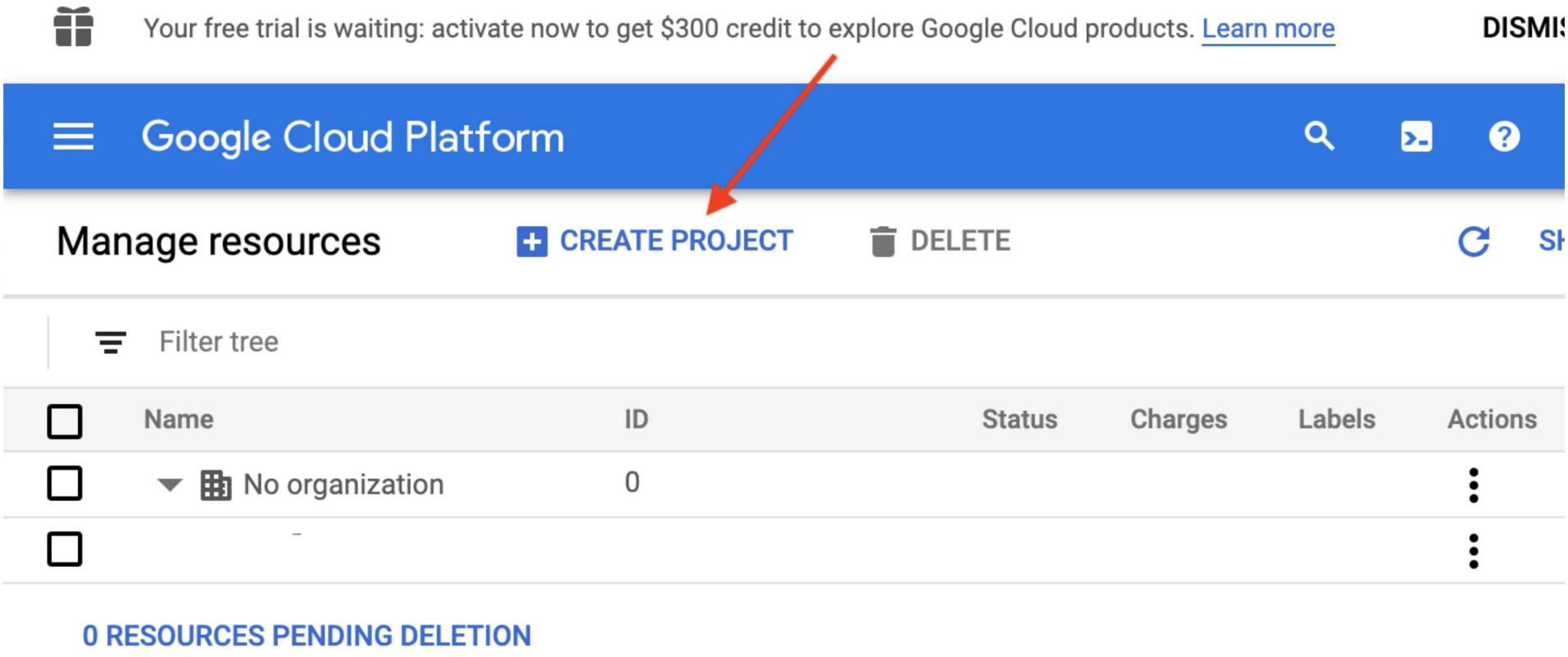
Google Project Setup with new UI

In the upcoming lecture, we will be going through the steps to create a new Google Project. Since the UI has changed, we have provided screenshots with the steps needed to create the project and obtain the Client Id and Client Secret.

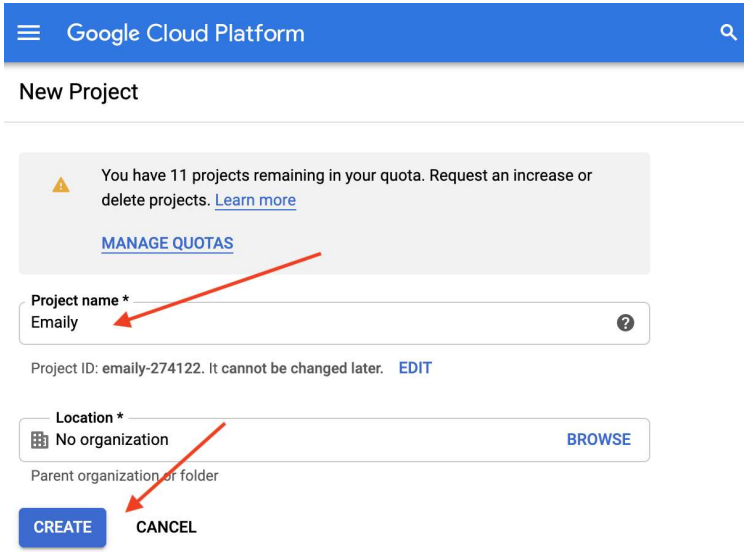
1. Go to the **Google Project Dashboard:**

https://console.cloud.google.com

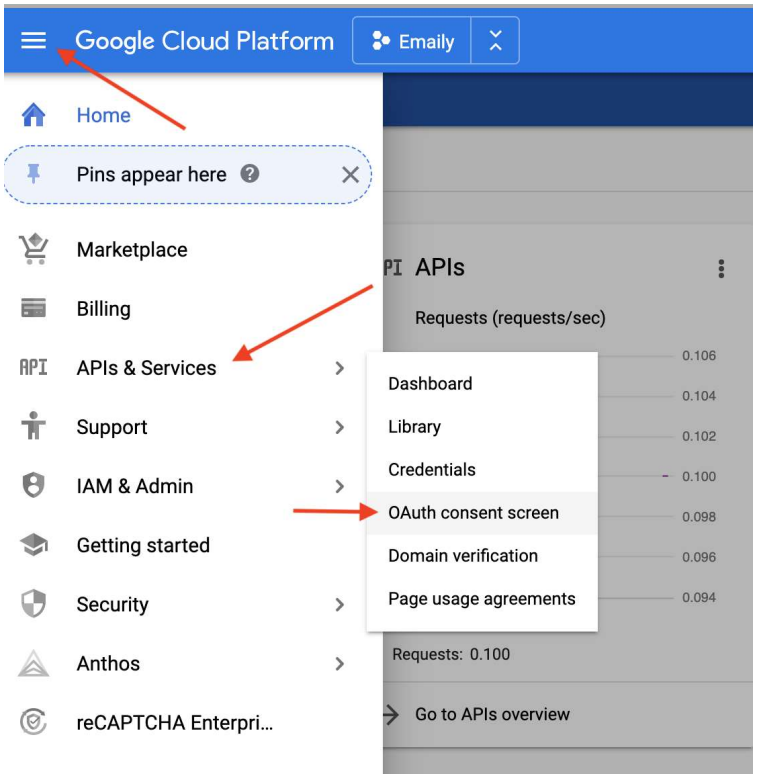
2. Click the **CREATE PROJECT** button



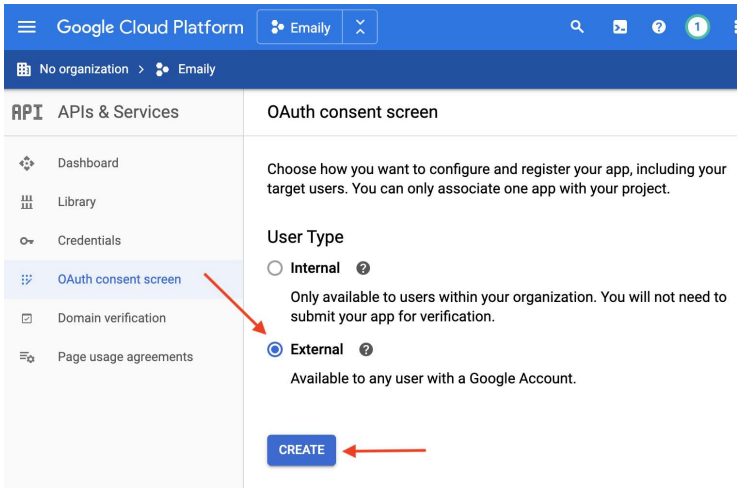
3. Name the project and click the **CREATE** button



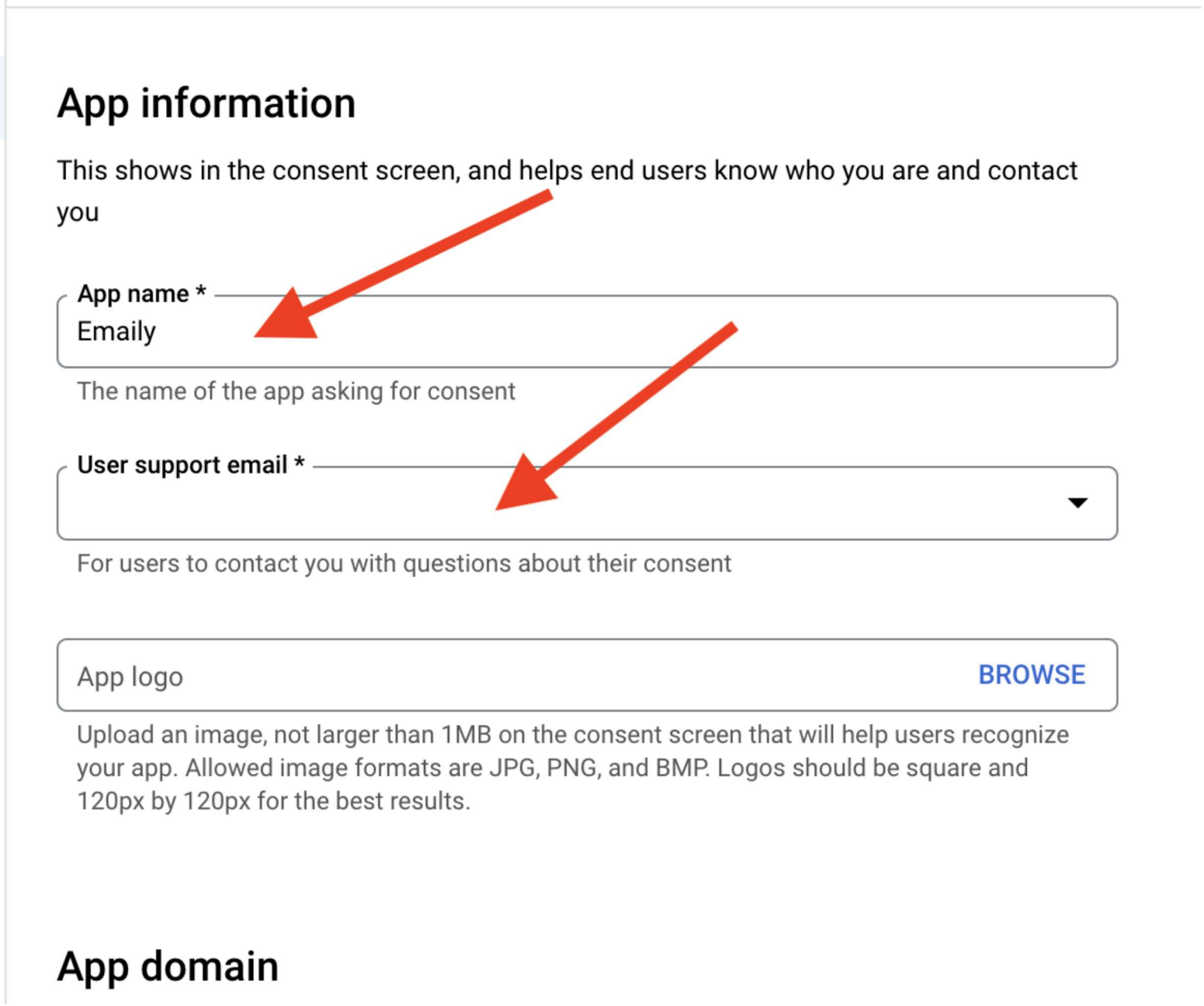
4. Click the menu button, select **APIs & Services**, then **OAuth Consent Screen**



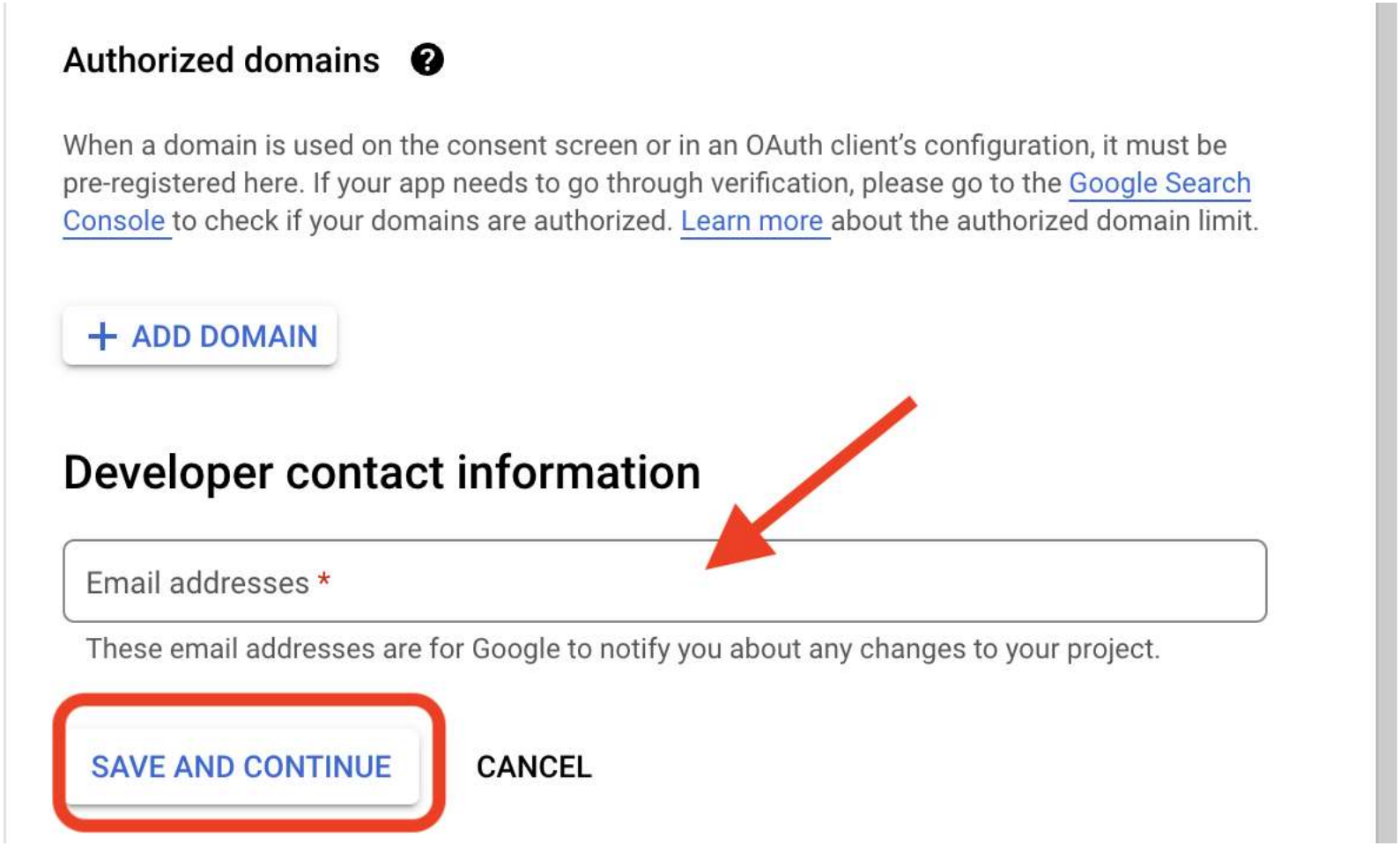
5. Select **External** and click the **CREATE** button



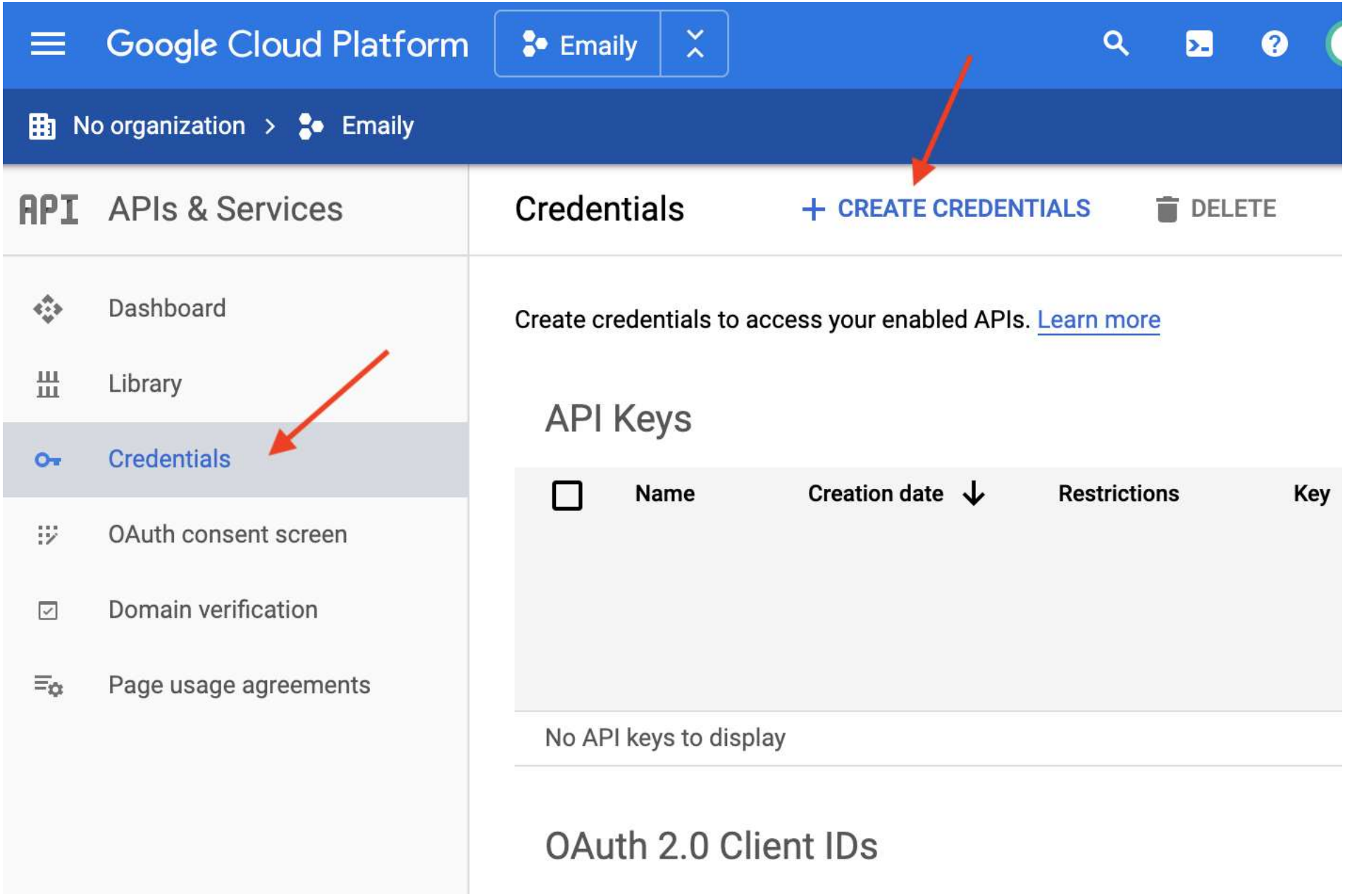
6. Fill out the **App Name** field. Then, add your email address to the **User support email** field.



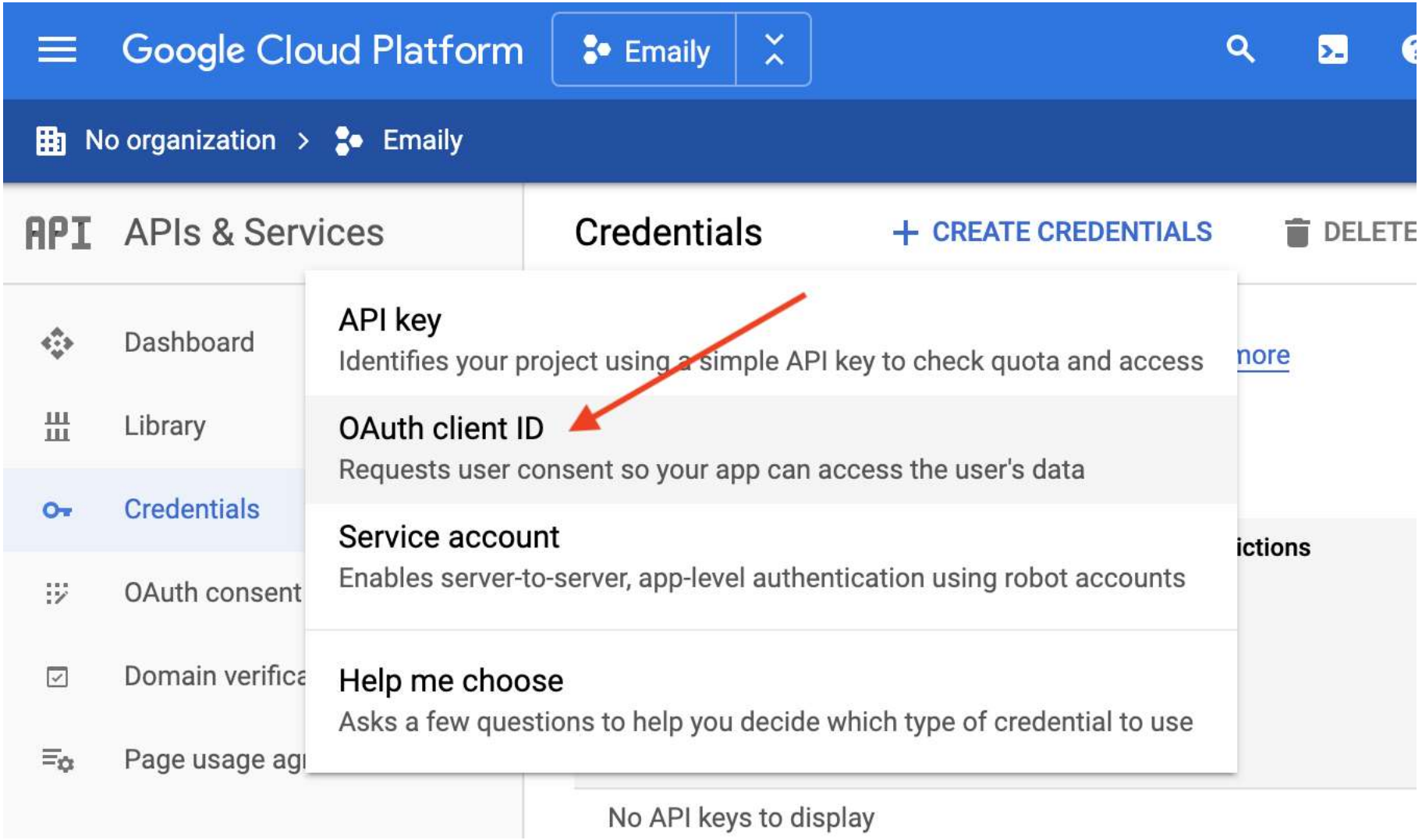
Scroll to the bottom under **Developer contact information** and add again your email address. Click the **SAVE AND CONTINUE** button. No other info should be filled out on the consent screen at this time.



7. Click **Credentials** in the sidebar and then click the **CREATE CREDENTIALS** button



9. Select **OAuth client ID**



10. Select **Web Application** and fill out the **Authorized JavaScript origins**, **Authorized redirect URIs,** and click the **Create** button.

Authorized JavaScript Origins:

http://localhost:5000

Authorized redirect URI

http://localhost:5000/auth/google/callback

Google Cloud Platform | Emaily

No organization > Emaily

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

Web client 1

Restrictions

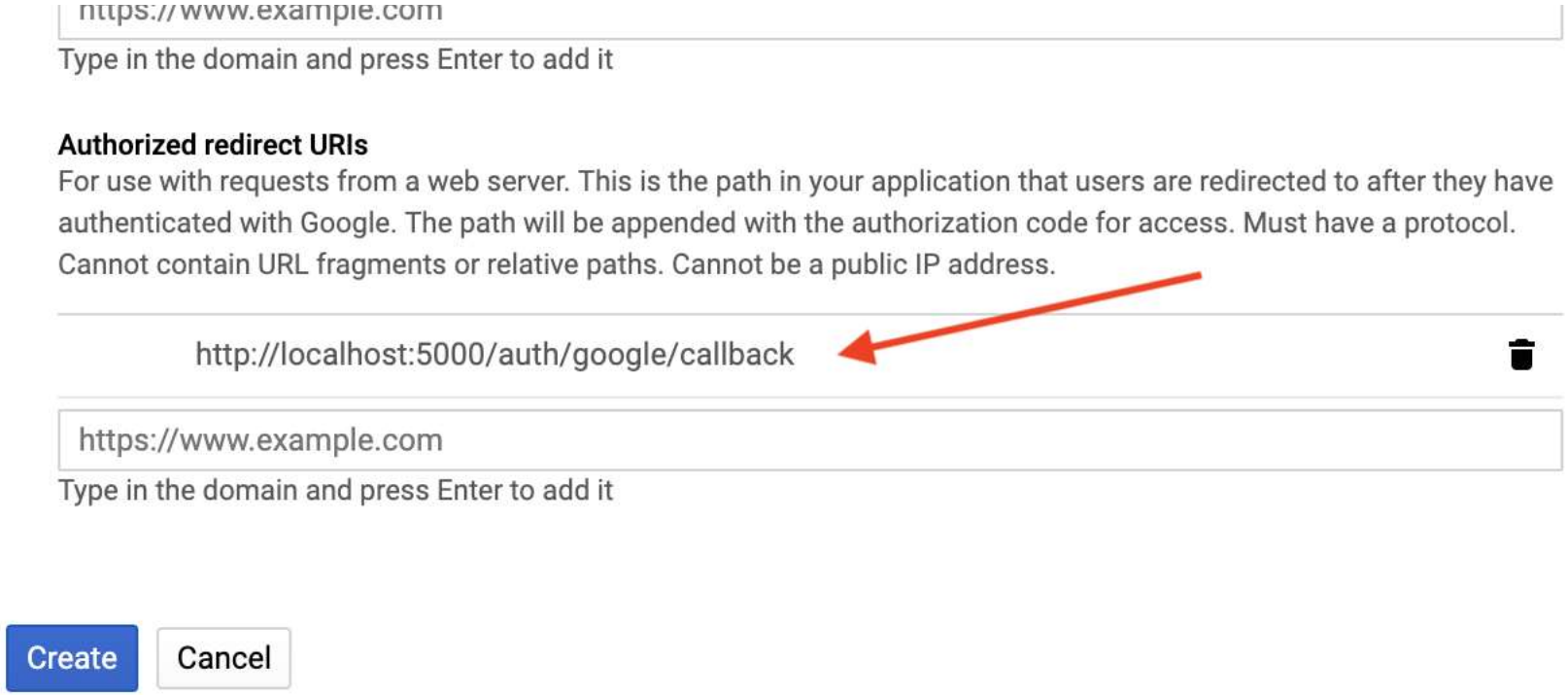
Enter JavaScript origins, redirect URIs, or both Learn More

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.

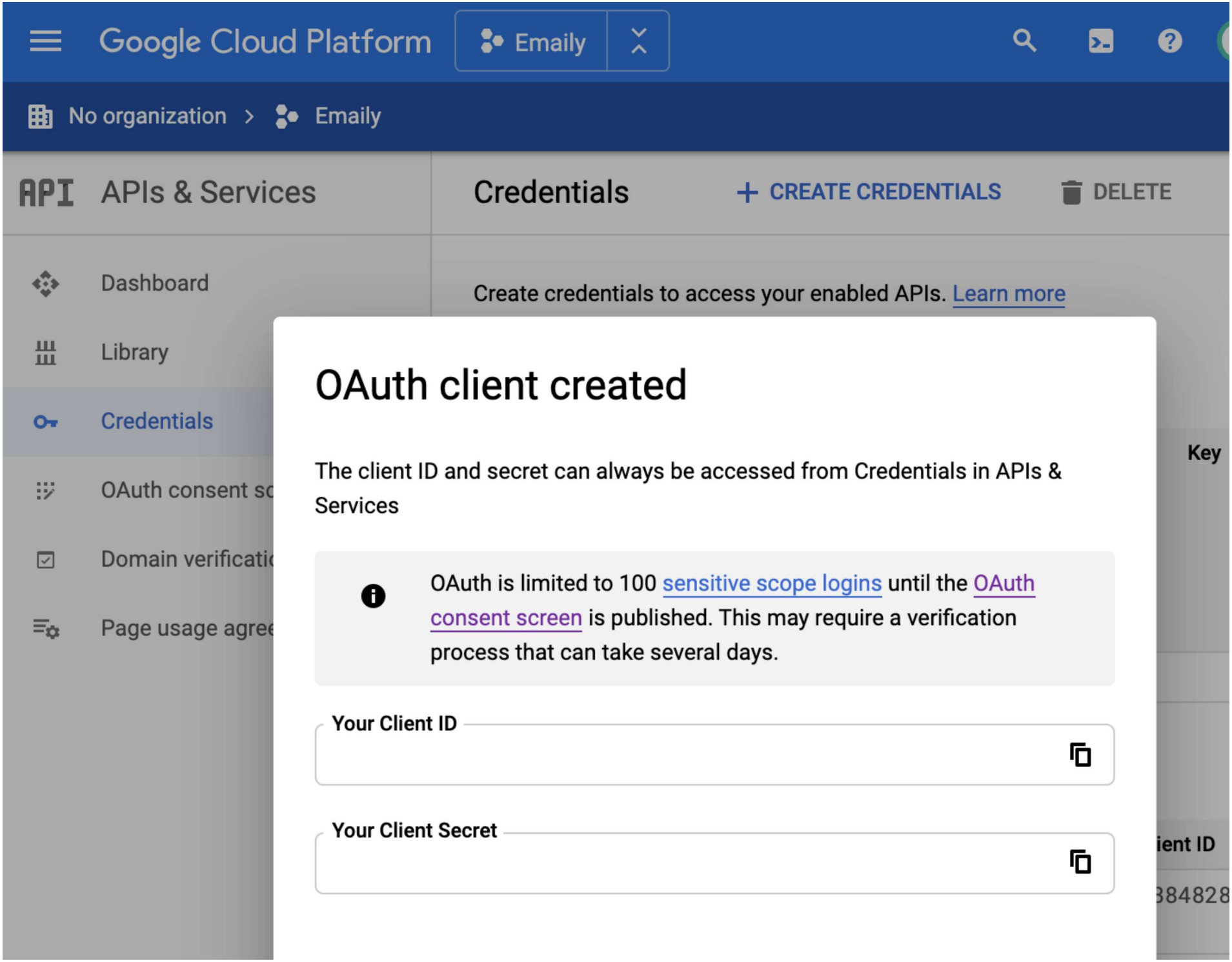
http://localhost:5000



Note! Google has made a number of changes to the OAuth credential's restrictions, and no longer allows wildcards in the redirect URI field. If you follow along with the upcoming video lecture you will get this error: ***Invalid Redirect: cannot contain a wildcard (*)***

Since the main goal of using *http://localhost:5000/** was to show the redirect error a few lectures later, we entered the correct redirect as shown above since this is what it will be changed to anyway.

11. Copy your Client ID and Client Secret in a safe place so you can use them in your application in a future lecture. (ID and Secret were redacted from the screenshot)


Google Cloud Platform
Emaily
No organization
Emaily
APIs & Services
Credentials
CREATE CREDENTIALS
DELETE
Dashboard
Library
Credentials
OAuth consent sc
Domain verificati
Page usage agree
Create credentials to access your enabled APIs. Learn more
Key
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
Your Client Secret


OK
Email
Name
Usage with all services (last 30 days