portainer.io

Portainer Extension Software

Implementation Guide

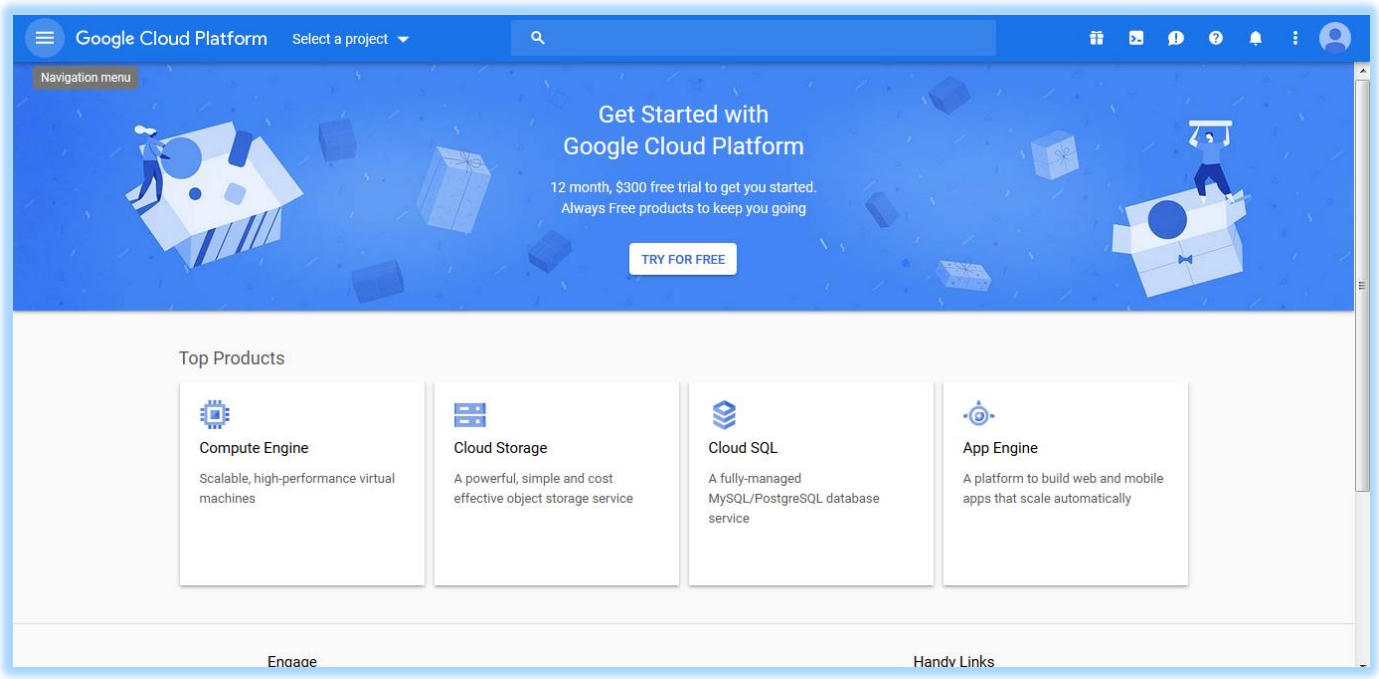
External Authentication for Google

March 2019

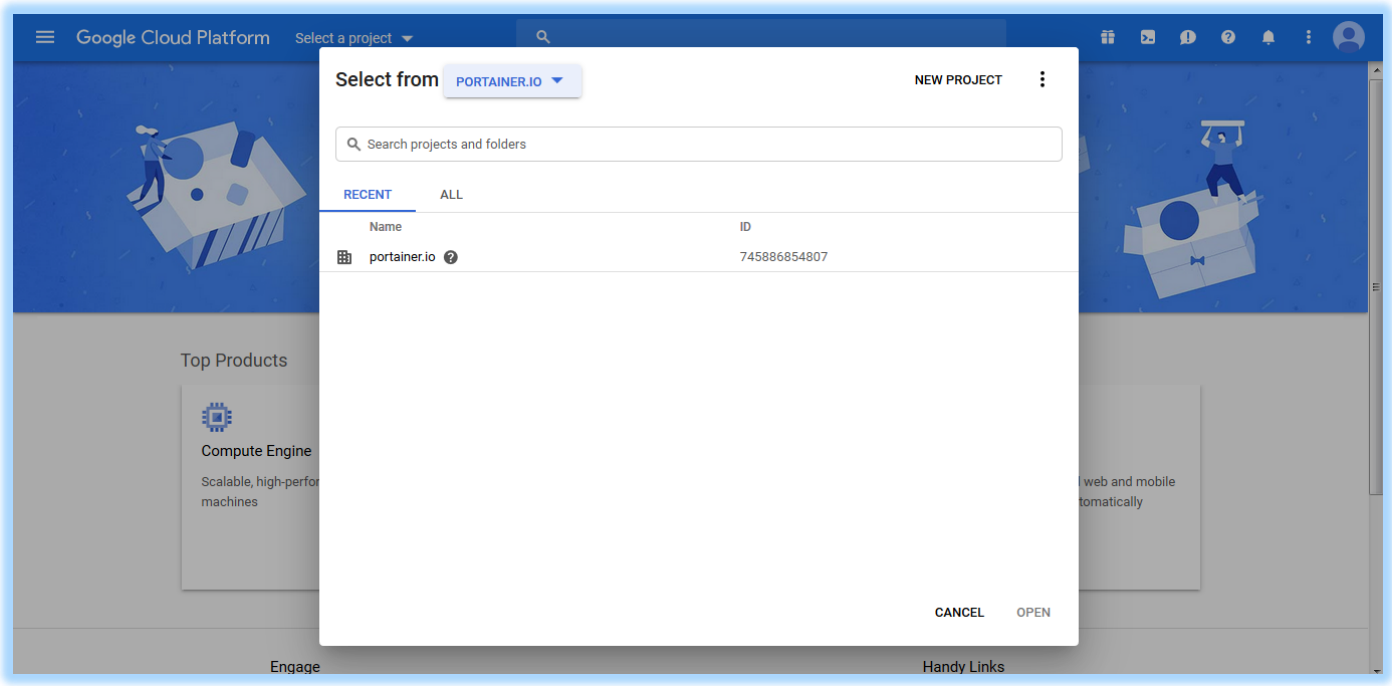
Implementation Guide

External Authentication for Google

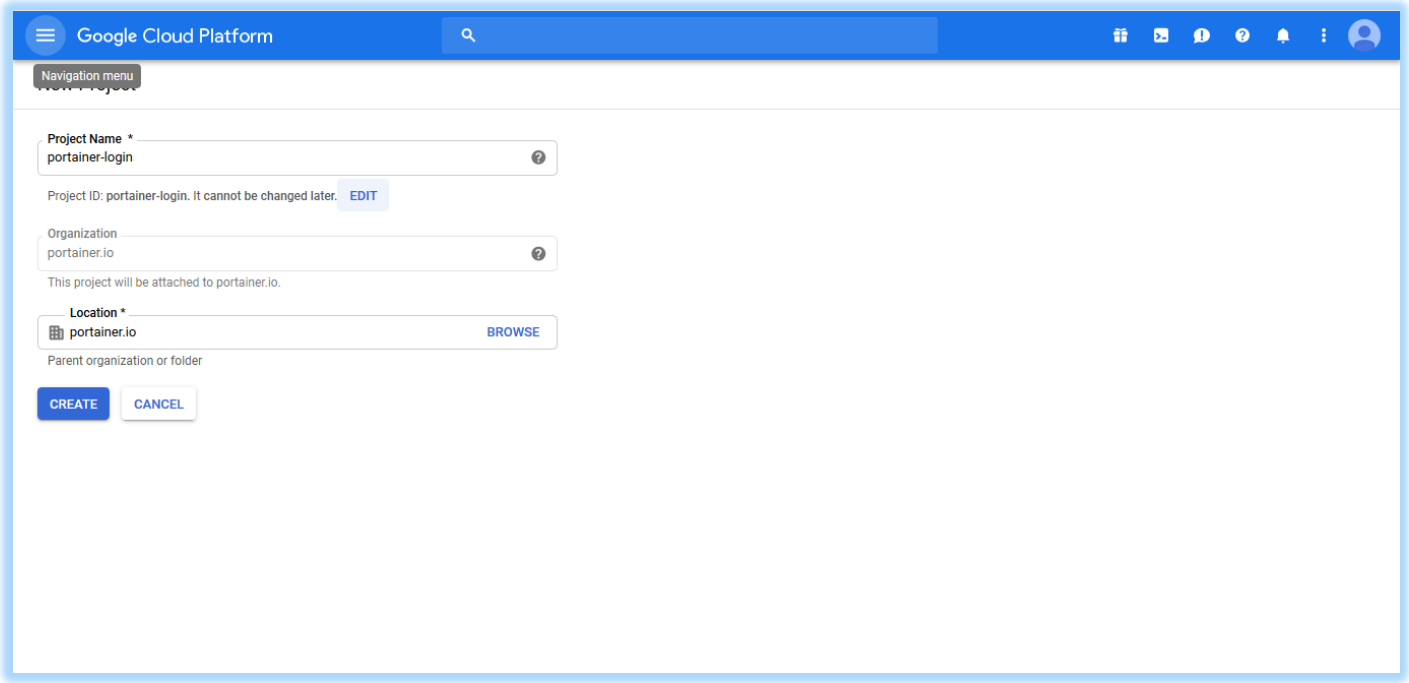
Step 1. Login to your Google Cloud Portal (console.cloud.google.com) as an Admin,



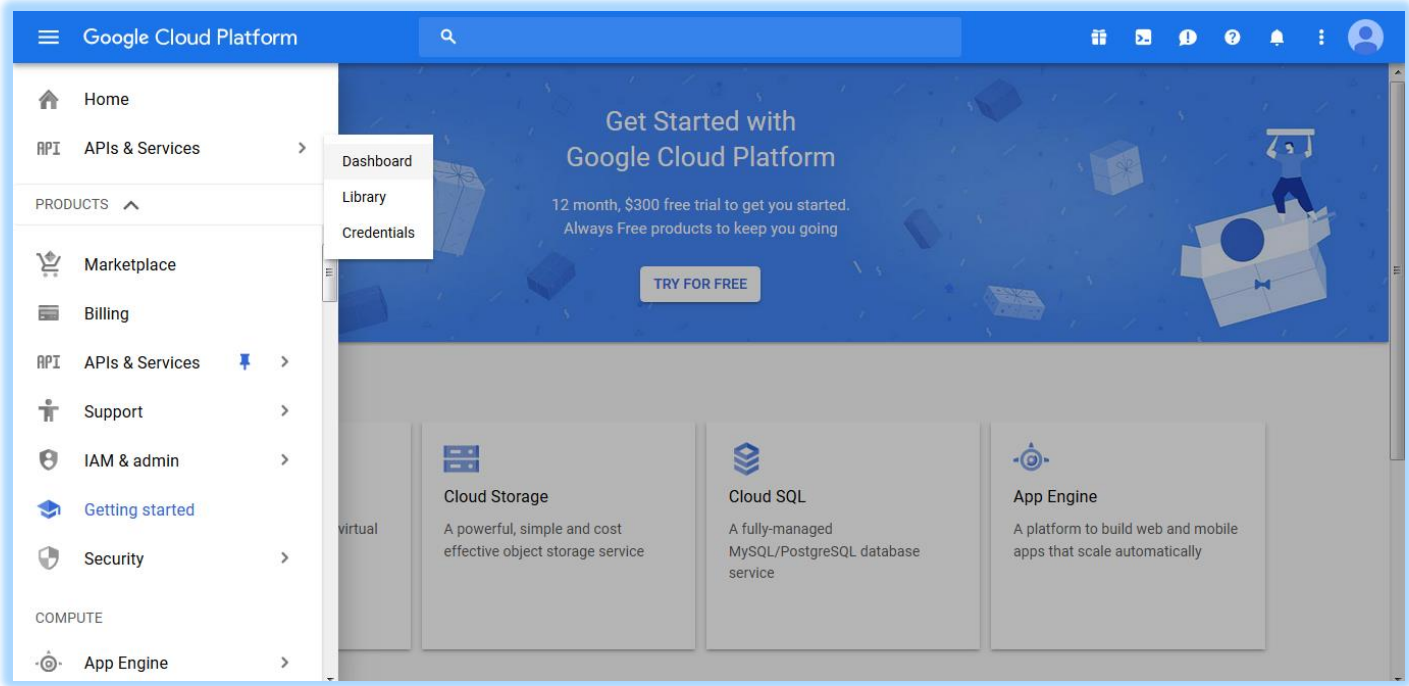
Step 2. Click on “Select Project”, then select your Org, and then select “NEW PROJECT”



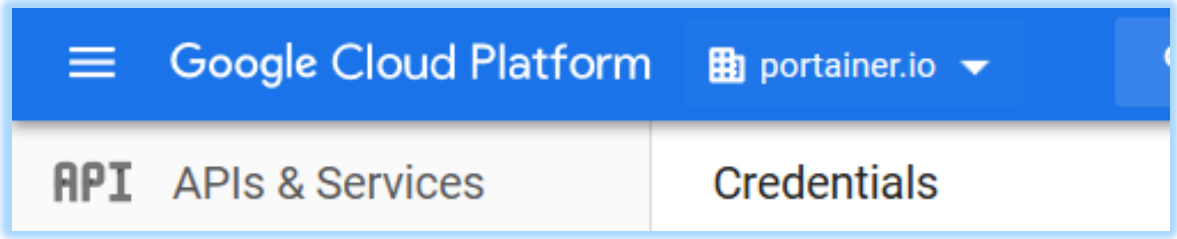
Step 3. Give the project a name, such as portainer-login, and then click “Create”

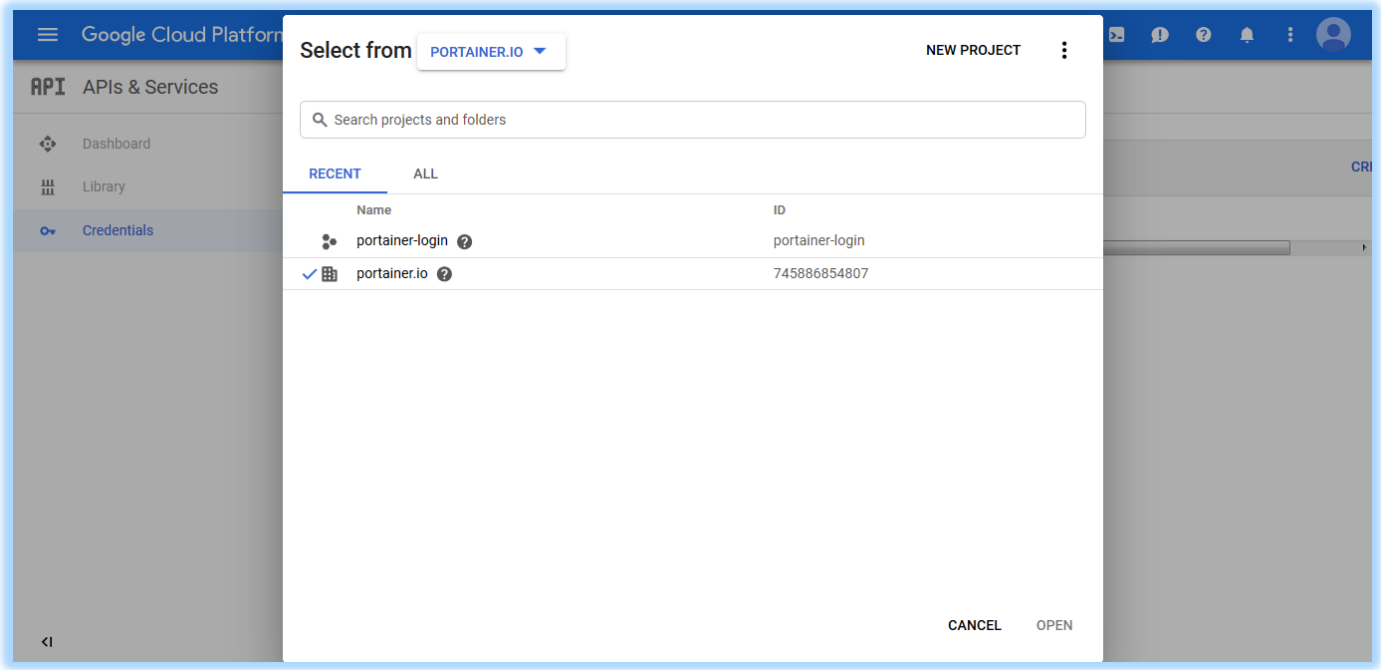


Step 4. Wait for the project to be created (30 seconds), and then click on the navigation bar, and select “APIs & Services”, Credentials.



Select the drop down list in the header bar, and change the focus to the “portainer-login” project


Google Cloud Platform
portainer.io
APIs & Services
Credentials

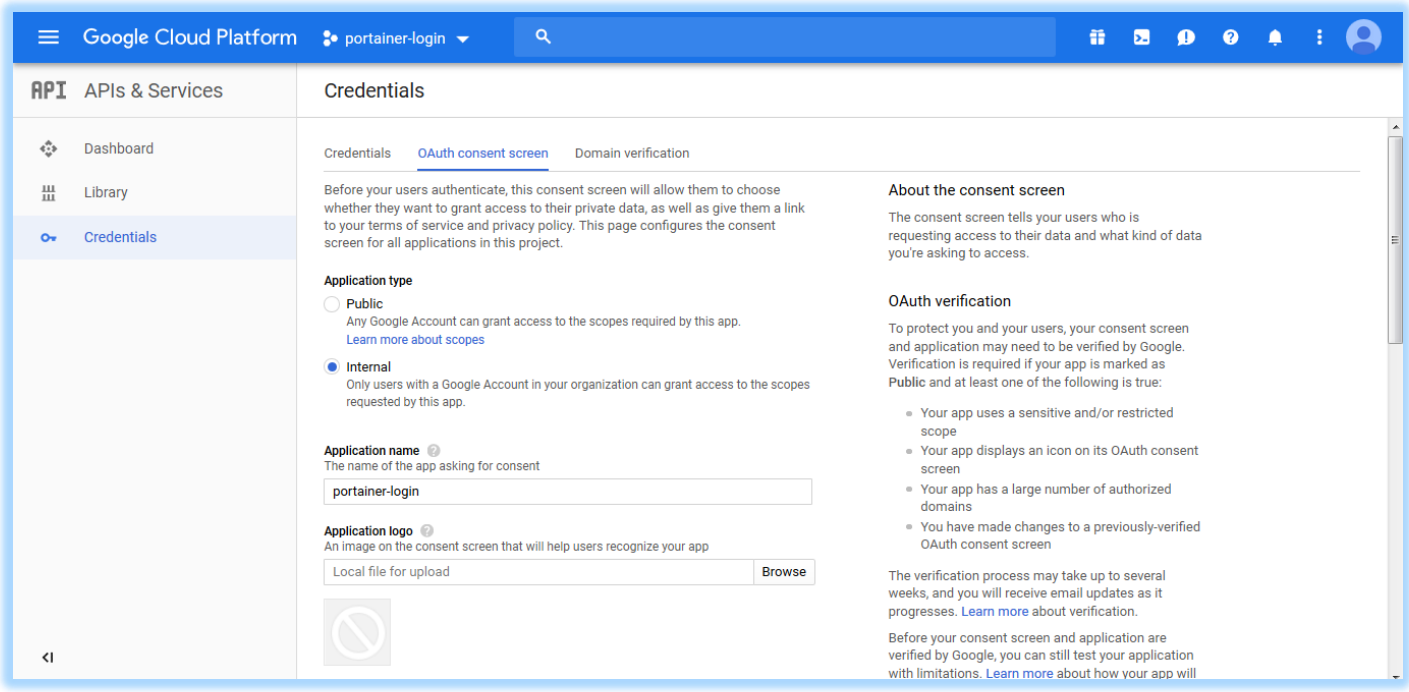

Google Cloud Platform
APIs & Services
Dashboard
Library
Credentials
Select from
PORTAINER.IO
NEW PROJECT
Search projects and folders
RECENT
ALL
Name
ID
portainer-login
portainer-login
portainer.io
745886854807
CANCEL
OPEN

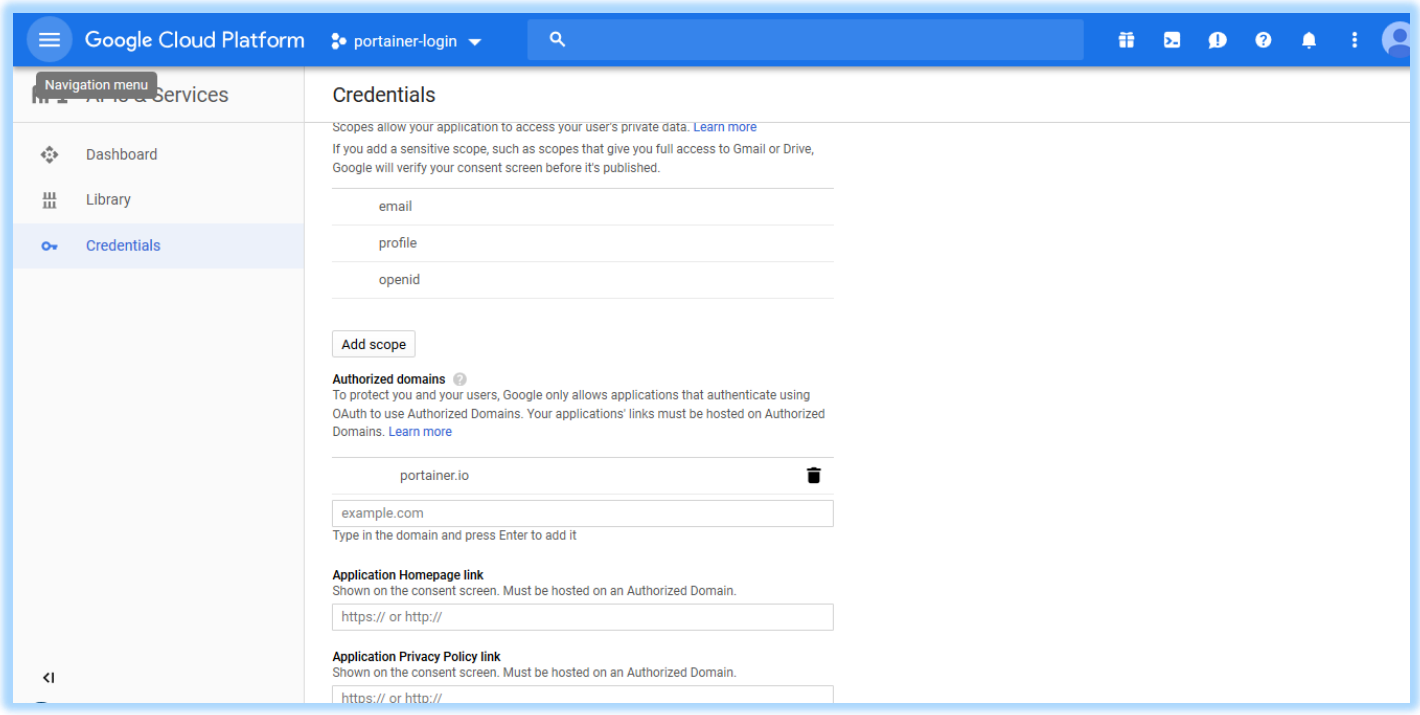
Step 5. Click on “OAuth consent screen”

Change the application type to “Internal”

In the “Application name” input box, enter the project name “portainer-login”

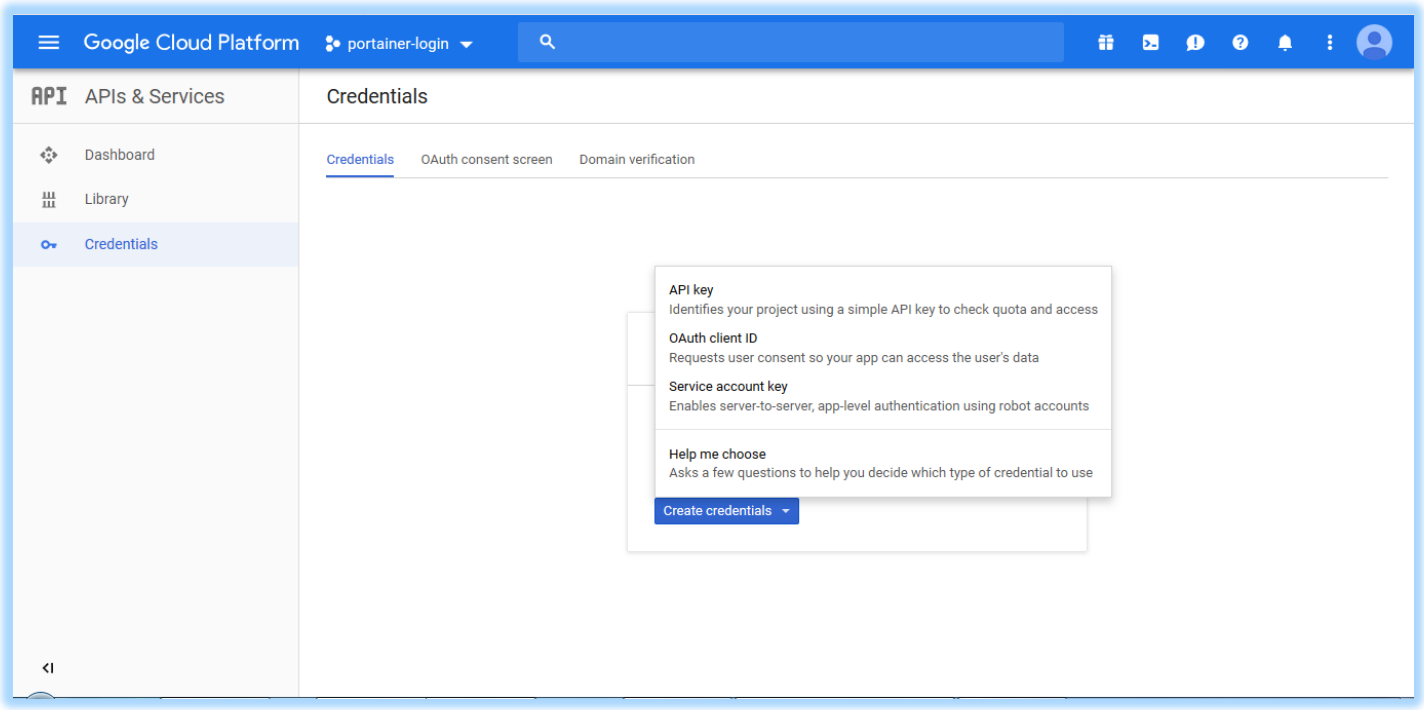
Scroll down to authorised domains, and enter in the FQDN of the server that hosts your Portainer instance (in our case, test.portainer.io)





Click Save.

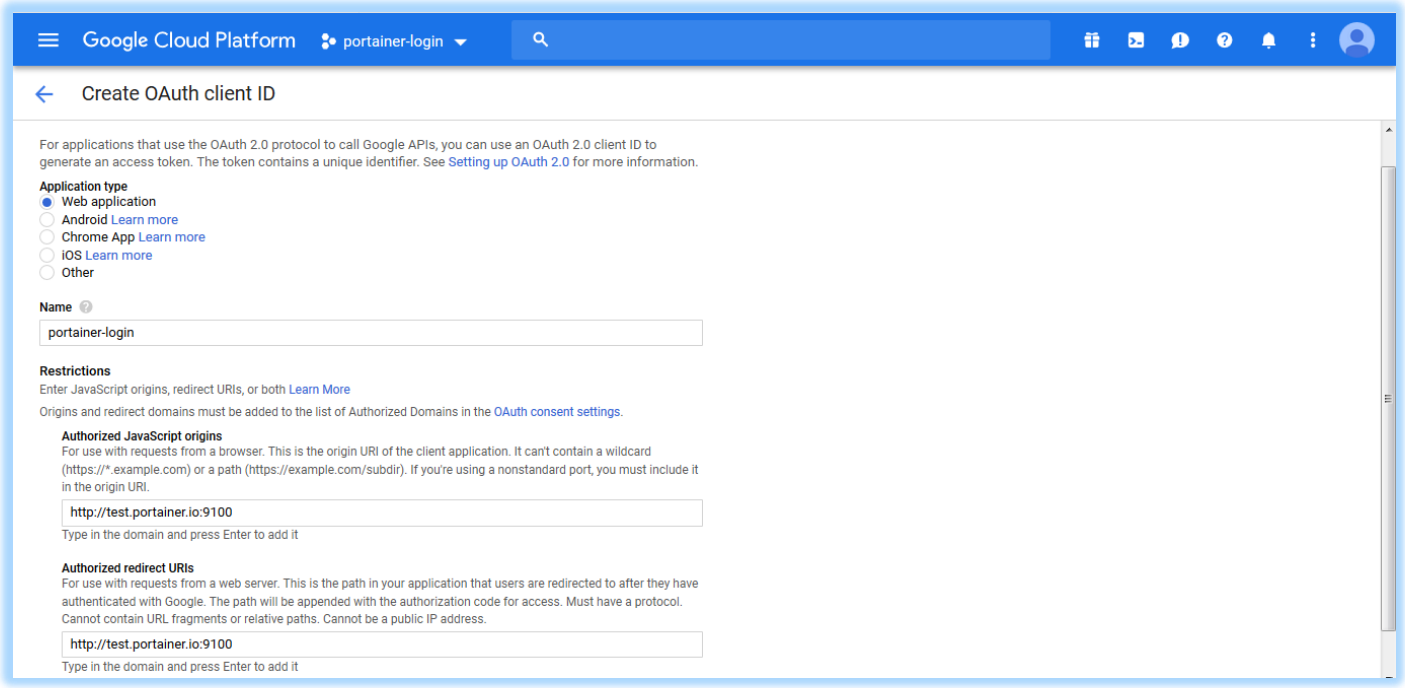
Step 6: Click on “Credentials”, and then “OAuth Client ID”



Select “Web Application” as the Application Type,

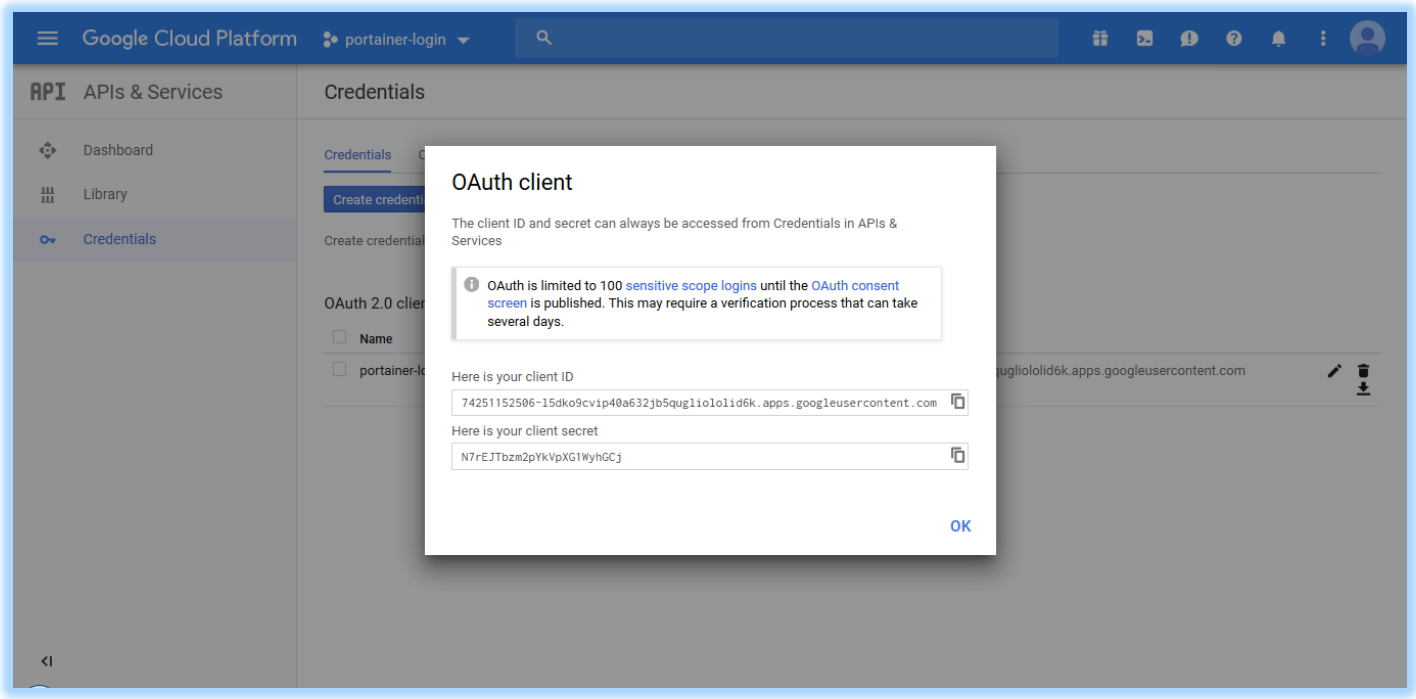
In the “Name” input box, enter the project name “portainer-login”.

In the “Javascript Origins” and “Redirect URI” text boxes, enter in the FDQN and Port of your Portainer instance.



Click “Create”

You will now be presented with your API tokens, copy these for later use (note be careful with trailing spaces as the auto-copy adds a trailing space, which breaks things)

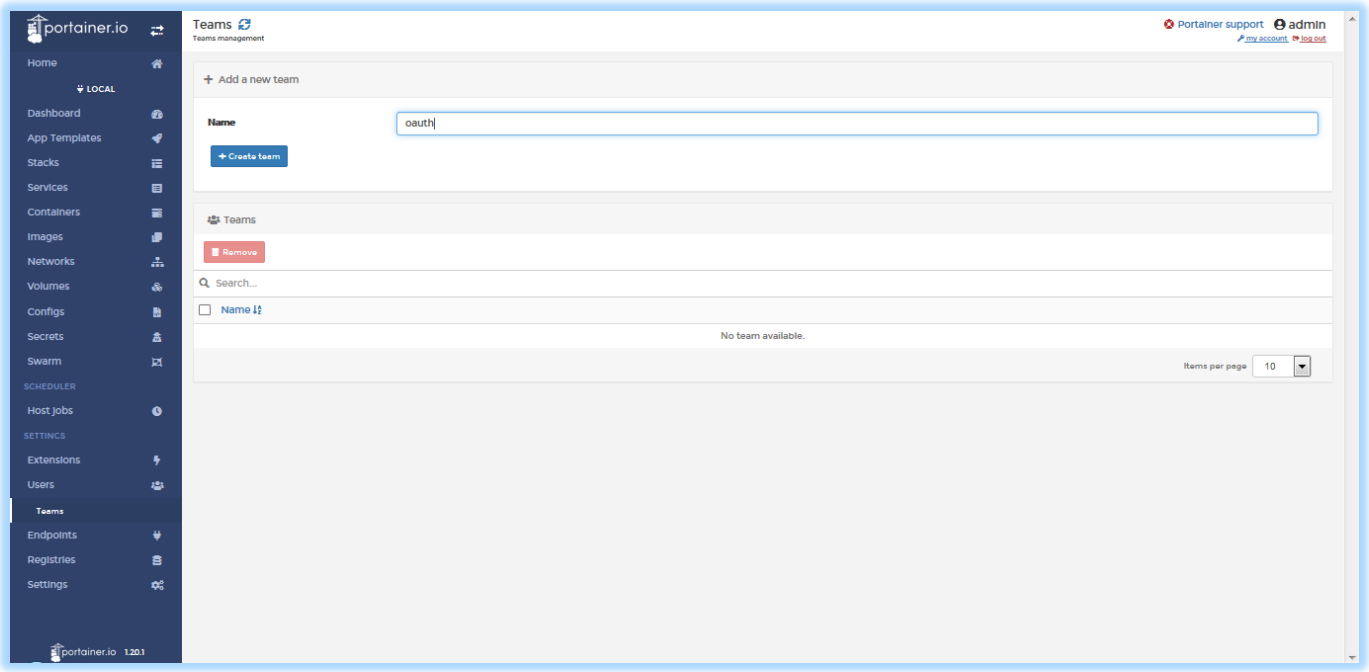


Step 7. Switch to your Portainer Instance and login as the local instance admin

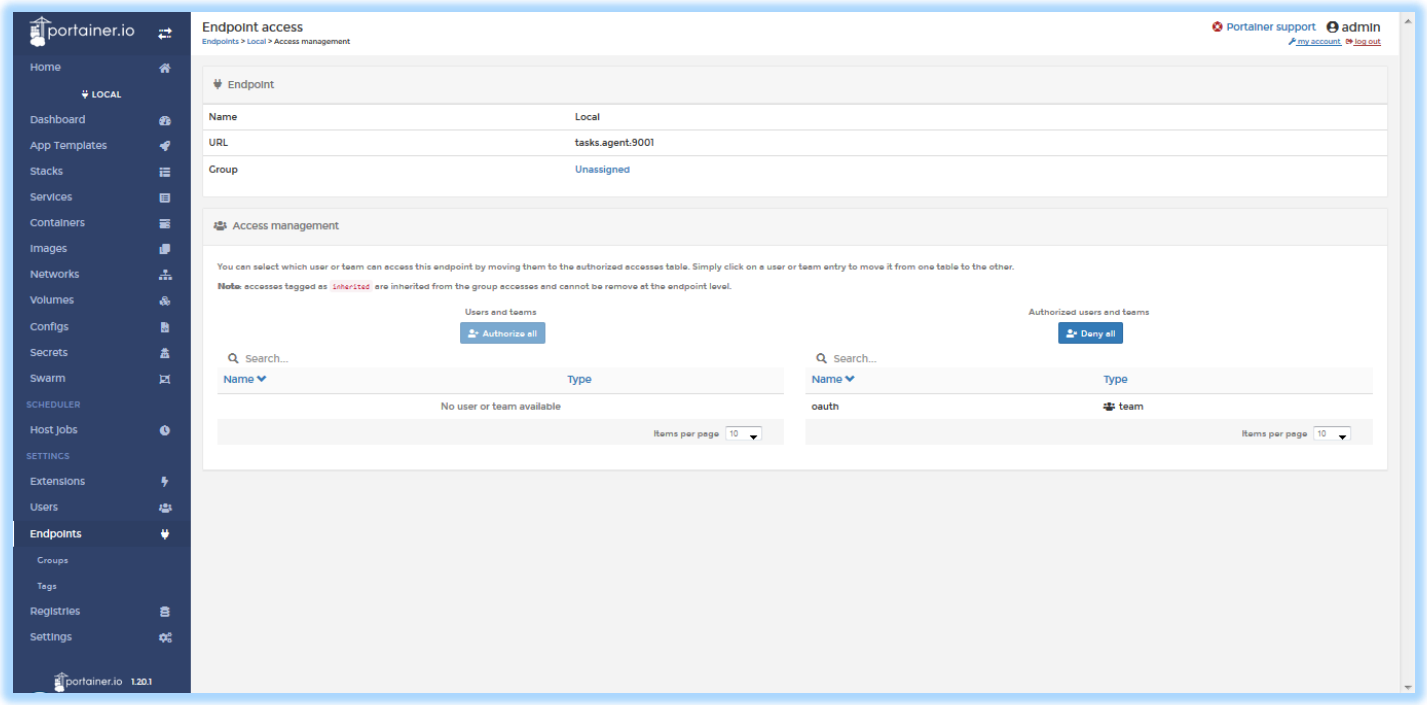
Purchase the Portainer External Authentication extension, and apply the license key (process not shown here).

Lets setup some basics, so that when user's login for the first time, they can actually access Portainer resources.

Click on "Users" and then "Teams", and create a team called "oauth" (or one of your choosing)



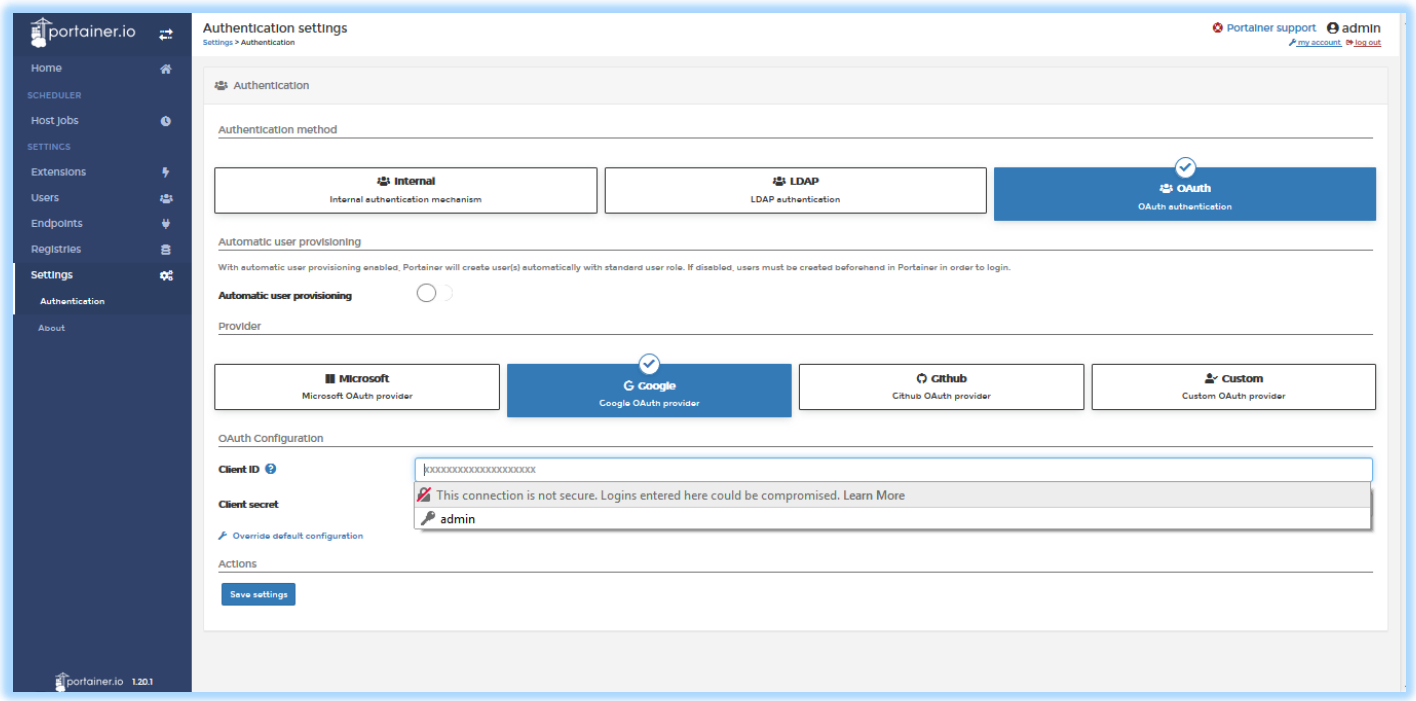
Click on "Endpoints" and then select the endpoints you would like to grant the oAUTH users access to manage, and then click "Manage Access". Assign the oAUTH group you created to the authorized list.



Step 8: Let's configure oAUTH.

Click on "settings" and then "Authentication"

Select "oAUTH" and then select "Google"

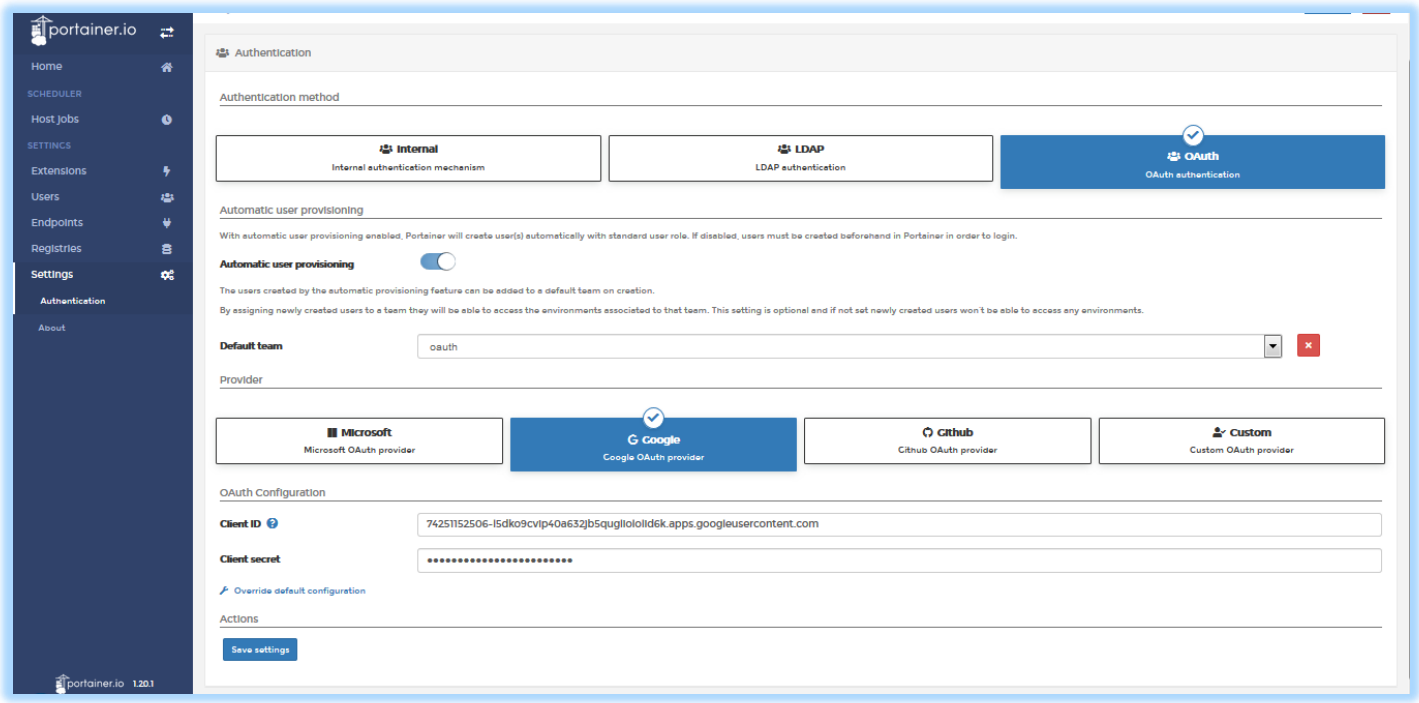


Enable Automatic User Provisioning, and select the default team (oAUTH or similar) that you created previously.

Enter in the Client ID that you noted previously.

Enter in the Client Secret that you noted previously.

Click Save.

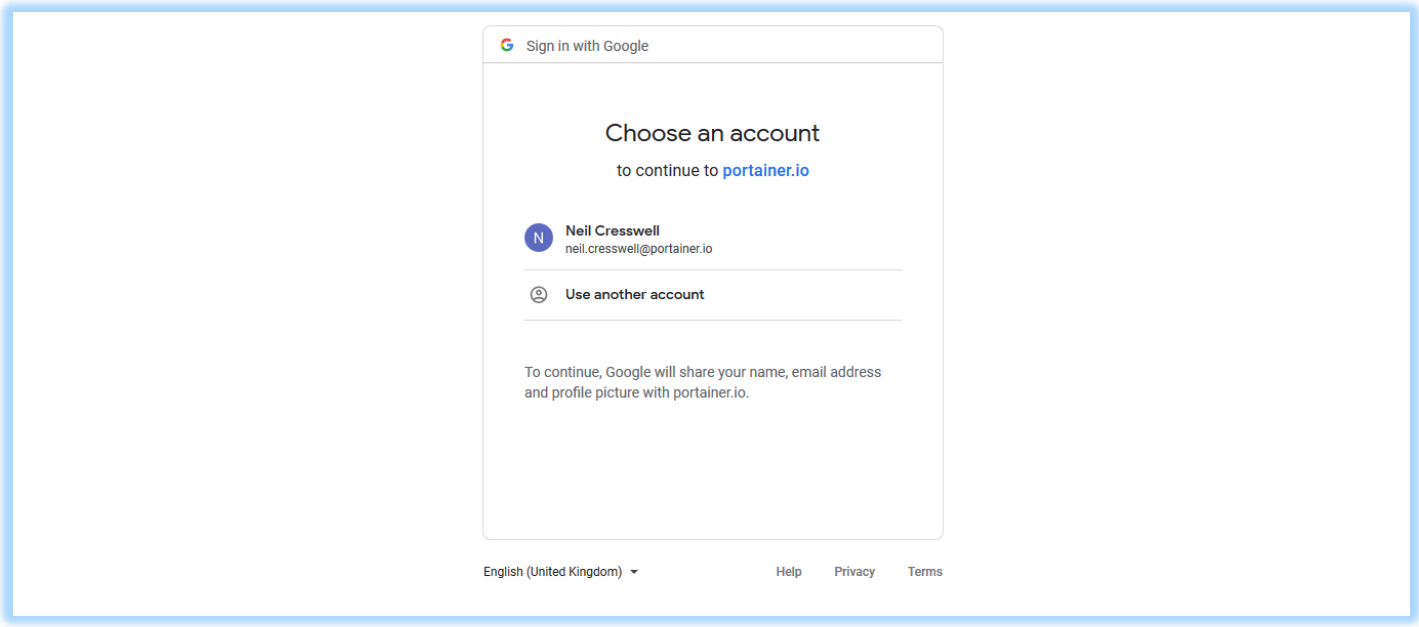


Logout as the Admin.

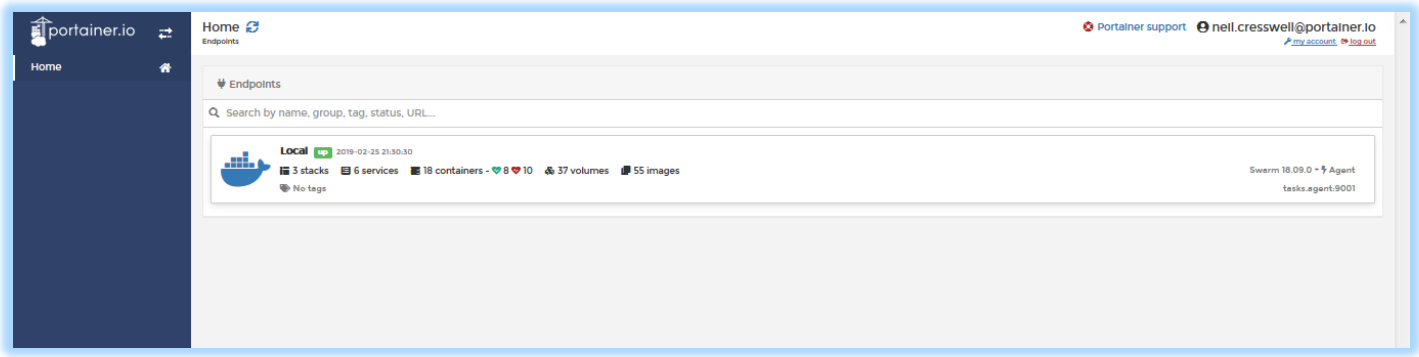
Step 9. Login using oAUTH

At the Login Page, click the “Login with Google” box for oAUTH login.

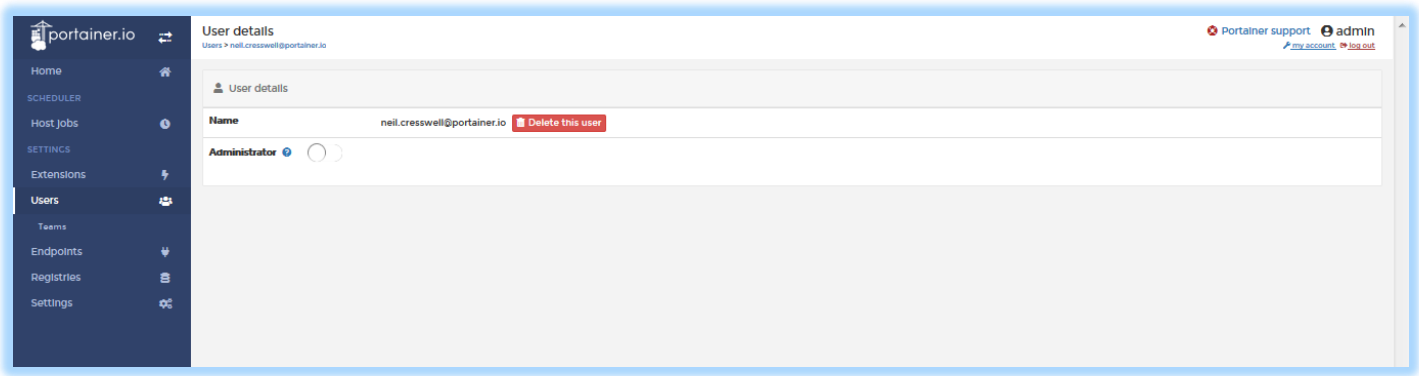
Enter your Google username and password where prompted (note you are redirected to Google for Auth)



You are now logged into Portainer using oAUTH from Google.



Optionally, if you want your oAUTH user to be a Portainer Admin, first login/logout as the oAUTH user to create the Portainer record, then login as the Portainer local admin (or as another admin), and then edit the user to elevate them to an admin.



.end.