portainer.io

Portainer Extension Software

Implementation Guide

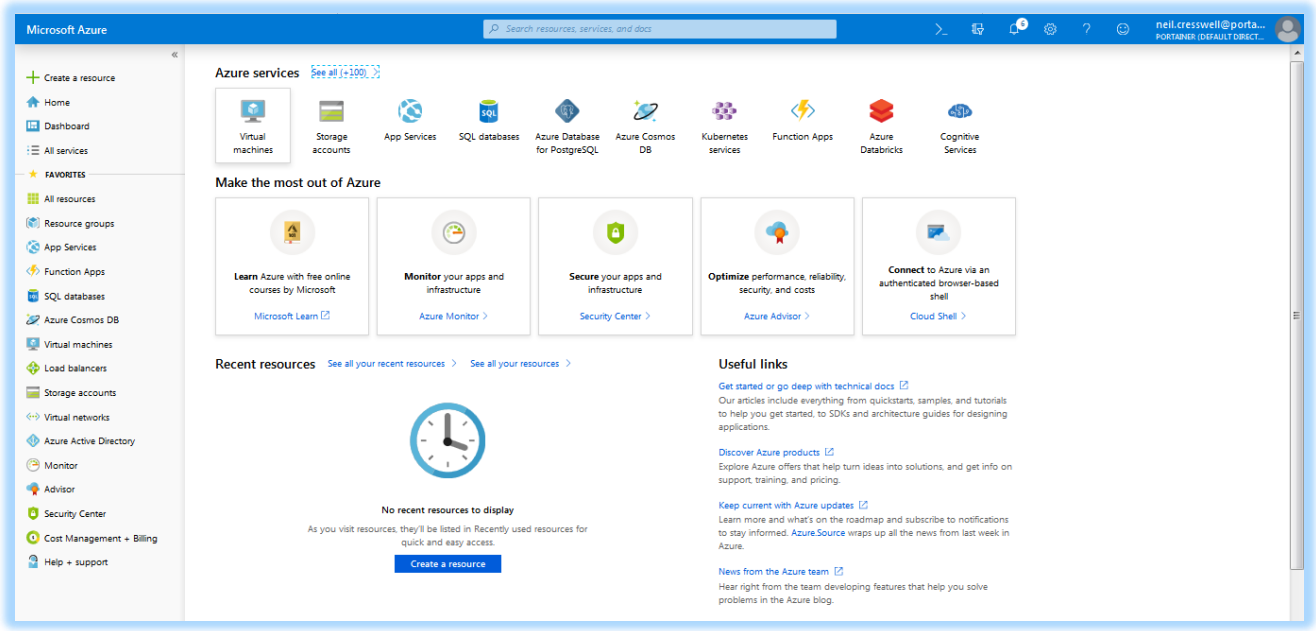
External Authentication for Microsoft Azure

March 2019

Implementation Guide

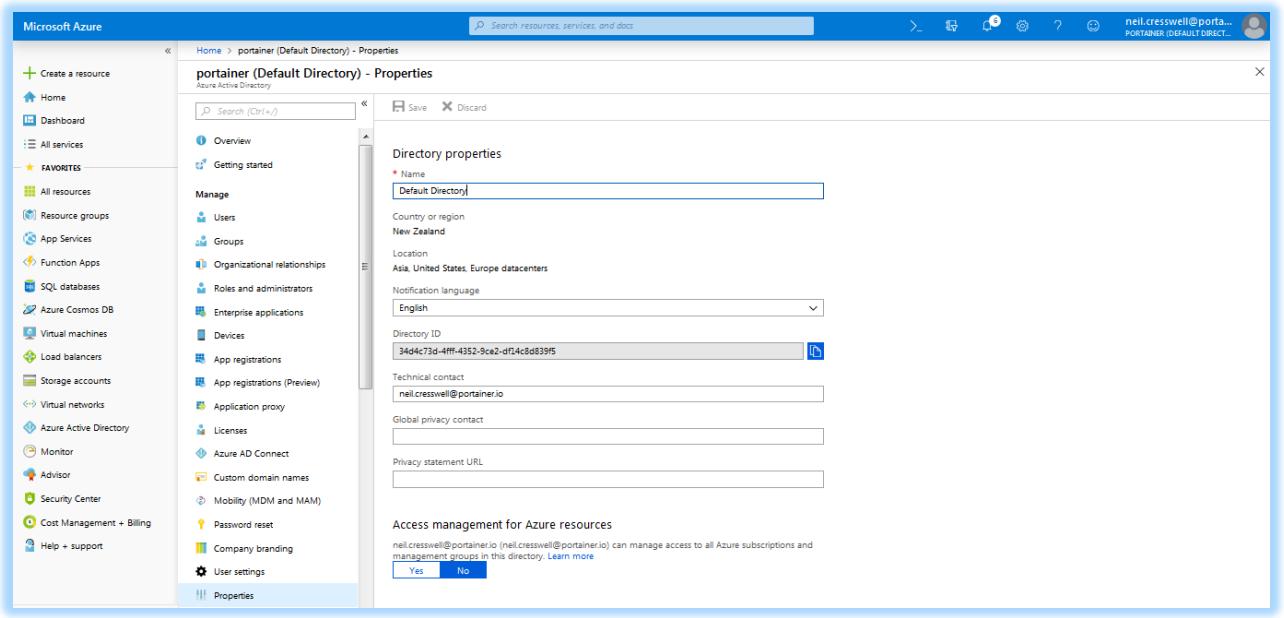
External Authentication for Azure

Step 1. Login to your Azure Portal as an Admin



Step 2. Retrieve your Tenant ID / Directory ID;

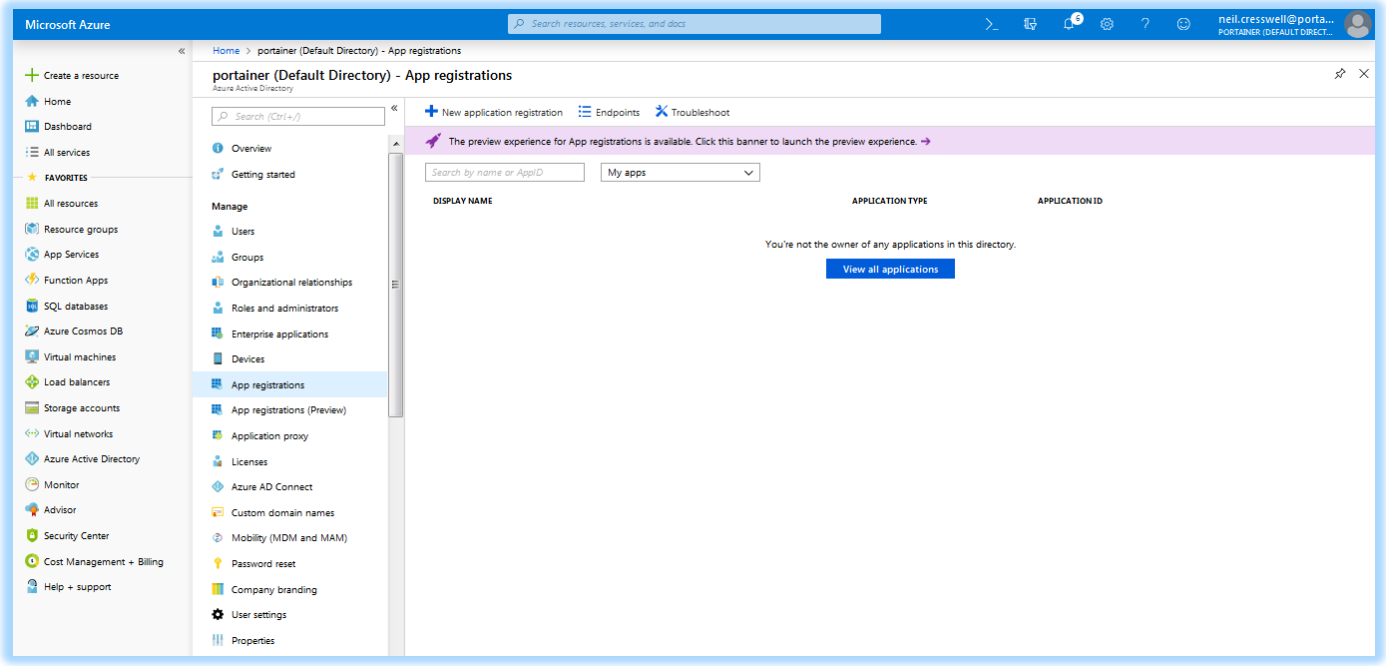
Click on “Azure Active Directory”, and then Click on “Properties”, and then note your “Directory ID” for later use.



Step 3. Define your Portainer Instance

Still in Azure Active Directory, Click on App Registrations

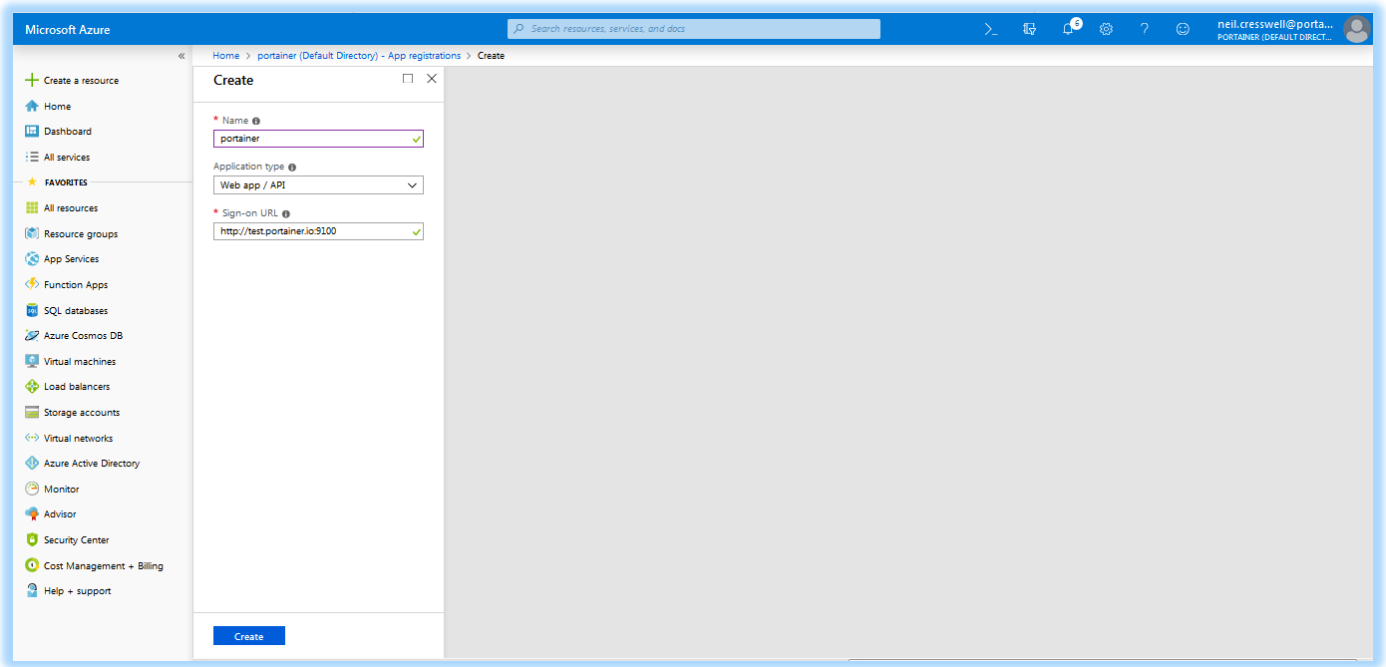
Click on “+ New Application Registration”



Enter in a friendly name for the Portainer Instance

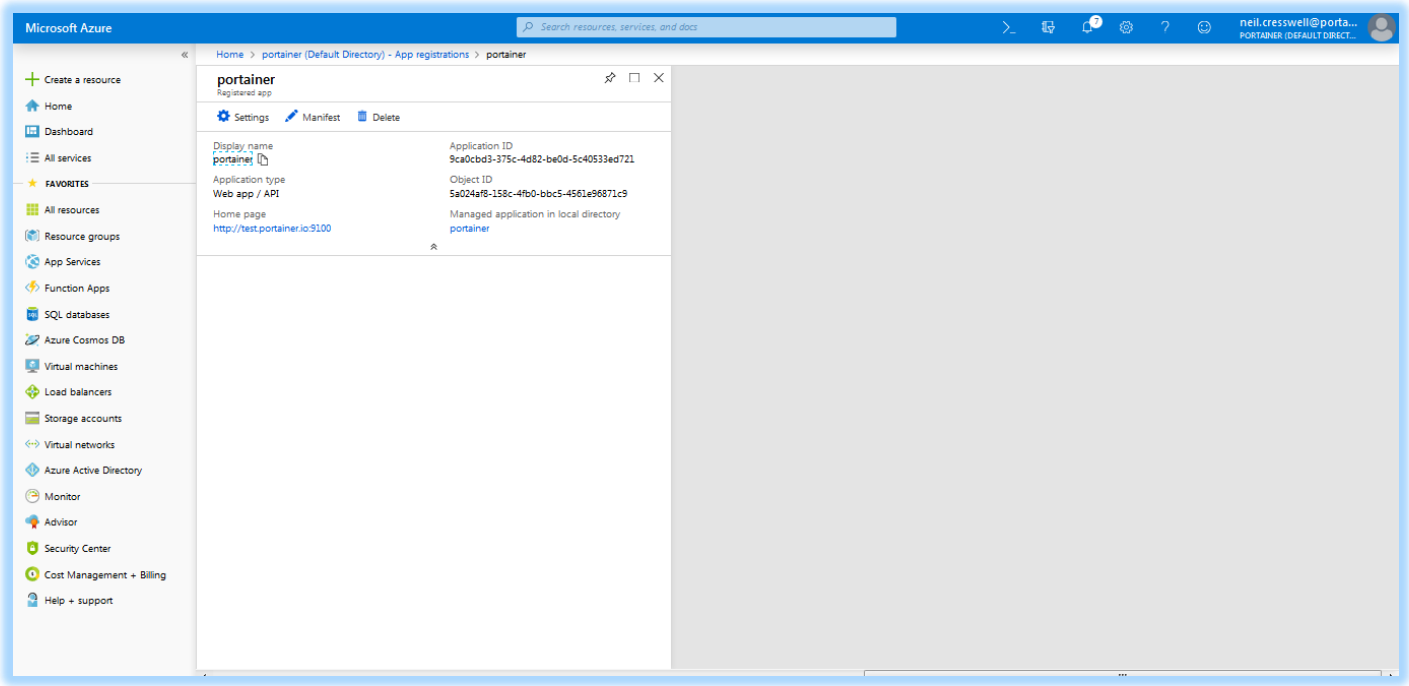
Keep the app type as Web App / API

In the “Sign-on URL” field, enter the FQDN or IP address that your Portainer instance listens on.



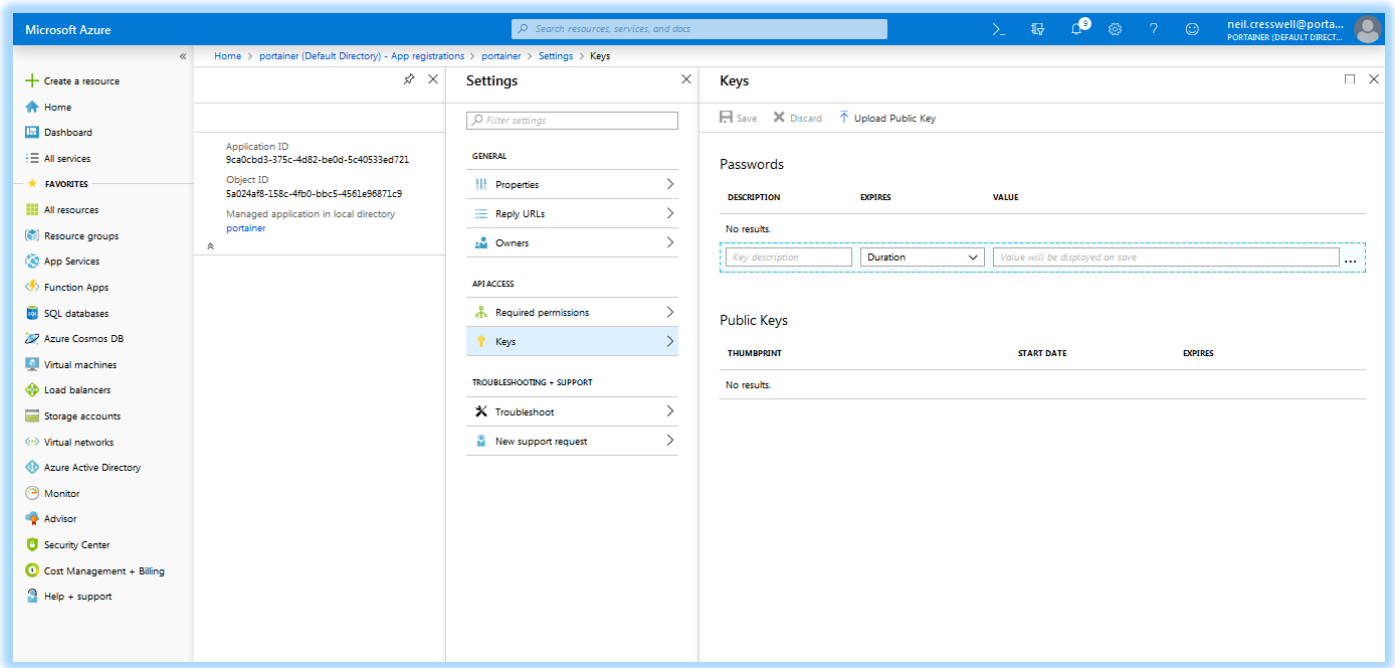
Step 4. Retrieve the Application ID

After creating the app, the screen below is displayed; record the application ID for later use.



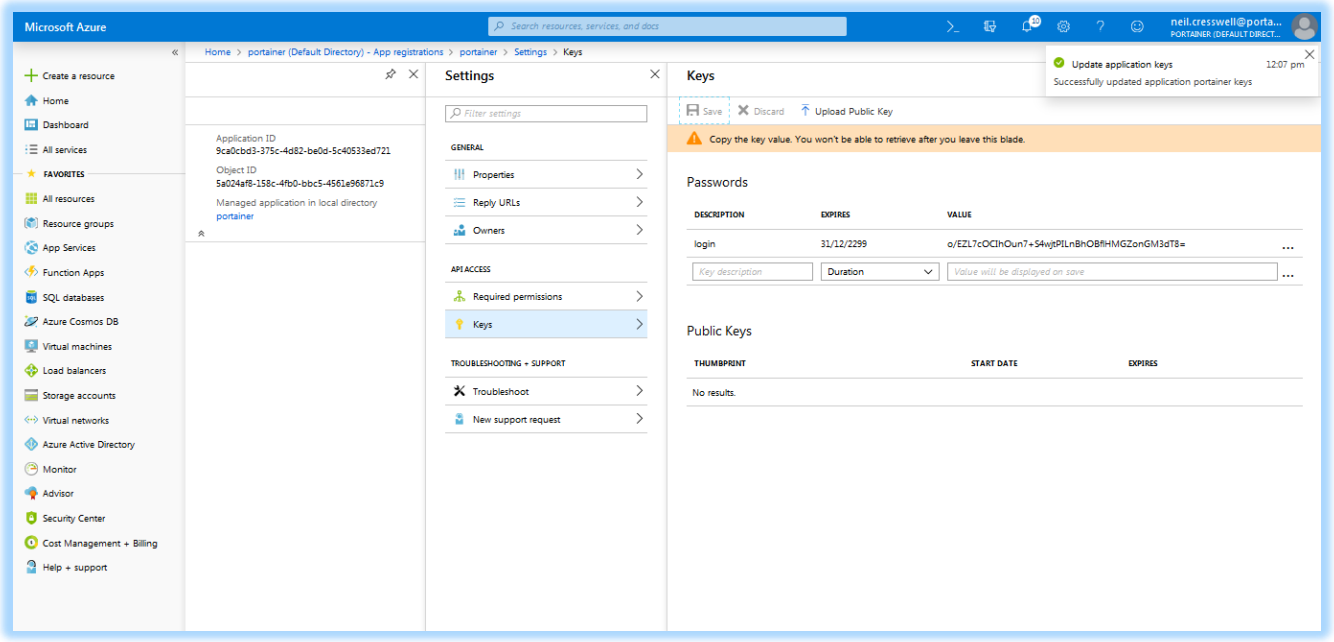
Step 5. Create The Application login key

Click on “Settings”, then “Keys”



Under the “Passwords” section, create a new key called “login”, set the Duration to “never expires”, and then click Save.

The Key will then be generated for you. Note this key Value for later use.

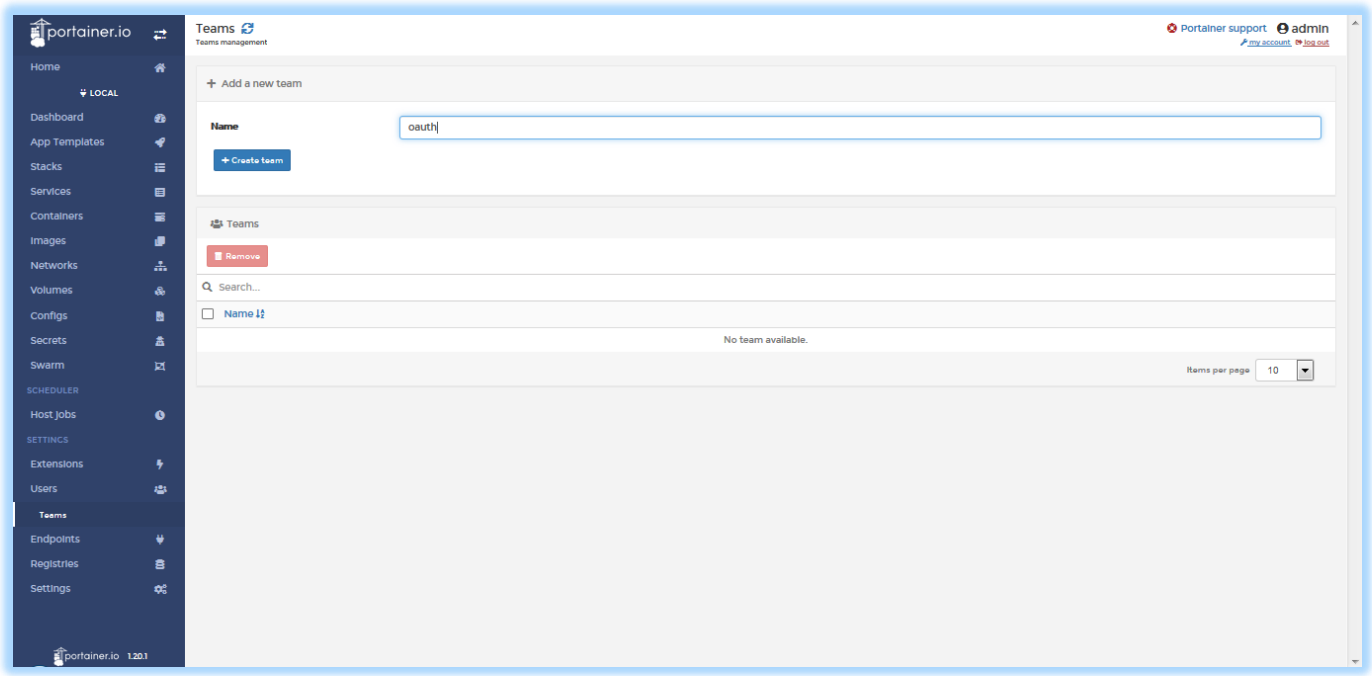


Step 6. Switch to your Portainer Instance and login as the local instance admin

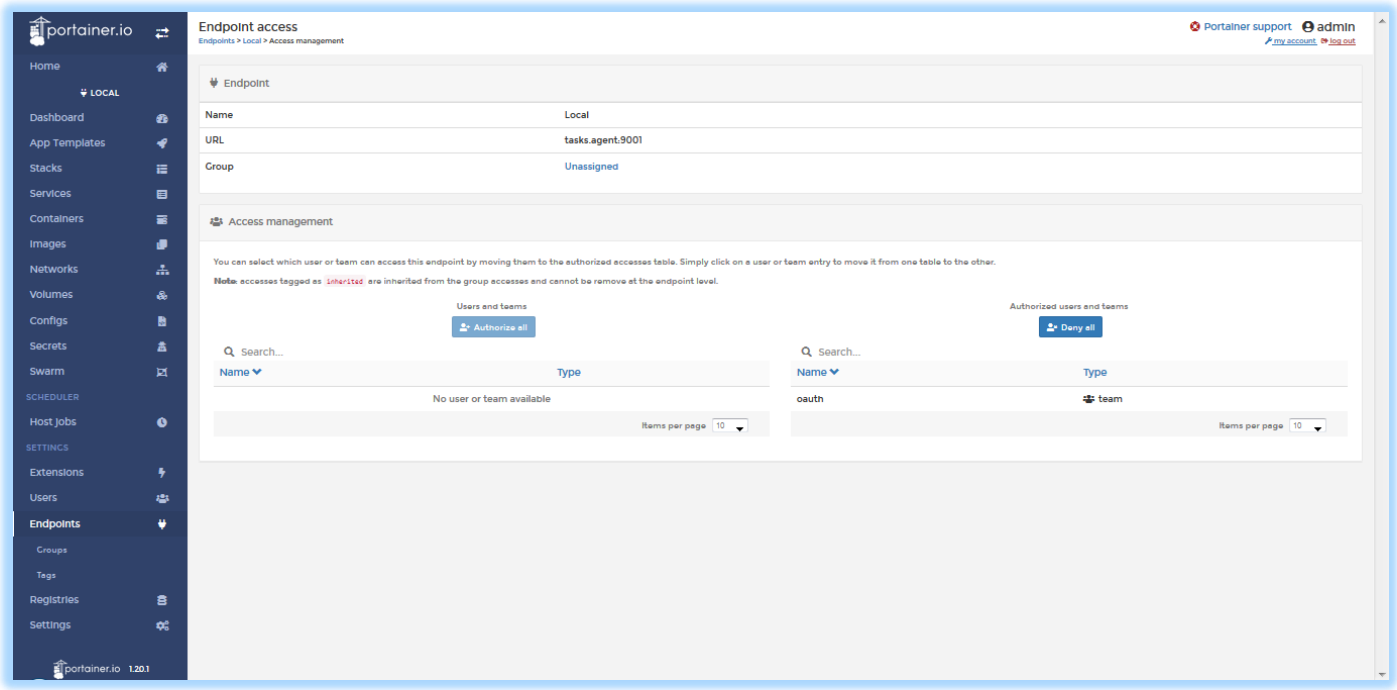
Purchase the Portainer Authentication Extension, and apply the license key (process not shown here).

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)



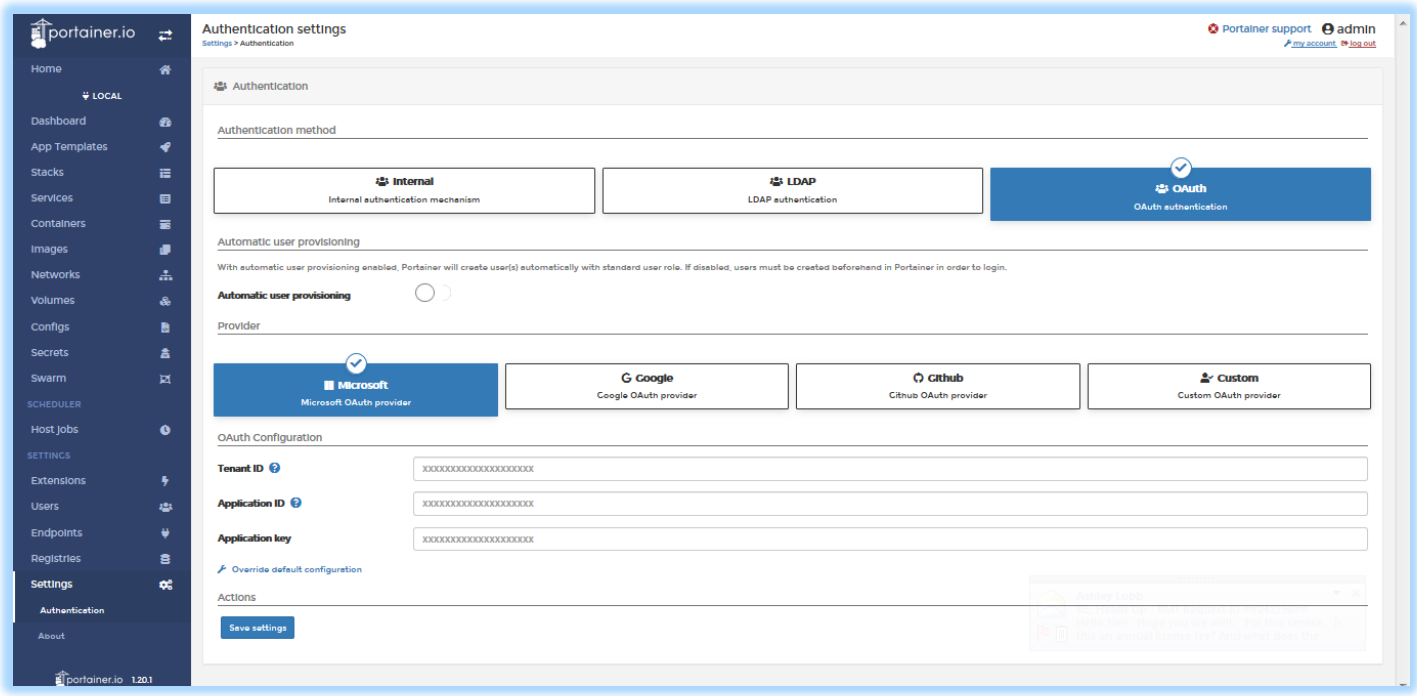
Click on “Endpoints” and then select the endpoints you would like to grant the oAUTH users access to manage, and then click “Manage Access”. Assign the oAUTH group you created to the authorised list.



Step 7. Let’s configure Portainer External Authenication extension.

Click on “settings” and then “Authentication”

Select “oAUTH” and then select “Microsoft”



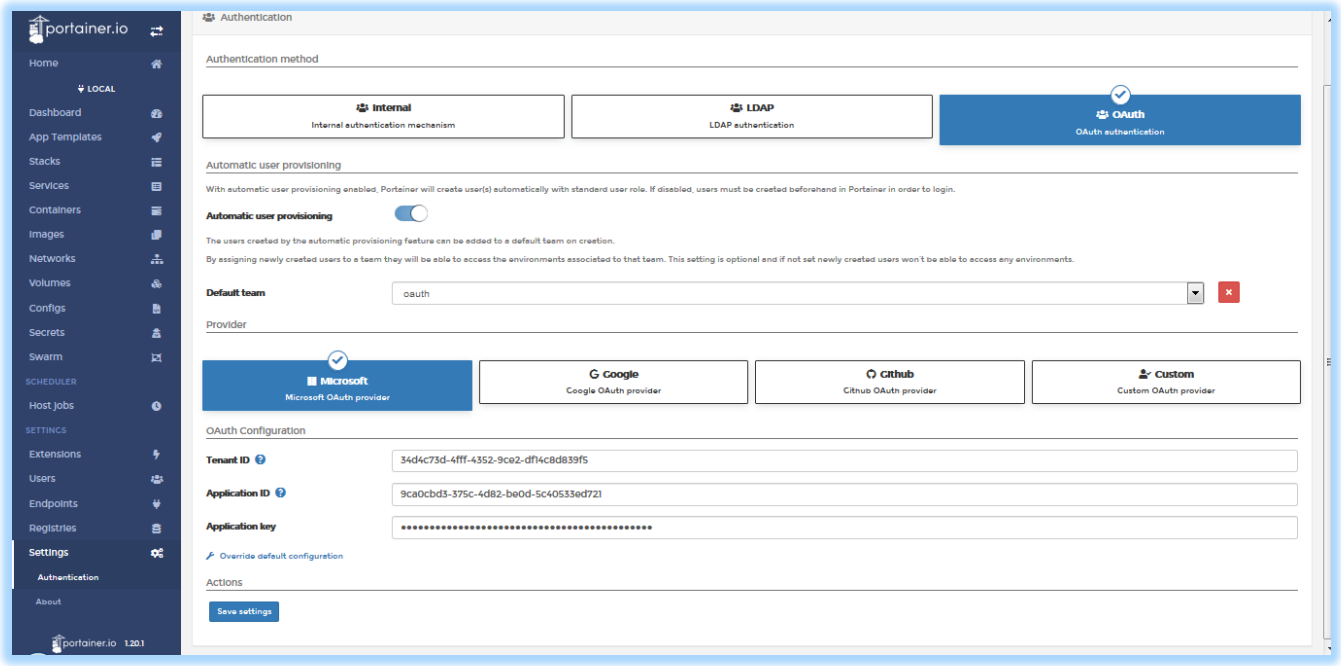
Enable Automatic User Provisioning, and select the default team (oAUTH or similar) that you created previously.

Enter in the Tenant ID (Directory ID) that you noted previously.

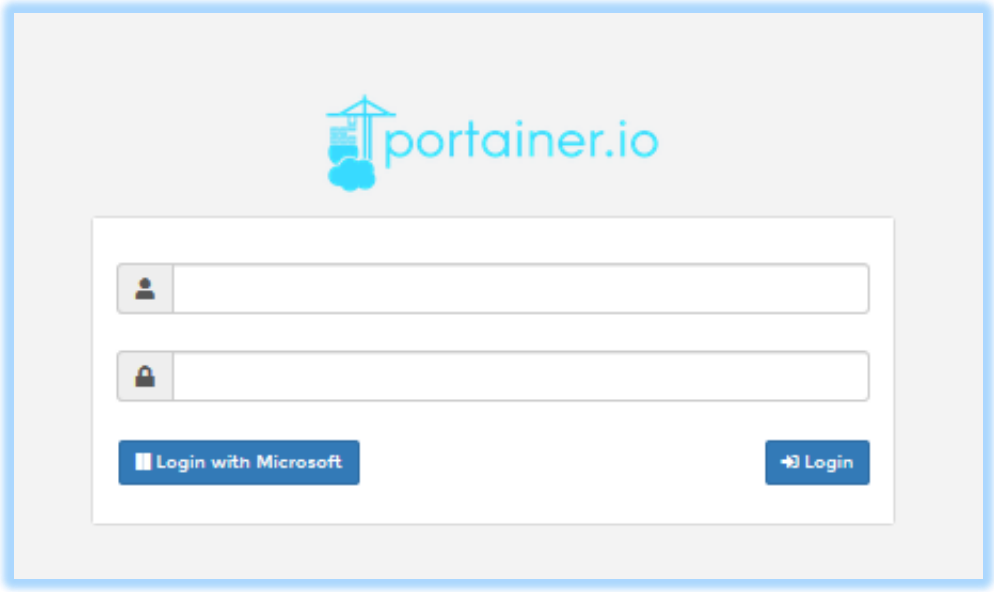
Enter in the Application ID that you noted previously.

Enter in the Application Key (Login key) that you noted previously.

Click Save.



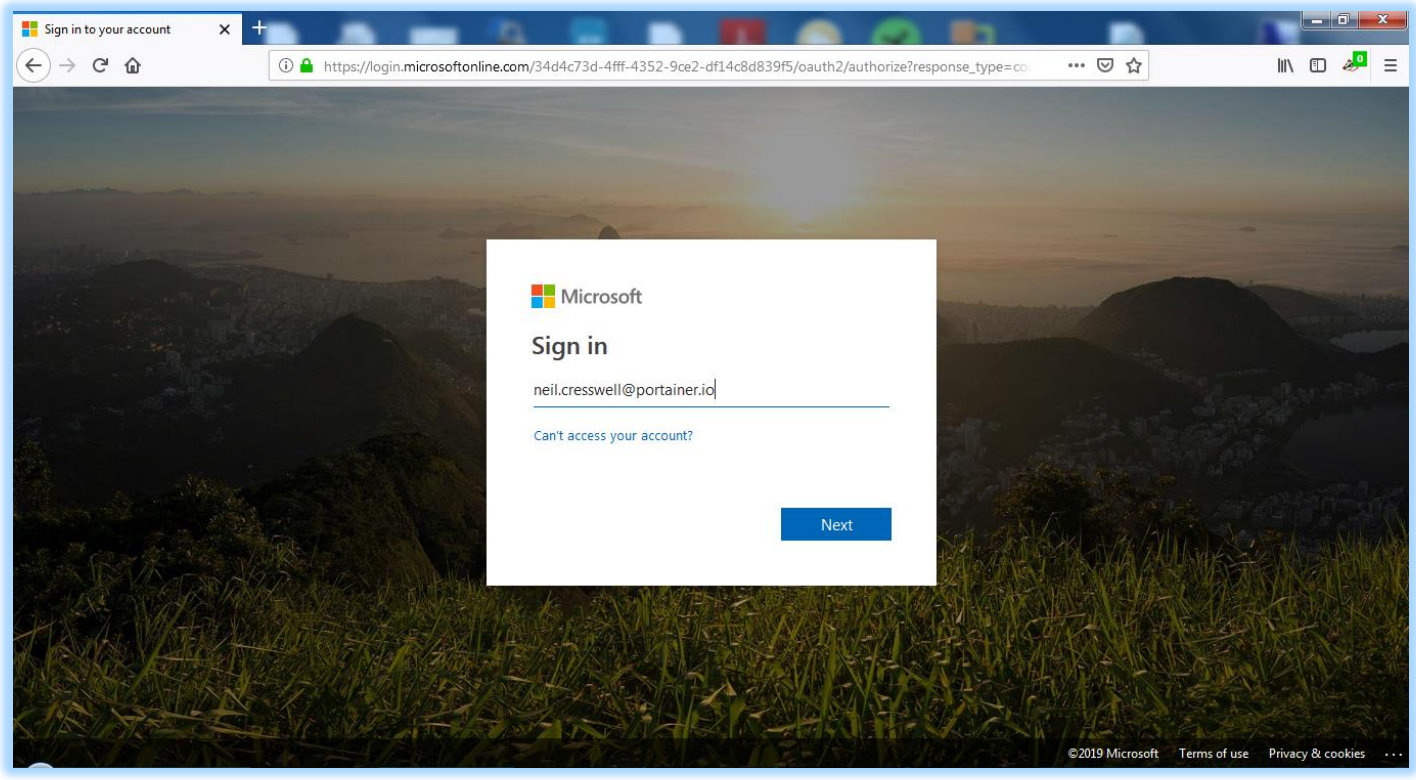
Logout as the Admin



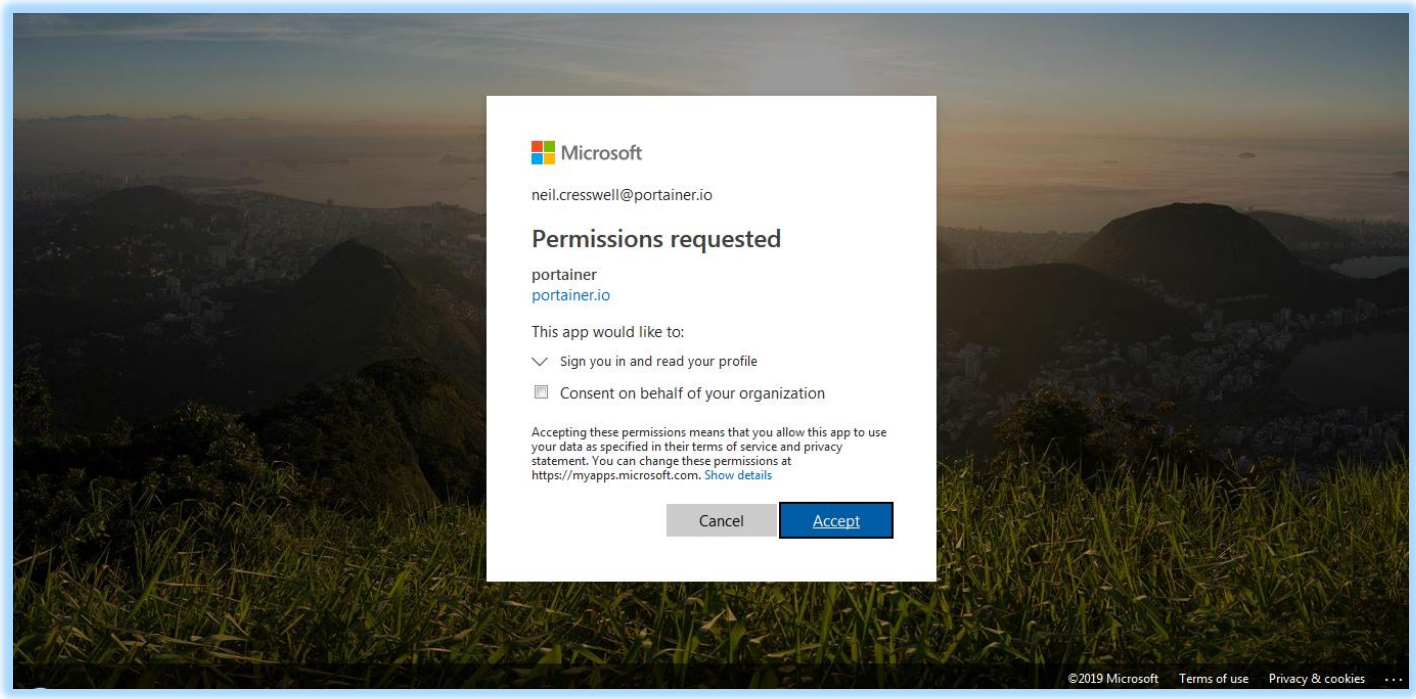
Step 8. Login using oAUTH

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

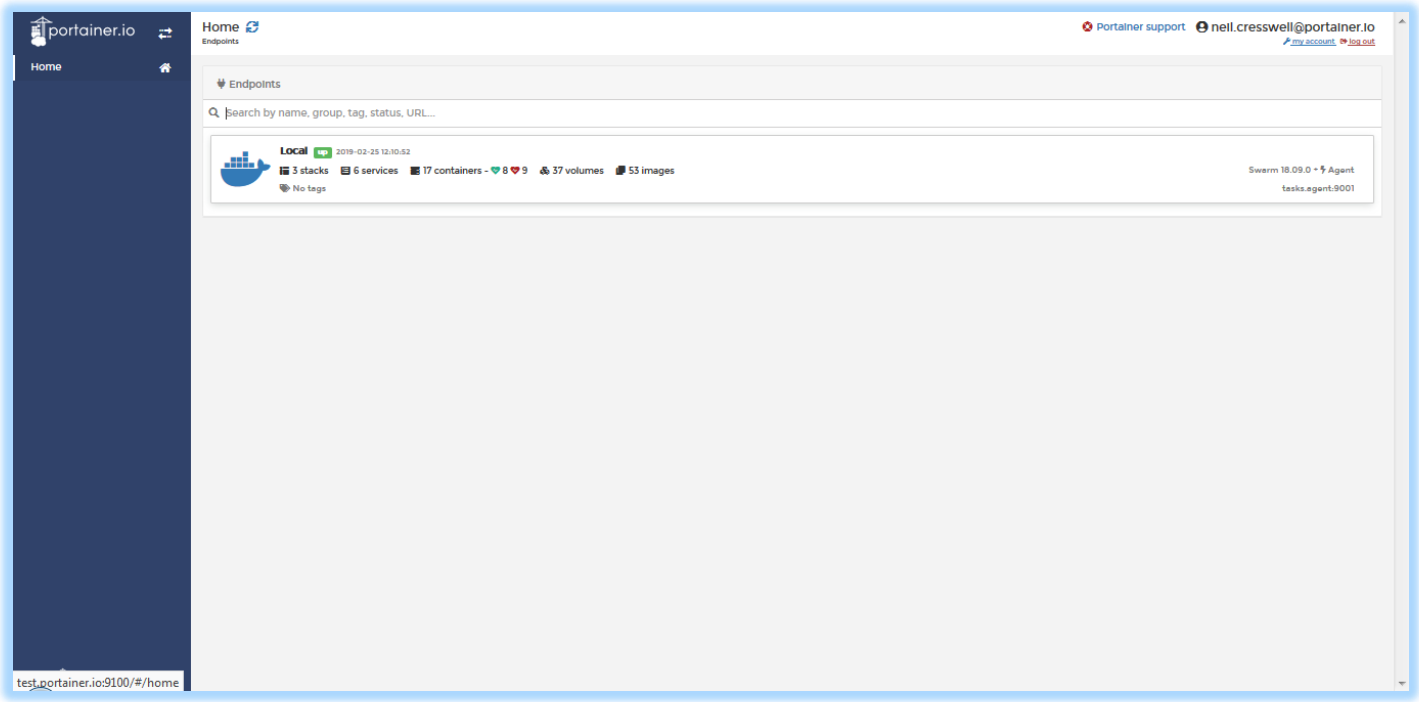
Enter your Azure Username and Password where prompted (note you are redirected to Azure for Auth)



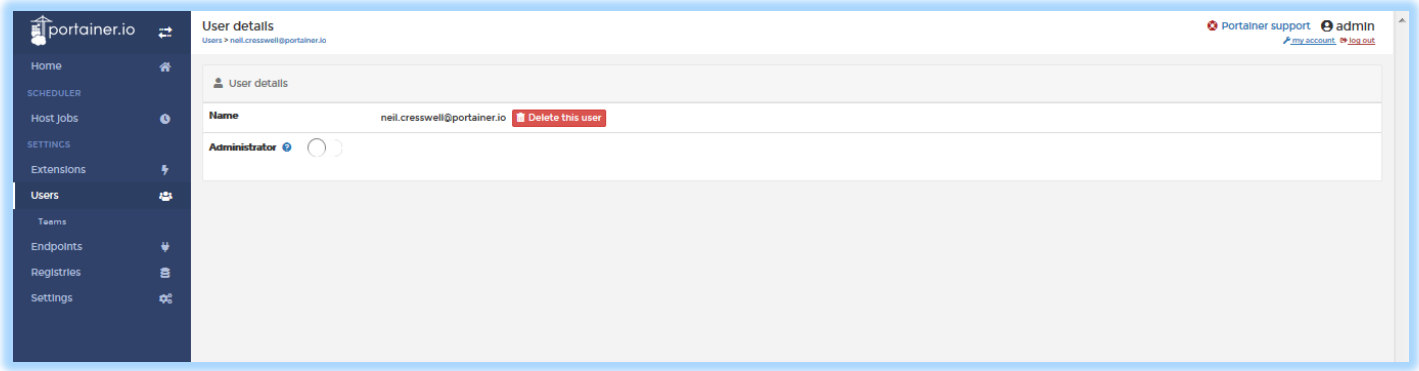
Accept the “Permissions Requested” box on behalf of your organisation (only occurs for the very first oAUTH login to Portainer).



You are now logged into Portainer using oAUTH from Microsoft.



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.