

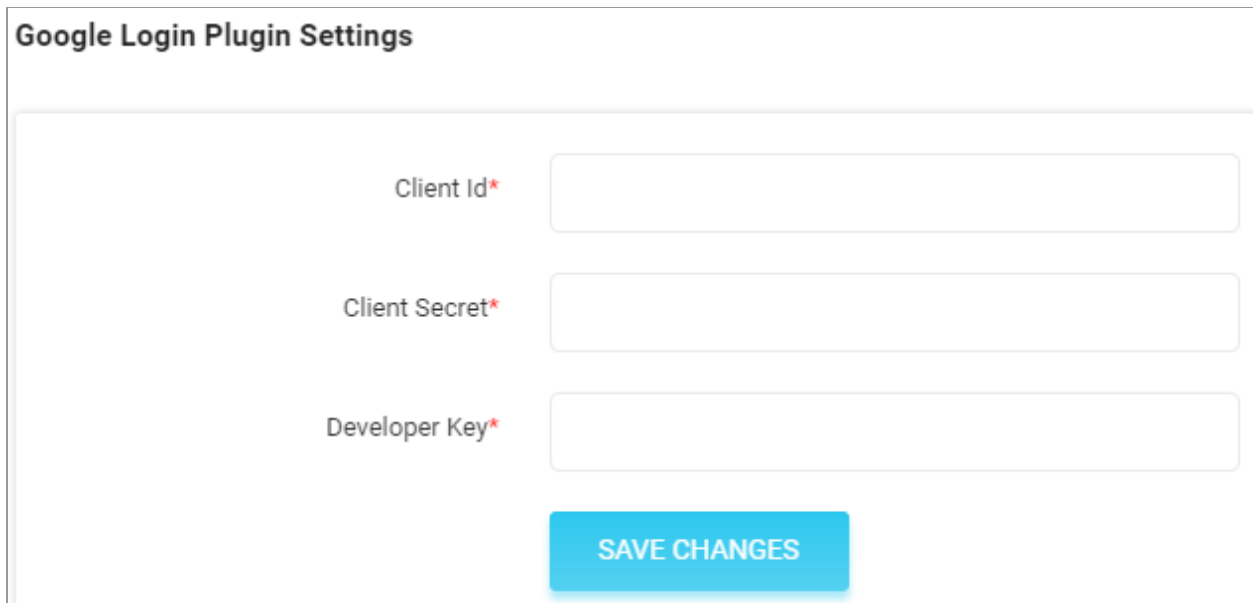
Google login Keys Setup Guide

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**



Google Login Plugin Settings

Client Id*

Client Secret*

Developer Key*

SAVE CHANGES

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.

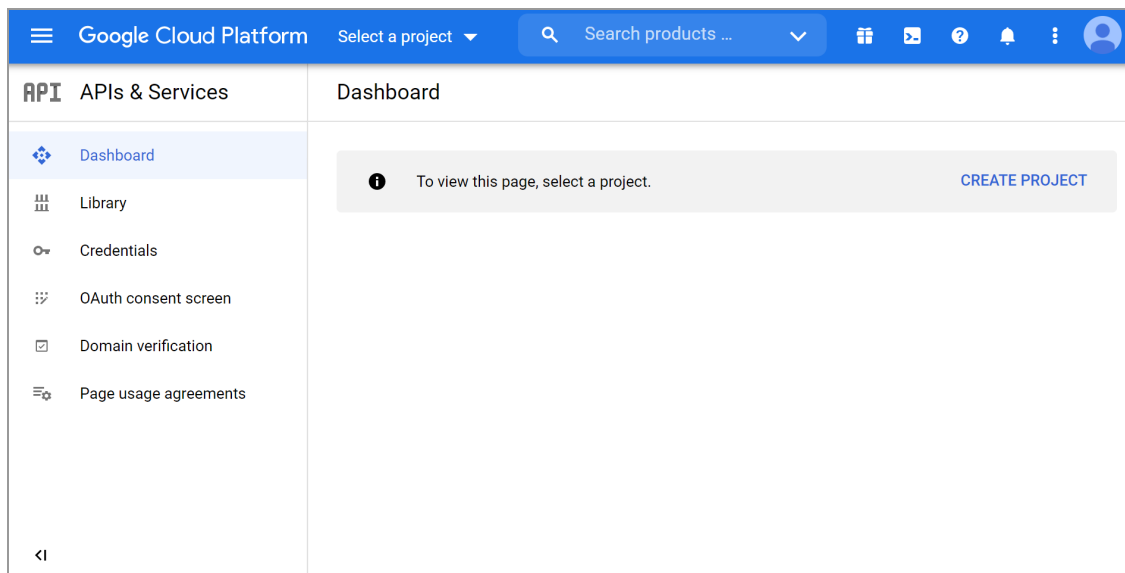


Fig. 2: Dashboard

- 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.

Select a project

NEW PROJECT

Go to the Manage Resources page.

Search projects and folders

RECENT STARRED ALL

Name	ID
✓ ☆ ● My Project 52722 ?	celtic-shape-318911

CANCEL OPEN

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.

New Project

⚠ You have 11 projects remaining in your quota. Request an increase or delete projects. [Learn more](#)

[MANAGE QUOTAS](#)

Project name * ?

Project ID: nifty-episode-318911. It cannot be changed later. [EDIT](#)

Organization * ▼ ?

Select an organization to attach it to a project. This selection can't be changed later.

Location * [BROWSE](#)

Parent organization or folder

[CREATE](#) [CANCEL](#)

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.

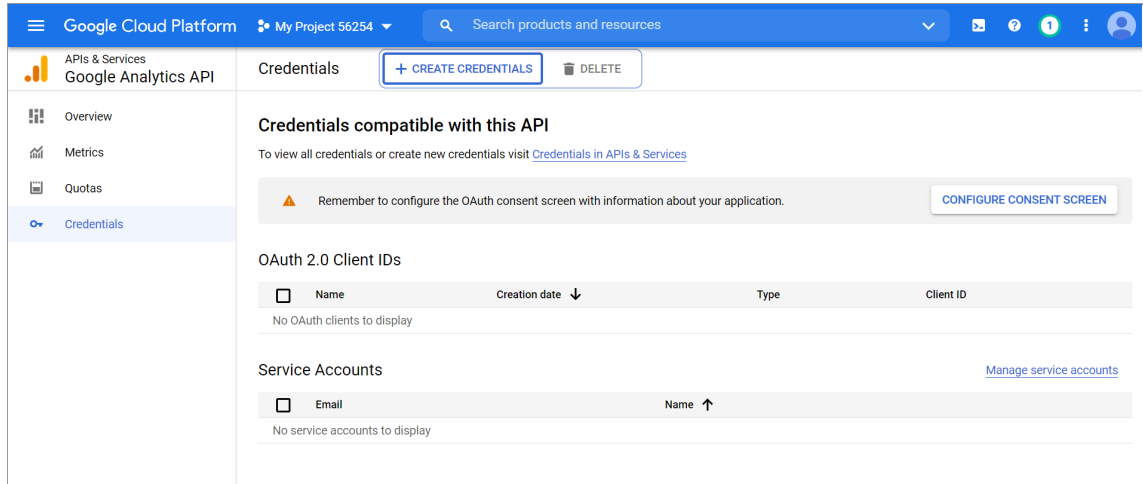


Fig. 5: Credentials Page

- 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.

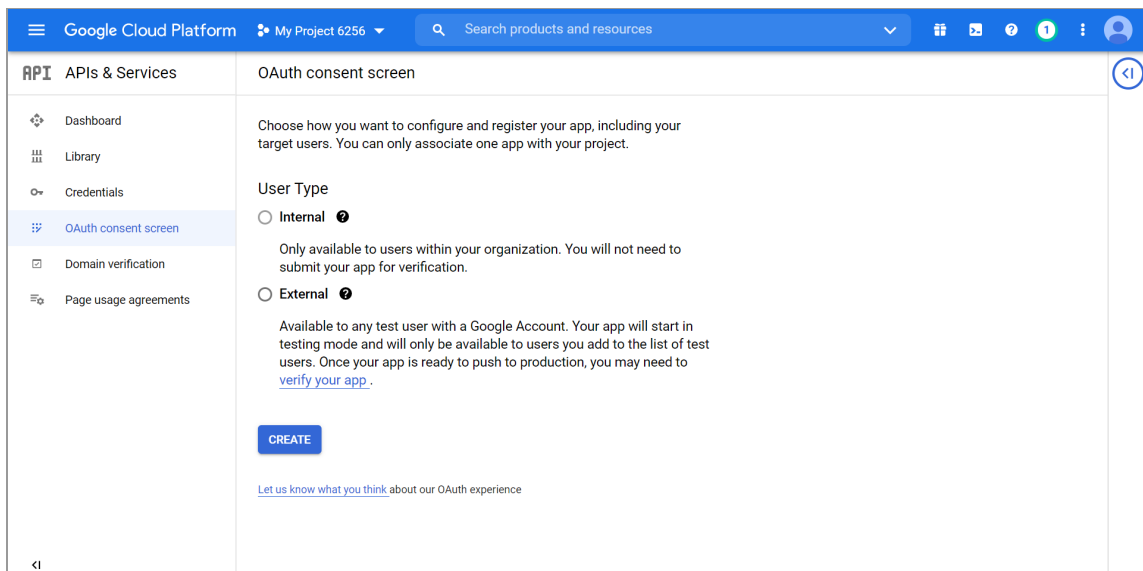


Fig. 6: OAuth Consent Screen Configuration page

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.

1 OAuth consent screen — 2 Scopes — 3 Summary

App information

This shows in the consent screen, and helps end users know who you are and contact you

App name *
project-761562400105
The name of the app asking for consent

User support email *
For users to contact you with questions about their consent

App logo [BROWSE](#)
Upload an image, not larger than 1MB on the consent screen that will help users recognize your app. Allowed image formats are JPG, PNG, and BMP. Logos should be square and 120px by 120px for the best results.

App domain

To protect you and your users, Google only allows apps using OAuth to use Authorized Domains. The following information will be shown to your users on the consent screen.

Application home page
Provide users a link to your home page

Application privacy policy link
Provide users a link to your public privacy policy

Application terms of service link
Provide users a link to your public terms of service

Authorized domains

When a domain is used on the consent screen or in an OAuth client's configuration, it must be pre-registered here. If your app needs to go through verification, please go to the [Google Search Console](#) to check if your domains are authorized. [Learn more](#) about the authorized domain limit.

maximal-park-296806.firebaseio.com

[+ ADD DOMAIN](#)

Developer contact information

Email addresses *
These email addresses are for Google to notify you about any changes to your project.

[SAVE AND CONTINUE](#) [CANCEL](#)

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**'.

Edit app registration

✓ OAuth consent screen — 2 **Scopes** — 3 Summary

Scopes express the permissions you request users to authorize for your app and allow your project to access specific types of private user data from their Google Account. [Learn more](#)

[ADD OR REMOVE SCOPES](#)

Your non-sensitive scopes

API ↑	Scope	User-facing description
No rows to display		

Your sensitive scopes

Sensitive scopes are scopes that request access to private user data.

API ↑	Scope	User-facing description
No rows to display		

Your restricted scopes

Restricted scopes are scopes that request access to highly sensitive user data.

API ↑	Scope	User-facing description
No rows to display		

[SAVE AND CONTINUE](#) CANCEL

Fig. 8: Scopes

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

Edit app registration

Scopes express the permissions you request users to authorize for your app and allow your project to access specific types of private user data from their Google Account. [Learn more](#)

ADD OR REMOVE SCOPES

Your non-sensitive scopes

API ↑	Scope	User-facing description
No rows to display		

Your sensitive scopes

Sensitive scopes are scopes that request access to private user data.

API ↑	Scope	User-facing description
No rows to display		

Your restricted scopes

Restricted scopes are scopes that request access to highly sensitive user data.

API ↑	Scope	User-facing description
No rows to display		

SAVE AND CONTINUE CANCEL

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.

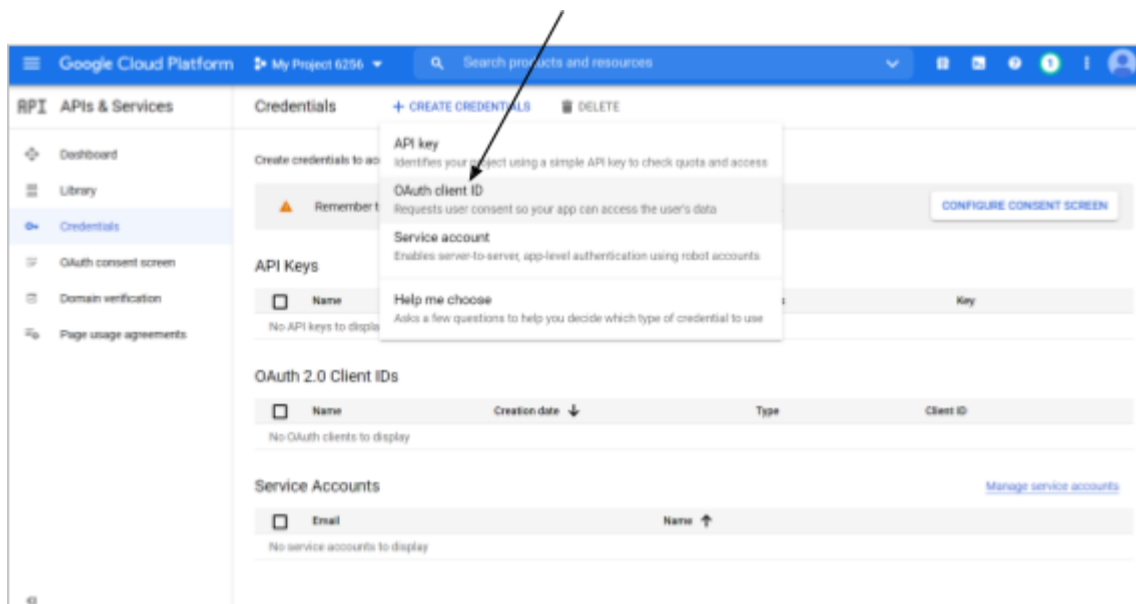


Fig. 10: Credentials Page

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

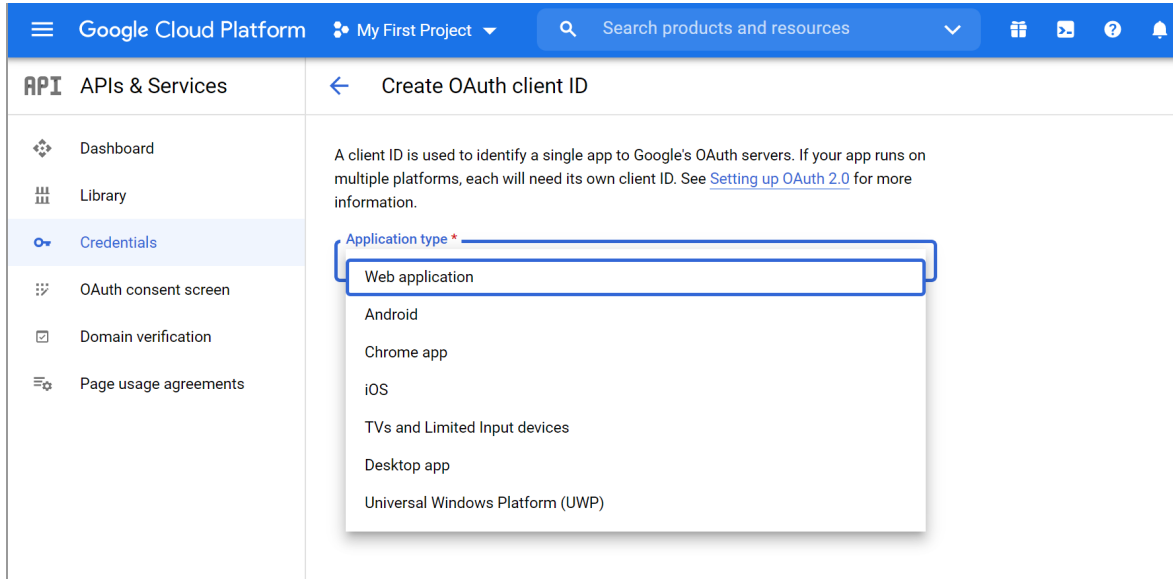


Fig. 11: 'Create OAuth Client ID' page

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.

Setting up OAuth 2.0 for more information.' The form contains several fields: 'Application type *' is a dropdown menu with 'Web application' selected; below it is a link 'Learn more about OAuth client types'; 'Name *' is a text input field containing 'Web client 1', with a note below it stating 'The name of your OAuth 2.0 client. This name is only used to identify the client in the console and will not be shown to end users.'; a grey informational box with an 'i' icon states 'The domains of the URIs you add below will be automatically added to your [OAuth consent screen](#) as [authorized domains](#).'; 'Authorized JavaScript origins ?' is a section with a help icon and the text 'For use with requests from a browser', containing a '+ ADD URI' button; 'Authorized redirect URIs ?' is a section with a help icon and the text 'For use with requests from a web server', also containing a '+ ADD URI' button; and at the bottom are 'CREATE' and 'CANCEL' buttons."/>

← Create OAuth client ID

A client ID is used to identify a single app to Google's OAuth servers. If your app runs on multiple platforms, each will need its own client ID. See [Setting up OAuth 2.0](#) for more information.

Application type *
Web application

[Learn more](#) about OAuth client types

Name *
Web client 1

The name of your OAuth 2.0 client. This name is only used to identify the client in the console and will not be shown to end users.

i The domains of the URIs you add below will be automatically added to your [OAuth consent screen](#) as [authorized domains](#).

Authorized JavaScript origins ?
For use with requests from a browser

+ ADD URI

Authorized redirect URIs ?
For use with requests from a web server

+ ADD URI

CREATE CANCEL

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.

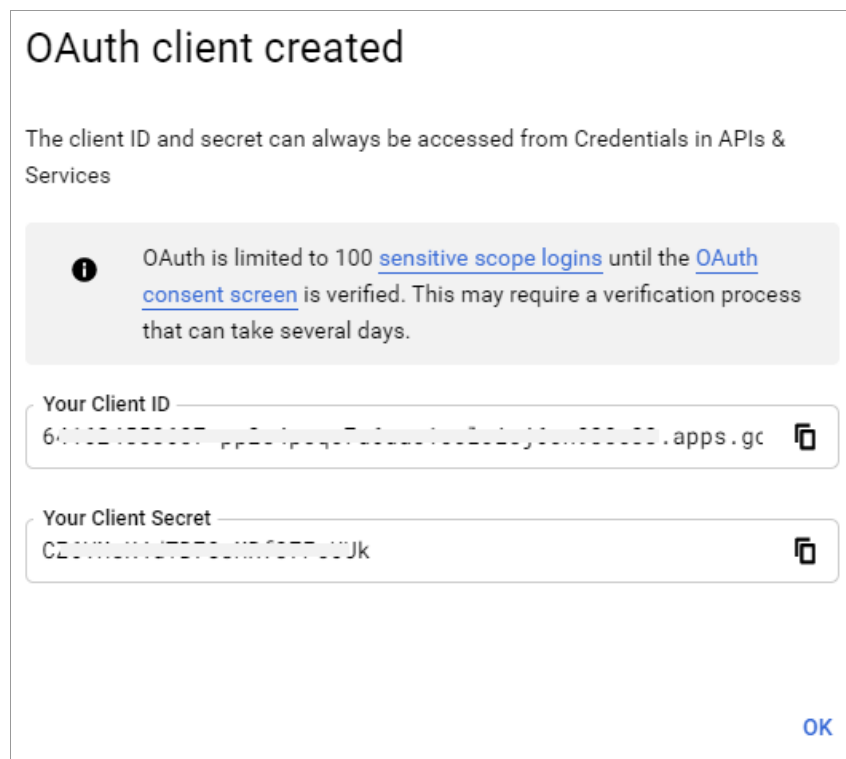


Fig. 13: OAuth Client Created

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

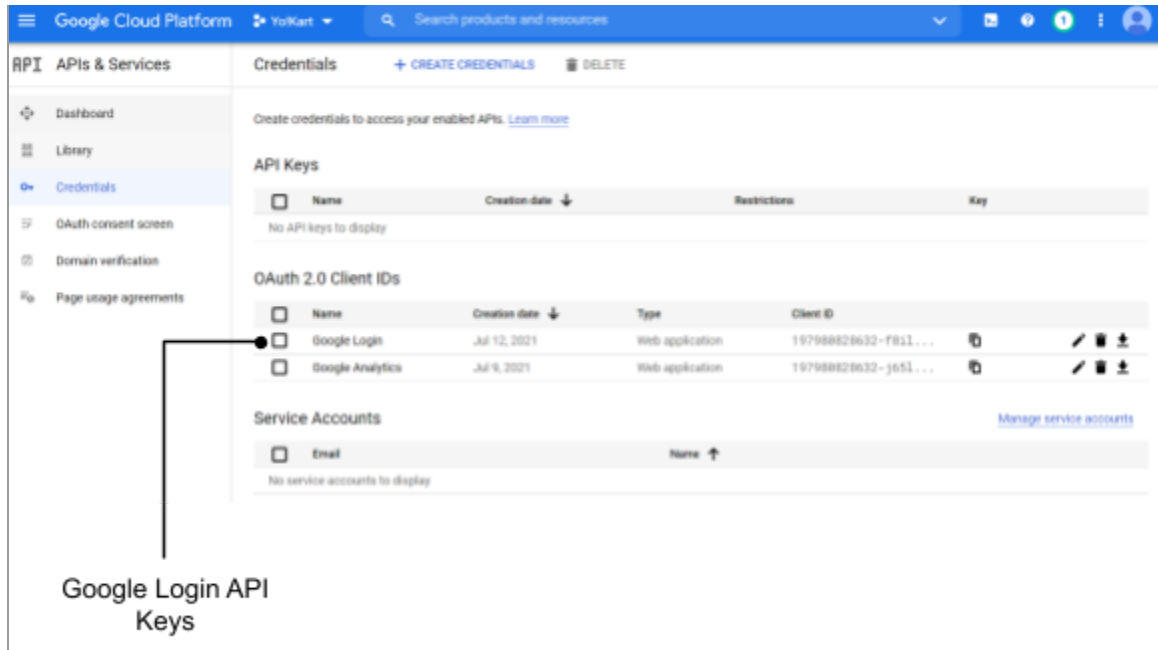


Fig. 14: Credentials Page

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.

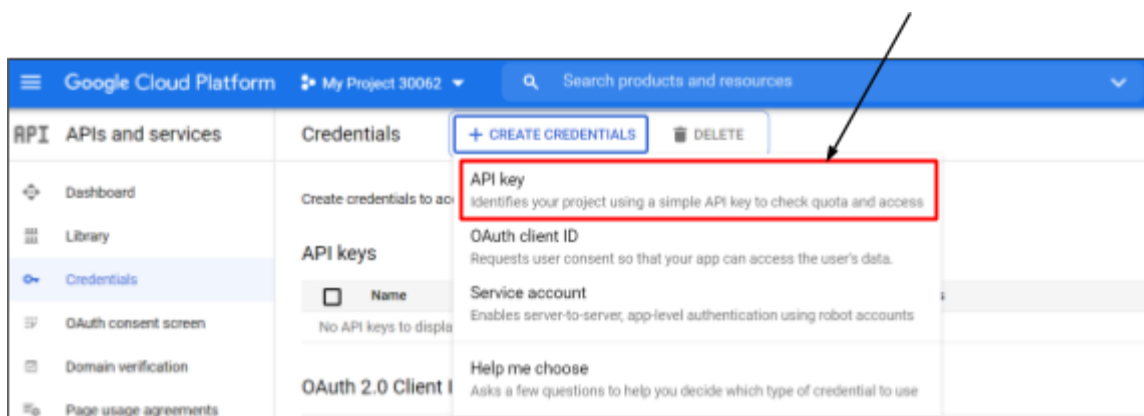


Fig. 15: Credentials Page

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

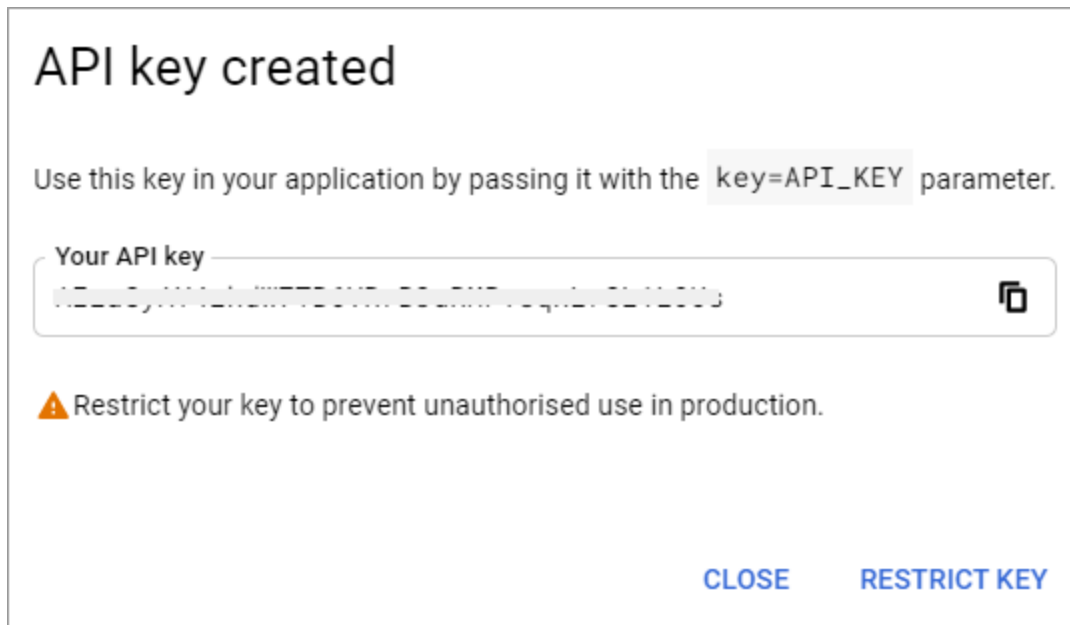



Fig. 16: API Key Created

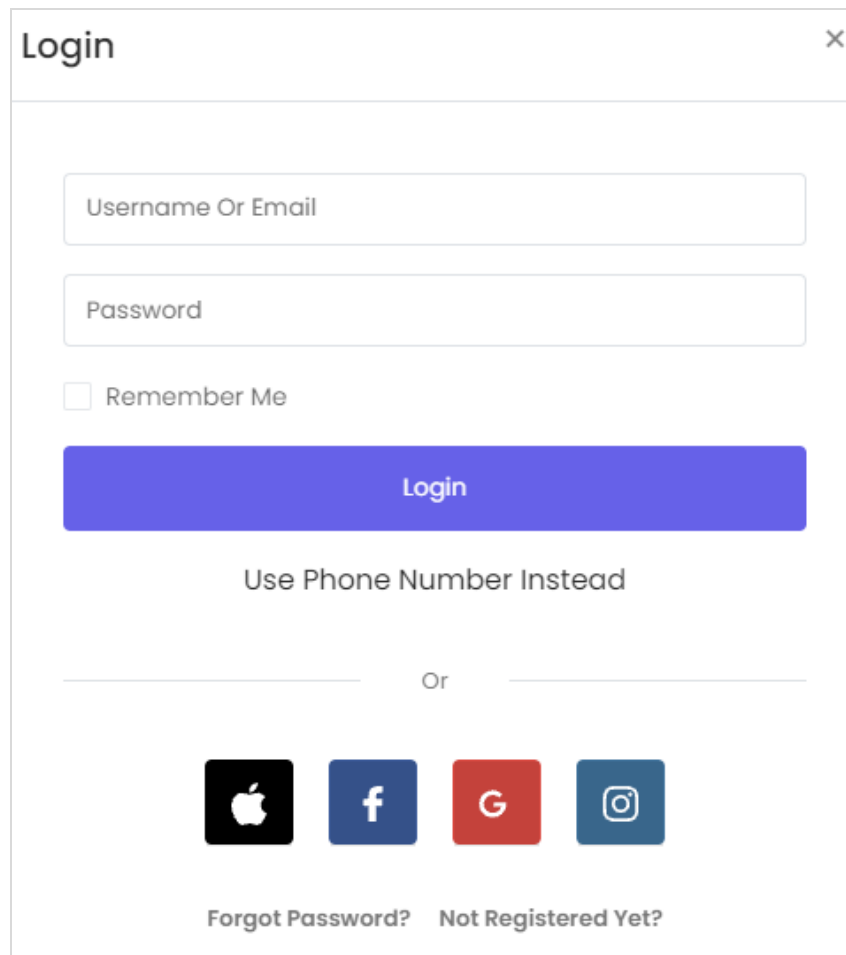
Please **copy** the key and paste it in the **Developer Key** input field provided under **Google Login plugin** settings provided in the admin panel as shown in [figure 1](#).

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.



The image shows a login form titled "Login" with a close button (X) in the top right corner. The form contains the following elements:

- A text input field labeled "Username Or Email".
- A text input field labeled "Password".
- A checkbox labeled "Remember Me".
- A large blue button labeled "Login".
- A link labeled "Use Phone Number Instead".
- A horizontal separator line with the word "Or" in the center.
- Four social media login buttons: Apple (black square with white Apple logo), Facebook (blue square with white 'f'), Google (red square with white 'G'), and Instagram (blue square with white camera icon).
- Two links at the bottom: "Forgot Password?" and "Not Registered Yet?".

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.