Google login Keys Setup Guide

Key Components:

1. Configure Google Login Keys
   1.1 Google Cloud Platform: Create Project & Configure Consent Screen
   1.2 Create Client Id and Secret Keys
   1.3 Create Developer Key
2. Testing the configuration

1. Configure Google Login keys

The admin can configure Google Login keys from **System Settings > Plugins > Social Login > Google Login > Settings**

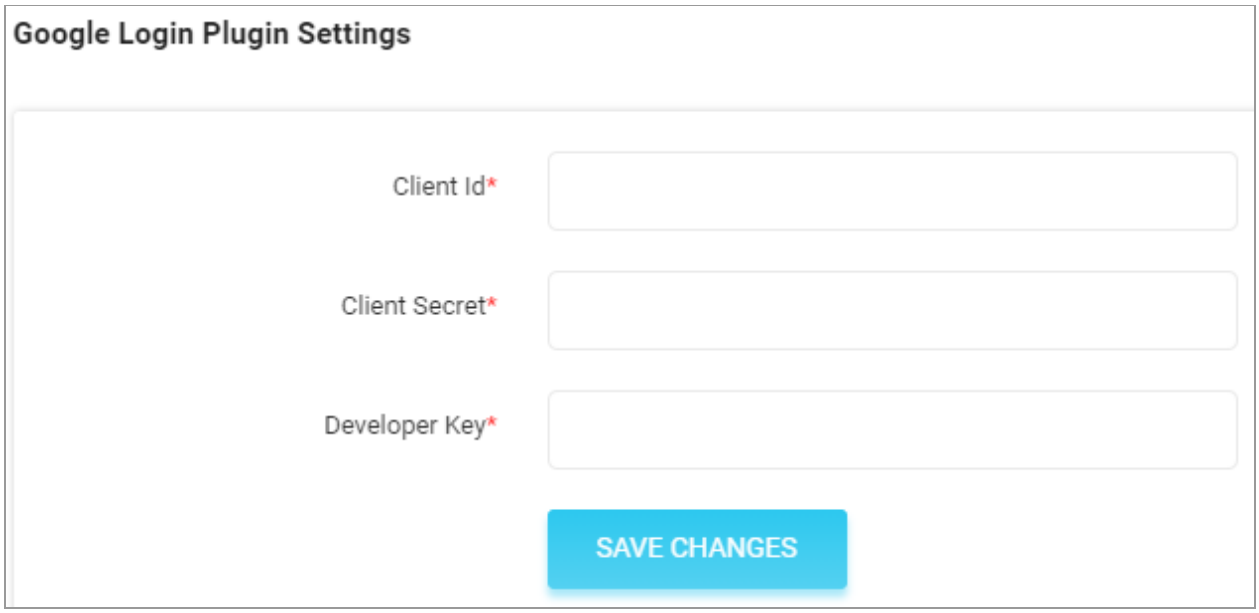

Fig. 1: Admin- Google Login Plugin Settings

The user must have a gmail account to proceed ahead. Log into your gmail account and then follow the below steps.

1.1 Google Cloud Platform: Create Project and Configure Consent Screen

NB: Please skip this step if you have already created a project and configured the consent screen linked with it. In this case, please select the appropriate project and then follow the steps provided in section 1.2 to create new client and secret keys.

i. Once logged into the google account, please visit https://console.developers.google.com/ to log into the **Google Cloud Platform**. As shown in figure 2, the dashboard will open on the screen.

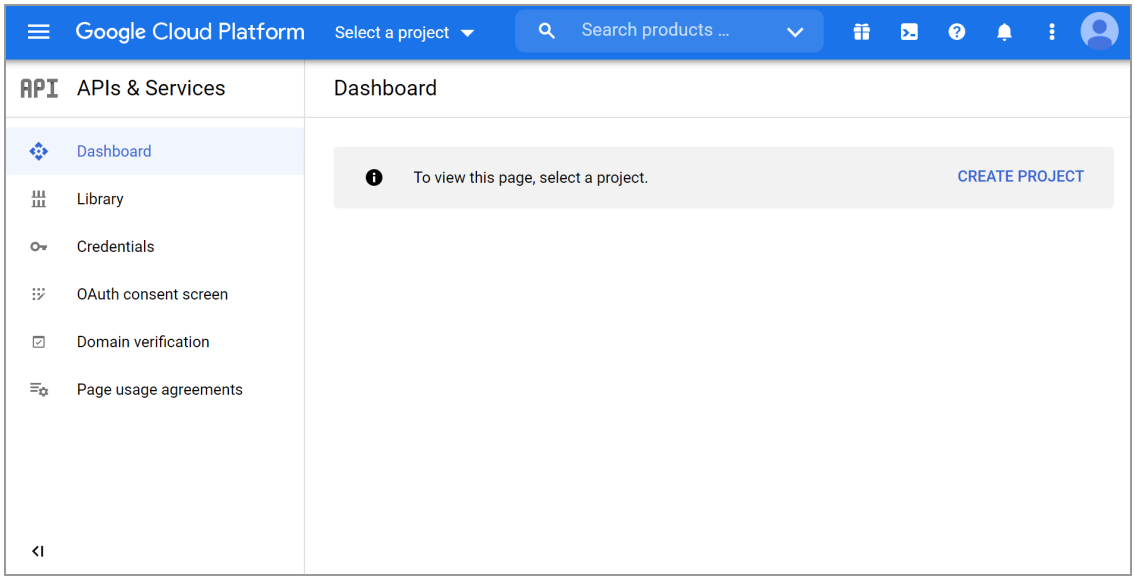

Fig. 2: Dashboard

ii. On the dashboard, please click on the '**Select a Project**' drop-down provided on the top-navigation panel. If no project has been created as shown in figure 3, click on the '**New Project**' button provided on the top-right corner.

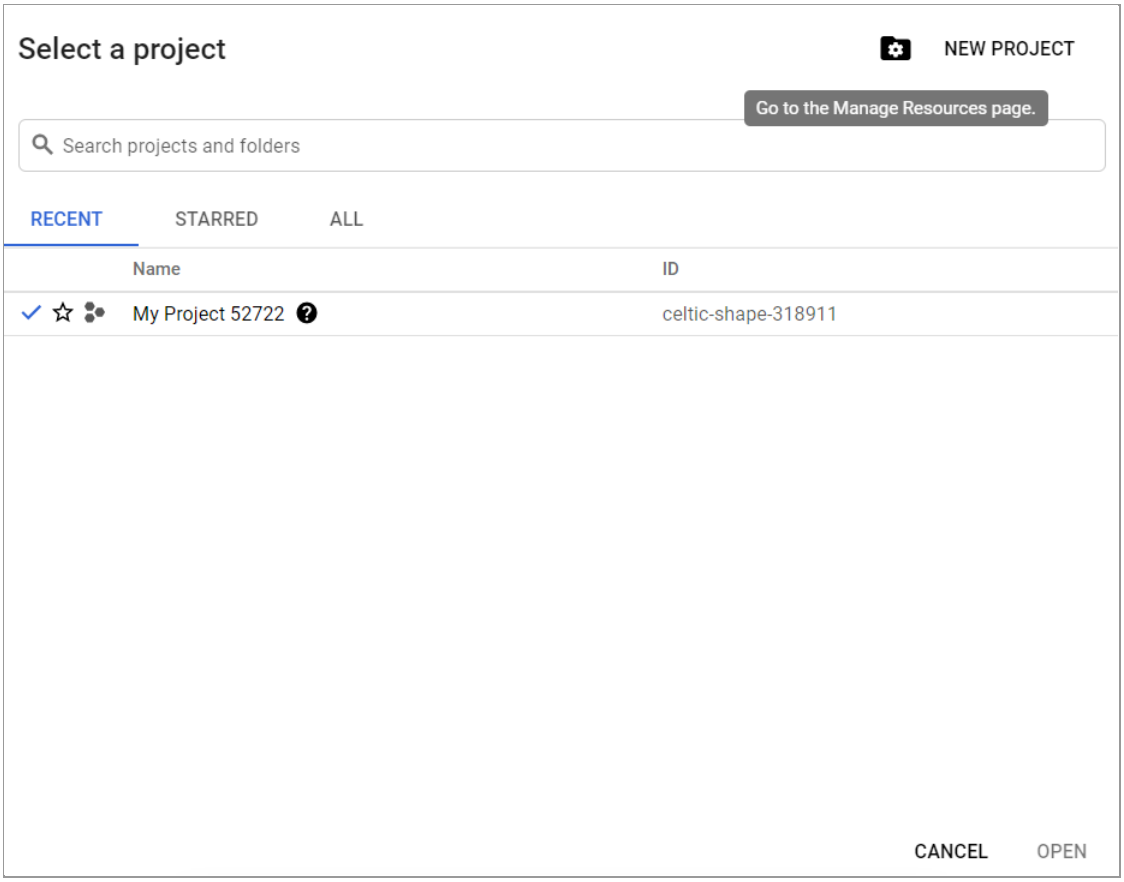

Fig. 3: Select a Project

iii. A '**New Project**' form will appear as shown in figure 4. Admin must:

- **Project Name*:** Enter a unique project name.
- **Organization*:** Select the organization in which you want to create a project. If you are a free trial user, skip this step, as this list does not appear.
- **Location*:** Enter the parent organization or folder. That resource will be the hierarchical parent of the new project.

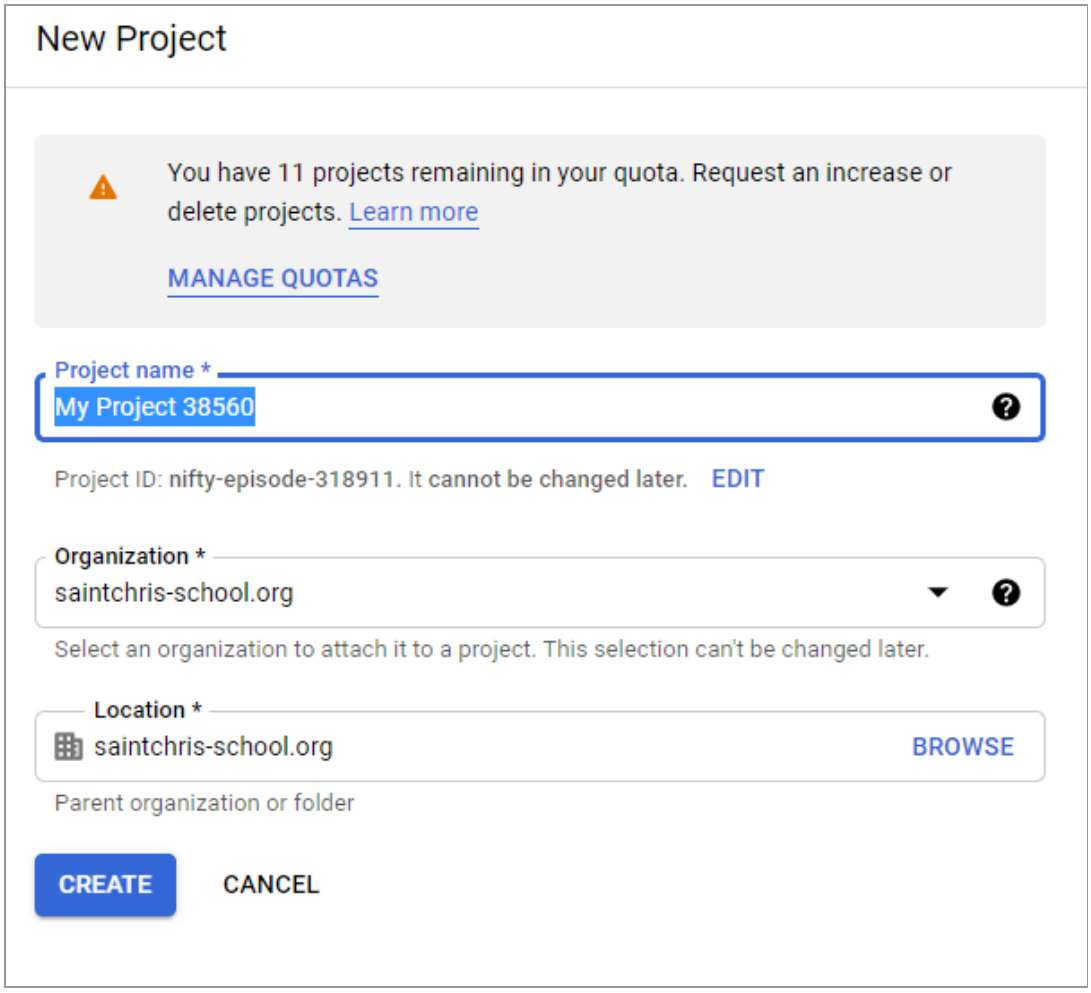

Fig. 4: Create New Project Form

Once the input fields have been entered, the admin must click on '**Create**' to add the new project.

iv. Now, please click on the '**Credentials**' tab from the side-navigation menu which will open the Credentials page as shown in the figure 5 below.

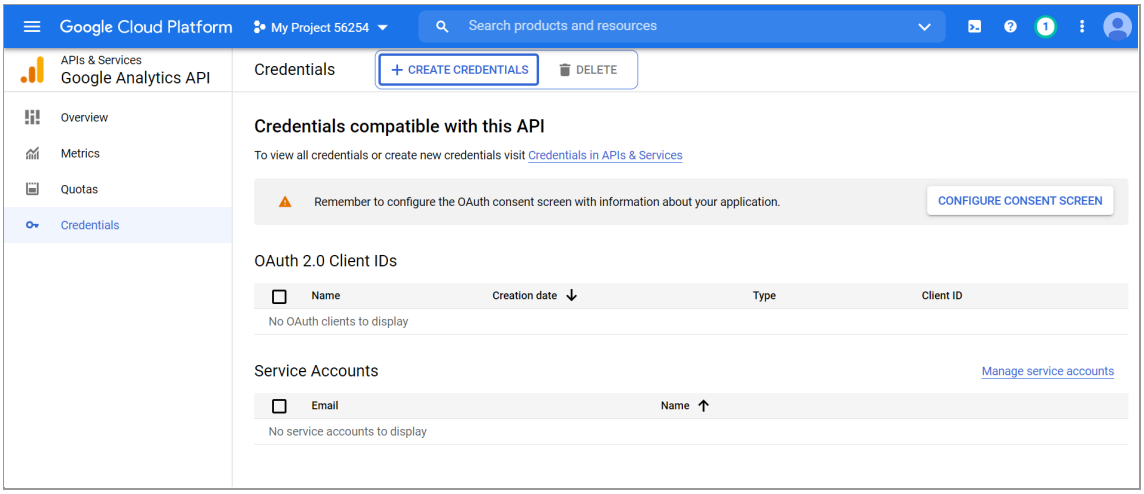

Fig. 5: Credentials Page

v. If **no Google services** have been used **previously**, the next step will be to '**Configure Consent Screen**'. However, if already using other google services, the Consent Screen needs **not** to be configured **again** due to which this button will **not** be displayed to such users.

To configure a consent screen, please click on the '**Configure Consent Screen**' button which will open the page displayed in figure 6.

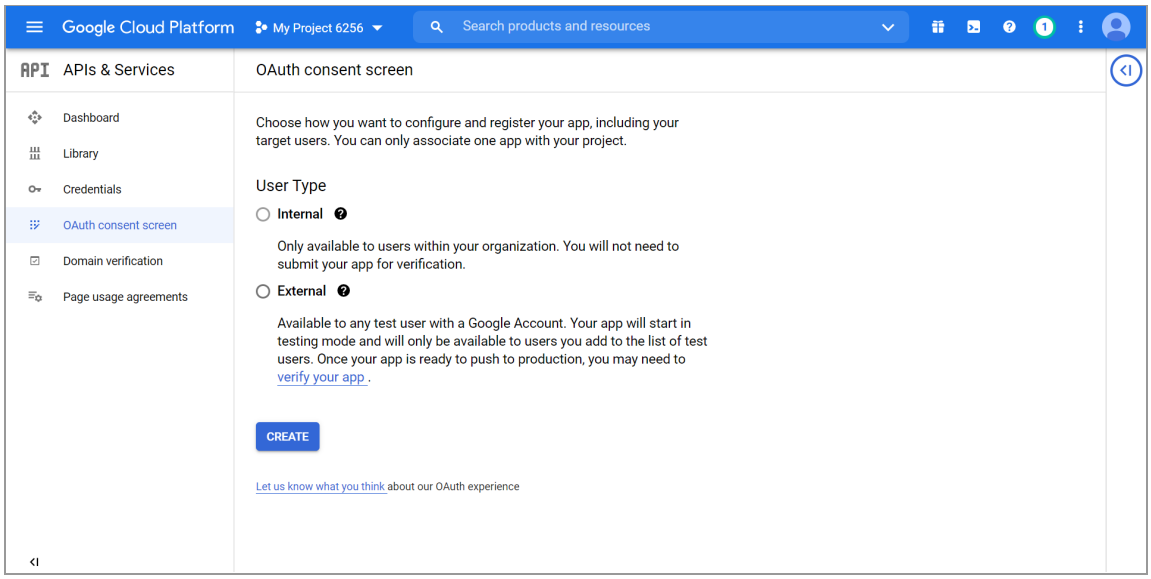

Fig. 6: OAuth Consent Screen Configuration page

Please select the **User Type** as '**Internal**' and then click on the '**Create**' button to proceed ahead (recommended for **Testing Mode**). Configuring **Internal** users will **limit authorization** requests to members of the organization. Additionally, there is **no** need to submit the **app for verification**.

Projects configured with a user type of **External** are available to any user with a Google Account (recommended for **Live Mode**). However, submitting your **app for verification** is **required** here once it is ready to be published.

vi. The admin will be redirected to the '**Edit App Registration**' form as shown in figure 7 below. This form includes **3 steps** that are explained ahead.

The **first** step is to configure '**OAuth Consent Screen**' that includes following sections -

i. **App Information:** Enter the mandatory fields that are **App Name** and **User Support Email**.
ii. **App Domain:** Enter the required application domains. The fields are not mandatory but the admin can enter the information to link their website with the analytics account.
iii. **Authorized Domains:** Click on '**Add Domain**' button to add authorized domain URLs.
iv. **Developer Contact Information:** Enter a valid email address that can be used by Google to send notifications.

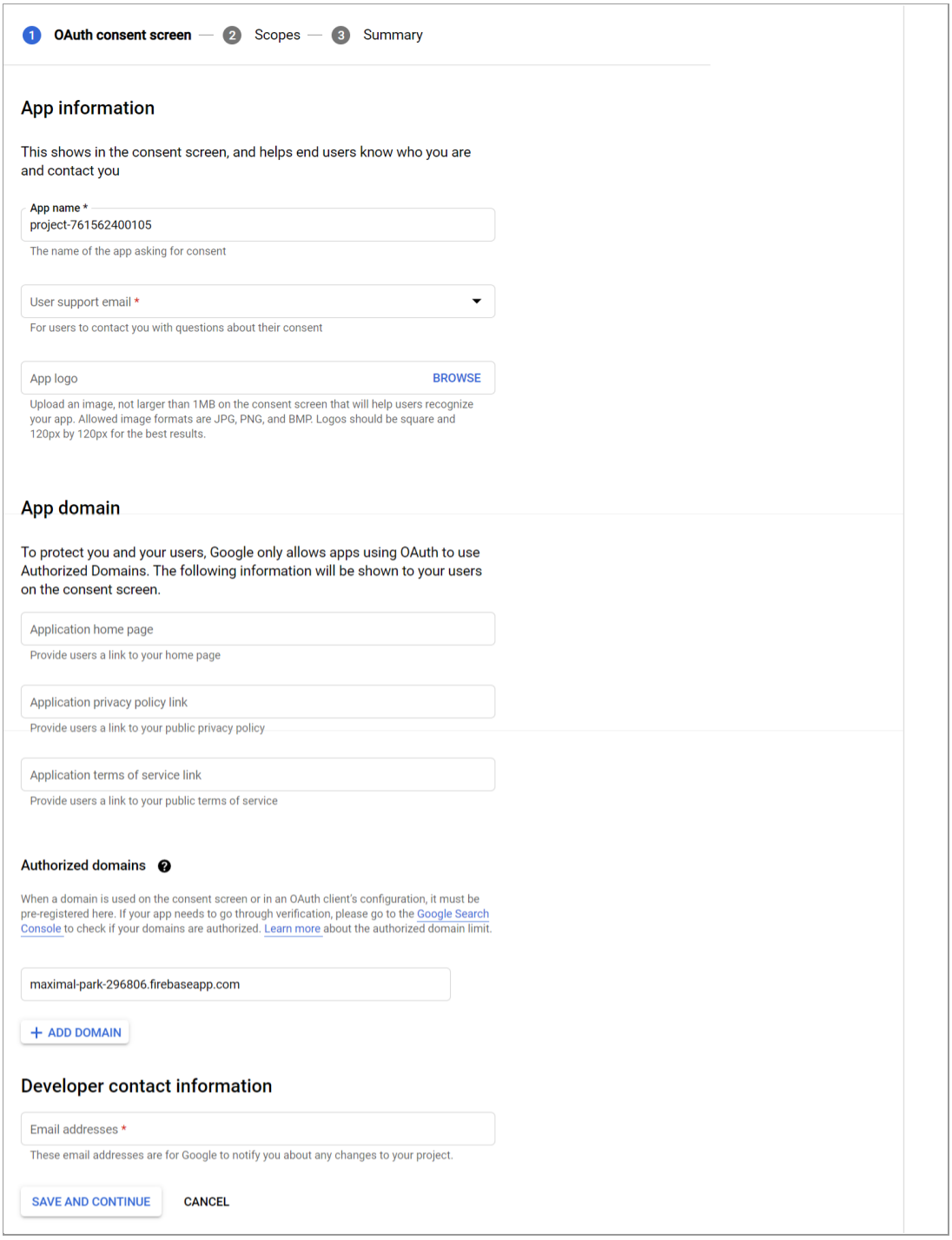

Fig. 7: OAuth Consent Screen

After adding all the necessary information, please click on the '**Save and Continue**' button.

vii. The **second** step is to add '**Scopes**'. The fields provided in this form are not mandatory. So, one can skip the step by clicking on '**Save and Continue**'.

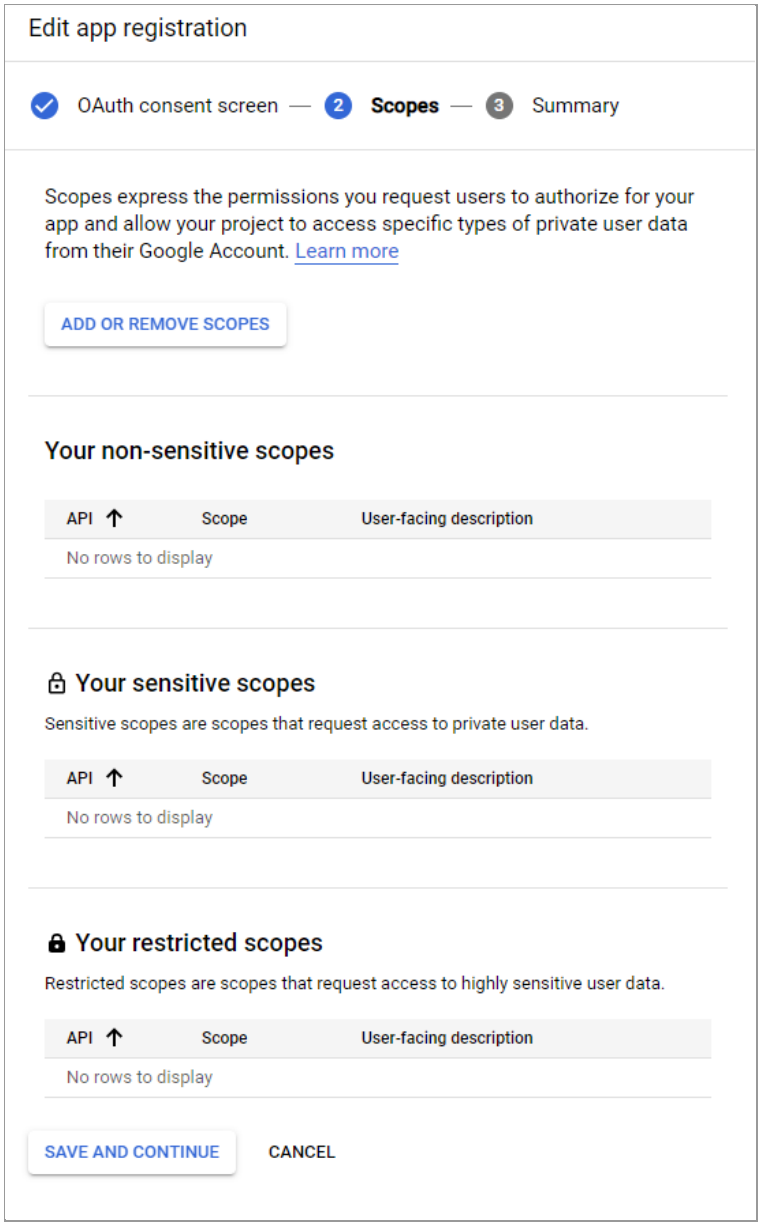

Fig. 8: Scopes

viii. The **third** step is to view the **Summary**.

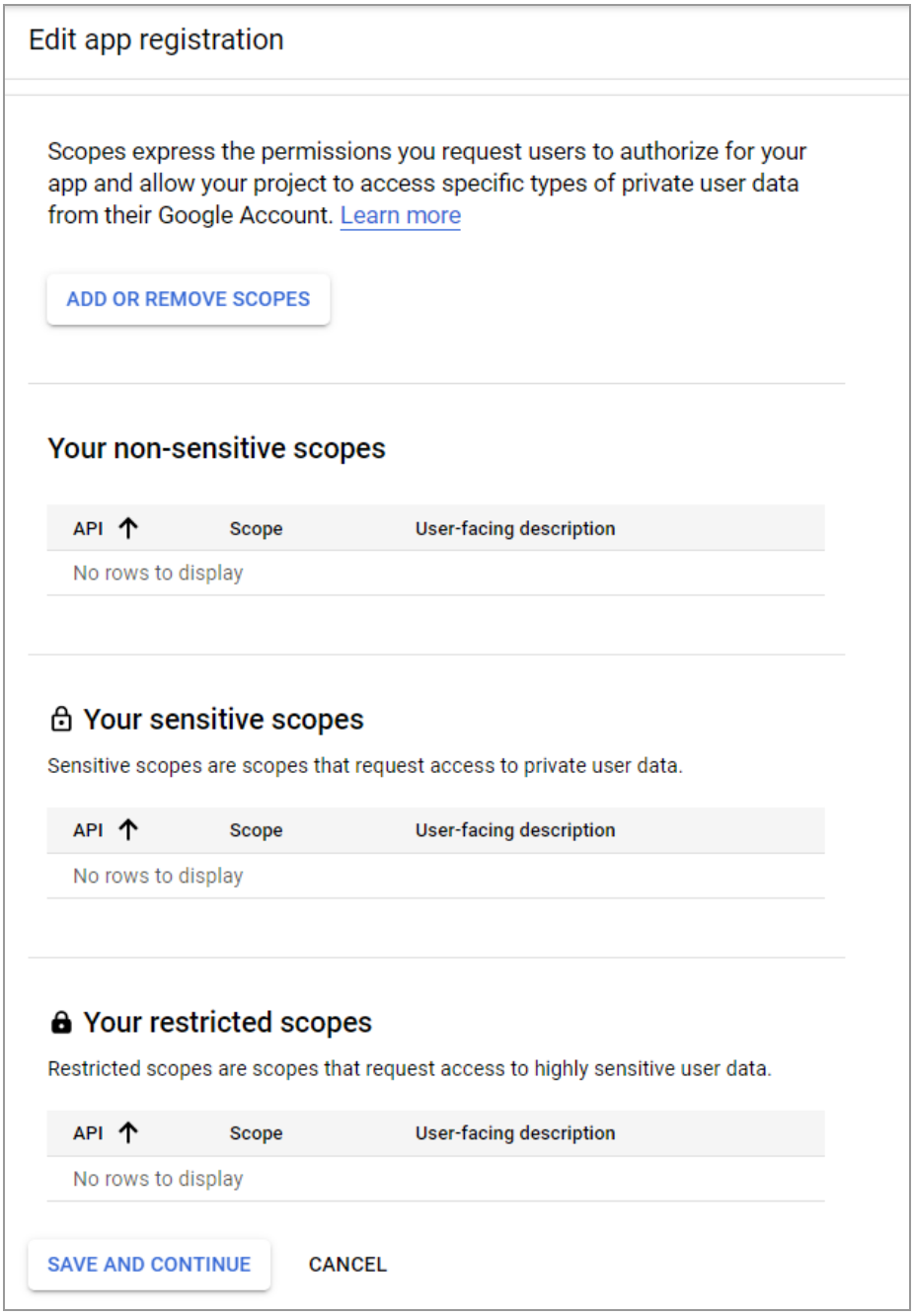

Fig. 9: Summary

Click on '**Save and Continue**' to complete the configuration process.

1.2 Create Client and Secret Keys

i. Now, please click on the '**Create Credentials**' button provided on the top-navigation bar of this page.

OR

Go to the **Credentials tab** provided in the left-side navigation bar and then click on '**Create Credentials**' button.

ii. Select '**OAuth Client ID**' from the drop-down list.

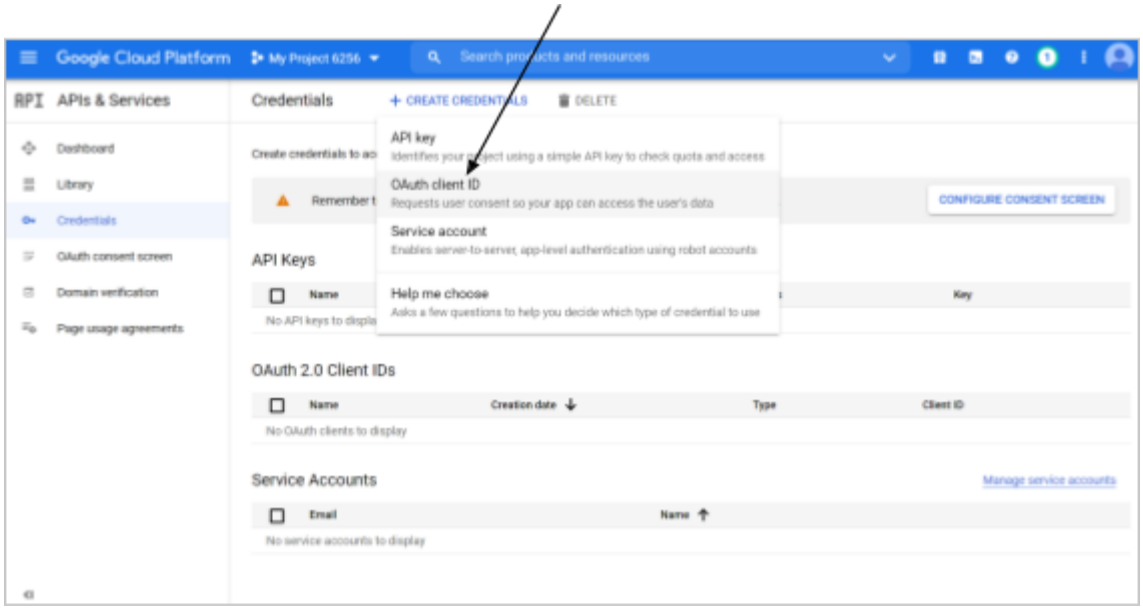

Fig. 10: Credentials Page

iii. The admin will be redirected to the '**Create OAuth Client ID**' page as shown in figure 11.

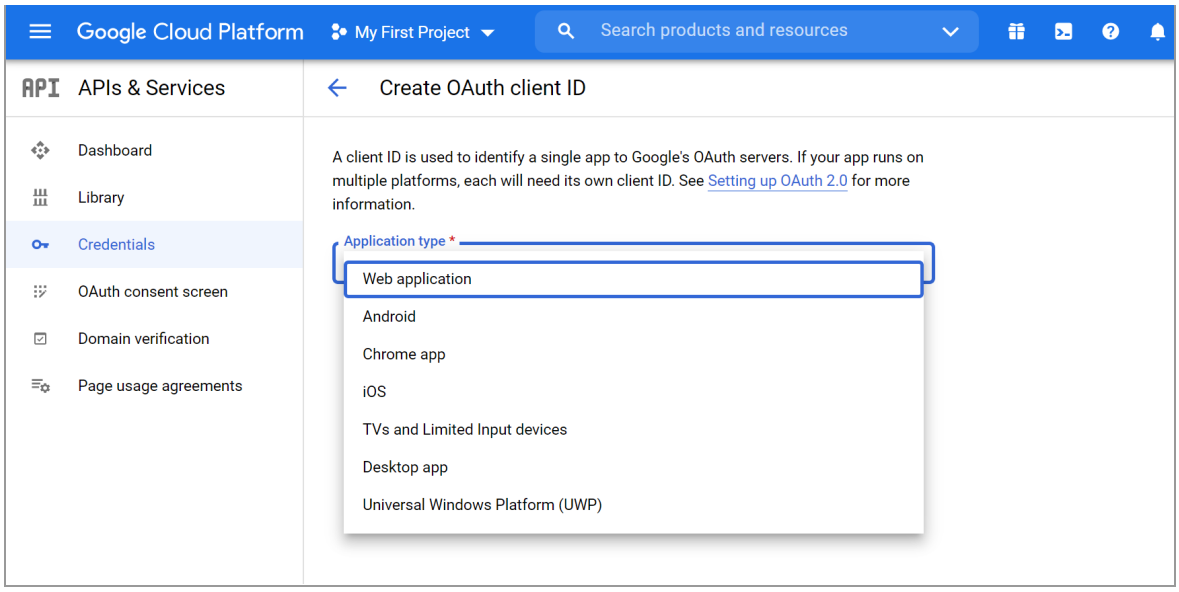

Fig. 11: 'Create OAuth Client ID' page

Admin must select the '**Application Type***' as '**Web Application**' from the drop-down list which will open an extended list as shown in figure 12, that is to be filled by admin.

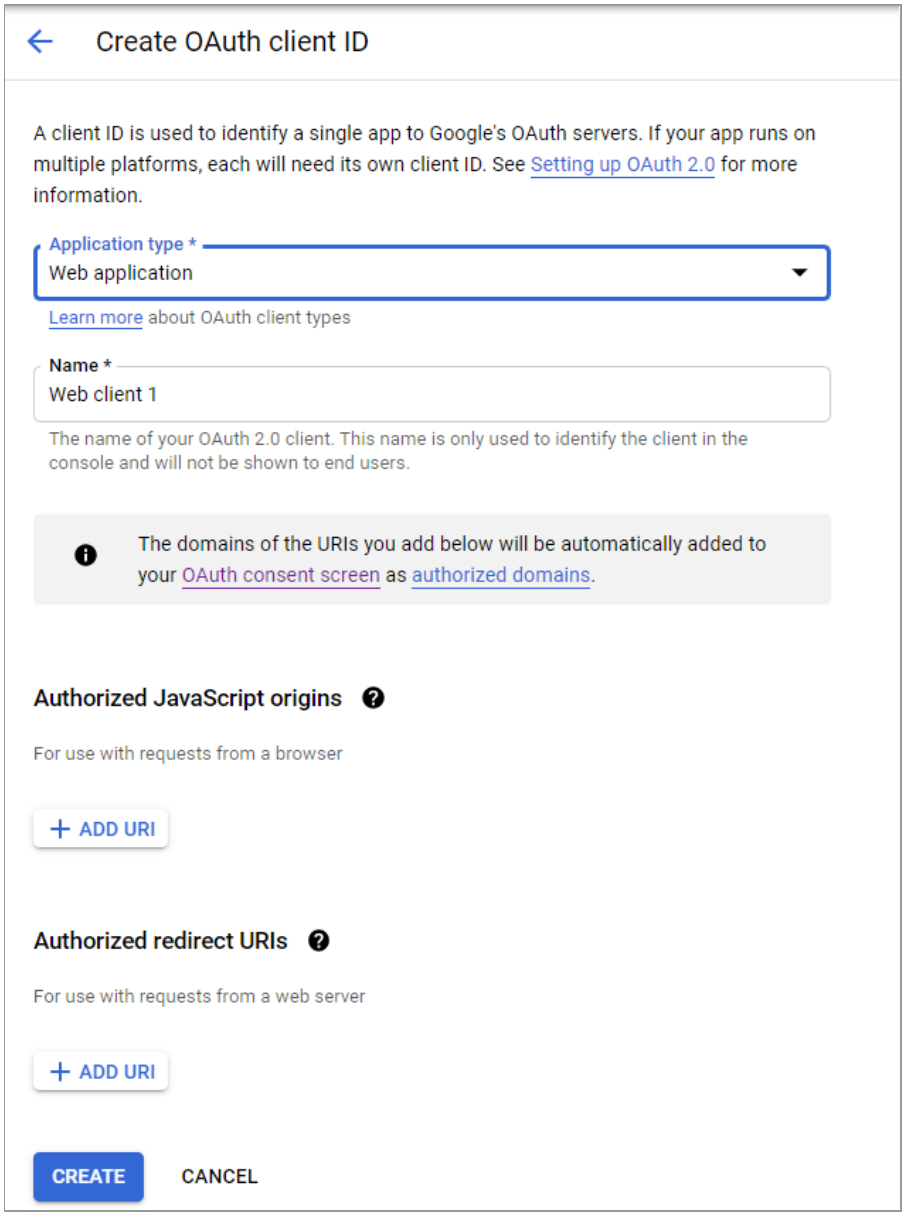

Fig. 12: 'Web Application' for 'Create OAuth Client ID'

Please add the following information in the form fields provided below-

- **Name:** Enter a **Name** for their client Id. To avoid confusions when generating multiple API keys, it is **recommended** to assign the **same name** to the key **as that of the application name**. For instance, when creating a separate key for Google Sign In, its name can be entered as 'Google Login' when generating it.

- **Authorizer JavaScript origins:** Add domain name with format – http://domainname.com or https://domainname.com (for SSL certificate enabled on server).
- **Authorized Redirect URIs:** Add callback URI on which it will redirect you back and provide merchant account details. The format to be used: http://domainname.com/public/index.php?url=google-login/index or https://domainname.com/public/index.php?url=google-login/index (if SSL certificate enabled on server).

iv. After entering the details, please click on '**Create**' which will create the **Client ID** and **Secret Key** and display them in a pop-up box as shown in figure 13.

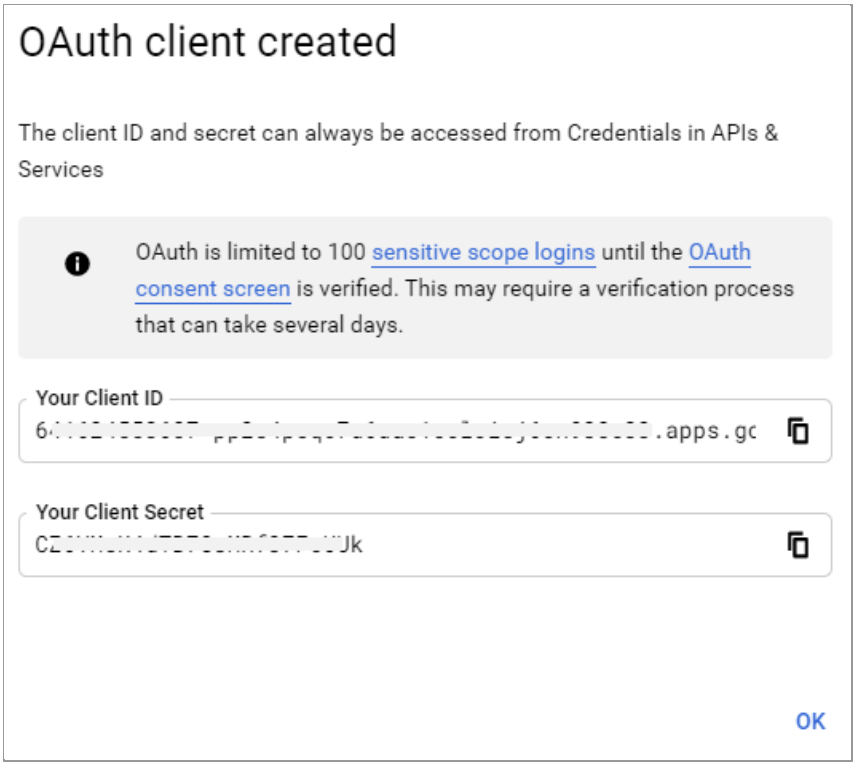

Fig. 13: OAuth Client Created

v. The keys generated will also appear on the **'Credentials'** page as shown in figure 14.

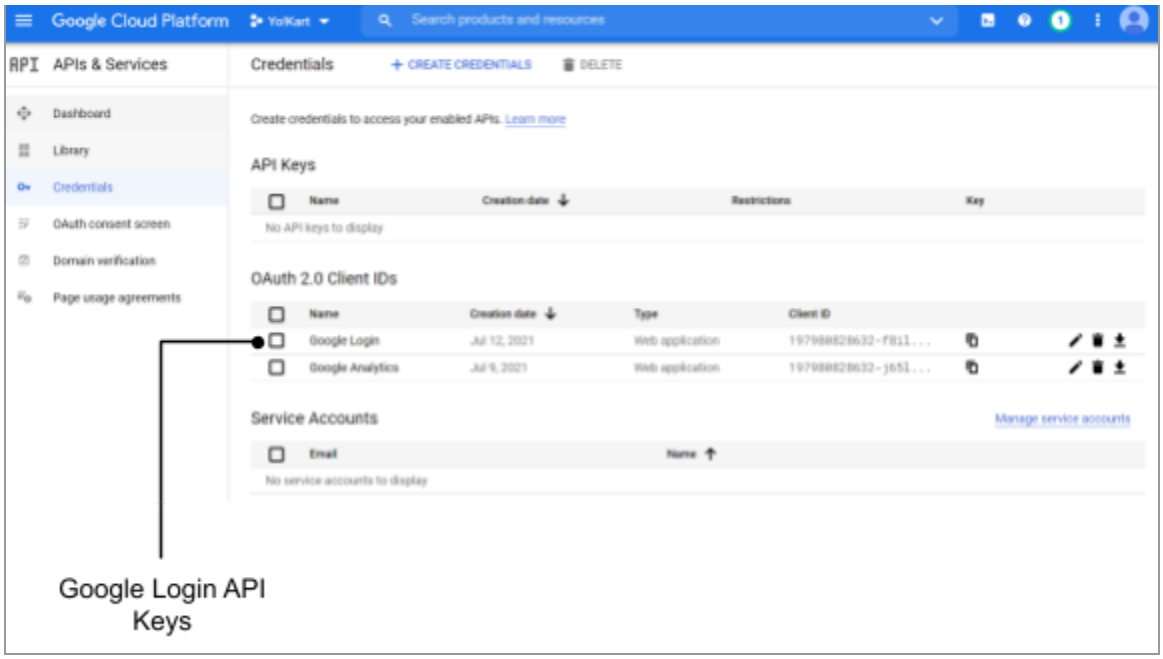

Fig. 14: Credentials Page

The generated keys must be copied and pasted by the admin into respective input-fields as shown in figure 1.

1.3 Create Developer Key

i. On the Google Cloud Platform panel, please click on the '**Create Credentials**' button and then select '**API Key**' from the drop-down list.

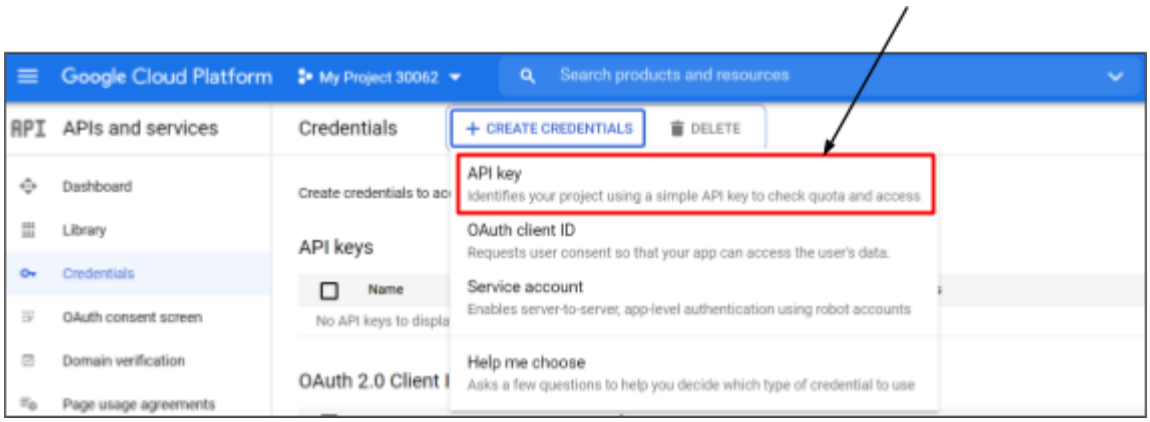

Fig. 15: Credentials Page

ii. A pop-up will appear displaying the newly created API key.

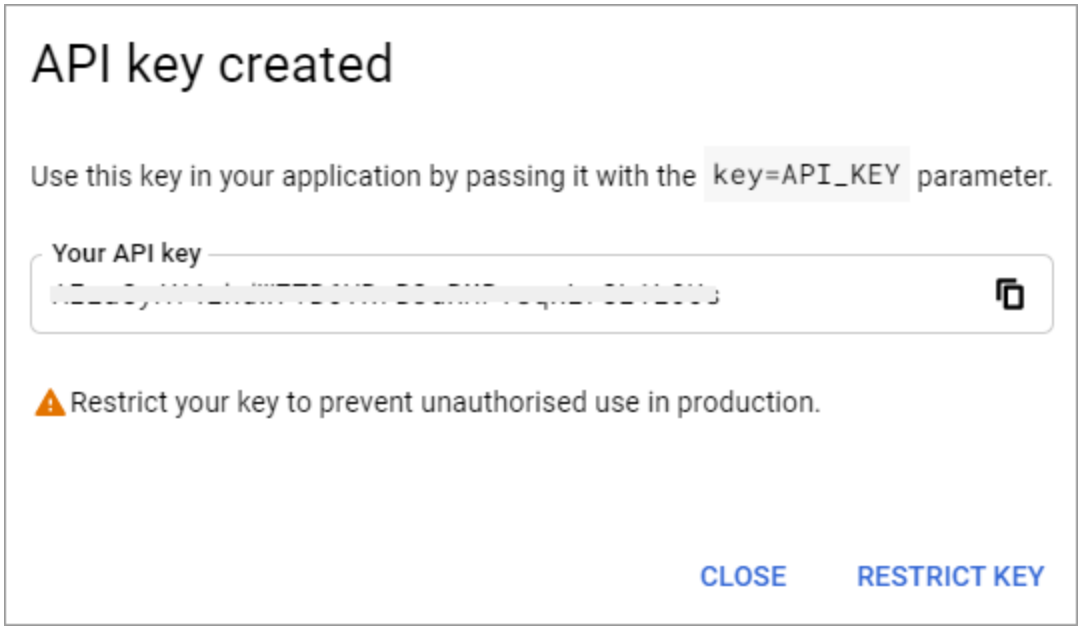

Fig. 16: API Key Created

Please **copy** the key and paste it in the **Developer Key** input field provided under **Google Login plugin** settings provided in the admin panel as shown in figure 1.

The '**Developer Key**' can also directly be copied by clicking on icon provided to its right on the '**Credentials**' page under **API keys** section.

NB: Please note that an already existing developer key can be used twice as well. So, if you have created a developer key when configuring Google Shopping Feed, the same developer key can be used for Google Login as well. However, creating a separate key helps track activities of that plugin in the console, due to which it is recommended to create separate keys for different plugins.

2. Testing the Configuration

To check if the **Google Login** is working correctly, please visit the login/signup page and click on the Google Login button being displayed in the form as shown in the figure 17 below.

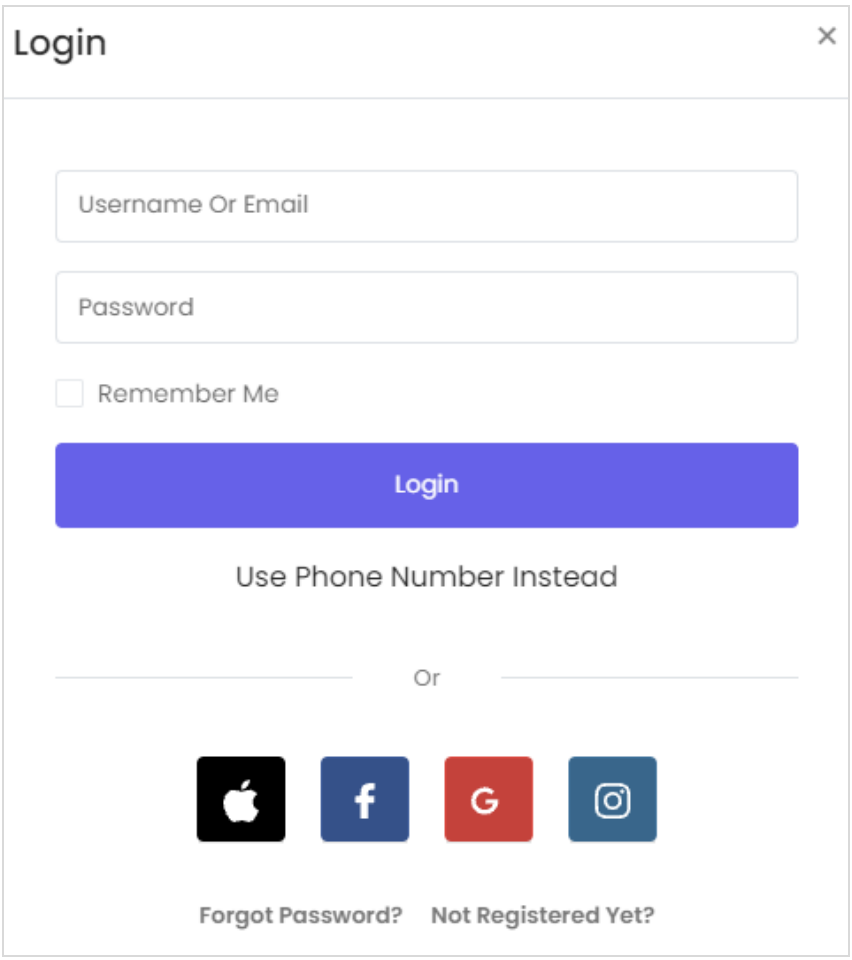

Fig. 17: Private Key Saved To Your Computer

Now, try to login with a google account. If the user logged in as a buyer, this means that the keys are configured correctly.