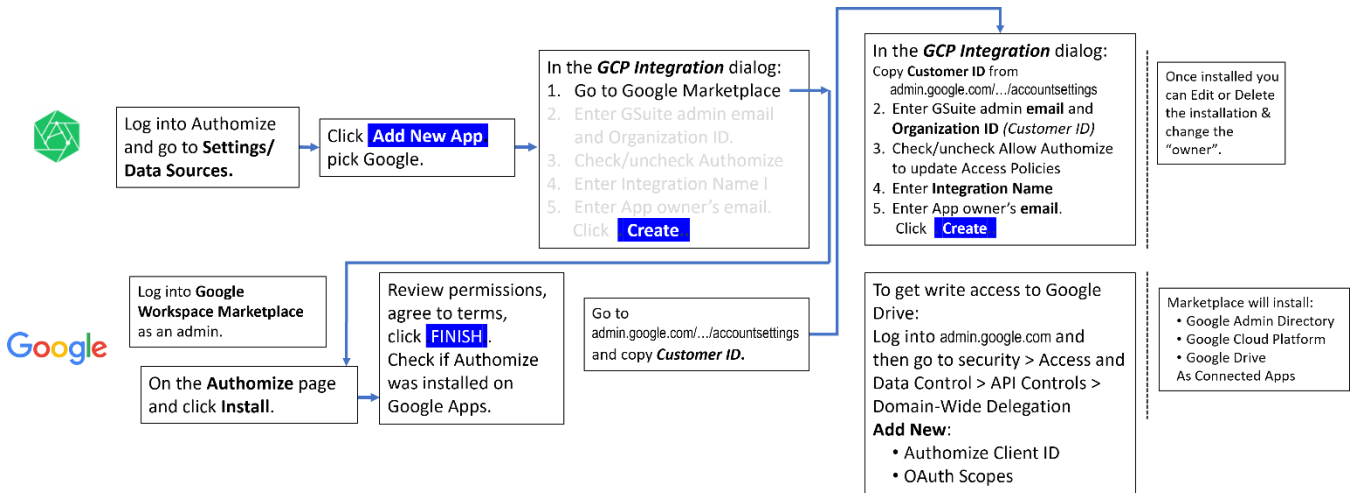# Integrating Google with Authomize

Integration with Google will provide visibility about your organization's identities and assets and their access across all of your Google stack, such as your cloud resources in GCP, your data in Google Drive, and your identities and their connected applications in your Google Admin Directory.
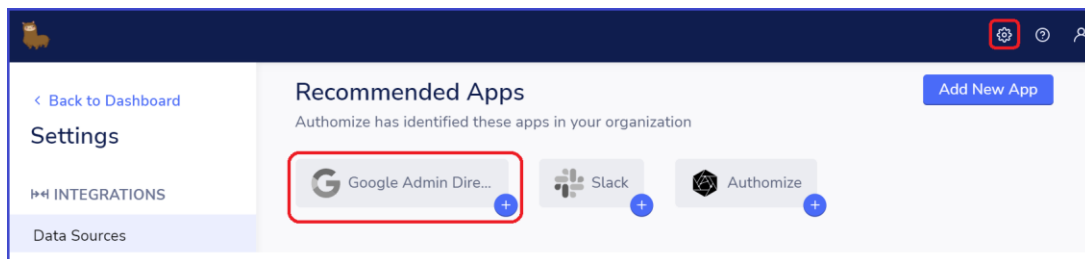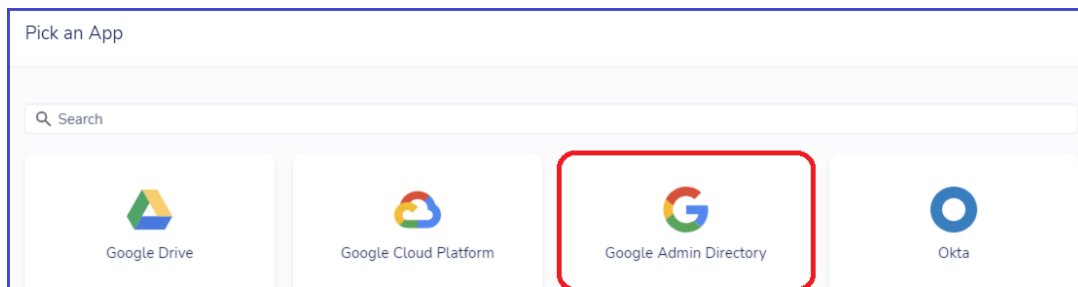
Google integration workflow

Installation

Start in Authomize

1. Log into **Authomize**
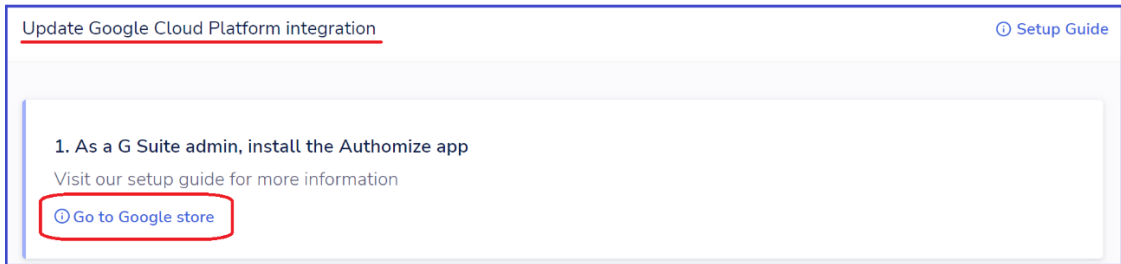2. Go to Settings/Data Sources and click **Google Admin Directory**.

3. Alternatively, click Add New App and then select the **Google Admin Directory**.

This opens the **Update Google Cloud Platform Integration** dialog.

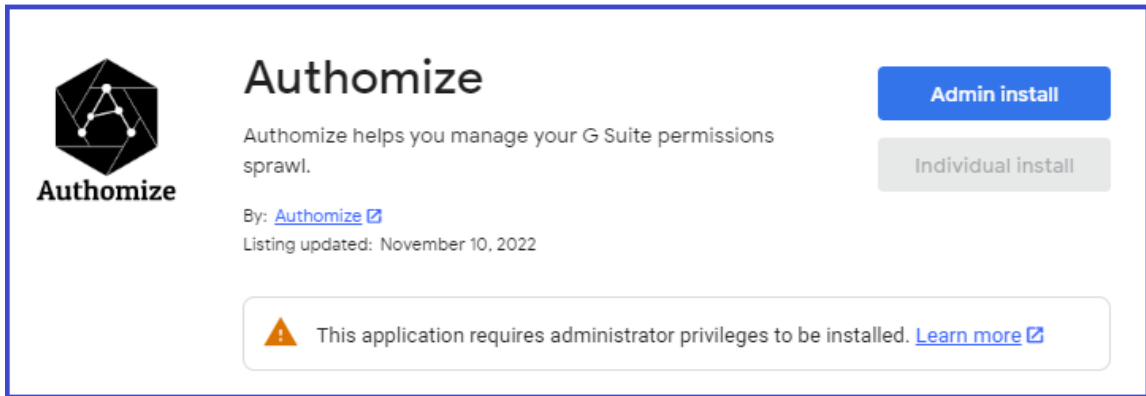4. In the Integrate Google Cloud Platform dialog:

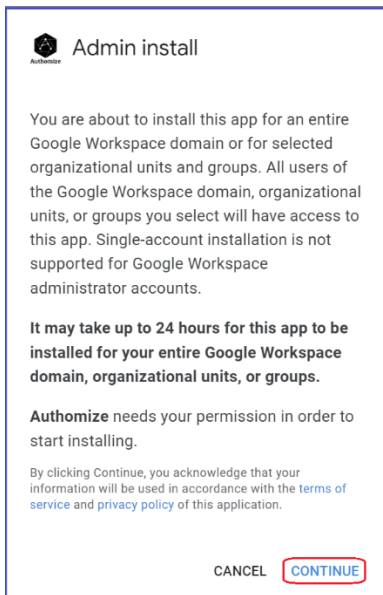**Step 1.** Click **`Go to Google store`**.

This open's Google's Marketplace (to the Authomize page).

Continue in Google Marketplace

1. On the Authomize page in GCP Marketplace (gsuite.google.com/u/0/marketplace/app/authomize/923330393623) click **Admin Install**.

If you agree to installing Authomize across your Google Workspace, click **Continue**.

2. At this point, a list of all the permissions needed by Authomize for the integration are displayed. To continue, click the agree checkbox and then click FINISH .

Note: You can use GCP to limit these further.

3. If, at this point, you go to Google Apps ( ), you will see that Authomize was installed.
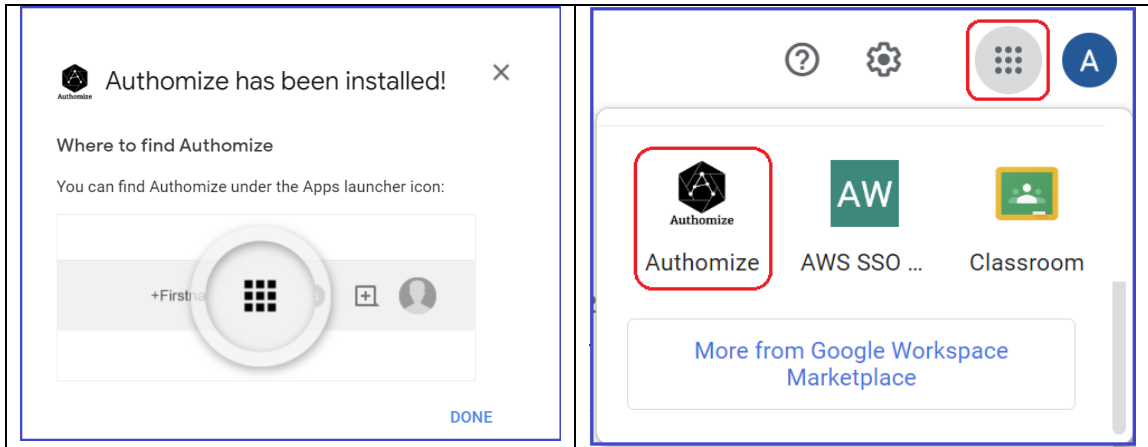
Return to Authomize GCP Integration page

4. Fill in the remaining steps with info from GCP.

Integrating Google with Authomize – 2.March.23

Step 2. Enter GSuite admin email address and Organization ID.

You can find your Customer ID at: **admin.google.com/u/1/ac/accountsettings**
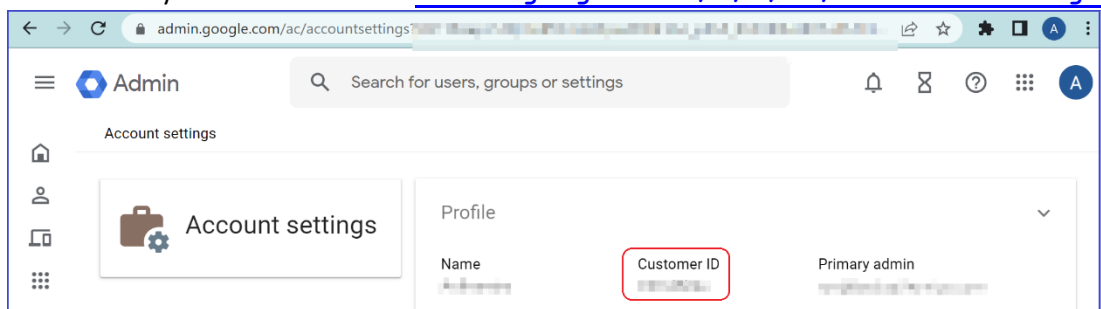
Step 3. Check/uncheck the Allow Authorize to update access policies.

Step 4. Enter a name for this integration

Step 5. Enter an integration owner's email.

Click **Integrate**

5. Integration will continue in the background. You can come back to check progress.at any time. When Google is integrated you will see three entries in your Connected Apps list.

What data is collected

Google Admin Directory
- User Data
    - User name
    - User admin roles
    - Last login
- User Groups
    - Group name
    - Group member name

Google Cloud Platform
- Cloud Assets
- GCP Account
- Server Names

Google Drive
- Personal drives
- Shared drive
- Files/Folders permissions
- Who has access to them

Google Calendar
- Personal calendar names
- Shared calendar names
- Who can see calendars

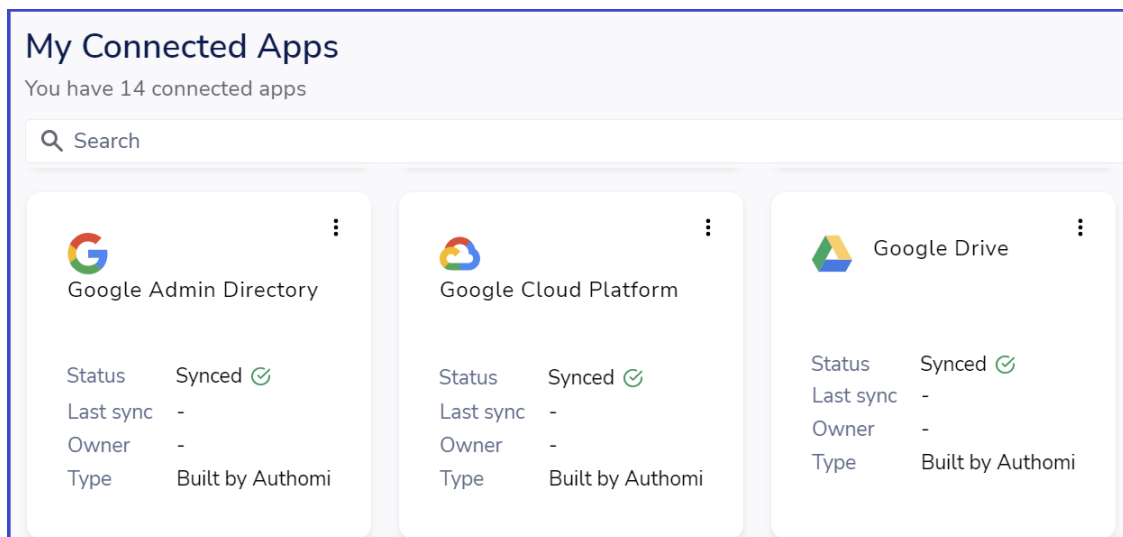# Enabling Write Access (File Share Removal Policies)

In order to enable file-sharing policies to take automatic remediation actions, Authomize needs write access to Google Drive. To do so:

1. Login to Google Admin console: https://admin.google.com.
2. Security -> Access and data control -> API controls -> Domain-wide Delegation
3. Click on **Add new** and add the following details:
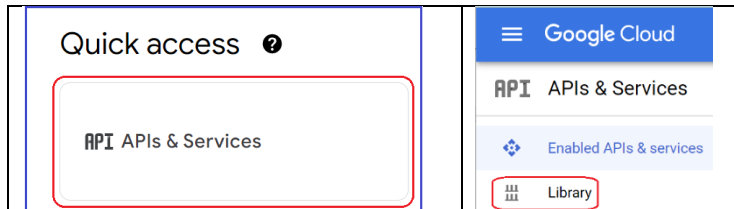   - Client ID: 117121108233648975035
    - OAuth scopes: https://www.googleapis.com/auth/drive
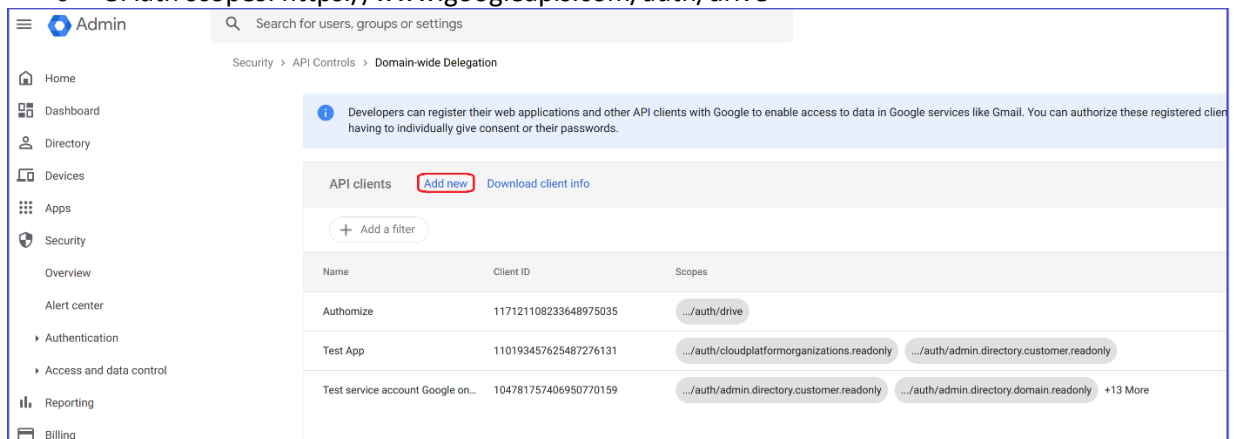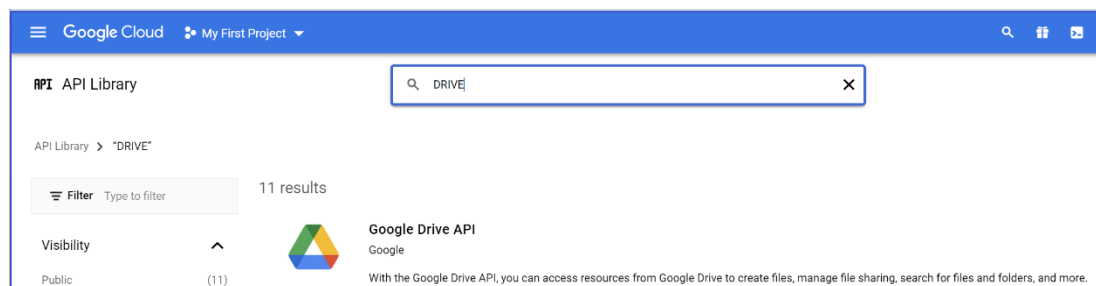

This additional set of permissions is used solely for revoking file shares.

Enabling Google APIs

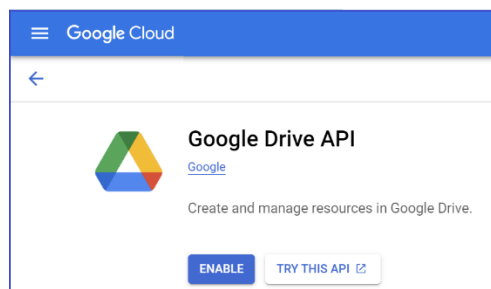If you need to enable Google APIs for your project, do this:

1. Go to console.cloud.google.com/
2. Click the **API & Services** button, and then go to the API **Library**.
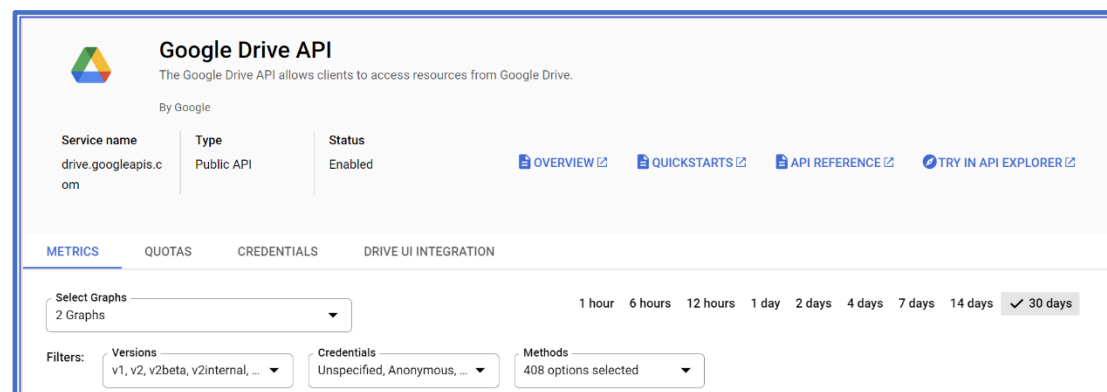

3. Search for one of the APIs you will need.

4. Click on it and **Enable** it.

5. If you succeeded, you will see this:

6. Repeat these steps for those services that you want Authomize to fetch data from, such as:
   - Admin SDK API
   - Cloud Resource Manager API
   - Cloud Asset APIs
   - Identity and Access Management APIs
   - Cloud Logging APIs