# Yo!Gigs

# Google Login API

## -v3.0 Setup Guide-

# Table of Contents

# What is Google login API?

The Google Login API, also known as Google Sign-In, is a service provided by Google that allows users to sign into third-party apps and websites using their Google account credentials. This can simplify the login process for users and can provide developers with a secure and easy way to authenticate users.

This API leverages OAuth 2.0 and OpenID Connect protocols to provide secure, streamlined authentication across web, iOS, and Android platforms. By integrating Google Sign-In, developers can enhance user experience with a single sign-on solution, reducing the need for multiple passwords and usernames.

Users benefit from a seamless login process, while developers gain access to essential user profile information with appropriate consent, facilitating personalized app experiences.

Google Sign-In's robust security and cross-platform support make it a valuable tool for modern application development.

Yo!Gigs has integrated this functionality into the platform to enhance the user experience.

# Configure the Google login API

Configure the Google login API under **Admin panel > Settings > System configurations > Third-party APIs** tab.
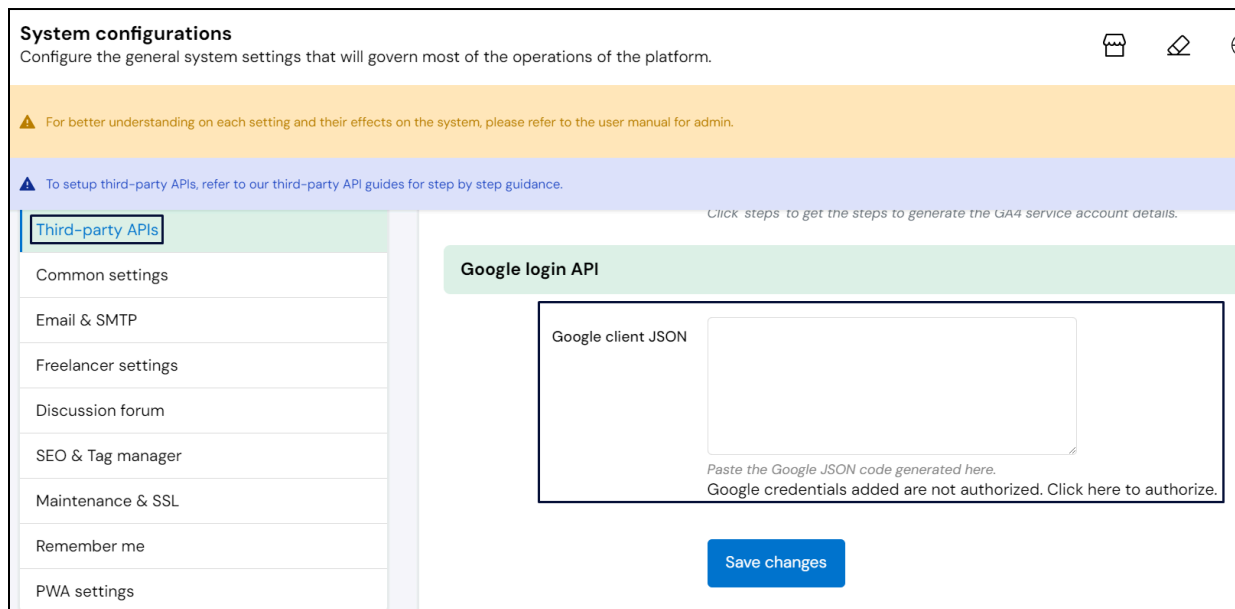


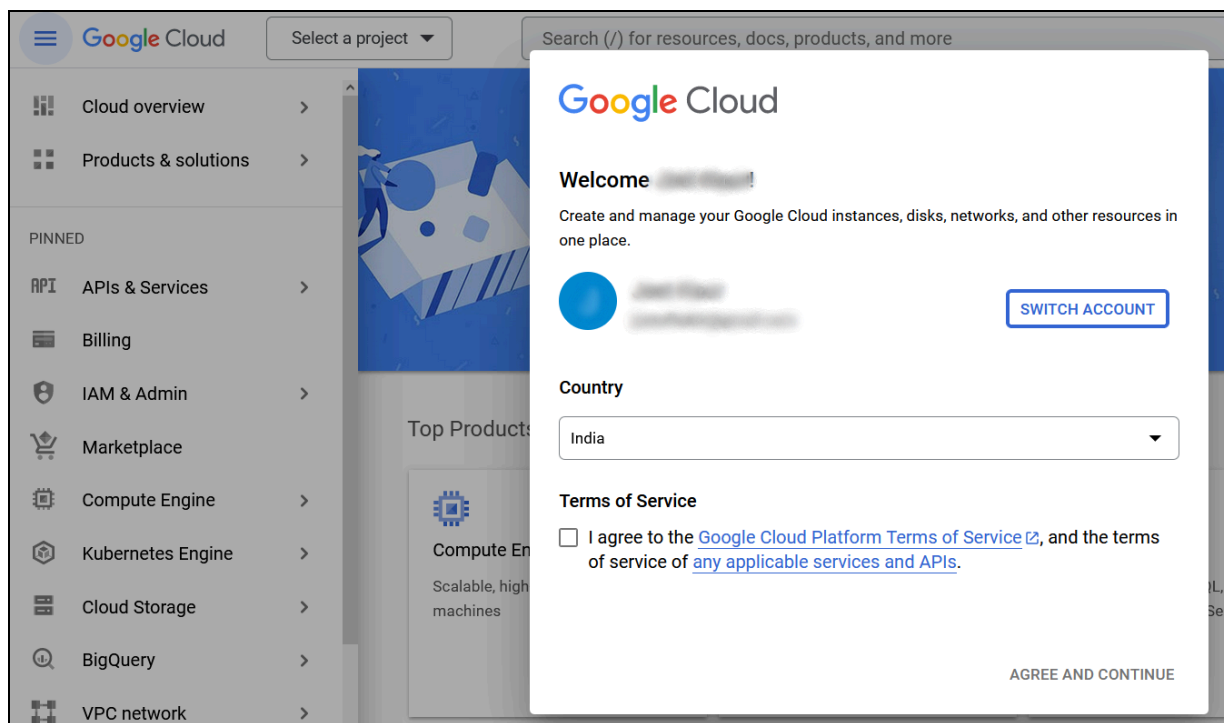Here are the steps to obtain the Google login API key:

> To obtain the key, you will need a Google account, so it's helpful to have a business Gmail account set up beforehand. If you don't have one, create it first, then follow the steps below.

## Step 1: Visit the Google Cloud Console platform

Log into your Gmail account.

Open a new tab and go to https://console.cloud.google.com/.

If you are a new user, the following pop-up will appear.

Before filling out the form, make sure you select the correct Gmail account; if not, switch to the appropriate one (using the **Switch account** button).

Update the following:

- **Country:** Click the field and select the country you are operating from, or select your current location from the dropdown list.

- **I agree to the Google Cloud Platform Terms of Service , and the terms of service of any applicable services and APIs.*:** Check mark this to accept the terms and conditions and move forward. If you do not check mark this, you won't be able to use the platform.

Once done, click **Agree and Continue.**

# Step 2: Go to APIs & Services

Click the **Hamburger menu** button to expand the navigation menu.

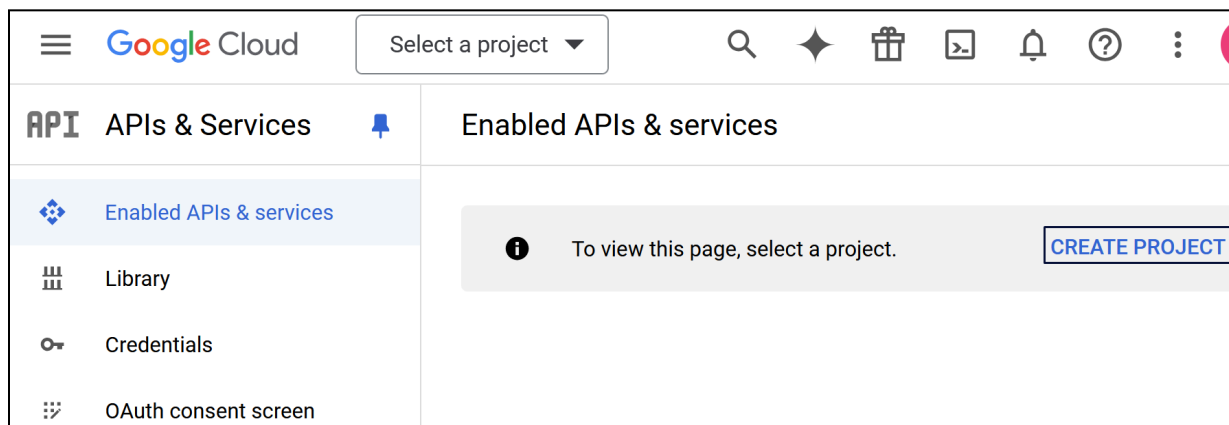Select **APIs & Services** to go to the **APIs & Services** page.
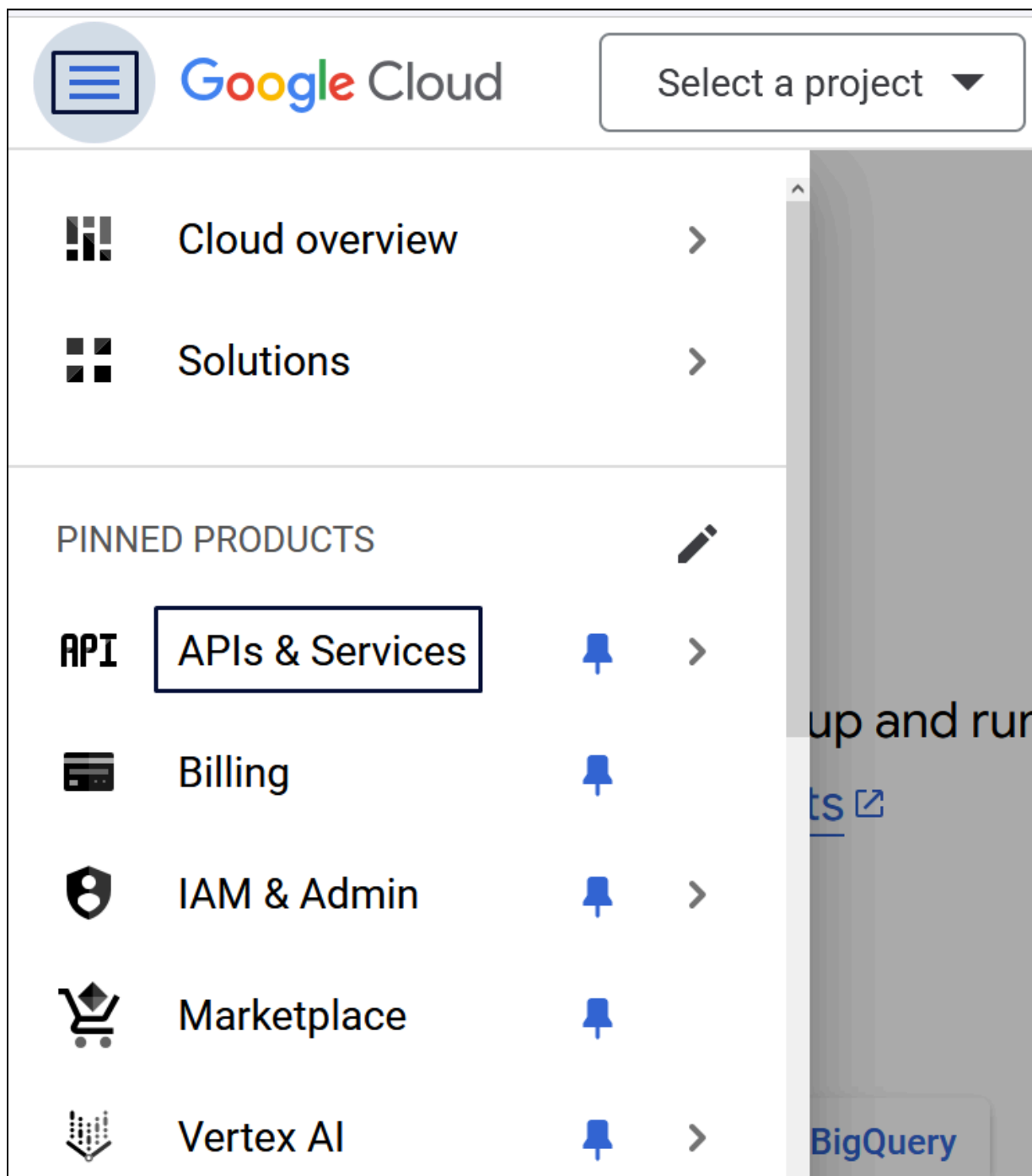
# Step 3: Create a project

As a new user, your first step is to create a project.

To do this, click **Create Project.**



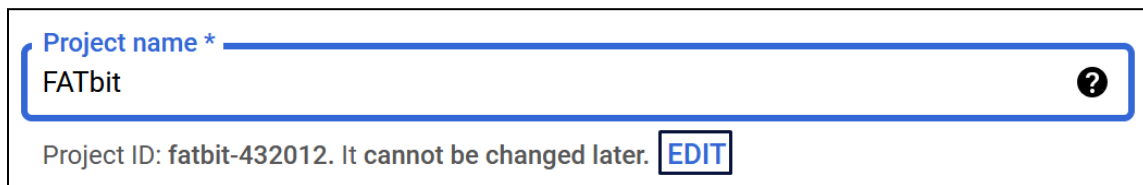This will direct you to the **New Project** page.



DISCLAIMER: The color theme and labels might differ in the screenshots as compared to on the platform.
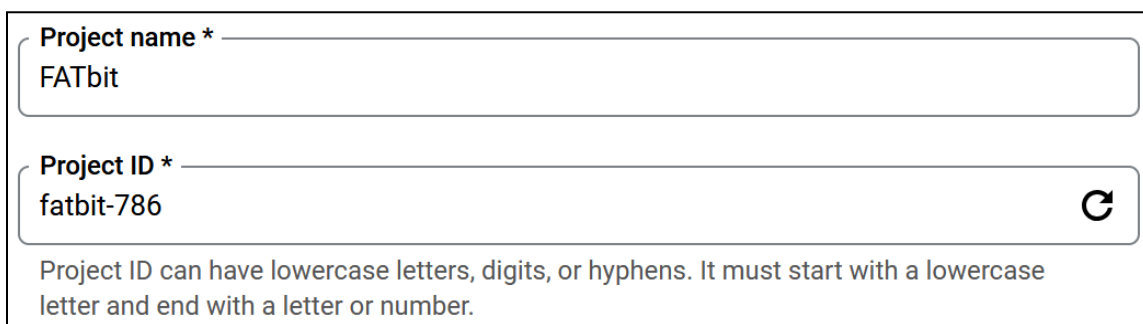An **asterisk (\*)** next to a label indicates that the information is mandatory.

Update the following:

- **Project name*:** Enter a project name.

Project name *
FATbit ❓

Project ID: **fatbit-432012**. It **cannot be changed later.** EDIT

When you enter a project name, the system automatically generates a project ID, which is displayed below the field.

To edit this ID, click **Edit**, and a new field appears.

Project name *
FATbit

Project ID *
fatbit-786 ⟳

Project ID can have lowercase letters, digits, or hyphens. It must start with a lowercase letter and end with a letter or number.

- **Project ID*:** Edit the project ID. This needs to be unique so you may need to try out different names before one is accepted.

- **Organization*:** Select the organization for your project.

> ⓘ *An organization in Google Cloud is a root node that allows you to manage and organize your cloud resources. It acts as a parent resource for all your projects and resources.*
>
> *This **field is visible** if you have logged in using an email address whose email domain (@yo-gigs.com) is the same as your business domain ([https://yo-gigs.com](https://yo-gigs.com)).*
>
> *In simple words, this field will be visible if your account is part of Google Workspace or Cloud Identity. This is because organizations allow for structured management of cloud resources.*
>
> *So, if you have multiple organizations, you can select which organization you want to create the project under.*

DISCLAIMER: The color theme and labels might differ in the screenshots as compared to on the platform.
An **asterisk (*)** next to a label indicates that the information is mandatory.

The available options under this will depend on the number of organizations your account is linked to. Select the appropriate one.

- **Location*:** Select a folder for your project. The location specifies where your resources will be physically hosted.

    > *Google Cloud automatically provides available regions based on the services you intend to use and your project's requirements. These regions are predefined by Google Cloud and depend on the services you select for your project.*

    If you don't have any options, leave it as it is.

    > *If you select '**No organization**' in the previous field, this field may appear **blank** or show "Global." Use the **Browse** button to select a specific location for your resources. If there is **no location available**, it is mostly because **Google Cloud services are not available** for the regions around you.*

    > *In this case, choose an organization and location that is available in the list (only those options are visible that are supported by Google Cloud services).*

Click **Create**.

With this, the project is created and you are directed back to the **APIs & Services** page.

---

# Step 4: Go to Credentials

Select **Credentials** from the navigation bar.

This will direct you to the credentials page.
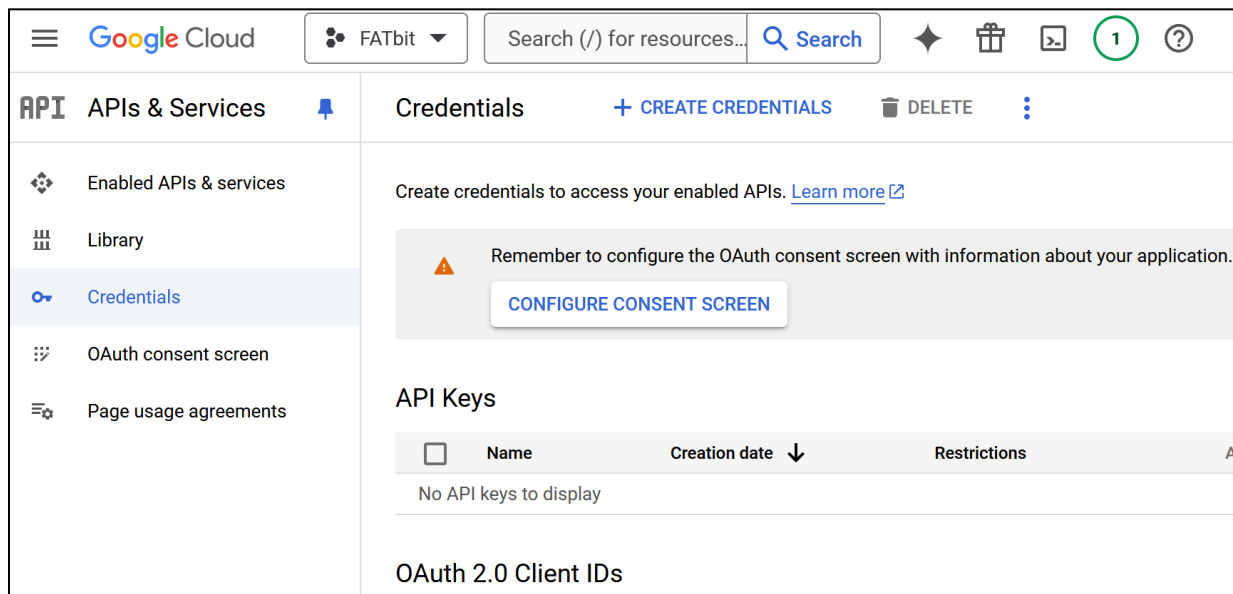
# Step 5: Configure the consent screen

Click **Configure consent screen** to go to the OAuth consent screen setup.
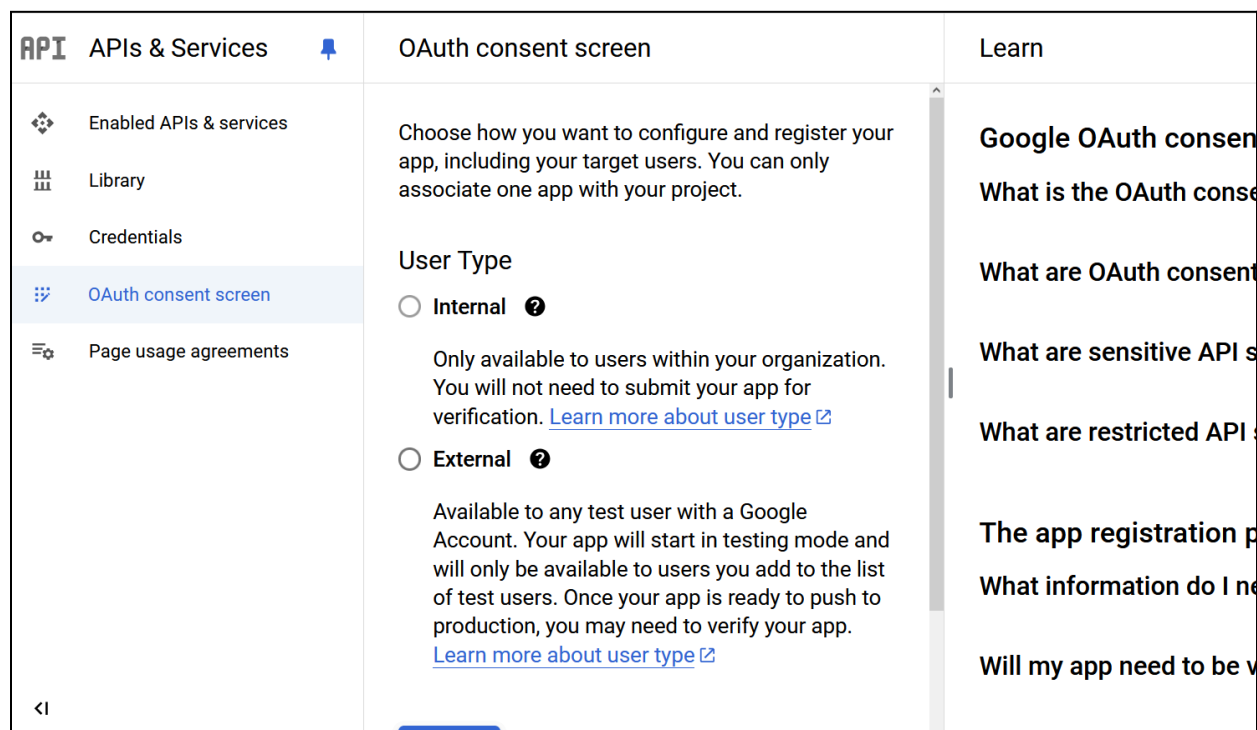


Based on whether you need keys for a live project or just for testing, choose the appropriate option:

- **Internal -** Select this option if you're just testing your platform and only want people within your own company or organization to use it.

  Do not select this if you plan to make your project available to the public or to people outside your organization. This option limits access to only your organization's members.

  > ⓘ *You won't be able to select this option if you do not have a Gmail Business account or do not belong to an organization.*

- **External -** Select this if your platform is live and you want it to be used by people outside your organization.

  > ⓘ *Selecting this option might require you to submit your project to Google for verification. After Google reviews and approves it, the API will be ready to use. Learn more about the [verification process here](#)!*

Once done, click **Create.**

DISCLAIMER: The color theme and labels might differ in the screenshots as compared to on the platform.
An **asterisk (\*)** next to a label indicates that the information is mandatory.

# Step 6: Fill the "Edit app registration" form

Register your web application on Google via the **Edit app registration** form. There are four steps (tabs) under this form.

## 1. OAuth consent screen



The form is divided into four sections. Update them following:

## 1. App information

- **App name\*:** Enter the platform's name - for which you will be generating the API key.

- **User support email\*:** Enter the email address on which users can contact you with questions about their consent.

## 2. App logo

- **Logo file to upload:** Click **Browse** and select your platform's logo to upload it.

## 3. App domain

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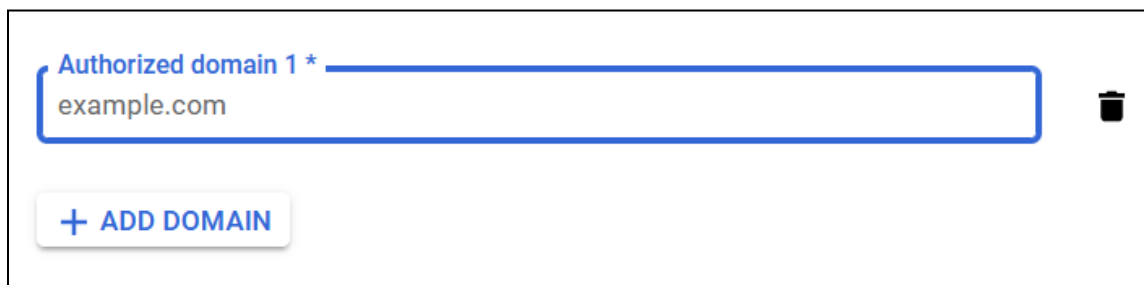
Provide users a link to your public terms of service

### 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.

+ ADD DOMAIN

---

DISCLAIMER: The color theme and labels might differ in the screenshots as compared to on the platform.
An **asterisk (\*)** next to a label indicates that the information is mandatory.

- **Application home page:** Enter your platform's home page URL.

- **Application privacy policy link:** Enter your platform's privacy policy page URL.

- **Application terms of service link:** Enter your platform's terms of service page URL.

- **Authorized domains:** Click the add domain button to add the authorized domains that will be used on the consent screen for the users, and a field appears.
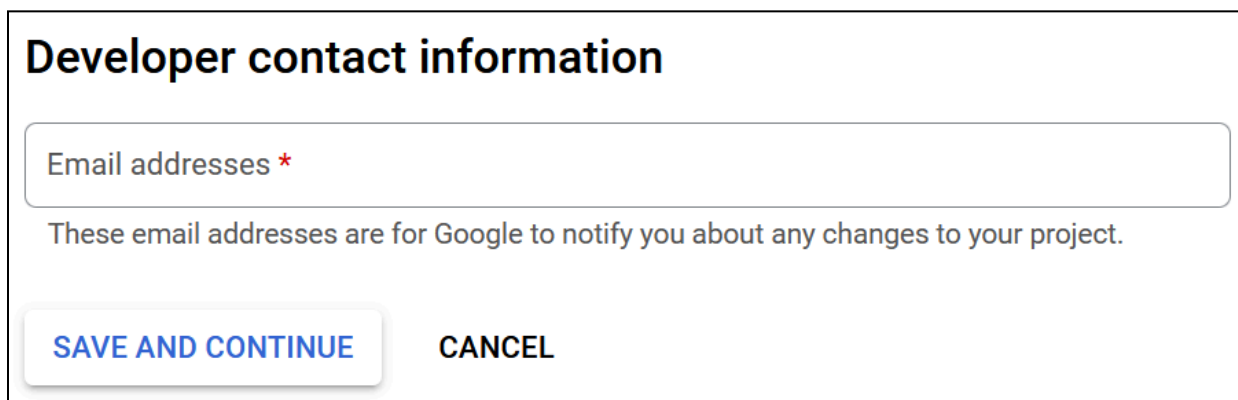


Add as many domains as applicable.

If you add a domain by mistake, click  beside it to delete it.

## 4. Developer contact information



- **Email addresses*:** Enter the email address(es) of the person who will be notified about any changes made to the project.

  You can enter more than one email address in this field.

  Click **Save and continue.**

## 2. Scopes

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 about **scopes here**.



Although this step is optional, you need to select a few scopes in this case.

Click **Add or remove scopes** to add a scope.

The **Update selected scopes** form will appear on the right side of the page.

Select the first two visible scopes from the list:

- .../auth/userinfo.email

- .../auth/userinfo.profile



Click **Update.**

The form will close, and the scopes will be updated accordingly.

Depending on their sensitivity, the scopes will be categorized into three sections.

## Your non-sensitive scopes

| API ↑ | Scope | User-facing description | |
|---|---|---|---|
| | .../auth/ userinfo .email | See your primary Google Account email address | 🗑 |
| | .../auth/ userinfo .profile | See your personal info, including any personal info you've made publicly available | 🗑 |

## 🔓 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 | | |

If you selected the wrong scope, click 🗑 beside it to delete it.

Then, scroll to the end of the form and click **Save and continue**.

## 3. Test users

⚠️ *This tab will only **be visible** if you selected **External** as the user type in the [first step](#). This is because it allows you to specify which external users can test your app before it goes live. For projects intended for public use, this helps ensure everything works properly for a wider audience.*

*For **Internal** projects (Internal user type), which are limited to users within your organization, testing is handled internally without the need for this tab.*

Add the users who will be able to access the app while the app is in the testing phase (if applicable).

Updating this tab is optional.

---

### Edit app registration

✅ OAuth consent screen — ✅ Scopes — ③ **Test users** — ④ Summary

### Test users

While publishing status is set to "Testing", only test users are able to access the app. Allowed user cap prior to app verification is 100, and is counted over the entire lifetime of the app. Learn more ↗

**+ ADD USERS**

≡ Filter   Enter property name or value                           ❓

**User information**

No rows to display

**SAVE AND CONTINUE**    CANCEL

---

This step is not required in this case. Click **Save and continue** to proceed.

---

# 4. Summary

Review the details added and edit if required.



From here, return to the **OAuth consent screen dashboard** by clicking **Back to dashboard** at the end of this tab.

# Step 7: Go to Credentials

Select **Credentials** from the navigation bar.

This will direct you to the credentials page.

# Step 8: Create OAuth 2.0 credentials
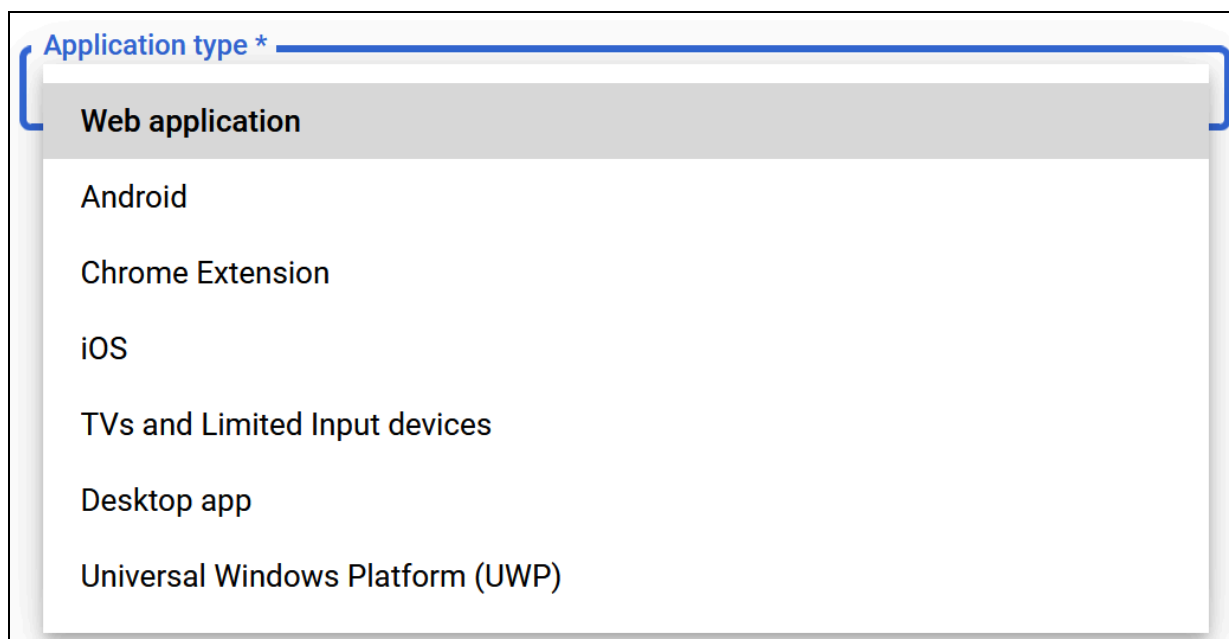
Click **+Create credentials** and select **OAuth Client IDs**.
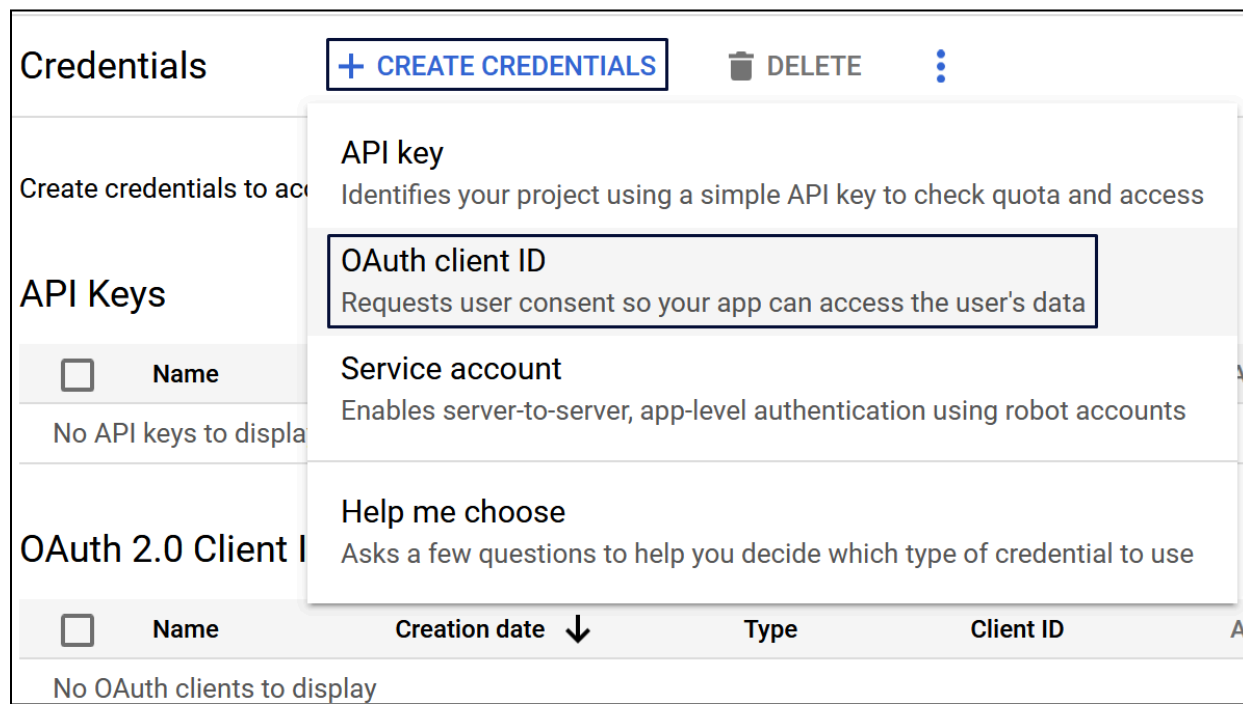


This will direct you to the **Create OAuth client ID** form.



Click the **Application type** field to select the application type.
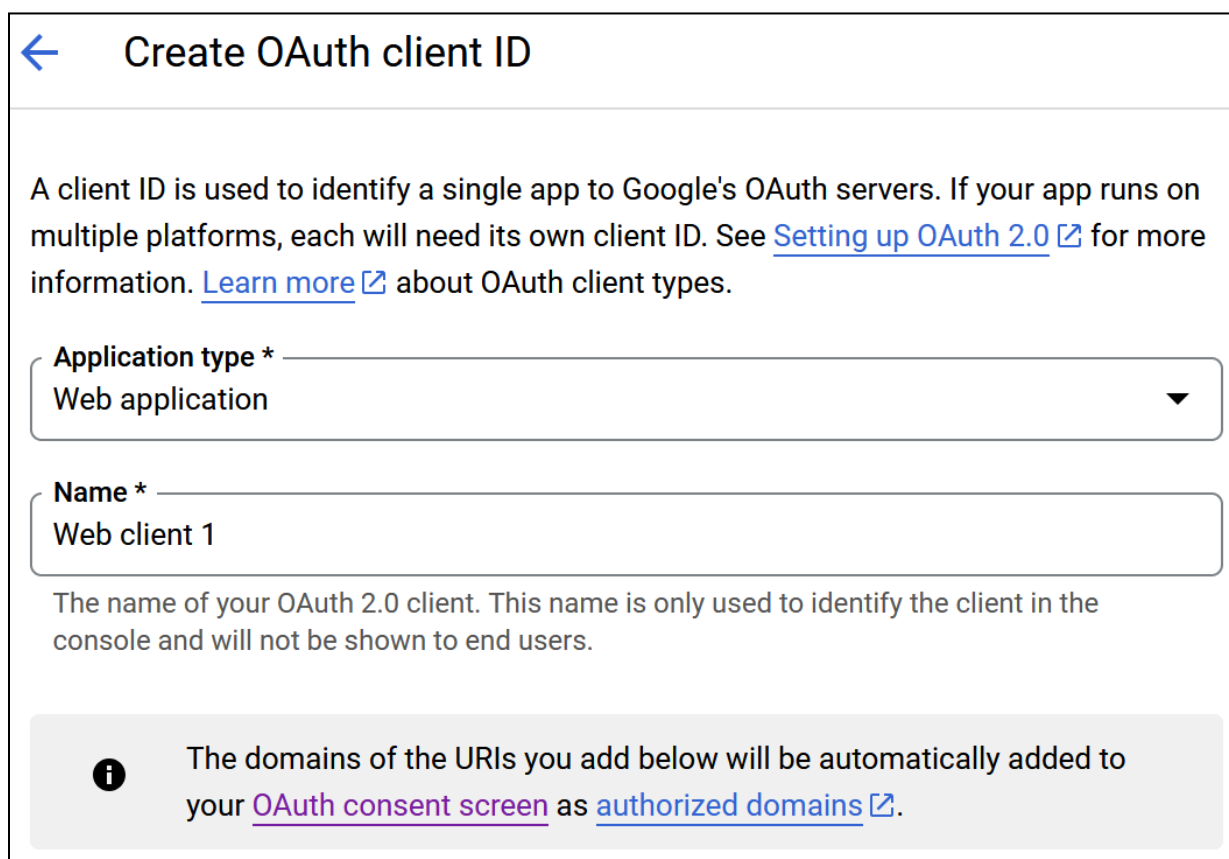
From the dropdown list, select **Web application**.

Once this option is selected, a new field and two additional sections will appear in the form.

- **Name\*:** Enter the name of your application.

Below this field are the two additional sections.

Update them accordingly:



- **Authorized JavaScript origins:** Click +Add URI to add your domain name.

    > *A URI (Uniform Resource Identifier) is a string that identifies and provides a means to access a resource on the internet.*

    A field will appear.

Add your domain name in the format - http://domainname.com or https://domainname.com (if your SSL certificate is enabled).

- **Authorized redirect URIs:** Click **+Add URI** to add a callback URI for redirection.

  A field will appear.

**Authorized redirect URIs** ❓

For use with requests from a web server

URIs 1 *

https://www.example.com    🗑

**+ ADD URI**

Note: It may take 5 minutes to a few hours for settings to take effect

CREATE        CANCEL

Enter in the following format: https://{domain-name}/guest-user/google-login

**For example**, if your domain is: https://demo.yo-gigs.com/ – the URI would be: https://demo.yo-gigs.com/guest-user/google-login

Click **Create.**

# Step 9: Download the JSON file

The keys will be created, and a pop-up dialog box displaying them will appear.

---

## OAuth client created

The client ID and secret can always be accessed from Credentials in APIs & Services

> ⓘ   OAuth access is restricted to the test users ↗ listed on your OAuth consent screen

**Client ID**

**Client secret**

**Creation date**          August 27, 2024 at 4:13:17 PM GMT+5

**Status**          ✅ Enabled

**⬇ DOWNLOAD JSON**

OK

---

Click **Download JSON** to save the JSON file to your system.
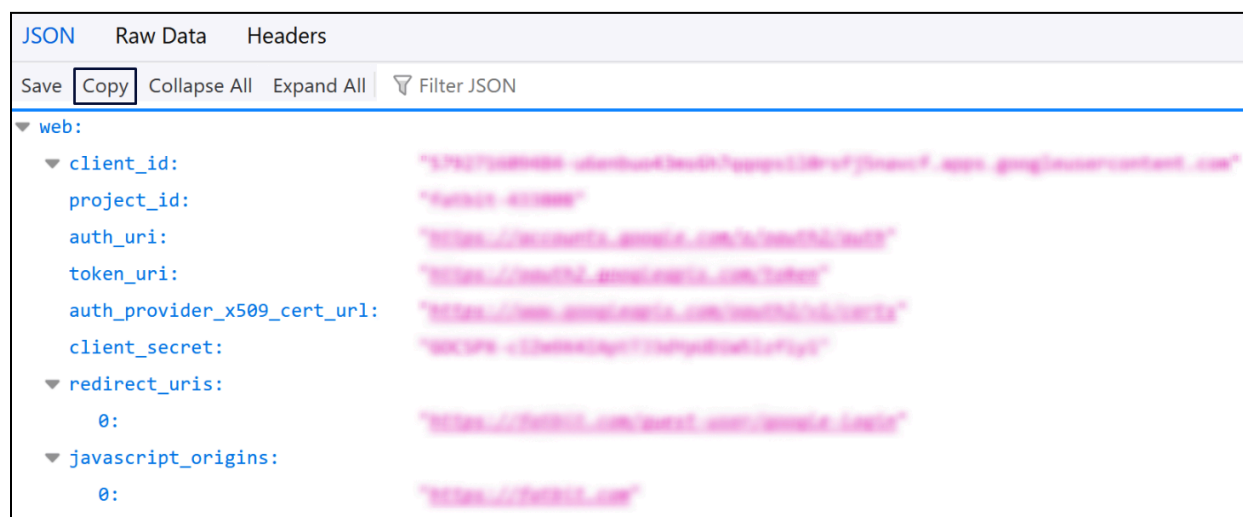
Then, click **OK** to close the dialog box.

---

# Step 10: Open the JSON file & copy it

Open the JSON file downloaded into your system.

The JSON will open in your web browser.
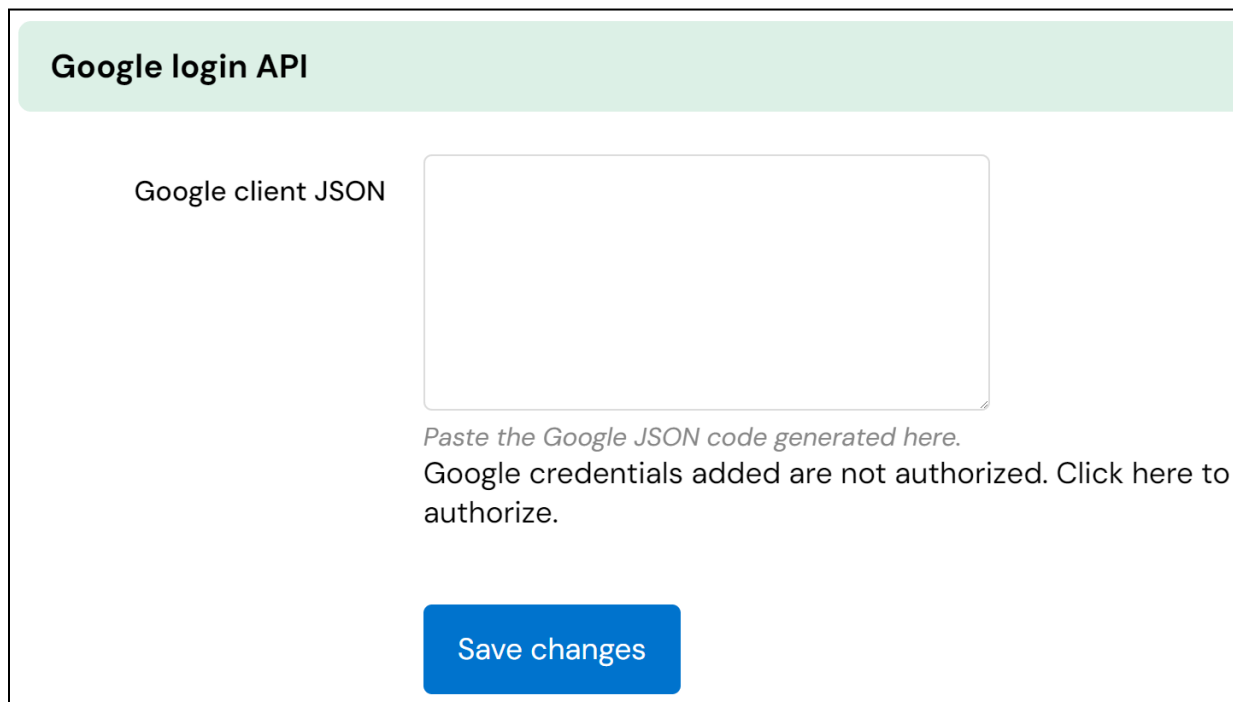
Select **Copy** to copy it.

# Step 11: Paste it on the Yo!Gigs admin panel

On another tab, open the admin panel of your platform.

Go to **Settings > System configurations > Third-party APIs tab.**

Paste this code in the **Google client JSON** field.



Click **Save changes** to update the details in the system.

Then, click the **Click here to authorize** link to complete the authorization process.



Click **Save changes** once again.

This will configure the **Google login API** in the system.

---

# Working of the Google login API

Users will be able to log into the platform and create their profiles using their Google credentials.



When a user selects **Sign in with Google**, they will be directed to the Google login page to log into their Google account. After logging in, they will be redirected back to the platform.

**DISCLAIMER:** The color theme and labels might differ in the screenshots as compared to on the platform.
An **asterisk (*)** next to a label indicates that the information is mandatory.

# Yo!Gigs - Online Service Marketplace Solution

**Visit https://www.yo-gigs.com/ to know more!**



**www.fatbit.com | sales@fatbit.com**

**Contact us**

**+91 95555 96666 / +91 73075 70707**

**Copyright ©FATbit Technologies (Ably Soft Pvt. Ltd). All Rights Reserved.**