

Portainer Extension Software

Implementation Guide

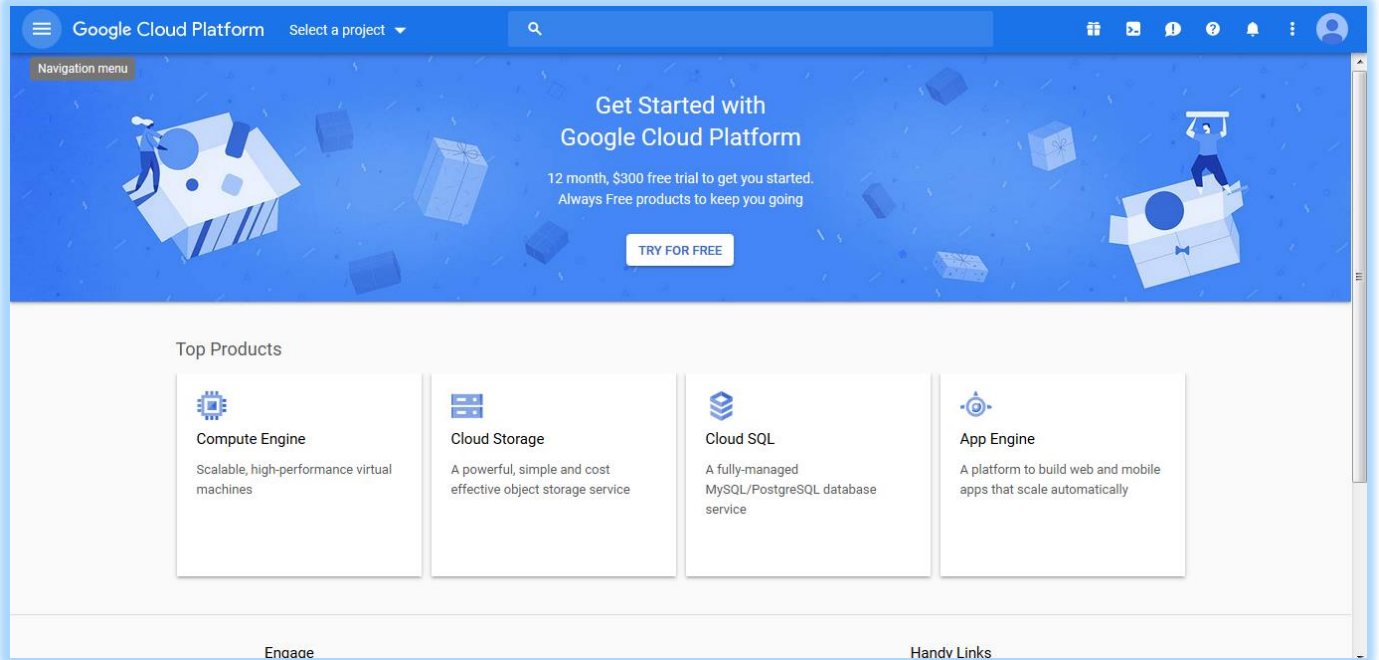
External Authentication for Google

March 2019

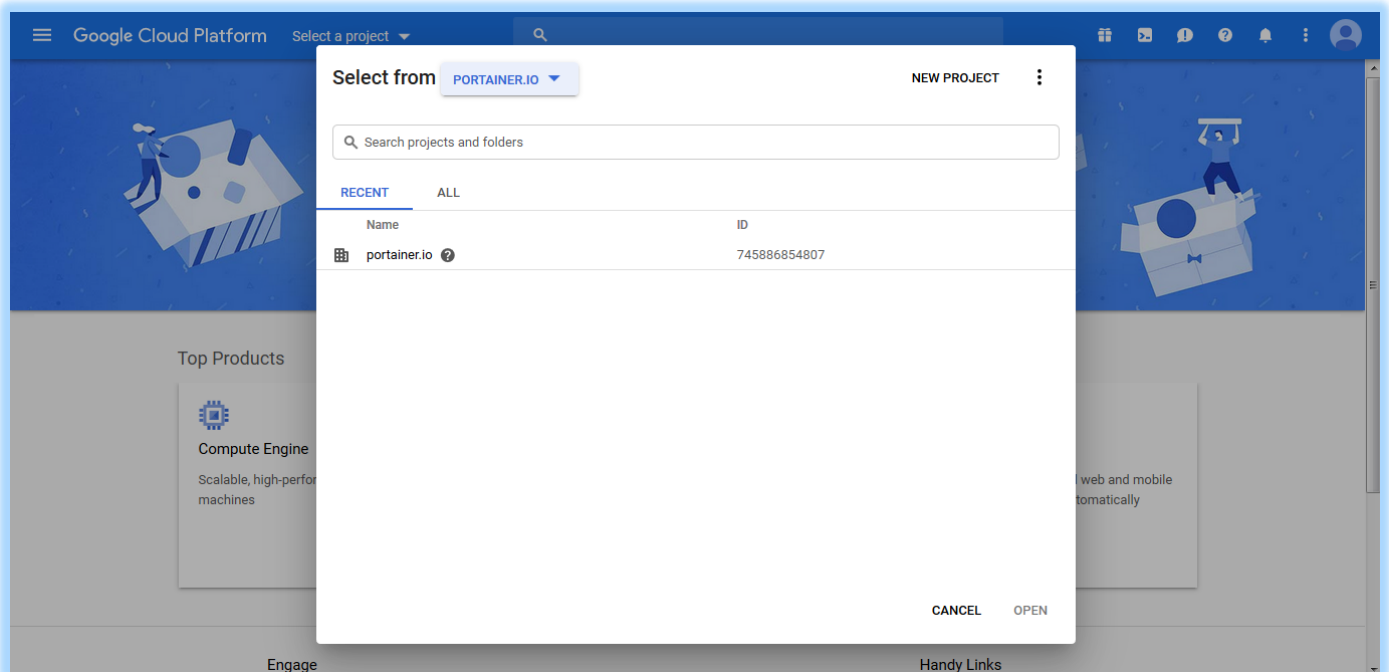
Implementation Guide

External Authentication for Google

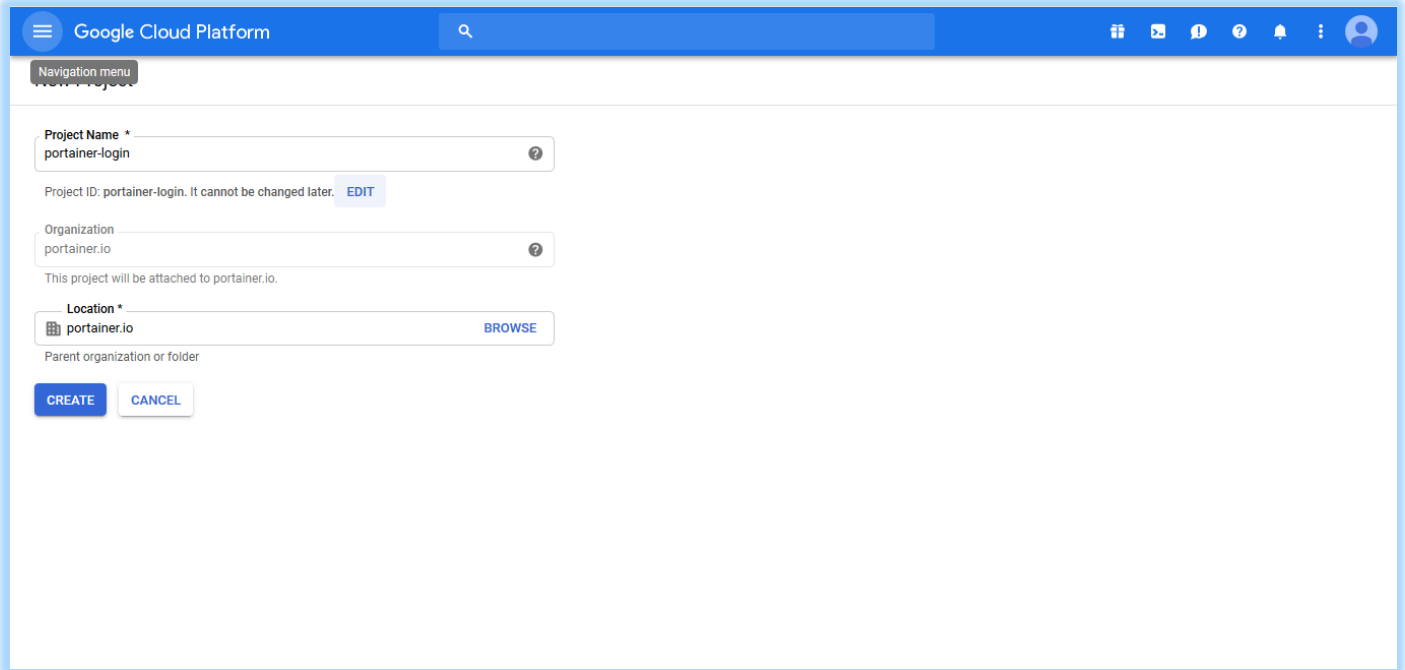
Step 1. Login to your Google Cloud Portal (console.cloud.google.com) as an Admin,



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



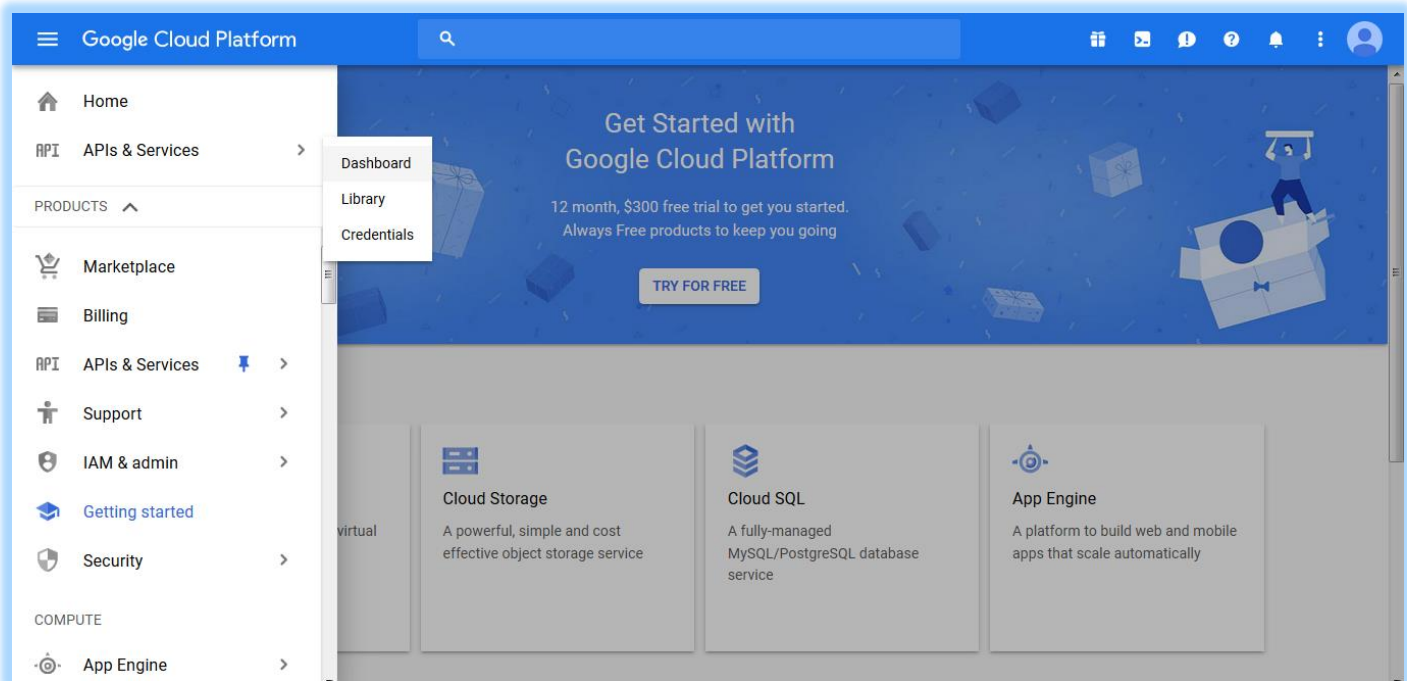
Step 3. Give the project a name, such as portainer-login, and then click “Create”



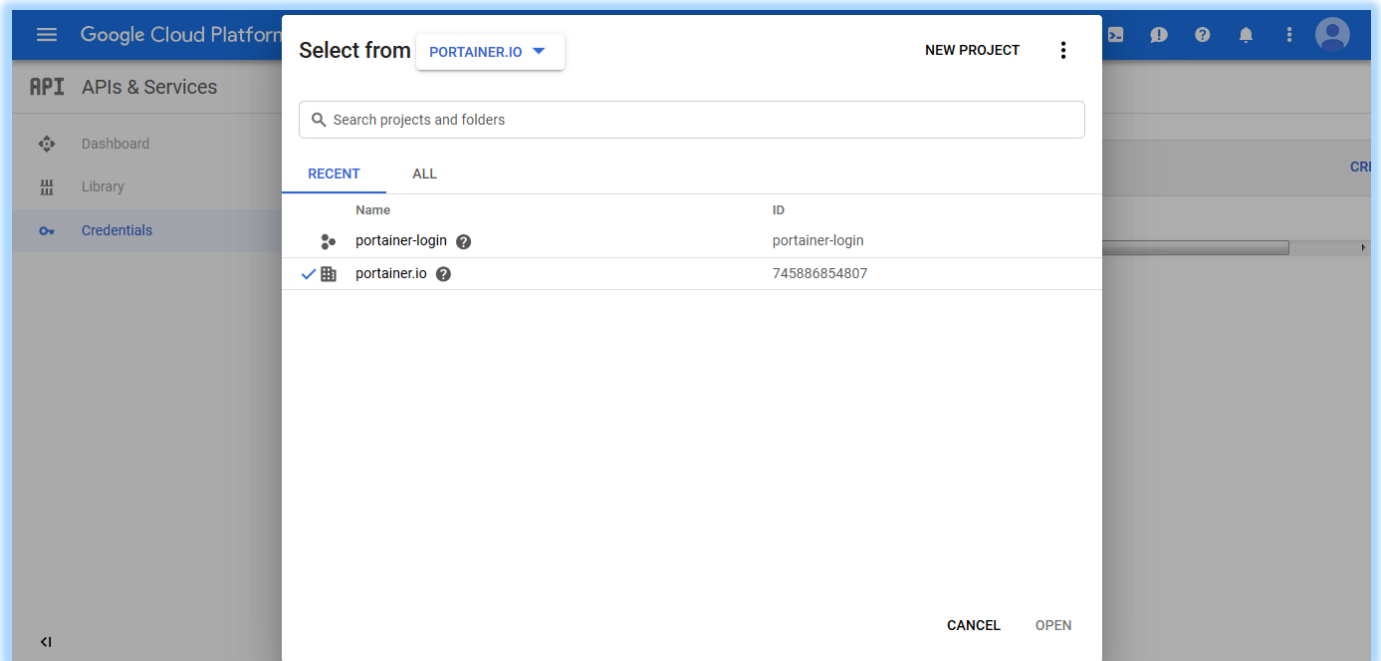
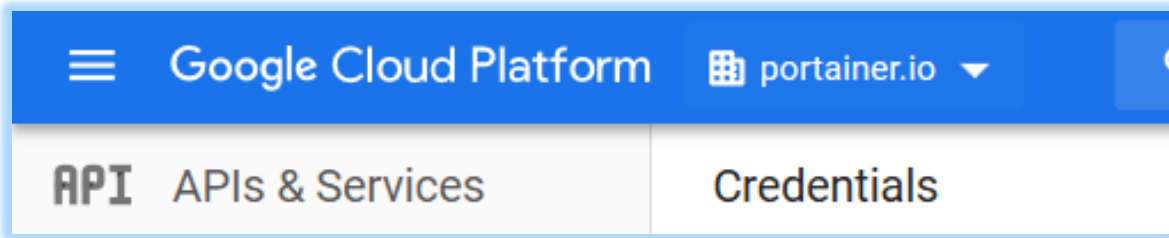
The screenshot shows the 'New Project' form in the Google Cloud Platform console. The form is titled 'Navigation menu' and contains the following fields and buttons:

- Project Name ***: A text input field containing 'portainer-login'.
- Project ID**: A text input field containing 'portainer-login'. Below it, a note states: 'Project ID: portainer-login. It cannot be changed later. [EDIT](#)'.
- Organization**: A text input field containing 'portainer.io'.
- Location ***: A dropdown menu showing 'portainer.io' with a 'BROWSE' button next to it.
- Buttons**: 'CREATE' and 'CANCEL' buttons at the bottom.

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

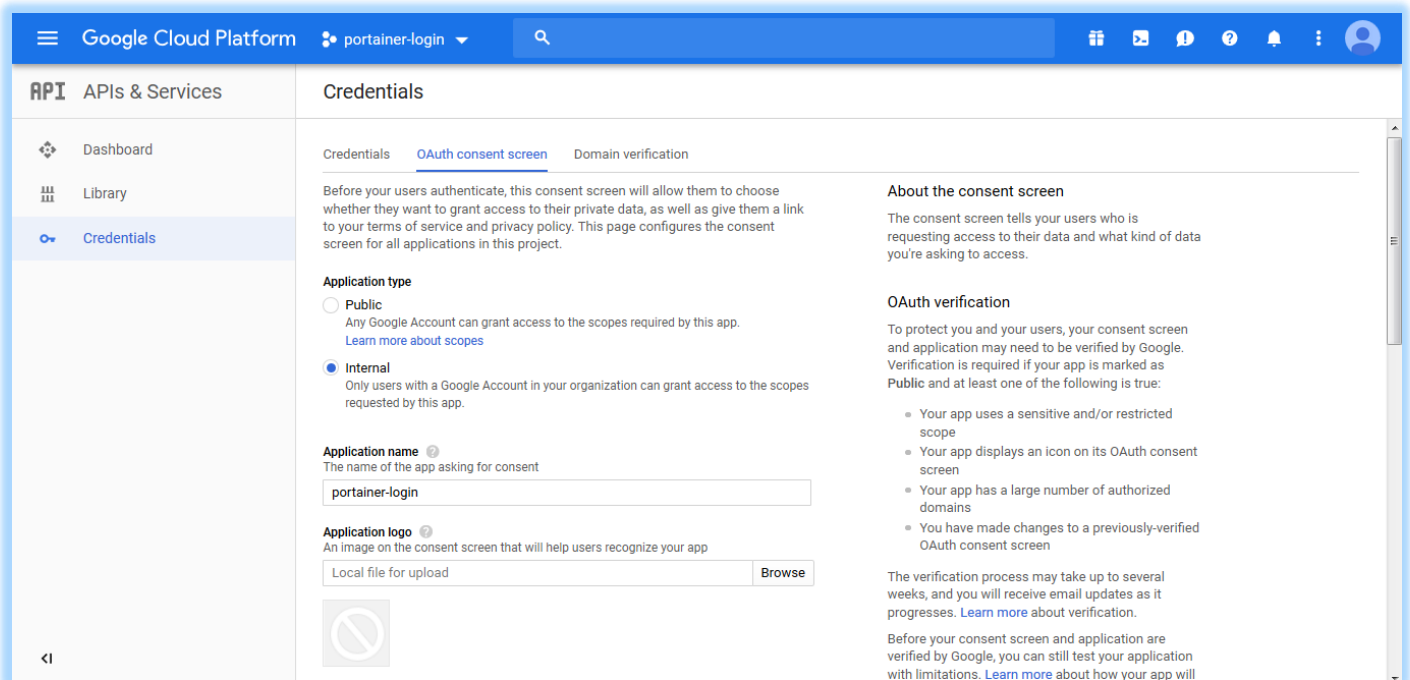


Step 5. Click on “OAuth consent screen”

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)



The screenshot shows the 'OAuth consent screen' configuration page in the Google Cloud Platform console. The left sidebar shows the 'APIs & Services' menu with 'Credentials' selected. The main content area has tabs for 'Credentials', 'OAuth consent screen' (active), and 'Domain verification'. The 'Application type' section has 'Internal' selected. The 'Application name' field contains 'portainer-login'. The 'Application logo' field has a 'Browse' button. The right sidebar contains information about the consent screen and OAuth verification.

Application type

☐ Public
Any Google Account can grant access to the scopes required by this app.
[Learn more about scopes](#)

☒ Internal
Only users with a Google Account in your organization can grant access to the scopes requested by this app.

Application name ⓘ
The name of the app asking for consent

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

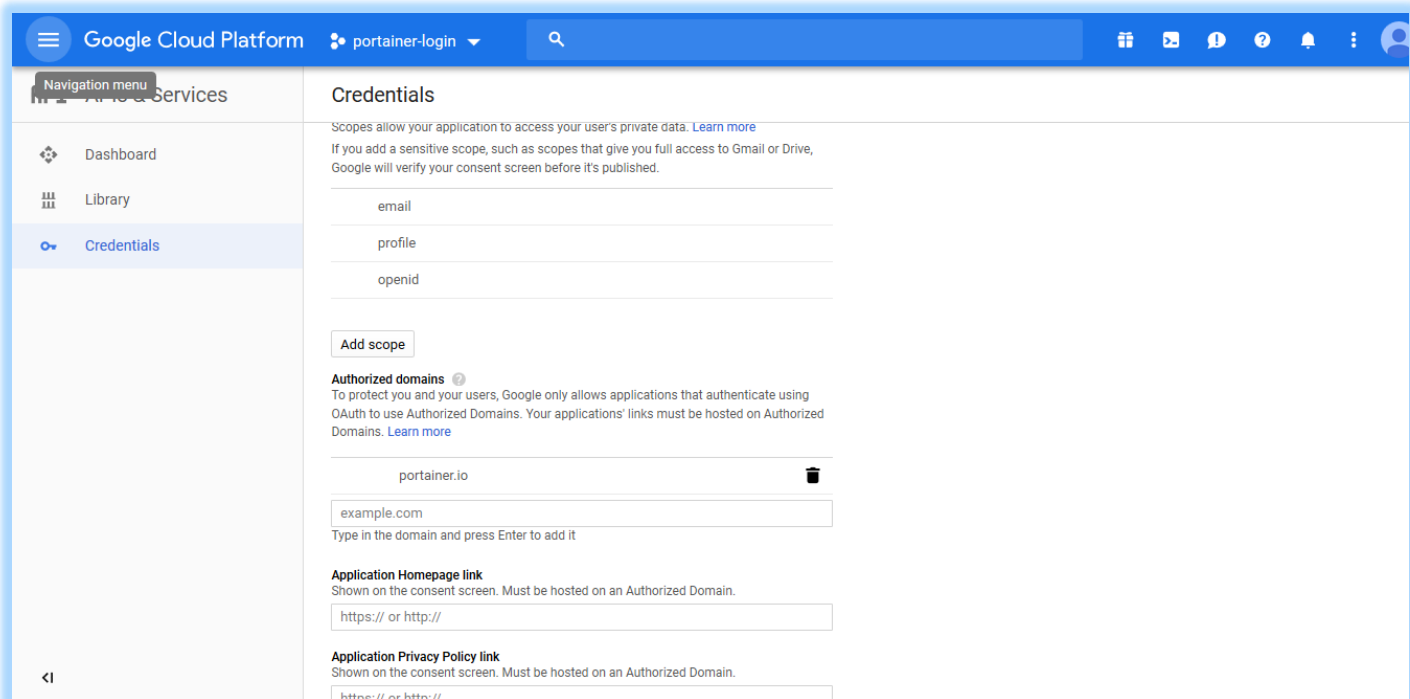
About the consent screen
The consent screen tells your users who is requesting access to their data and what kind of data you're asking to access.

OAuth verification
To protect you and your users, your consent screen and application may need to be verified by Google. Verification is required if your app is marked as **Public** and at least one of the following is true:

- Your app uses a sensitive and/or restricted scope
- Your app displays an icon on its OAuth consent screen
- Your app has a large number of authorized domains
- You have made changes to a previously-verified OAuth consent screen

The verification process may take up to several weeks, and you will receive email updates as it progresses. [Learn more](#) about verification.

Before your consent screen and application are verified by Google, you can still test your application with limitations. [Learn more](#) about how your app will



The screenshot shows the 'Authorized domains' configuration page in the Google Cloud Platform console. The left sidebar shows the 'APIs & Services' menu with 'Credentials' selected. The main content area has tabs for 'Credentials', 'OAuth consent screen', and 'Authorized domains' (active). The 'Scopes' section lists 'email', 'profile', and 'openid'. The 'Authorized domains' section has 'portainer.io' entered. The 'Application Homepage link' and 'Application Privacy Policy link' fields are empty.

Scopes ⓘ
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 Gmail or Drive, Google will verify your consent screen before it's published.

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](#)

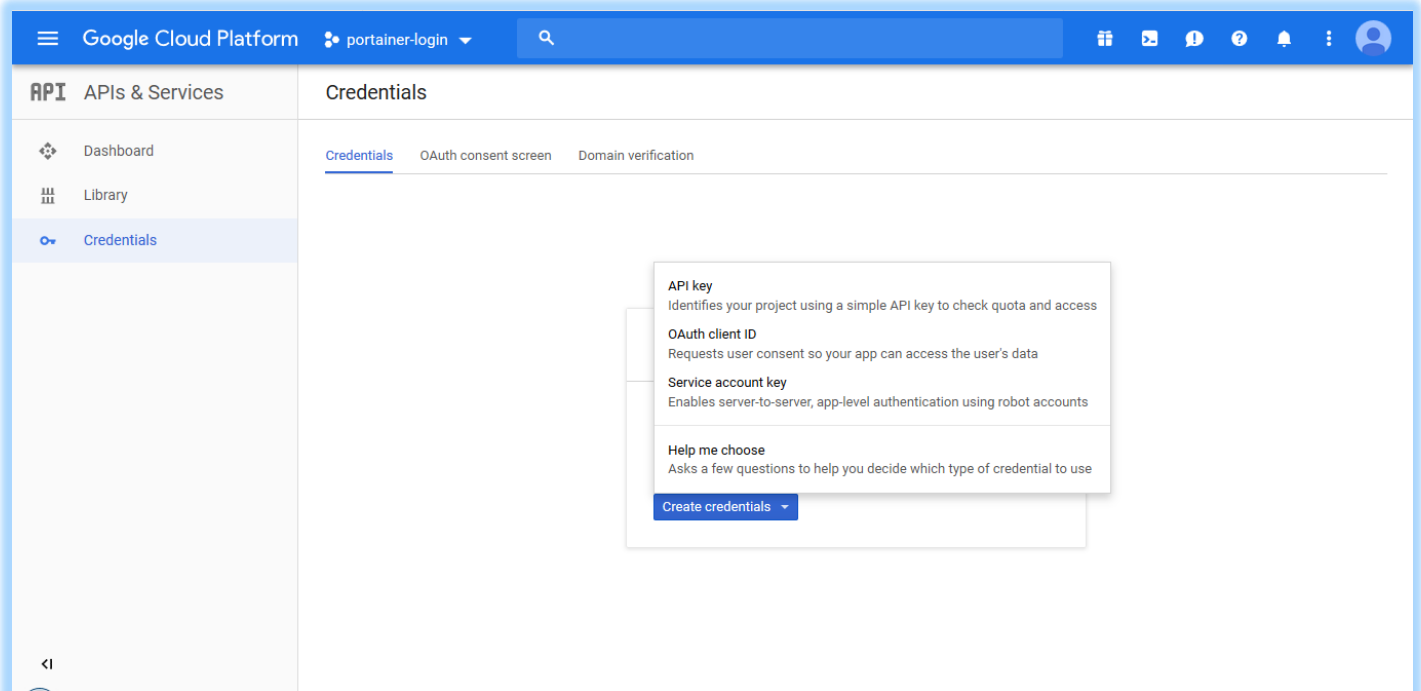
Type in the domain and press Enter to add it

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

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

Click Save.

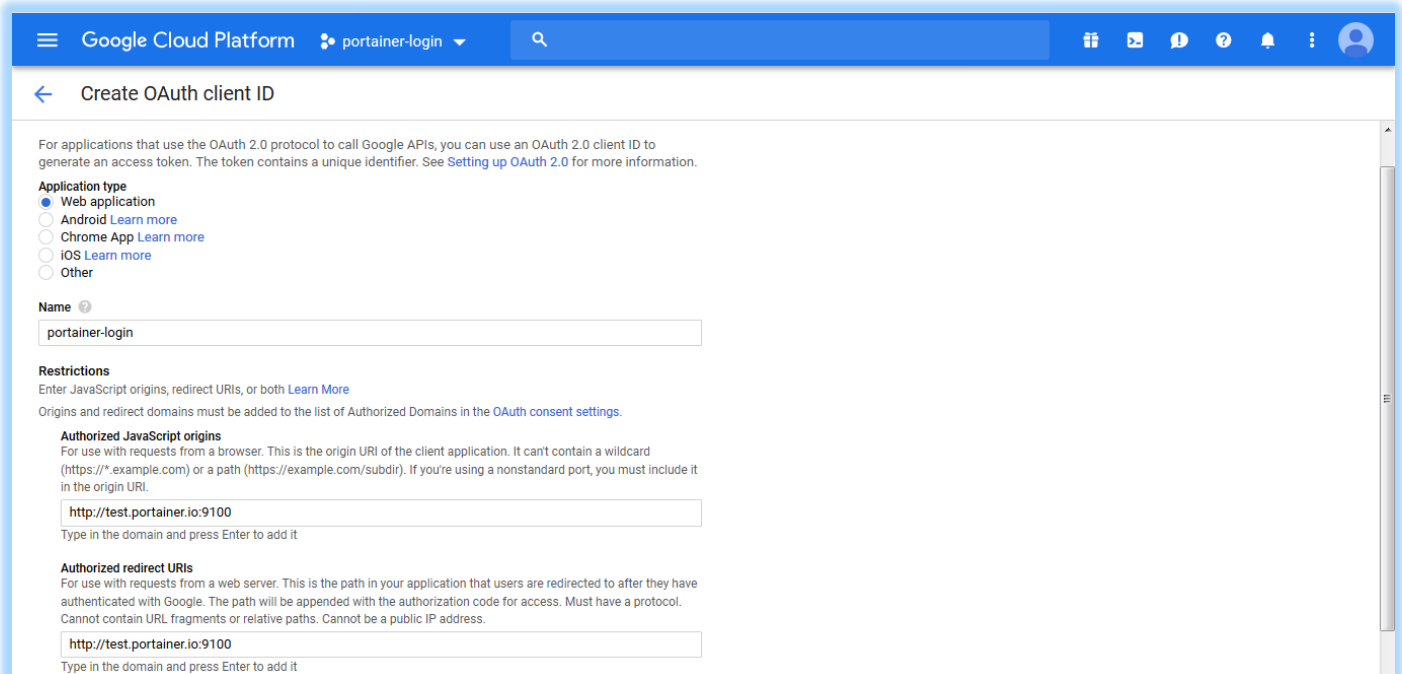
Step 6: Click on “Credentials”, and then “OAuth Client ID”



Select “Web Application” as the Application Type,

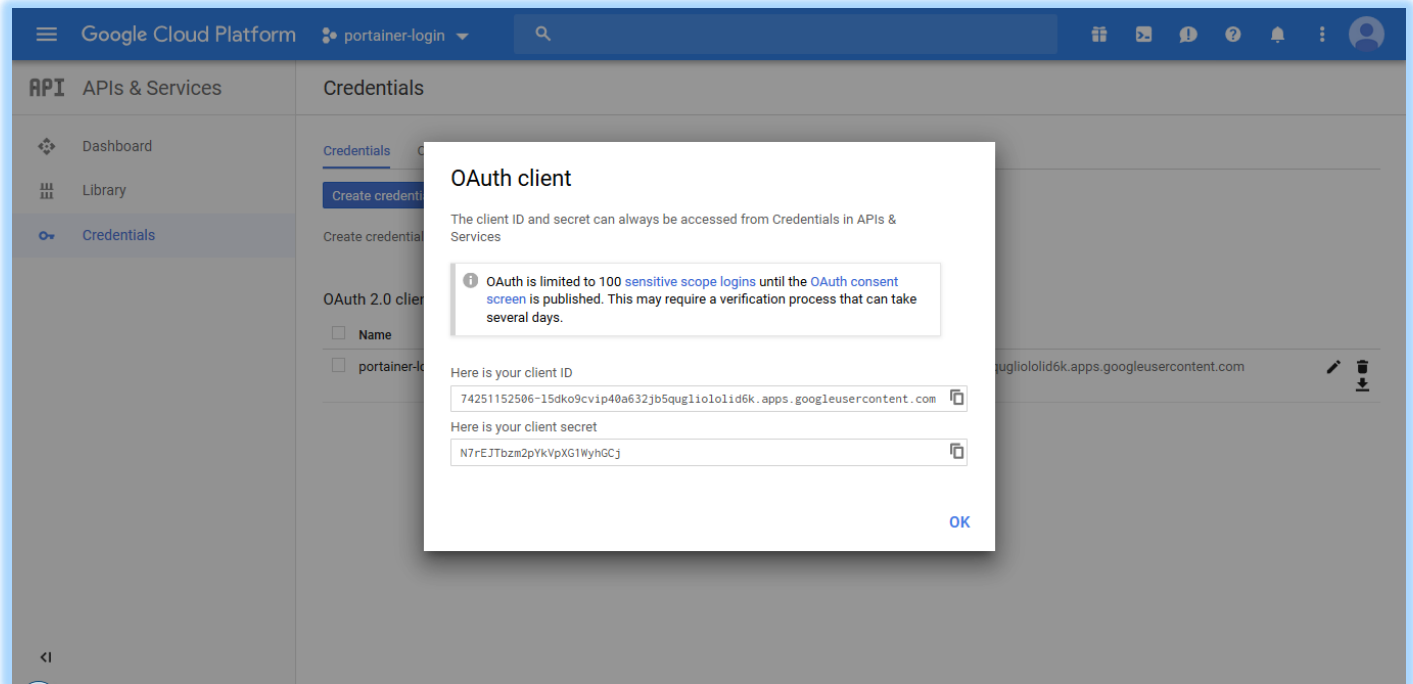
In the “Name” input box, enter the project name “portainer-login”.

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)

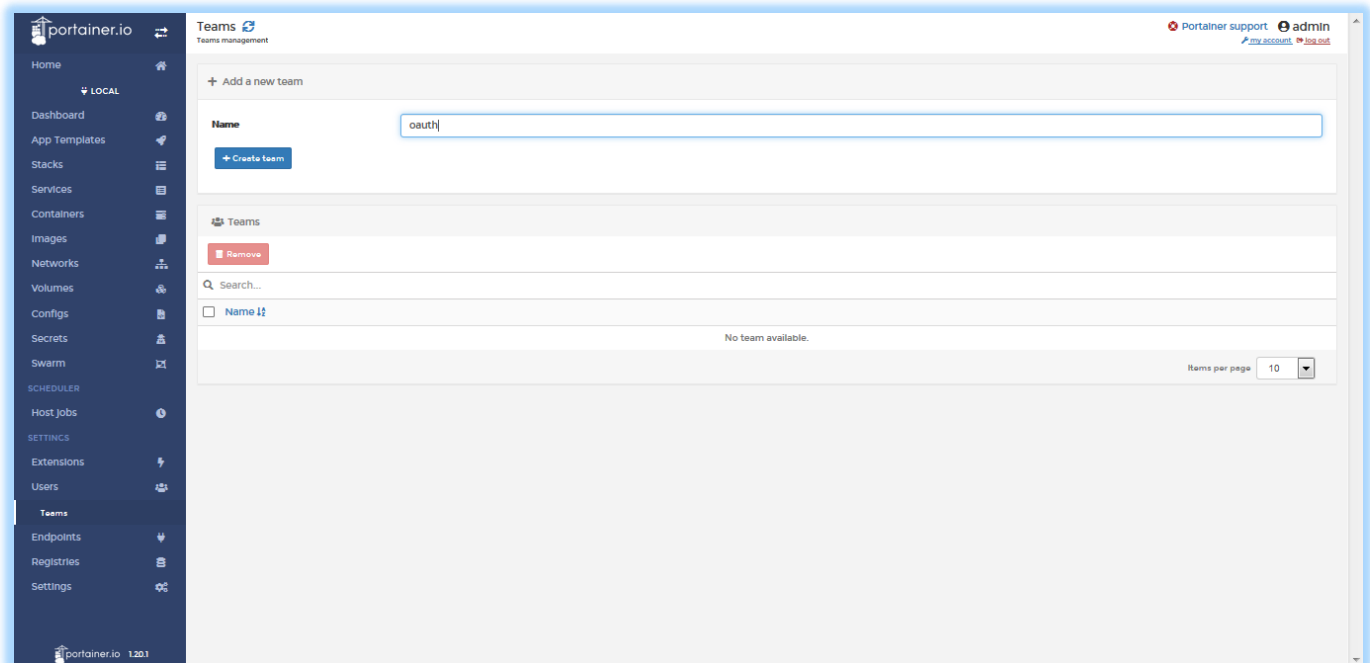


Step 7. Switch to your Portainer Instance and login as the local instance admin

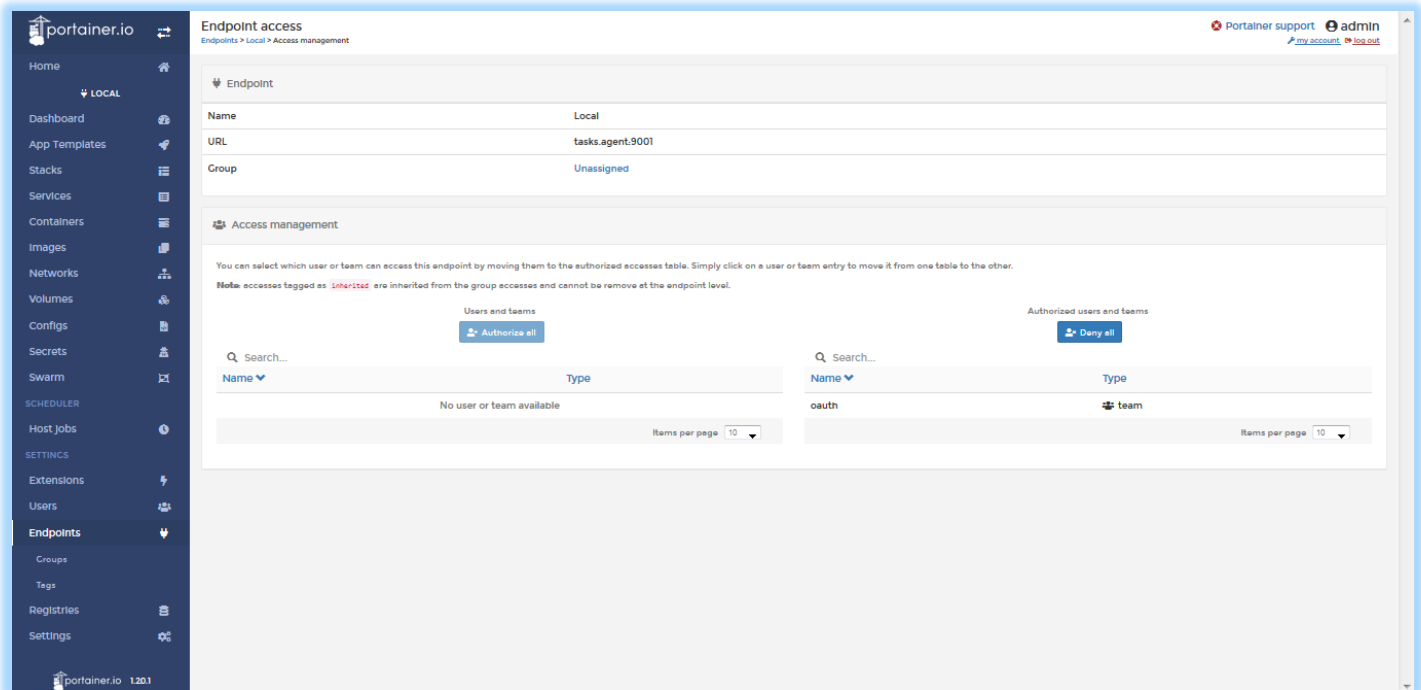
Purchase the Portainer External Authentication extension, and apply the license key (process not shown here).

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)



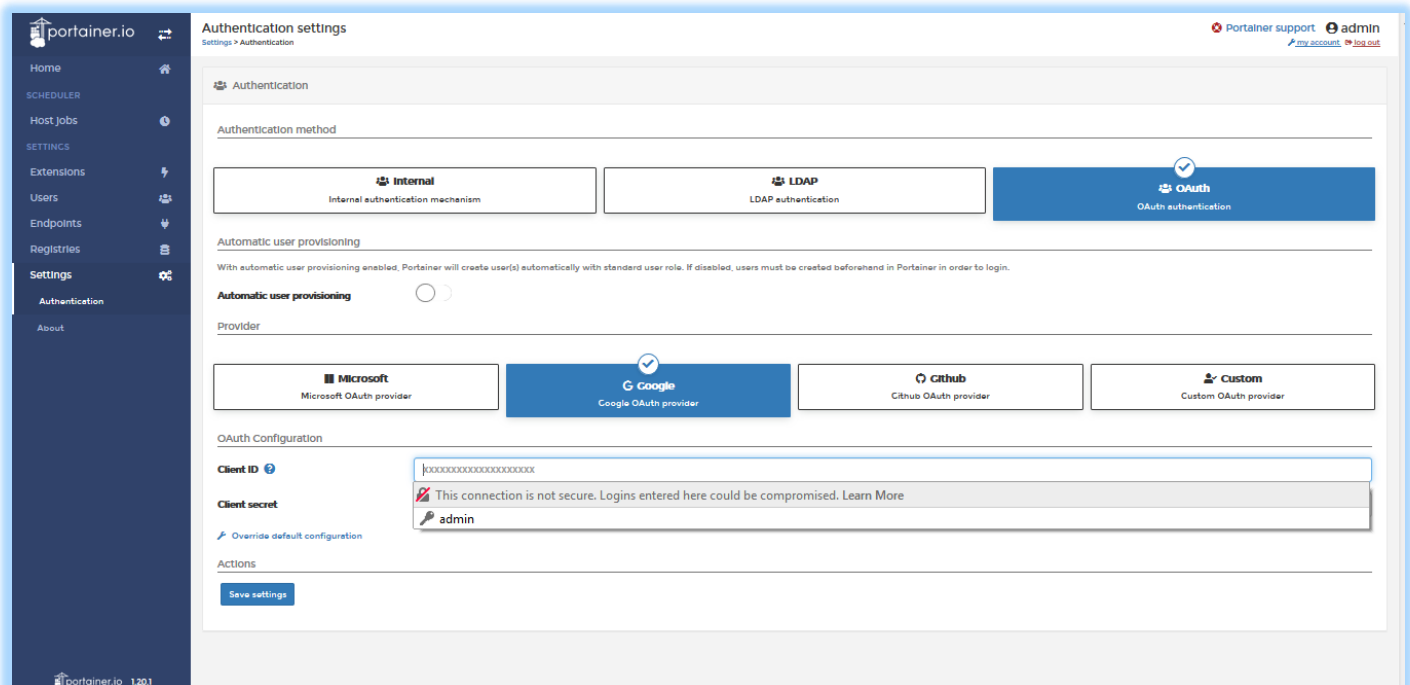
Click on "Endpoints" and then select the endpoints you would like to grant the oAUTH users access to manage, and then click "Manage Access". Assign the oAUTH group you created to the authorized list.



Step 8: Let's configure oAUTH.

Click on "settings" and then "Authentication"

Select "oAUTH" and then select "Google"

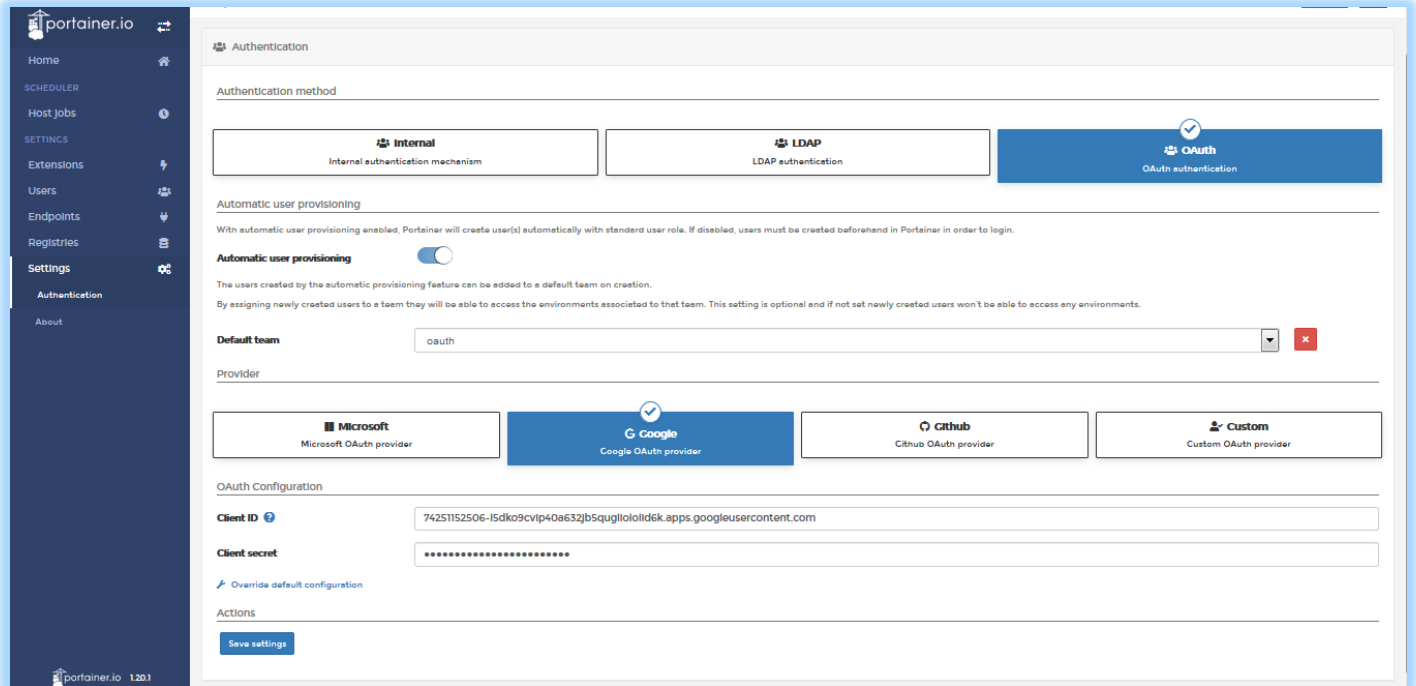


Enable Automatic User Provisioning, and select the default team (oAUTH or similar) that you created previously.

Enter in the Client ID that you noted previously.

Enter in the Client Secret that you noted previously.

Click Save.



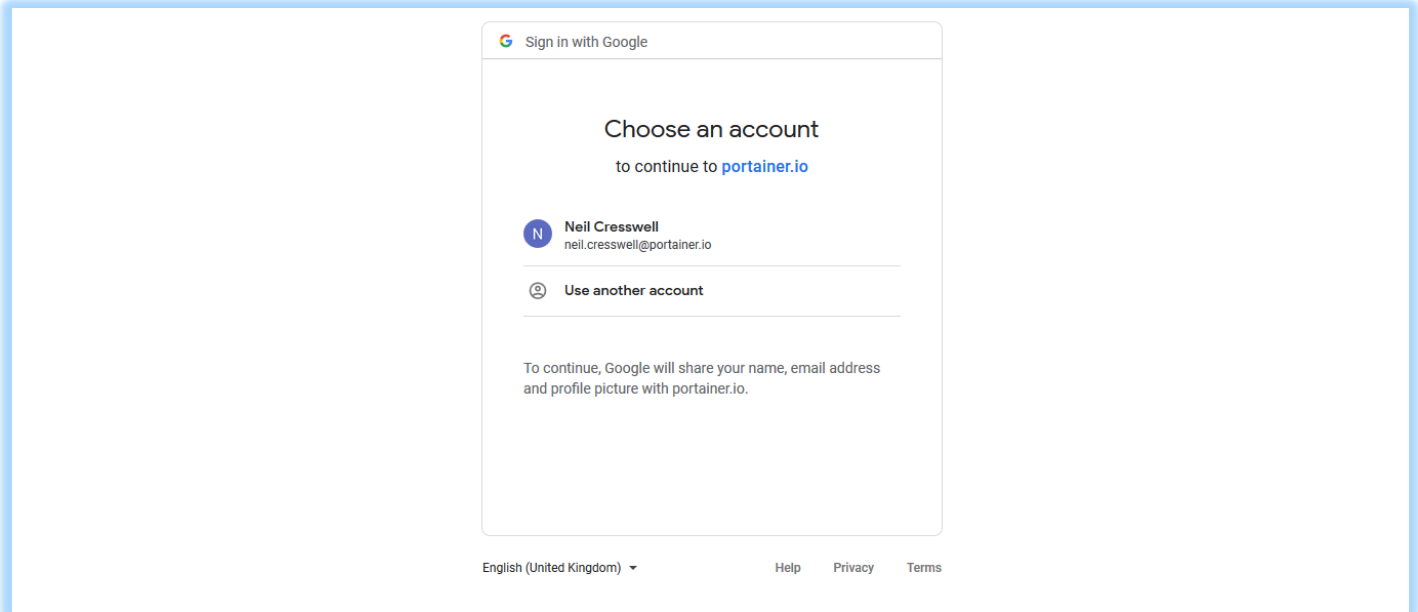
Logout as the Admin.

Step 9. Login using oAUTH

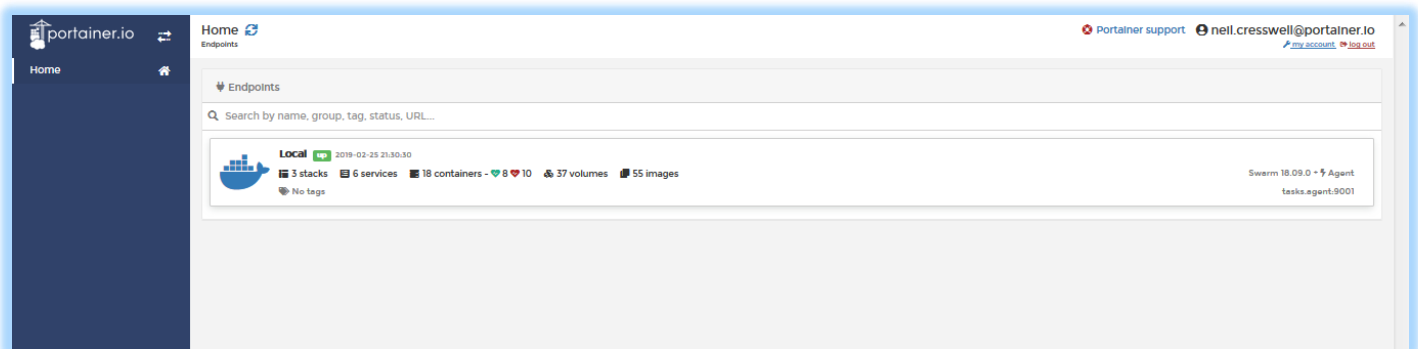
At the Login Page, click the “Login with Google” box for oAUTH login.



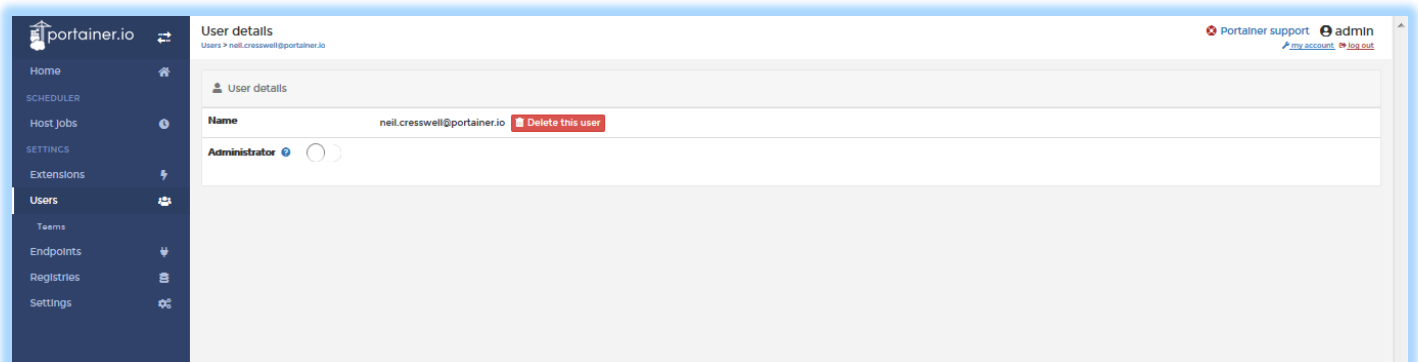
Enter your Google username and password where prompted (note you are redirected to Google for Auth)



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.