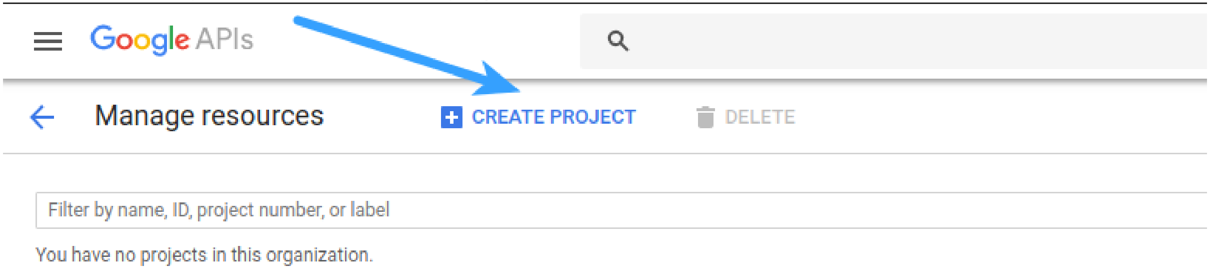
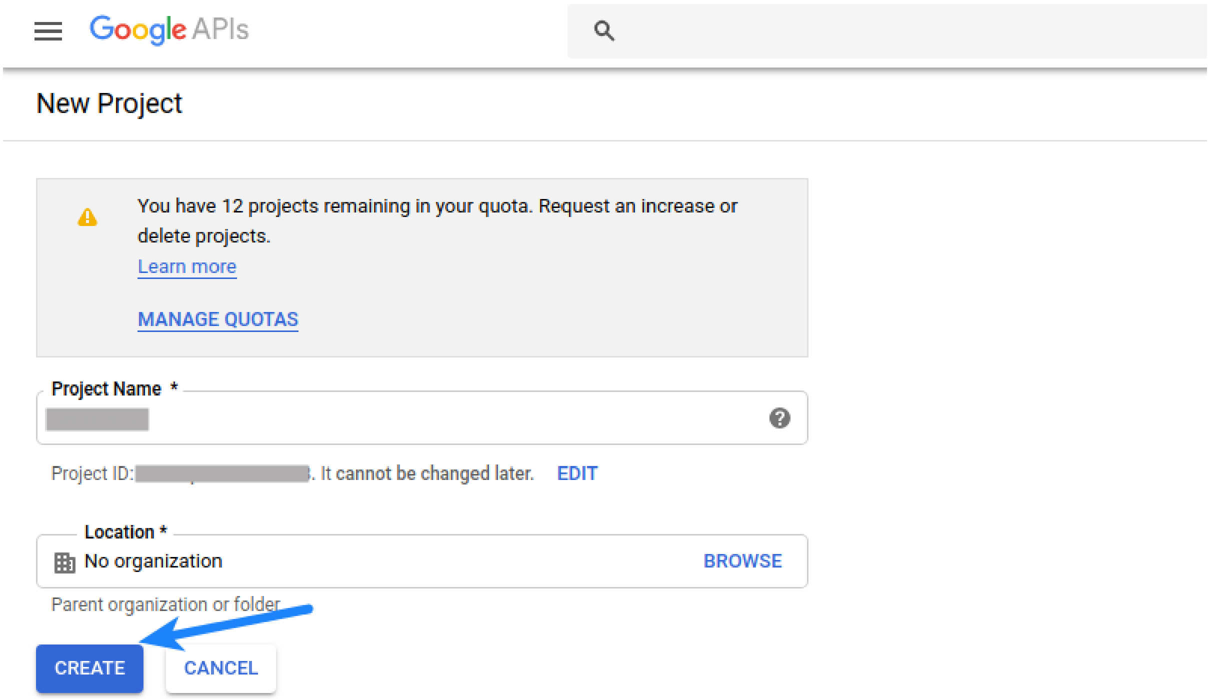
Steps To Enable Google Login

1. Navigate to Google API Console section and login to your Google account if required.
2. If this is your first app, you will need to "**Create a project**" and also might need to accept **Terms and Conditions**. **If you do not see this page, move to step 3.**



You have no projects in this organization.



You have 12 projects remaining in your quota. Request an increase or delete projects.

Project Name * [redacted]

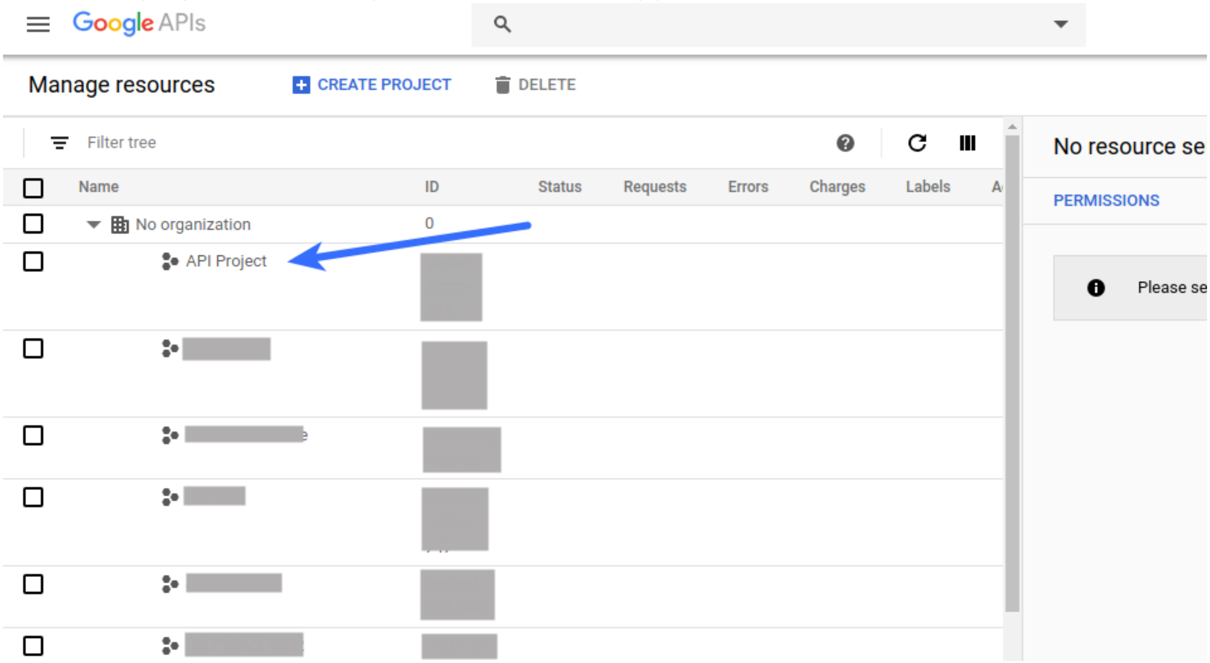
Project ID: [redacted]. It cannot be changed later.

Location * No organization

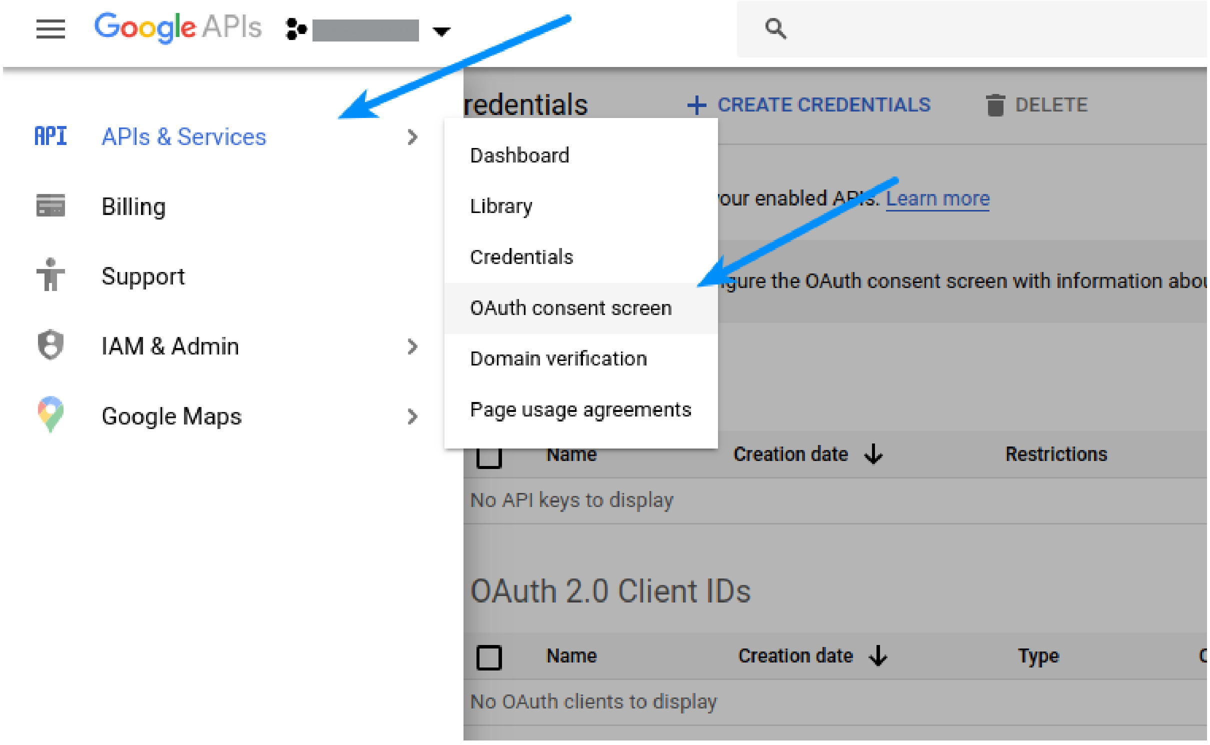
Parent organization or folder

3. If you have created apps before, you will be able to see the list of projects. You can also create a new project by clicking "**CREATE PROJECT**" at the top.

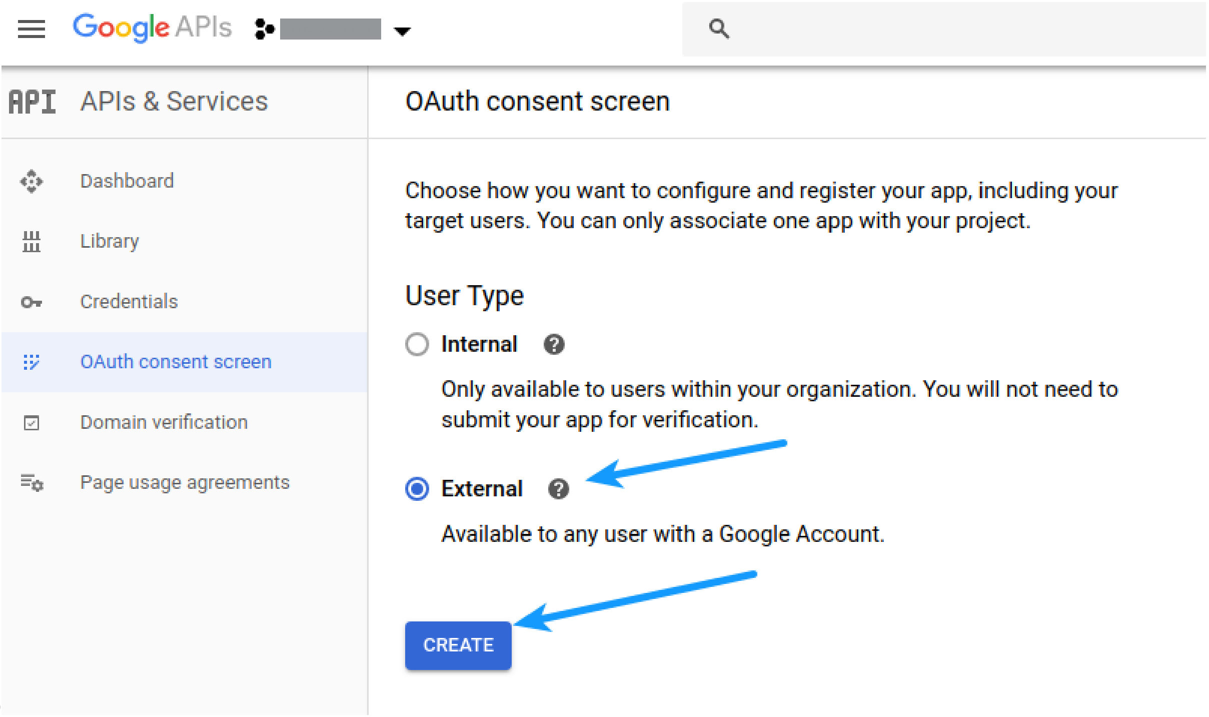
Select the project for which you want to create app.



4. Navigate to **APIs and Services > OAuth consent screen** section from the menu in top-left corner



5. If you see the following screen, select **External** in **User Type** and click **Create** button, else move to next step



OAuth consent screen

Choose how you want to configure and register your app, including your target users. You can only associate one app with your project.

User Type

○ Internal

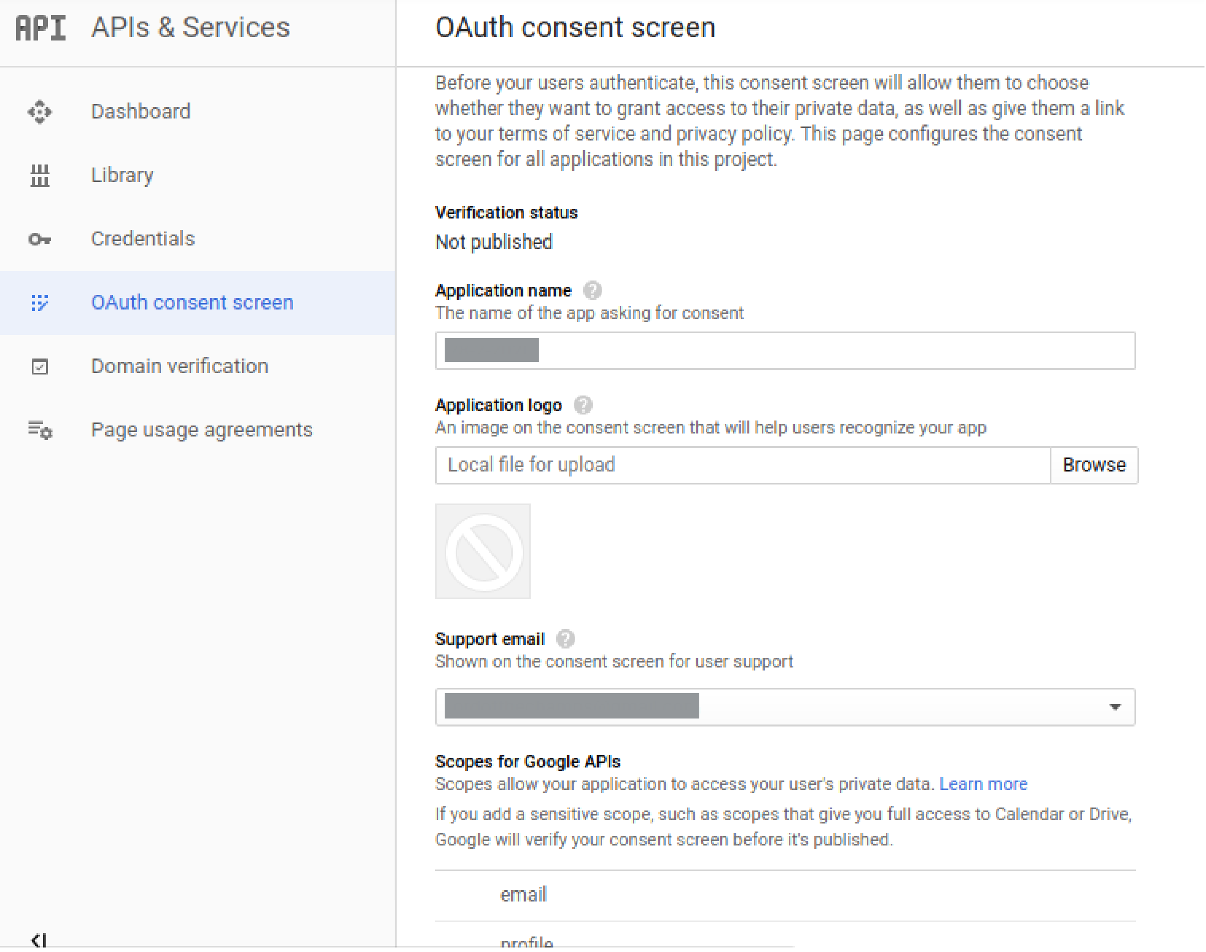
Only available to users within your organization. You will not need to submit your app for verification.

● External

Available to any user with a Google Account.

CREATE

6. Fill the fields as described below:



OAuth consent screen

Before your users authenticate, this consent screen will allow them to choose whether they want to grant access to their private data, as well as give them a link to your terms of service and privacy policy. This page configures the consent screen for all applications in this project.

Verification status

Not published

Application name

The name of the app asking for consent

[redacted]

Application logo

An image on the consent screen that will help users recognize your app

Local file for upload | Browse

Support email

Shown on the consent screen for user support

[redacted]

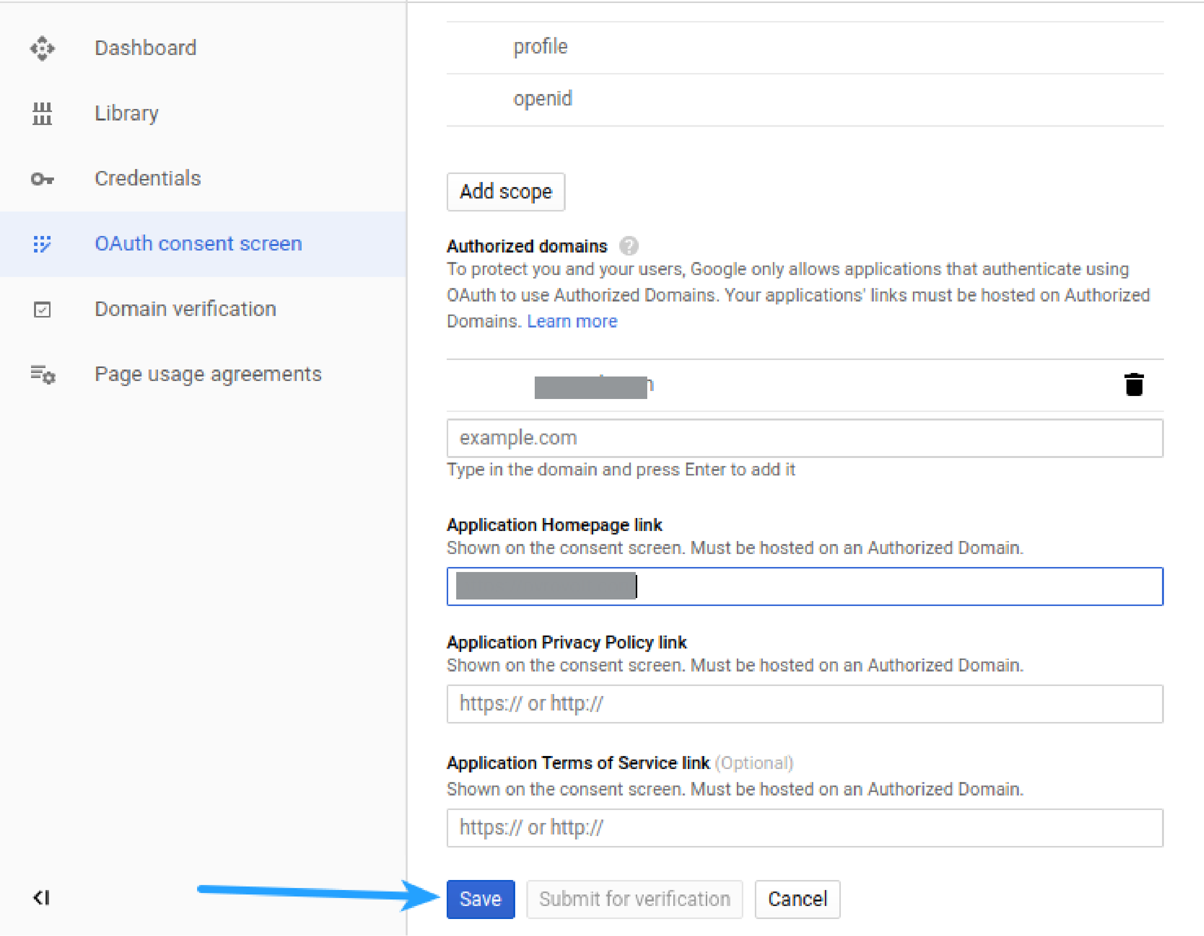
Scopes for Google APIs

Scopes allow your application to access your user's private data. Learn more

If you add a sensitive scope, such as scopes that give you full access to Calendar or Drive, Google will verify your consent screen before it's published.

email

profile



profile

openid

Add scope

Authorized domains
To protect you and your users, Google only allows applications that authenticate using OAuth to use Authorized Domains. Your applications' links must be hosted on Authorized Domains. Learn more

[redacted]

example.com
Type in the domain and press Enter to add it

Application Homepage link
Shown on the consent screen. Must be hosted on an Authorized Domain.

[redacted]

Application Privacy Policy link
Shown on the consent screen. Must be hosted on an Authorized Domain.

https:// or http://

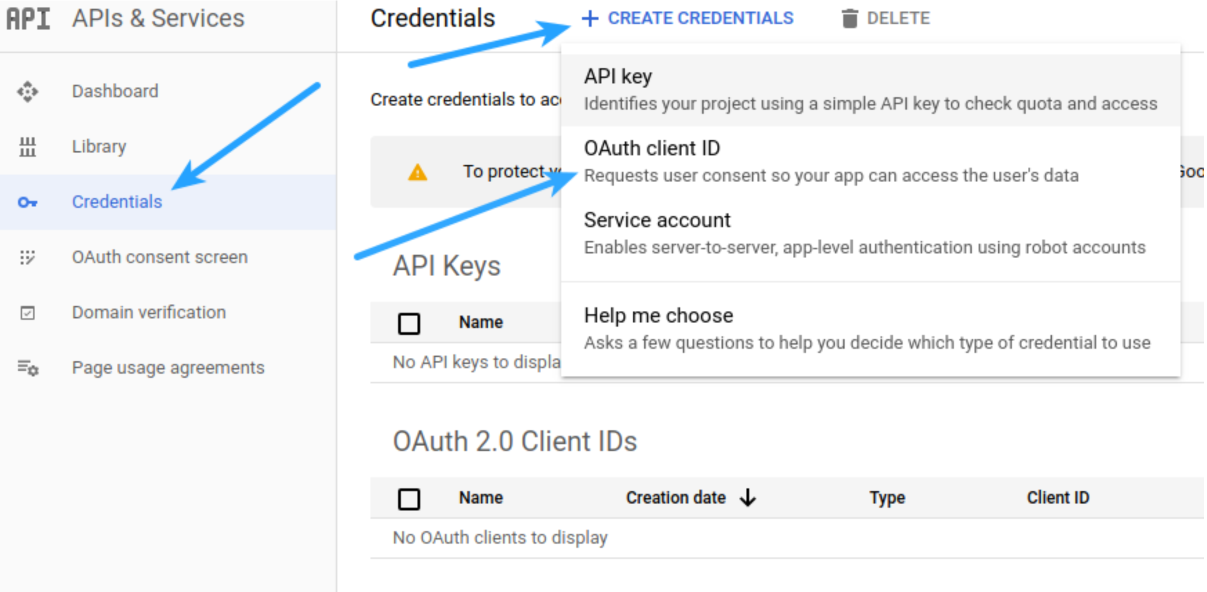
Application Terms of Service link (Optional)
Shown on the consent screen. Must be hosted on an Authorized Domain.

https:// or http://

Save | Submit for verification | Cancel

Application name: Specify the name of your app (You can enter whatever name you like, but it's recommended to enter your website or company name in this field)
Application Logo: (Optional) Upload logo representing your website with which you are going to integrate social login.
Note: If you upload logo, you need to get your app verified by Google
Support email: Select/Specify email
Authorized domains: Specify your website domain. For example, if your website homepage url is **www.mywebsite.com** or **mywebsite.com**, you have to save **mywebsite.com.** After entering the domain name, click outside the textbox otherwise it won't be saved. You can fill other **optional** fields.
Optionally, you can fill remaining fields.
Click **Save** button.

7. Navigate to **Credentials** section, click **OAuth client ID** after clicking **CREATE CREDENTIALS** button



API key
Identifies your project using a simple API key to check quota and access

OAuth client ID
Requests user consent so your app can access the user's data

Service account
Enables server-to-server, app-level authentication using robot accounts

Help me choose
Asks a few questions to help you decide which type of credential to use

Create credentials to ac

To protect y

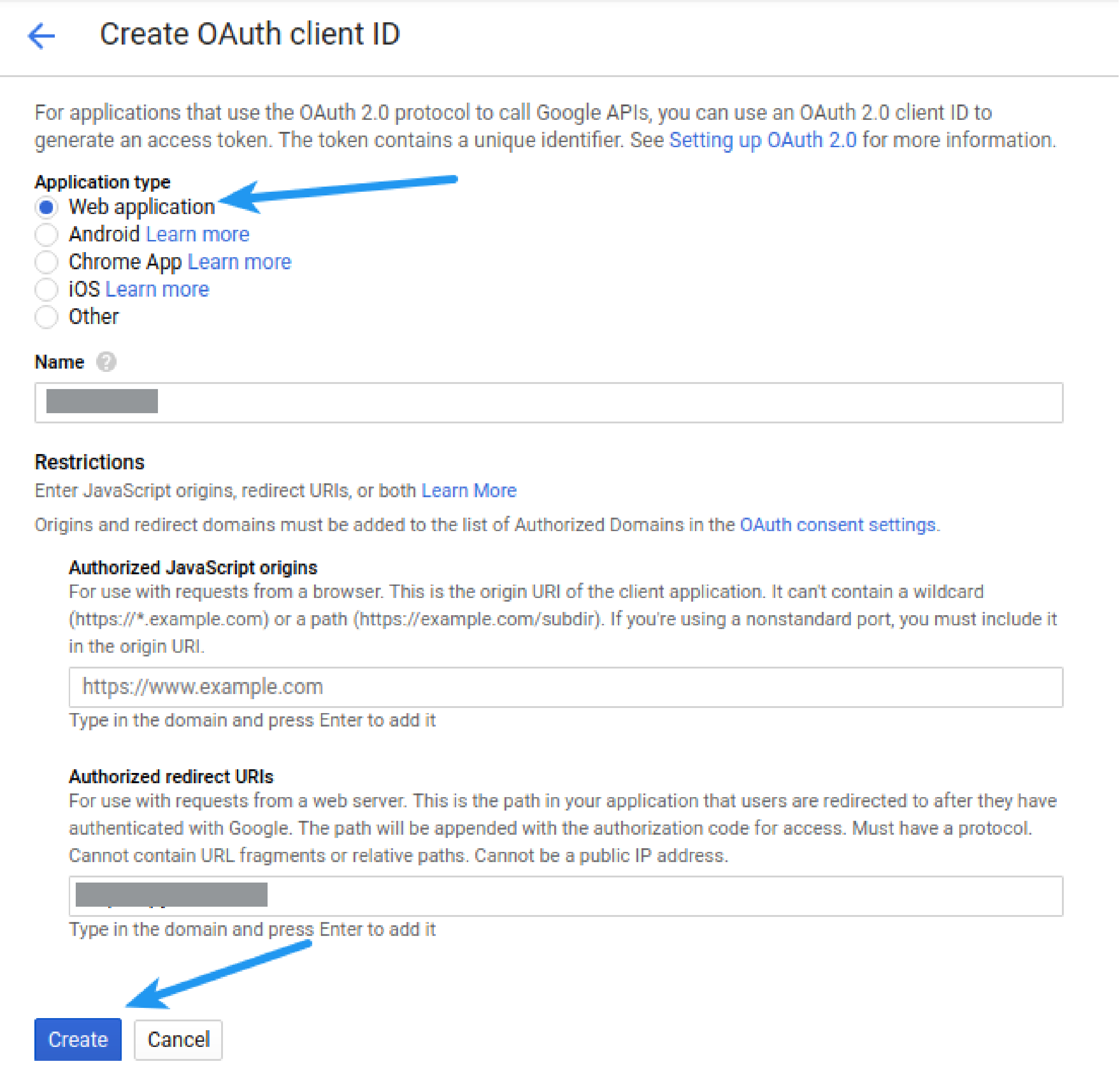
API Keys

□	Name
No API keys to displa	

OAuth 2.0 Client IDs

□	Name	Creation date ↓	Type	Client ID
No OAuth clients to display				

8. Fill the fields as described below



Create OAuth client ID

For applications that use the OAuth 2.0 protocol to call Google APIs, you can use an OAuth 2.0 client ID to generate an access token. The token contains a unique identifier. See Setting up OAuth 2.0 for more information.

Application type

● Web application
○ Android Learn more
○ Chrome App Learn more
○ iOS Learn more
○ Other

Name

[redacted]

Restrictions

Enter JavaScript origins, redirect URIs, or both Learn More

Origins and redirect domains must be added to the list of Authorized Domains in the OAuth consent settings.

Authorized JavaScript origins

For use with requests from a browser. This is the origin URI of the client application. It can't contain a wildcard (https://*.example.com) or a path (https://example.com/subdir). If you're using a nonstandard port, you must include it in the origin URI.

https://www.example.com

Type in the domain and press Enter to add it

Authorized redirect URIs

For use with requests from a web server. This is the path in your application that users are redirected to after they have authenticated with Google. The path will be appended with the authorization code for access. Must have a protocol. Cannot contain URL fragments or relative paths. Cannot be a public IP address.

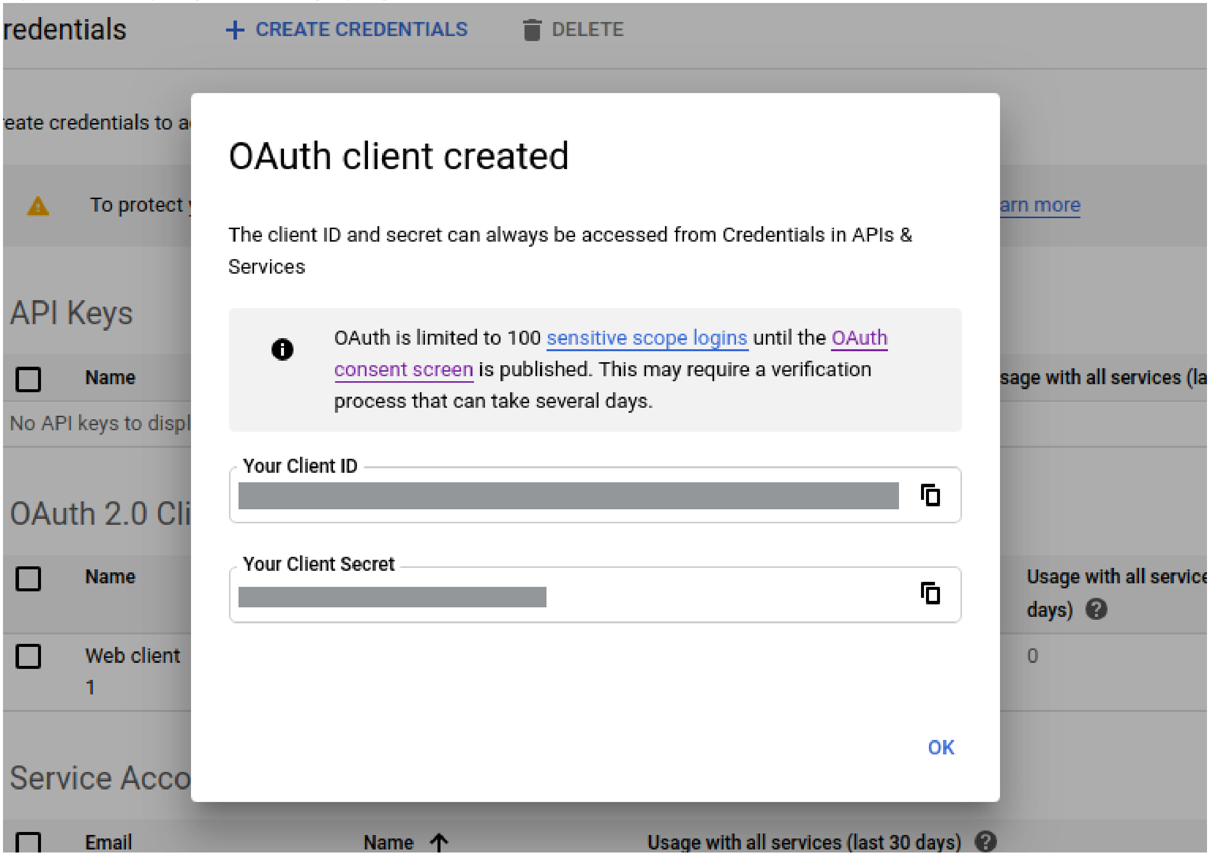
[redacted]

Type in the domain and press Enter to add it

- **Application type:** Select **Web application**
- **Name:** Specify the name of your app (You can enter whatever name you like, but it's recommended to enter your website or company name in this field)
- **Authorized JavaScript origins:** Leave empty
- **Authorized redirect URIs:** Append **/social-auth/google/callback** to the homepage url.
  - For example, if **http://mywebsite.com** is the homepage url of your website, you need to save **http://mywebsite.com/social-auth/ google/callback** in this option. **After entering the url, hit Enter key otherwise it won't be saved.**
  - (Keep https or https://www as per your website configuration or Copy paste your homepage URL from browser address bar)
  - Click **Create** button

9. Copy **Client ID** and **Client Secret** and paste these in the **Google Client ID** and **Google Client Secret** options of your plugin, respectively. Do not forget to **Save Changes** after configuring all the

options on plugin settings page.



OAuth client created

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

OAuth is limited to 100 sensitive scope logins until the OAuth consent screen is published. This may require a verification process that can take several days.

Your Client ID [redacted]

Your Client Secret [redacted]

OK

10. Once done, you can configure the Keys in the
    Admin Panel -> Settings -> Settings -> Third Party Integrations
    - Google Login Client Id
    - Google Login Client Secret