Software Security - Assignment 2

# Environment Details

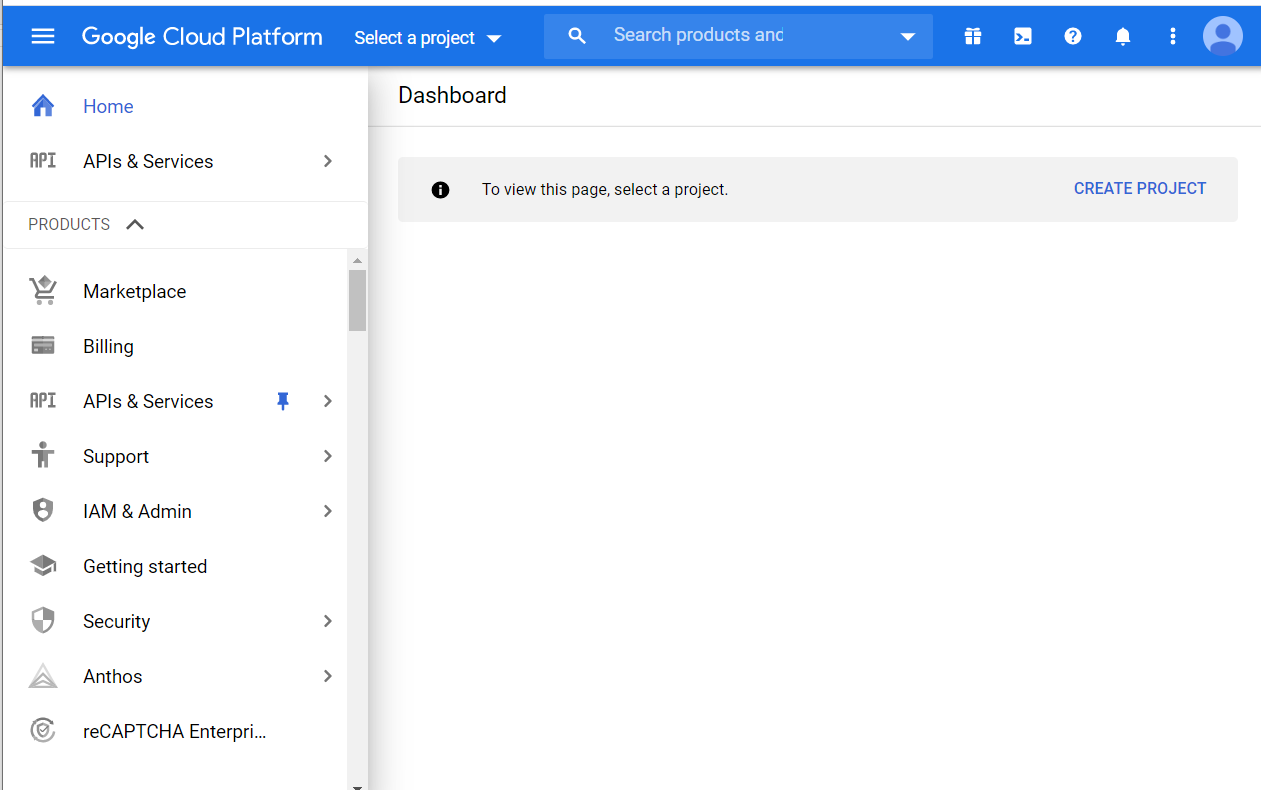
|  |  |  |
| --- | --- | --- |
| Item | Description | Link(s) |
| Operating System | Ubuntu 19.10 (eoan) | <https://releases.ubuntu.com/eoan/> |
| Development IDE | PhpStorm 2020.1 Ultimate | <https://www.jetbrains.com/phpstorm/> |
| Development Language | PHP 7.3 | <https://www.php.net/> |
| Dependency Manager | Composer 1.10.6 | <https://getcomposer.org/> |
| Authorization Server | Google OAuth2 | <https://developers.google.com/identity/protocols/oauth2> |
| Resource Server | Google Drive API | <https://developers.google.com/drive> |

# Set up Authorization Server

## Create a new project

Navigate to <https://console.developers.google.com/>

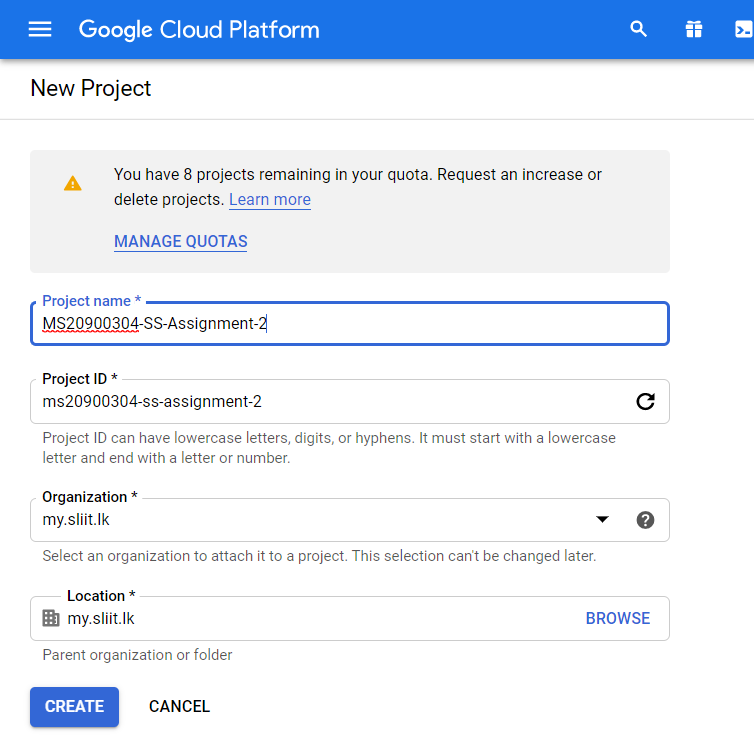
If you don’t have any projects created, a new project should be created:



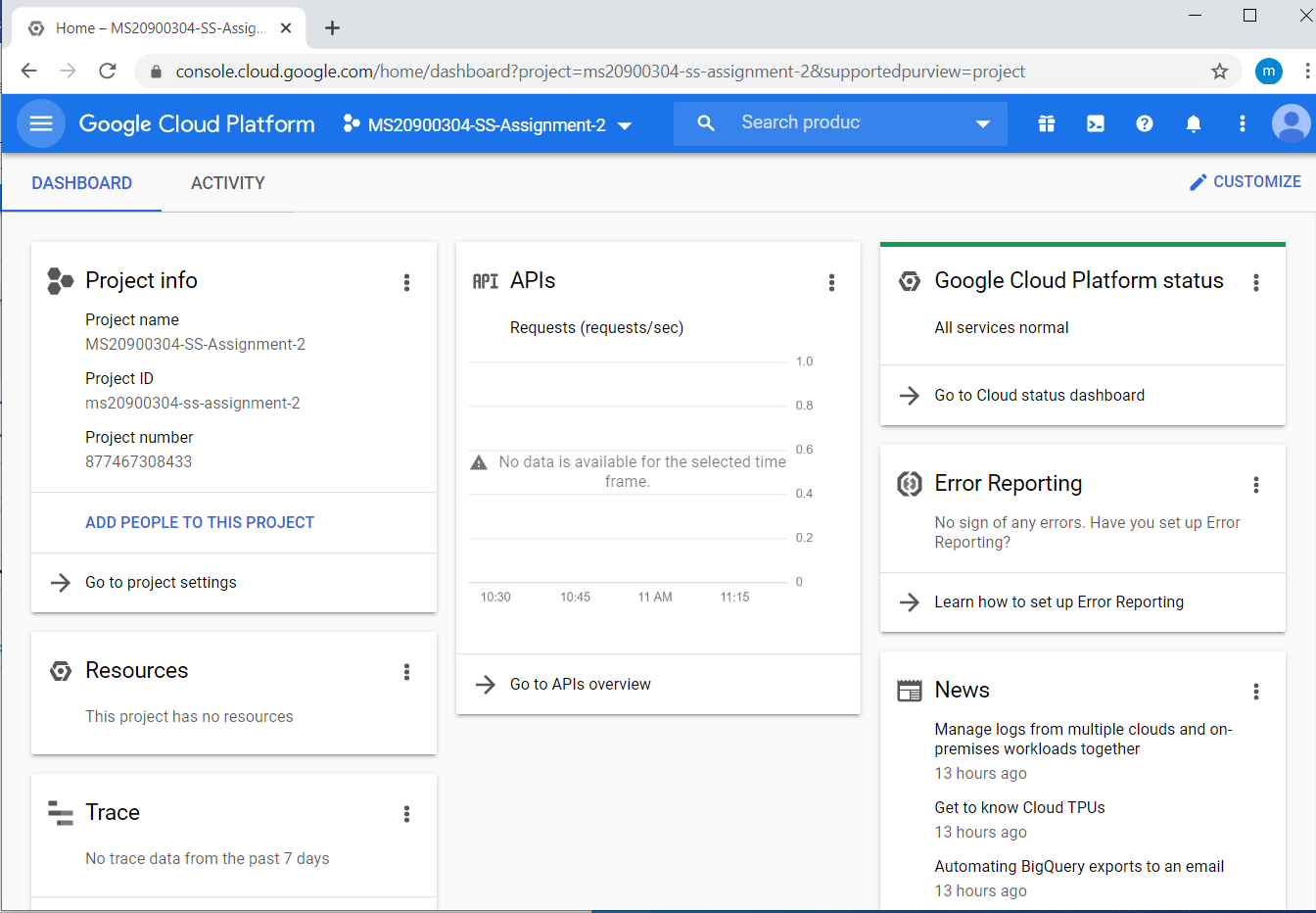
Click “Create Project”

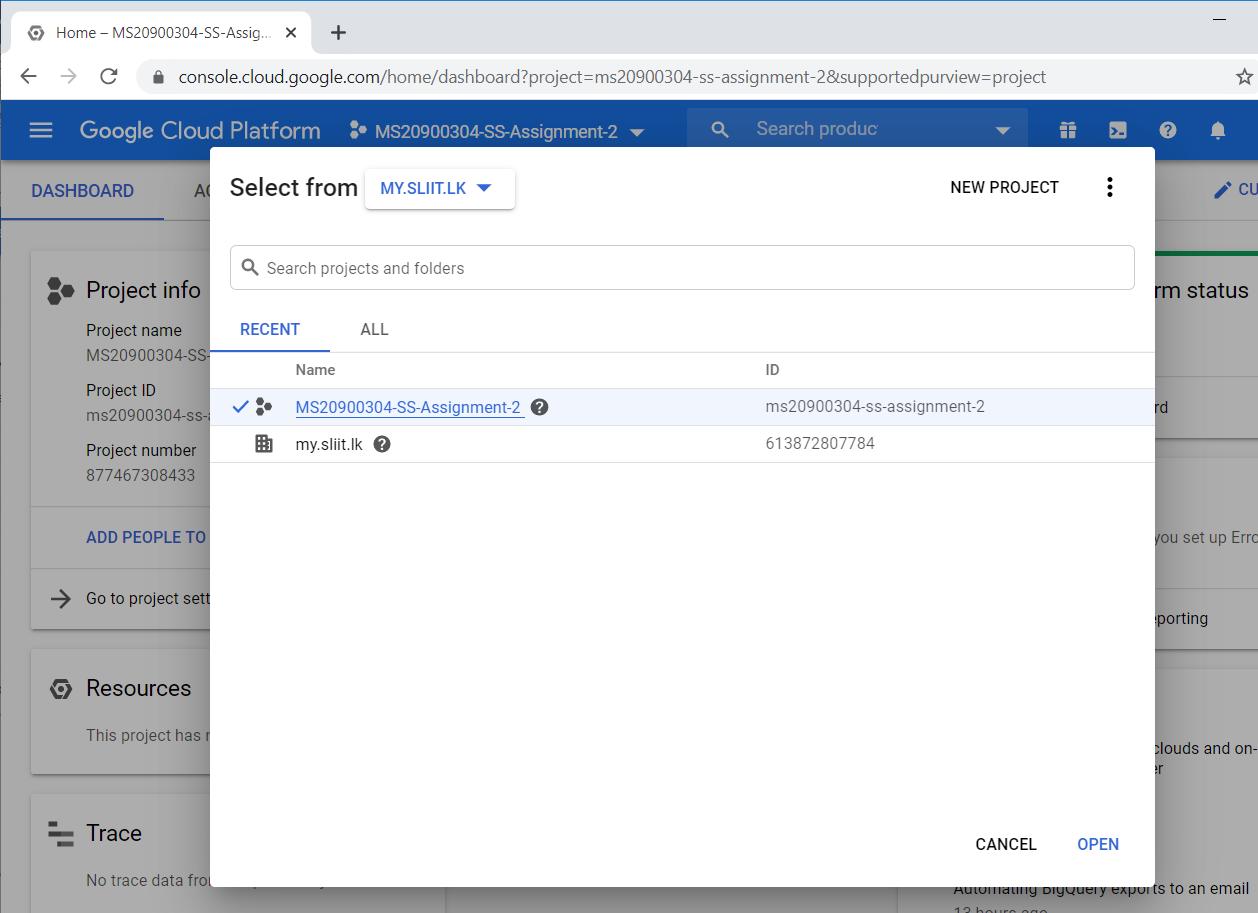
Enter the project name, click EDIT button to change the project ID. For this, following values were used:

**Project Name:** MS20900304-SS-Assignment-2  
**ID**: ms20900304-ss-assignment-2



Click “Create” to create the project.

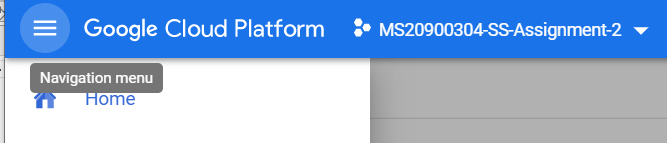




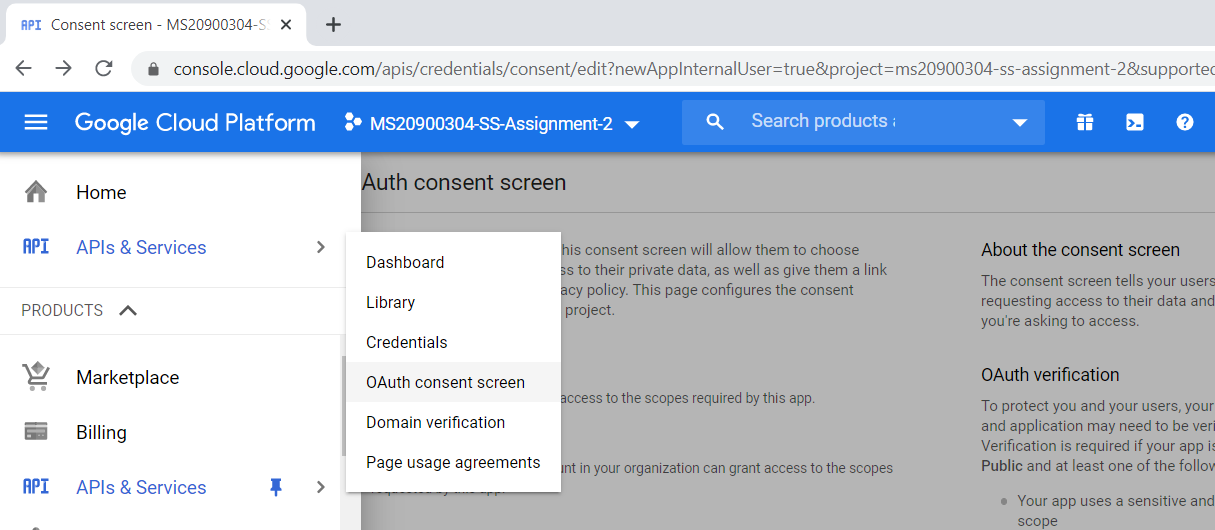
## Generate OAuth client ID

### Configuring OAuth Consent Screen

Go to “Navigation Menu”



Navigate to **APIs & Services** -> **OAuth consent screen**

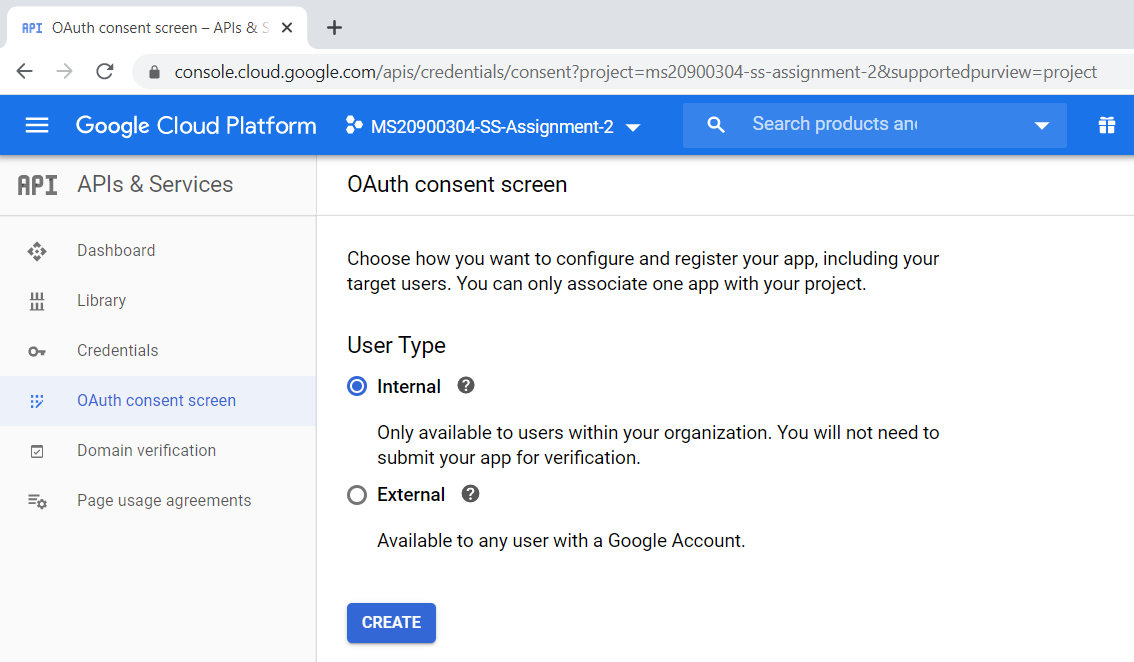


In the **OAuth consent screen**,a user type should be selected from the below options:

* **Internal**: Provides access only to the accounts belonging to the organization (in this scenario, my.sliiit.lk)
* **External**: Provides access to any user with a Google Account.

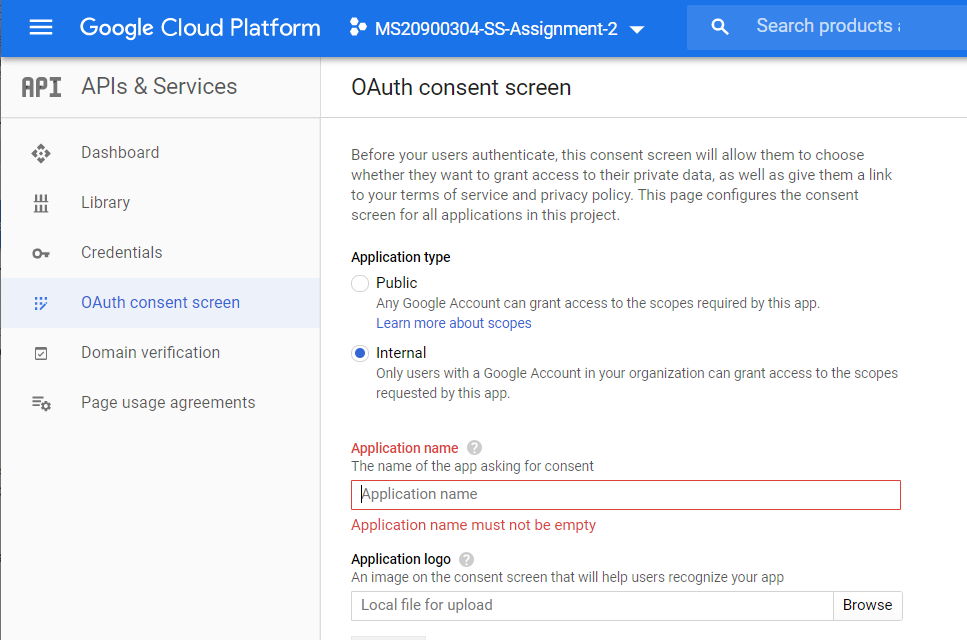
In this project, **Internal** option is selected.

Click **CREATE**



User will redirected to configure the OAuth consent screen:

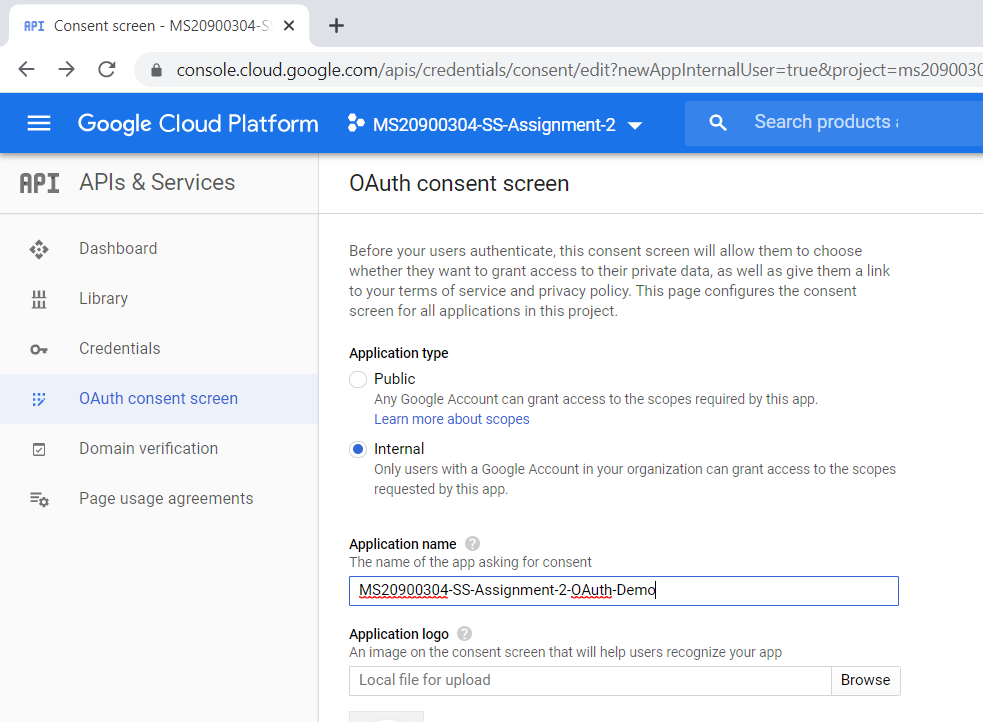
Keep the option **Internal**, based on the previous input.



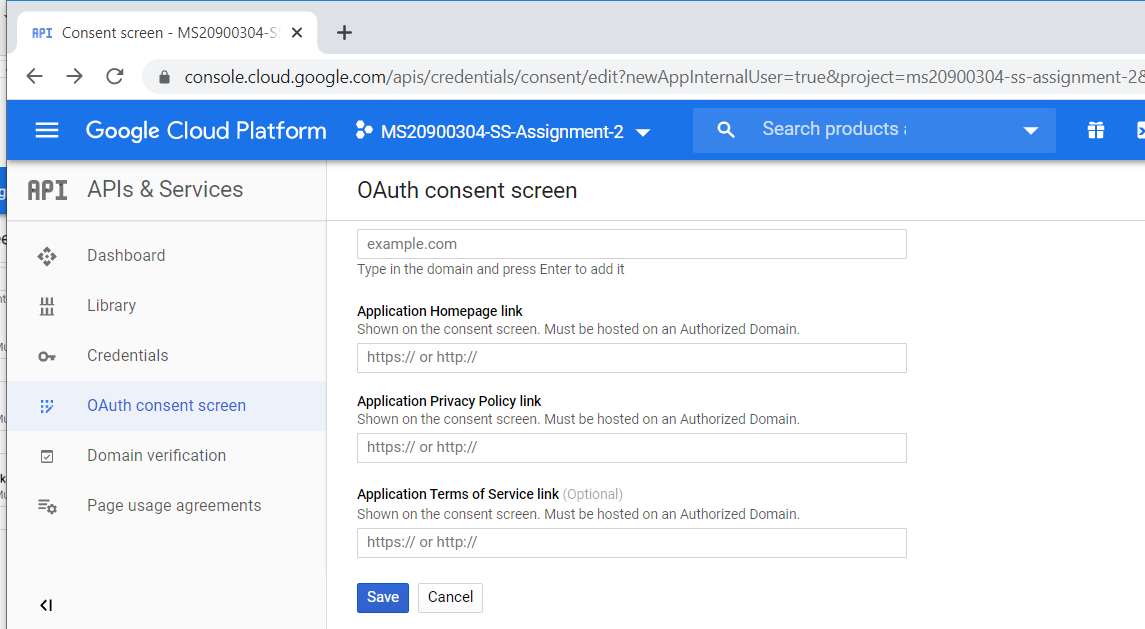
Provide an application name. This will be the name of the app asking for consent:

For this assignment, following name is used:

**MS20900304-SS-Assignment-2-OAuth-Demo**

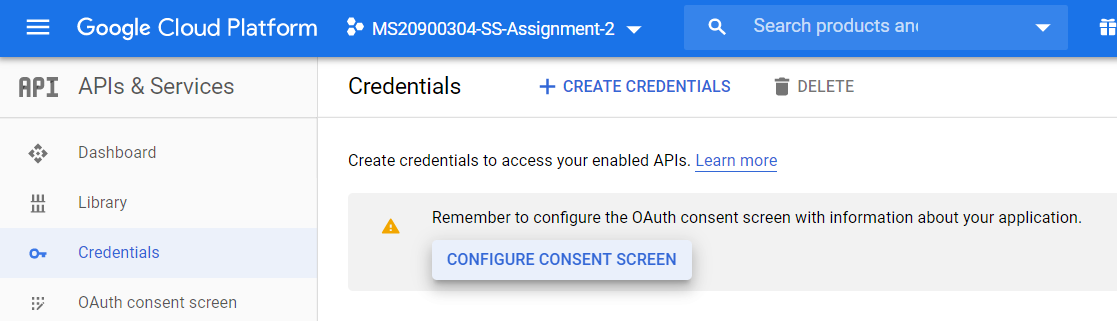


Navigate to the bottom of the screen and click **SAVE**



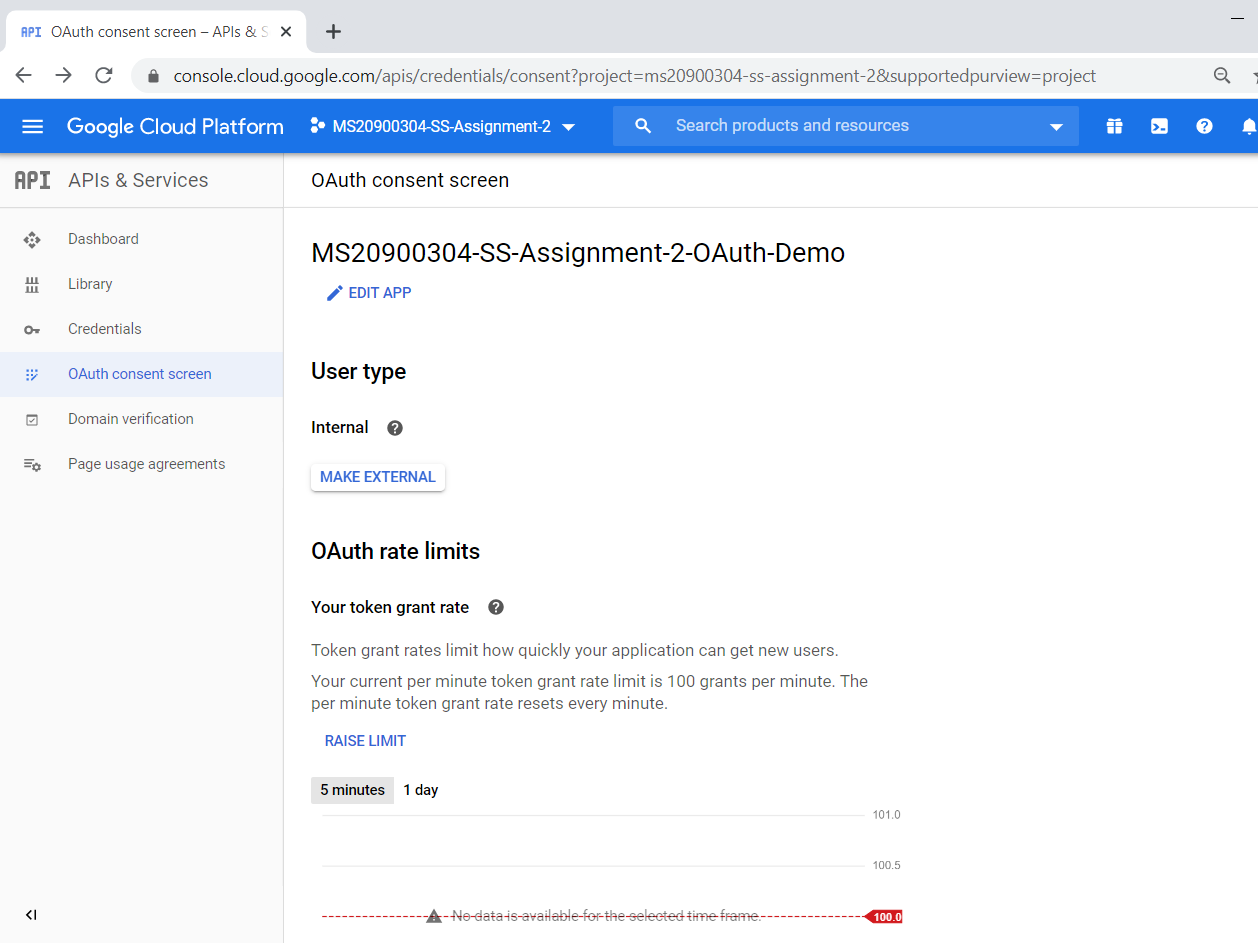
If this complete the Configure Consent Screen process, before creating an OAuth Client ID

To do this, click **CONFIGURE CONSENT SCREEN**



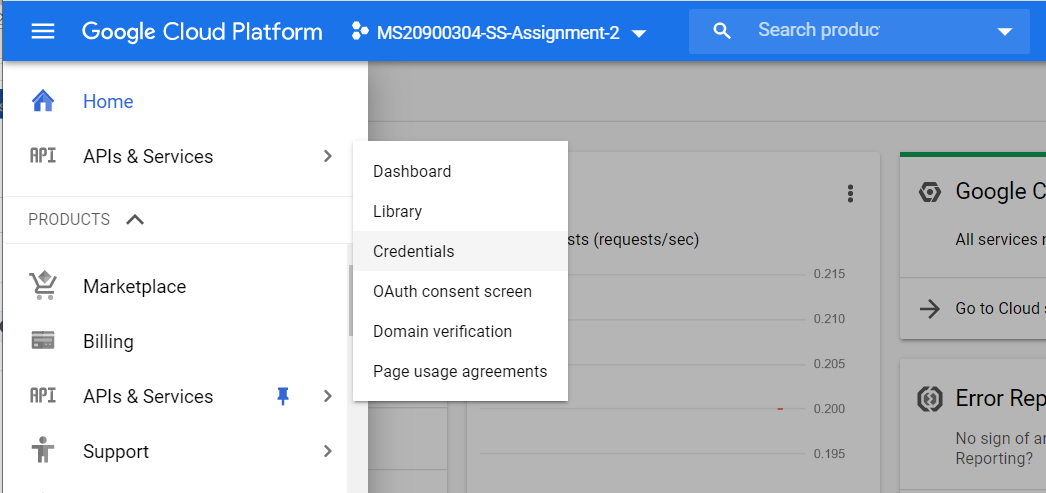
User will be redirected to the following page:

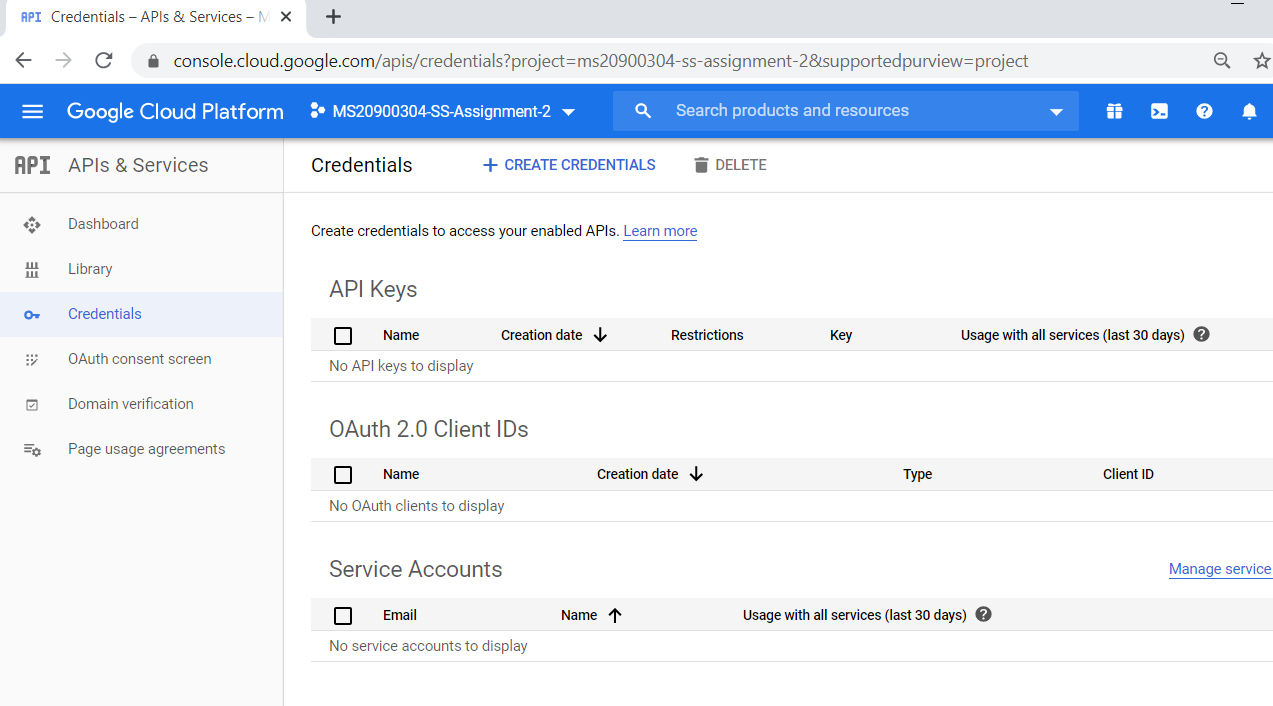
OAuth rate limits can be configured on needs basis.



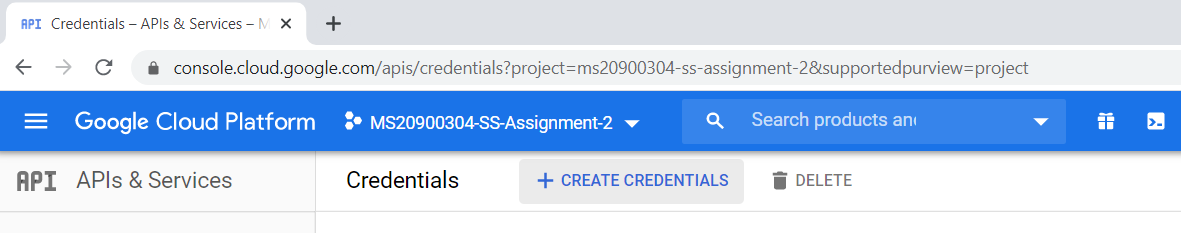
### OAuth Client ID

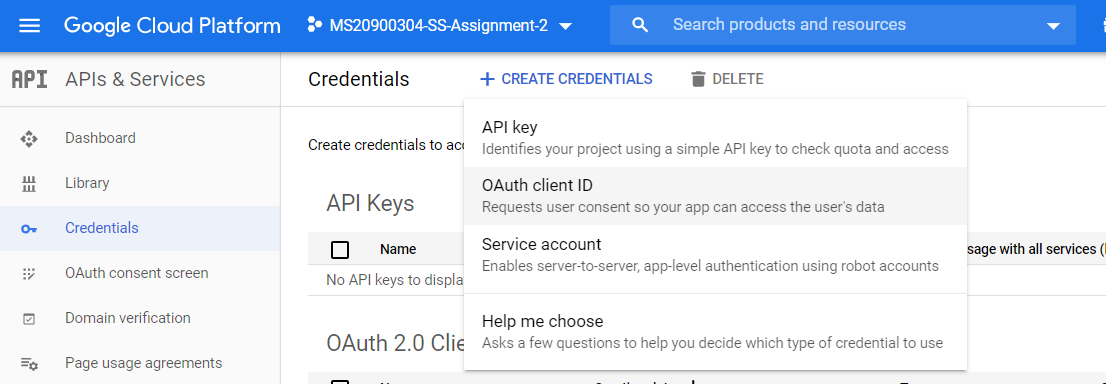
Navigate to **APIs & Services** -> **Credentials**



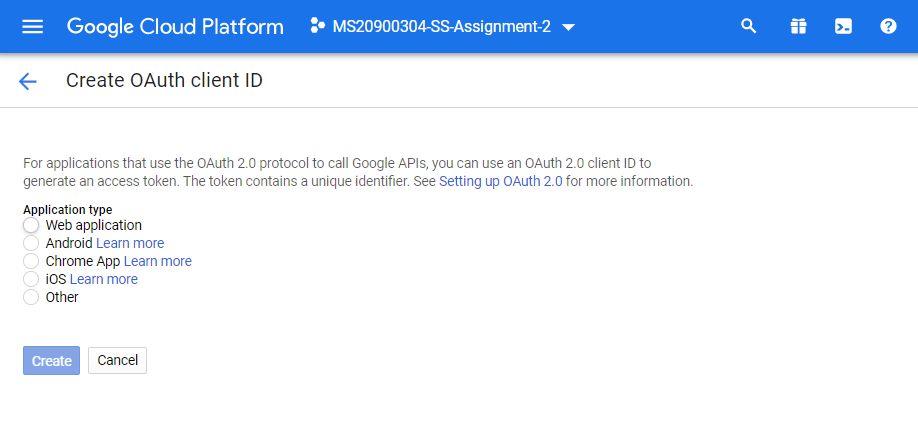


Navigate to **CREATE CREDENTIALS** -> **OAuth Client ID**





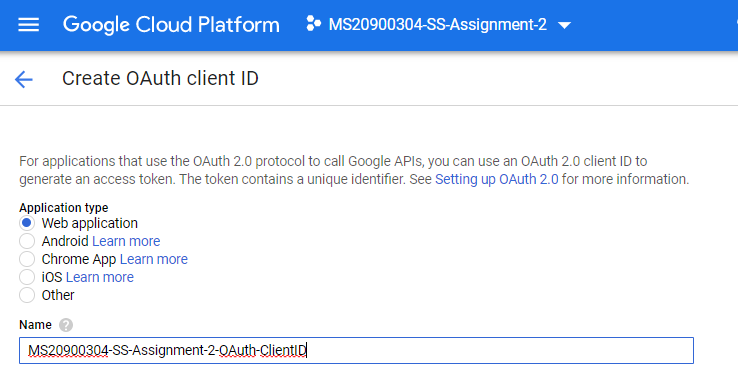
For this assignment, select **Web Application** option:



Enter a name for the OAuth client ID:

Following name was used:

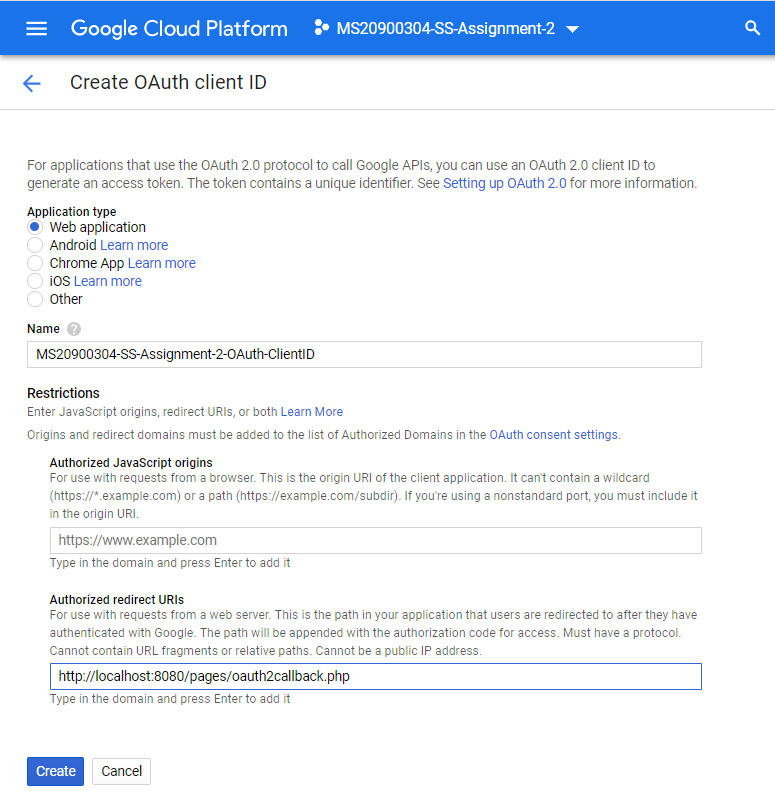
MS20900304-SS-Assignment-2-OAuth-ClientID



For the Authorized redirect URIs field, following path is used, which the application users are redirected to after authenticated with Google:

<http://localhost:8080/pages/oauth2callback.php>

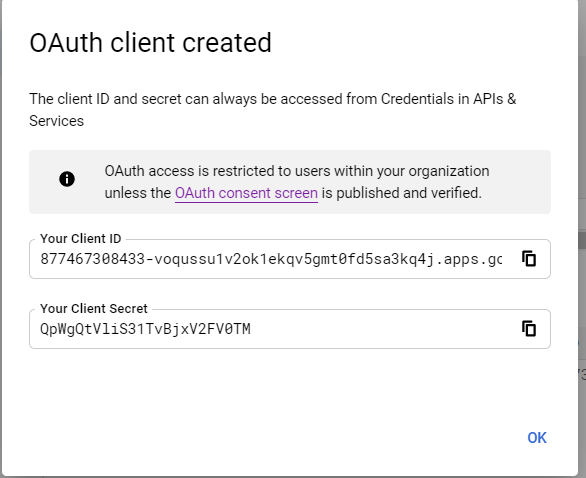
Click **Create** to save changes.



After successful submission, following popup will appear, with the Client ID and Client Secret:

**Client ID:** 877467308433-voqussu1v2ok1ekqv5gmt0fd5sa3kq4j.apps.googleusercontent.com

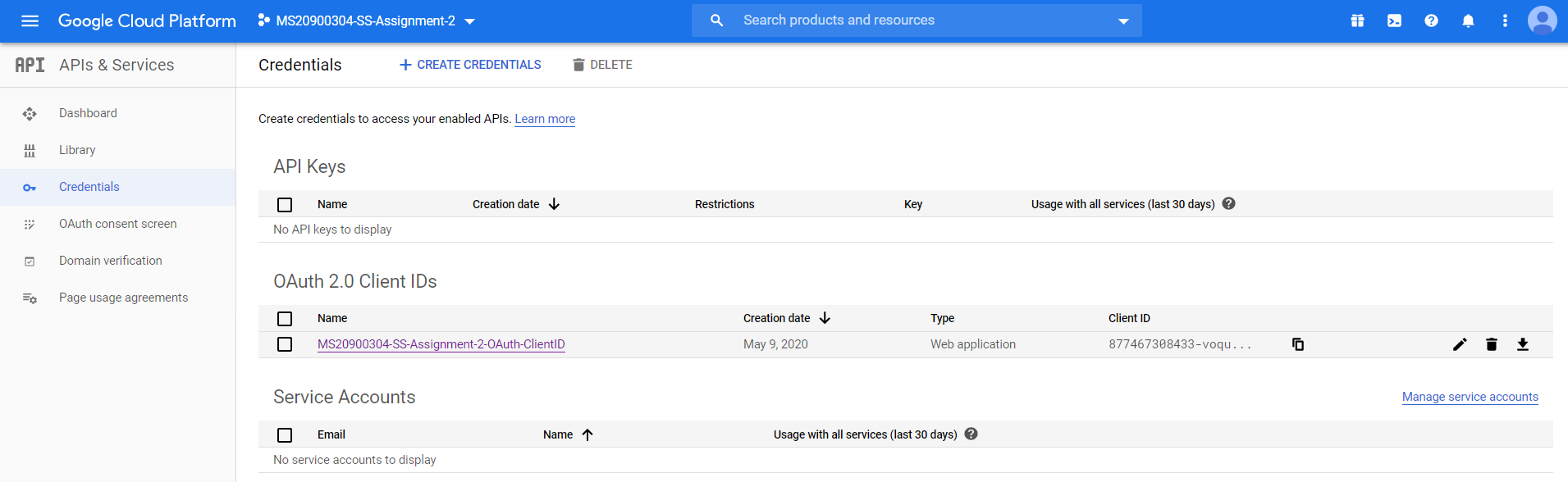
**Client Secret:** QpWgQtVliS31TvBjxV2FV0TM

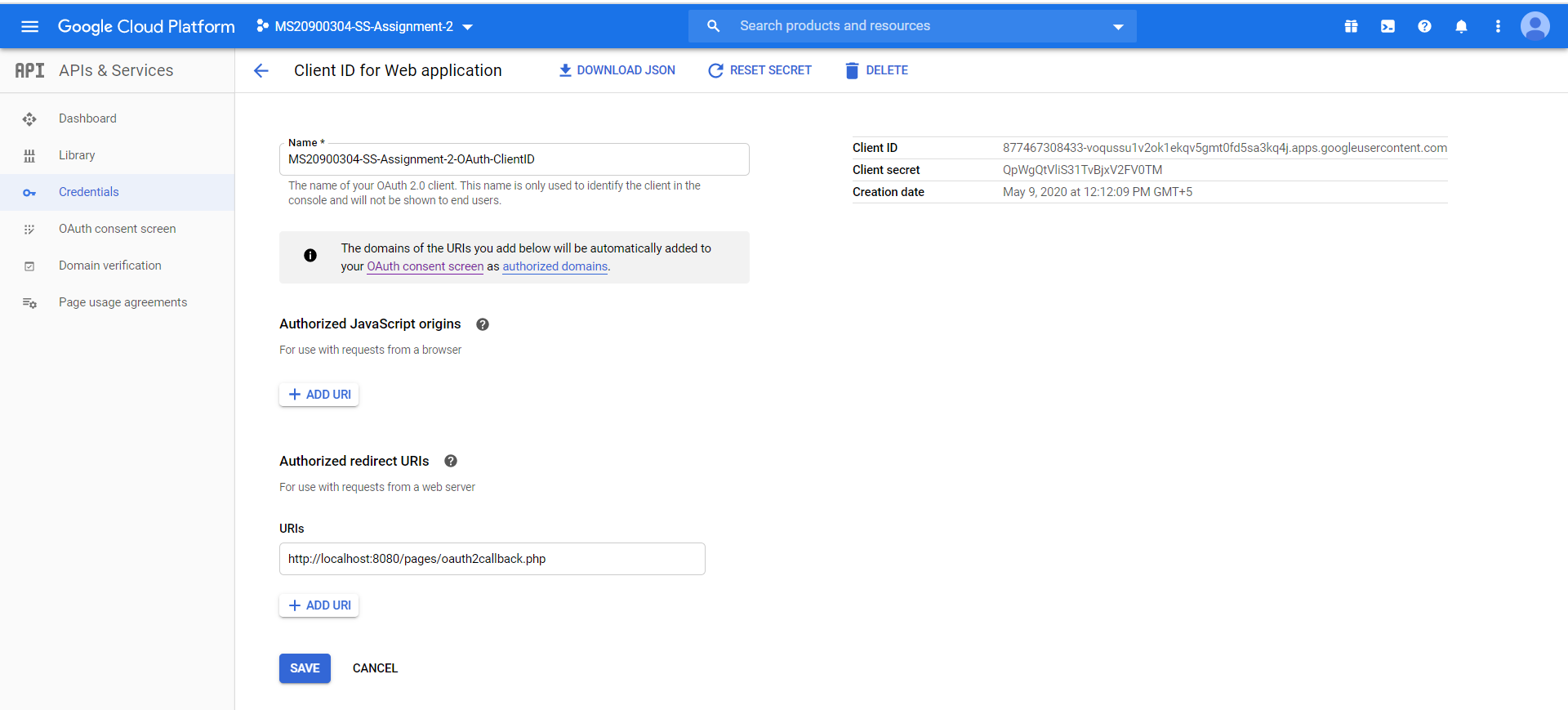


Click OK.

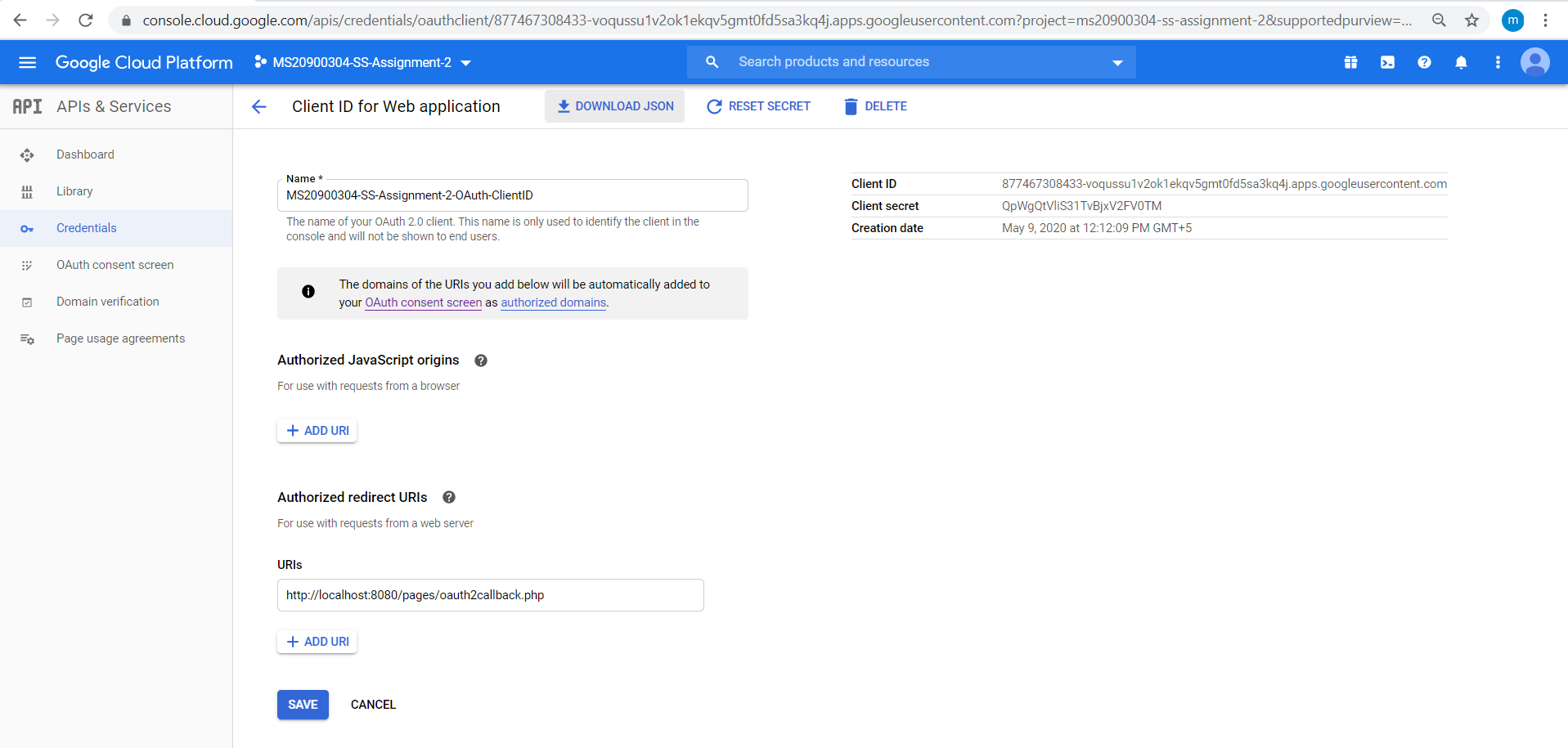
### Generate OAuth Client ID JSON file

Navigate to **Credentials** - OAuth 2.0 Client IDs -> [Client ID Name] **MS20900304-SS-Assignment-2-OAuth-ClientID** to view the created Client ID details





Click **DOWNLOAD JSON** button to get the Client ID information as a JSON file.



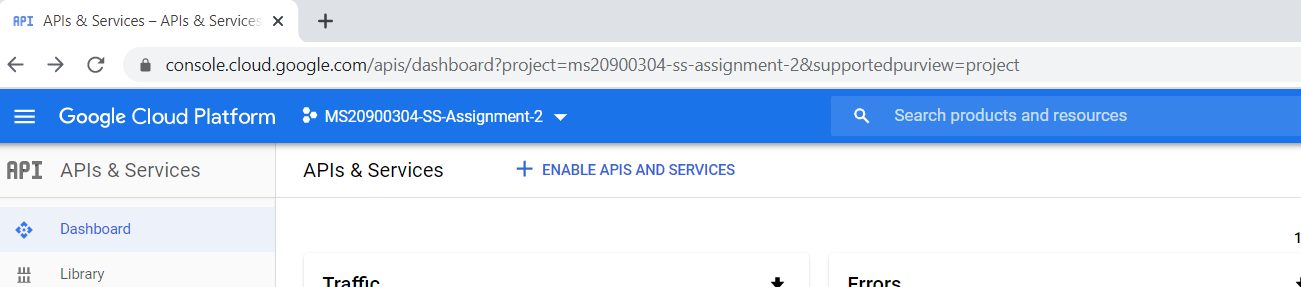
Please refer for APPENDIX - A for the contents of the JSON file.

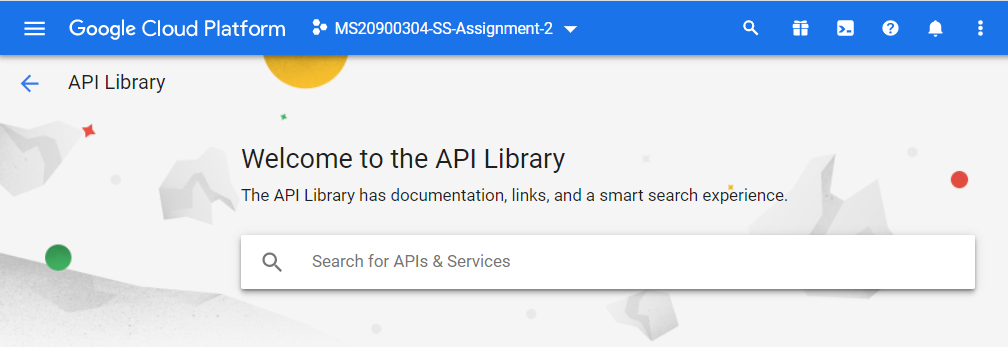
# Set up Resource Server

For this assignment, Google Drive was used as the resource server.

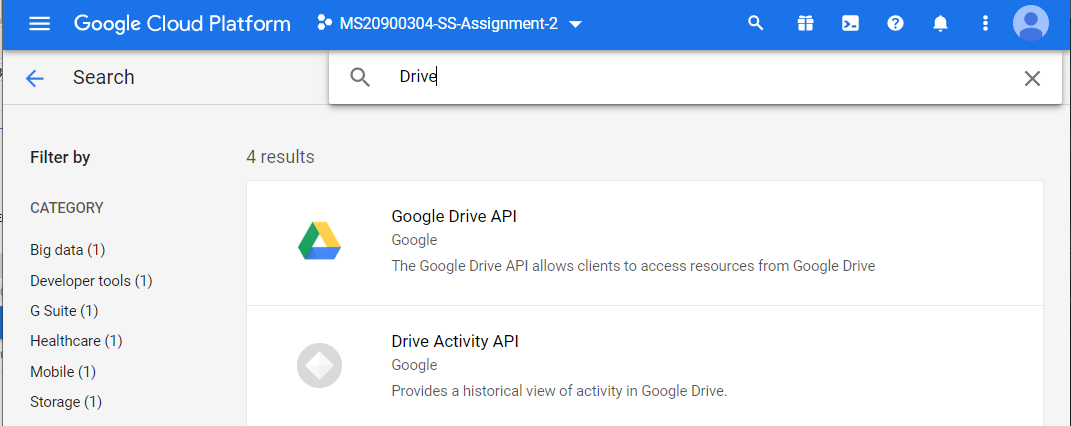
## Enable Google Drive API

Navigate to **APIs & Services** -> **Dashboard** -> Click **+ ENABLE APIS AND SERVICES**

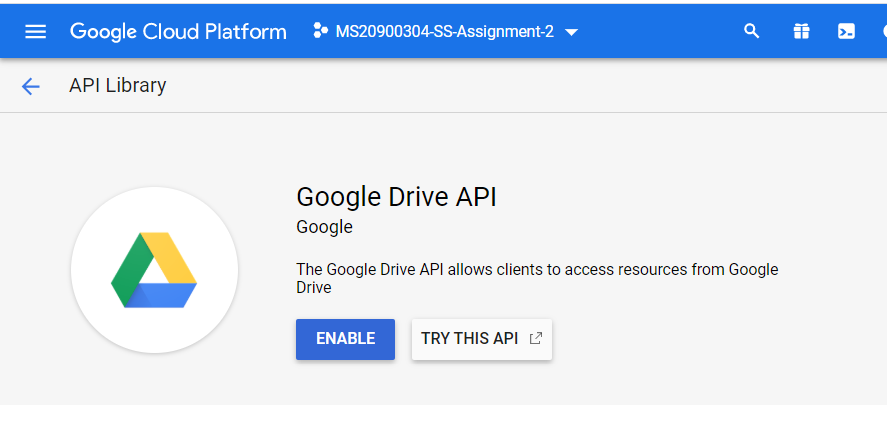




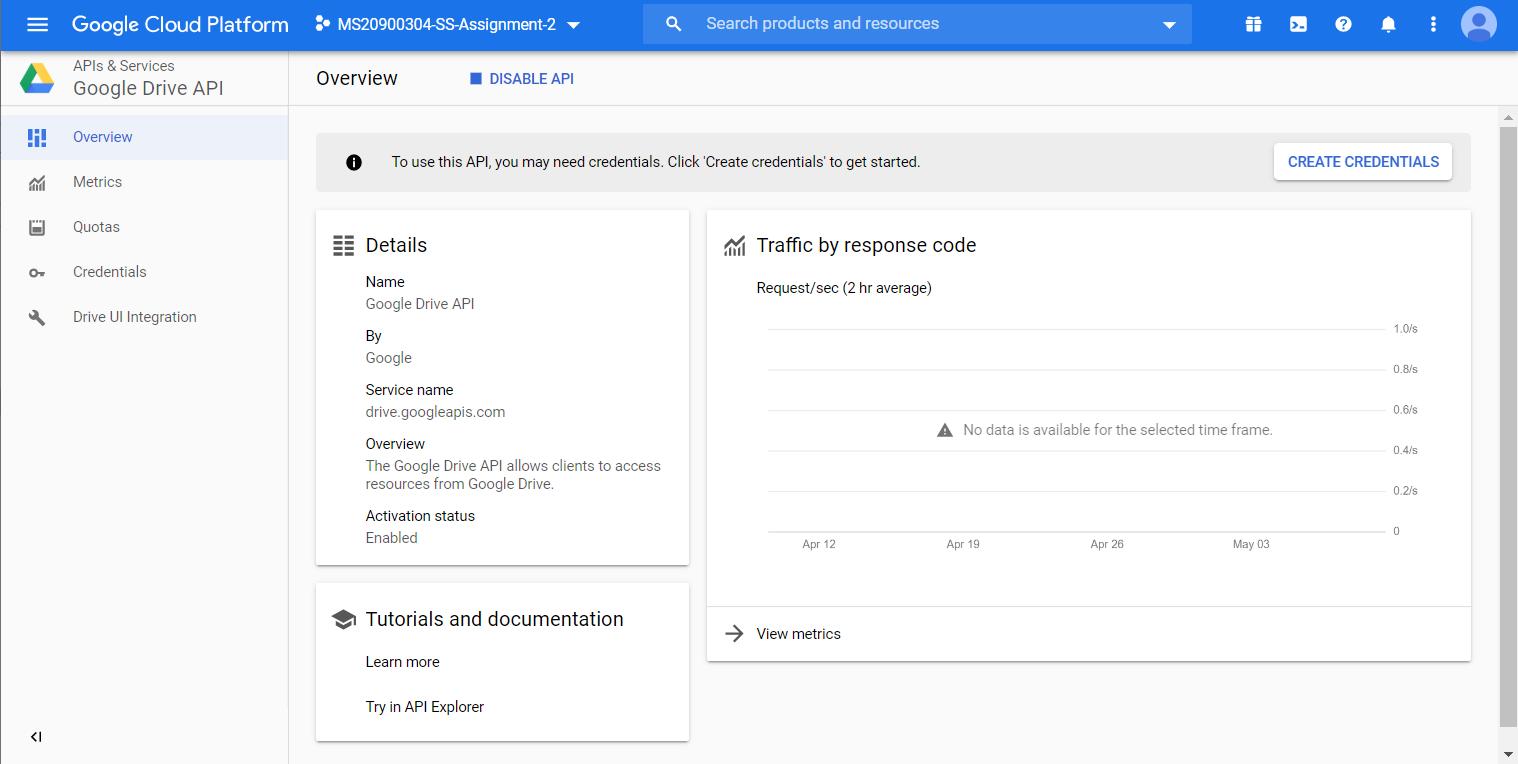
Search for Google Drive API -> Navigate to Google Drive API



Click ENABLE



After enabling, the user will be redirected to the API’s dashboard



# Code flows

REFERENCES

APPENDICES

1. OAuth Client ID contents

(Use a text editor to view the file contents)



Contents:

{"web":{"client\_id":"877467308433-voqussu1v2ok1ekqv5gmt0fd5sa3kq4j.apps.googleusercontent.com","project\_id":"ms20900304-ss-assignment-2","auth\_uri":"https://accounts.google.com/o/oauth2/auth","token\_uri":"https://oauth2.googleapis.com/token","auth\_provider\_x509\_cert\_url":"https://www.googleapis.com/oauth2/v1/certs","client\_secret":"QpWgQtVliS31TvBjxV2FV0TM","redirect\_uris":["http://localhost:8080/pages/oauth2callback.php"]}}