

Portainer Extension Software

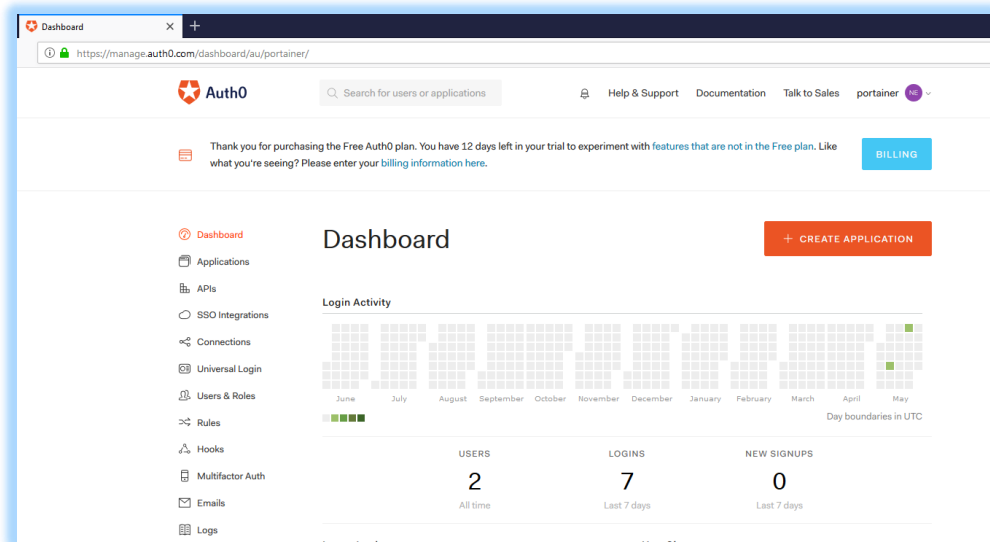
Implementation Guide

External Authentication for Auth0

May 2019

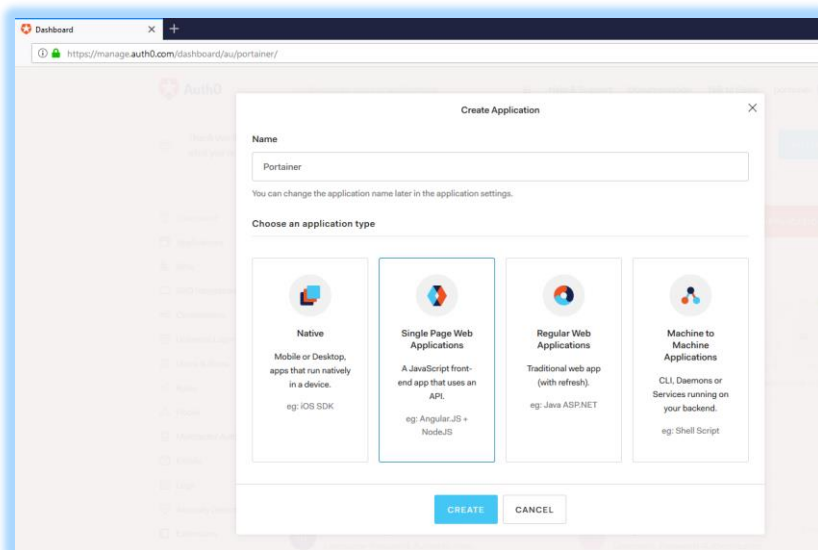
Implementation Guide External Authentication for Auth0

Step 1. Login to Auth0 Administration Console as an Admin

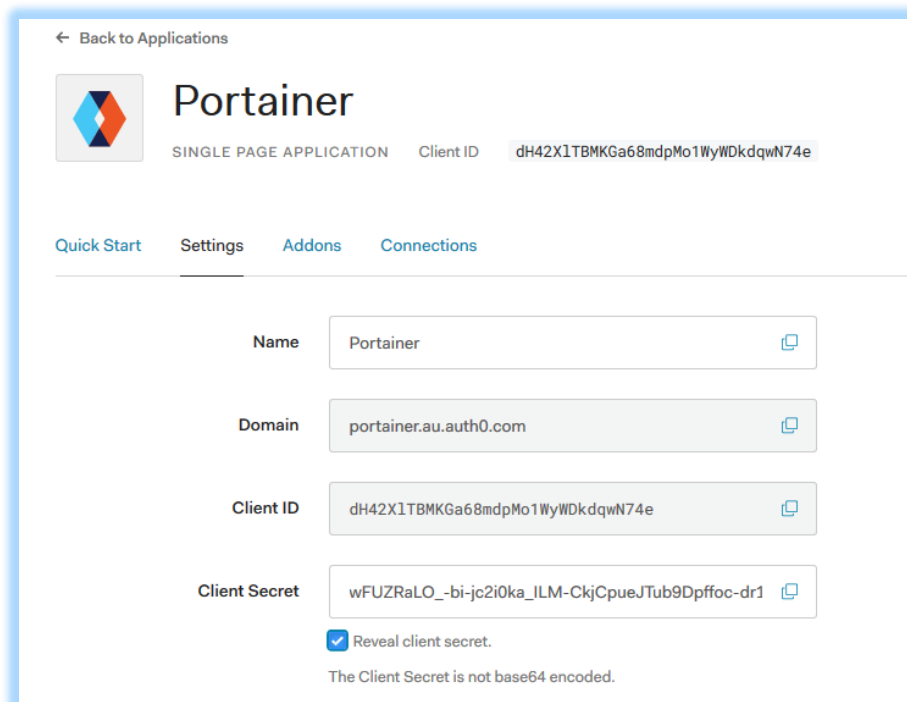


Step 2. Click “+ Create Application”

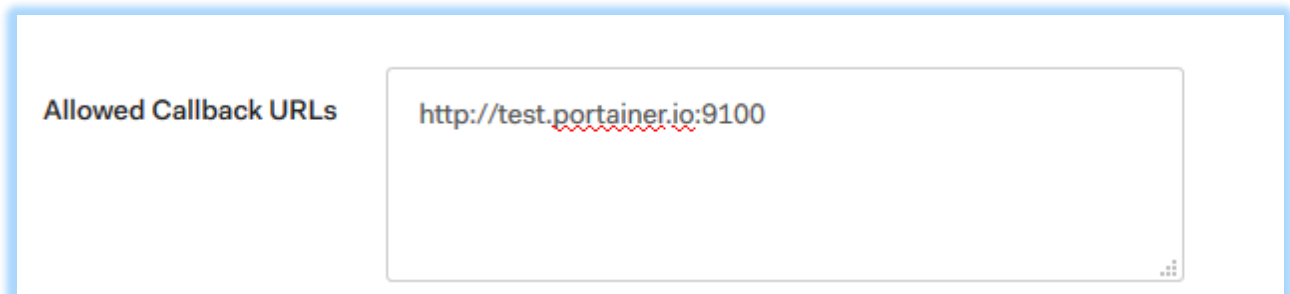
Give the application a name, and select “Single Page Web Applications”, and then click “Create”.



Step 3. Click on “Settings” in your new Application. Note down the “Domain”, Client ID” and “Client Secret”, you will need these later.



Scroll down to “Allowed Callback URLs” and enter in the FQDN:Port of your Portainer instance, then click “Save changes”



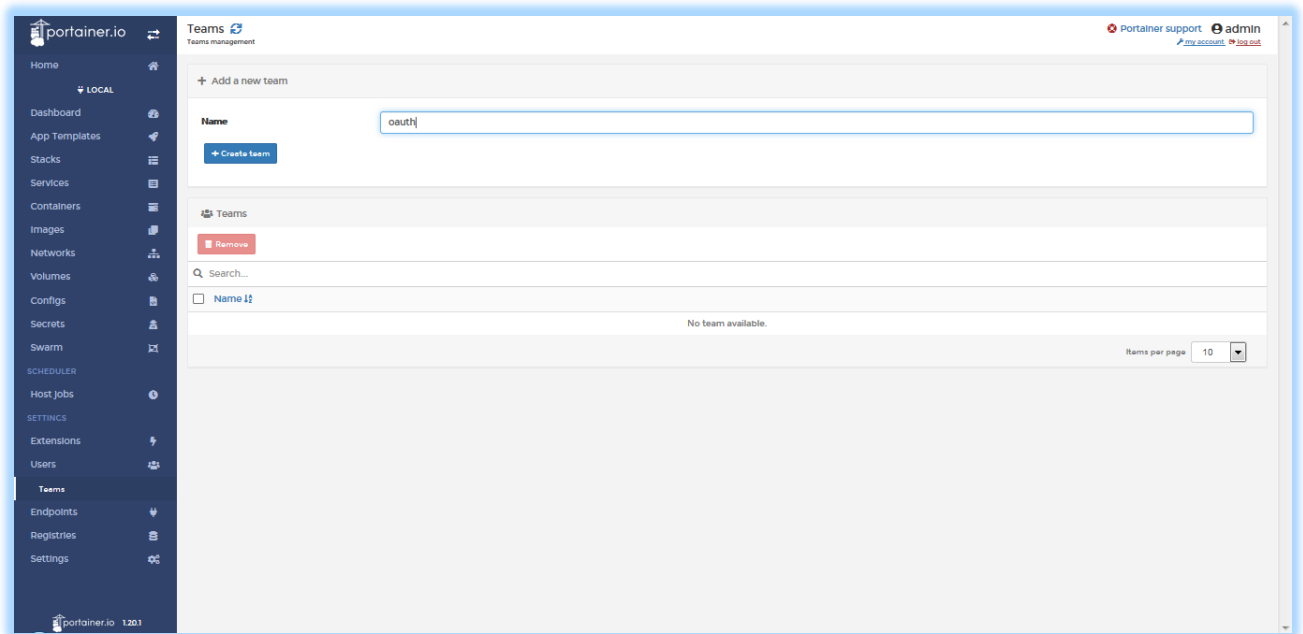
Now, we assume you already have users defined in your Auth0 system, but if not, click on “Users & Roles” in the left sidebar and add users as required.

Step 4: Switch to your Portainer Instance and login as the local instance admin

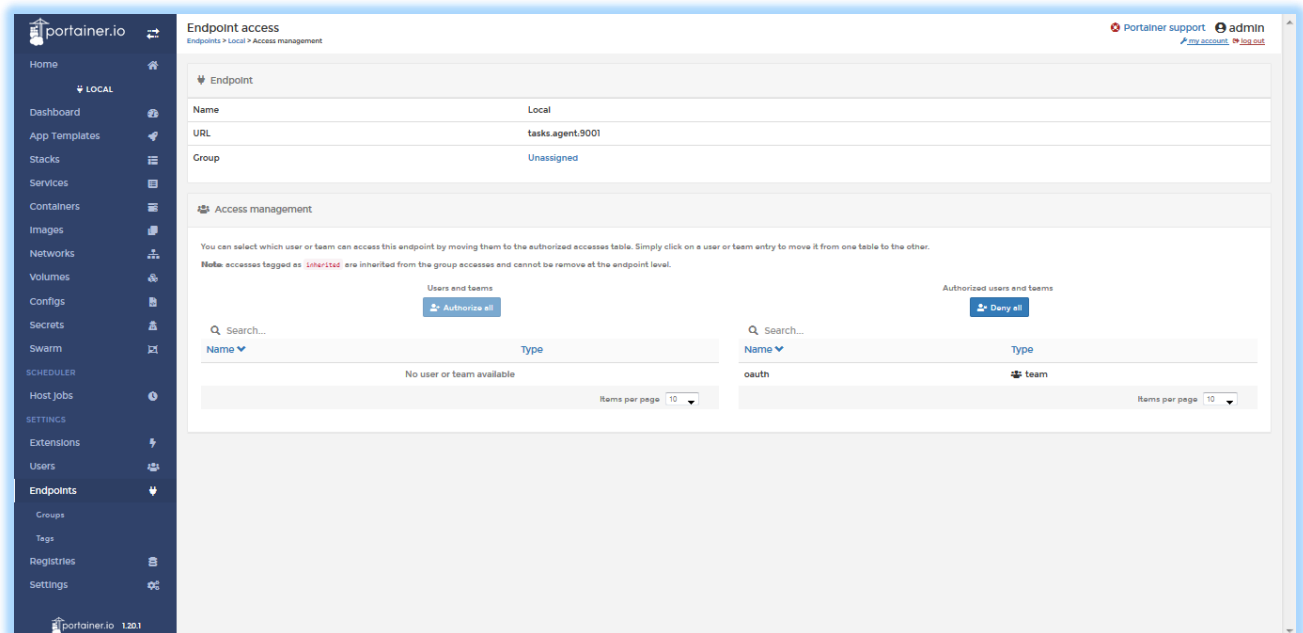
Purchase the Portainer External Authentication extension, and apply the license key (process not shown here).

Let’s 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)



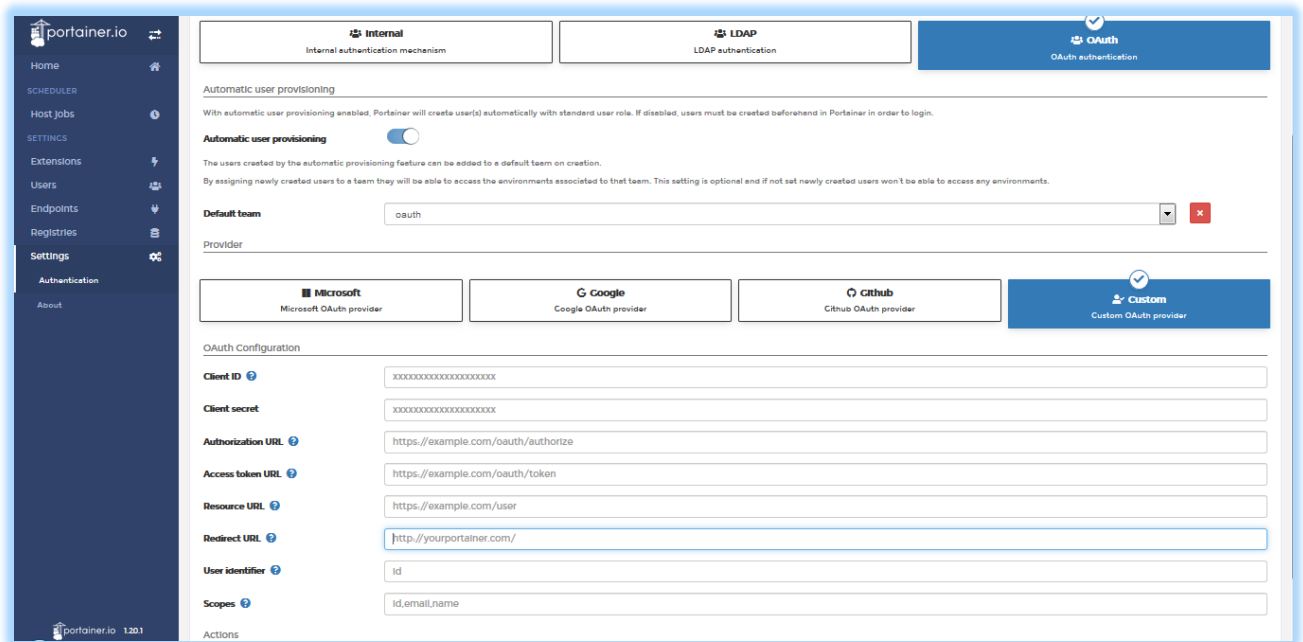
Click on “Endpoints” and then select the endpoints you would like to grant the oAUTH users access to manage, and then click “Manage Access”. Assign the oAUTH group you created to the authorized list.



Step 5. Let's configure Portainer External Authentication.

Click on "settings" and then "Authentication"

Select "oAUTH" and then select "Custom"



The screenshot shows the Portainer.io web interface. On the left is a dark sidebar with navigation links: Home, SCHEDULER, Host Jobs, SETTINGS, Extensions, Users, Endpoints, Registries, Settings, Authentication, and About. The 'Authentication' link is highlighted. The main panel has three tabs: 'Internal' (Internal authentication mechanism), 'LDAP' (LDAP authentication), and 'OAuth' (OAuth authentication). The 'OAuth' tab is selected. Below the tabs, there's a section for 'Automatic user provisioning' with a toggle switch and explanatory text. A 'Default team' dropdown menu is set to 'oauth'. Below this is a 'Provider' section with four buttons: 'Microsoft' (Microsoft OAuth provider), 'Google' (Google OAuth provider), 'GitHub' (GitHub OAuth provider), and 'Custom' (Custom OAuth provider). The 'Custom' button is highlighted. Underneath is the 'OAuth Configuration' section with several input fields: 'Client ID' (masked with x's), 'Client secret' (masked with x's), 'Authorization URL' (https://example.com/oauth/authorize), 'Access token URL' (https://example.com/oauth/token), 'Resource URL' (https://example.com/user), 'Redirect URL' (http://yourportainer.com/), 'User identifier' (id), and 'Scopes' (id,email,name). At the bottom left of the main panel is an 'Actions' button.

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

In "Client ID" enter the Client ID as previously obtained in the Auth0 application page.

In the "Client Secret" enter the Client Secret as previously obtained in the Auth0 application page.

In the "Authorisation URL" field, enter <https://portainer.au.auth0.com/authorize>. Make sure to replace "portainer.au.auth0.com" with the "domain" you previously obtained in the Auth0 application page.

In the "Access token URL" field, enter <https://portainer.au.auth0.com/oauth/token>. Make sure to replace "portainer.au.auth0.com" with the "domain" you previously obtained in the Auth0 application page.

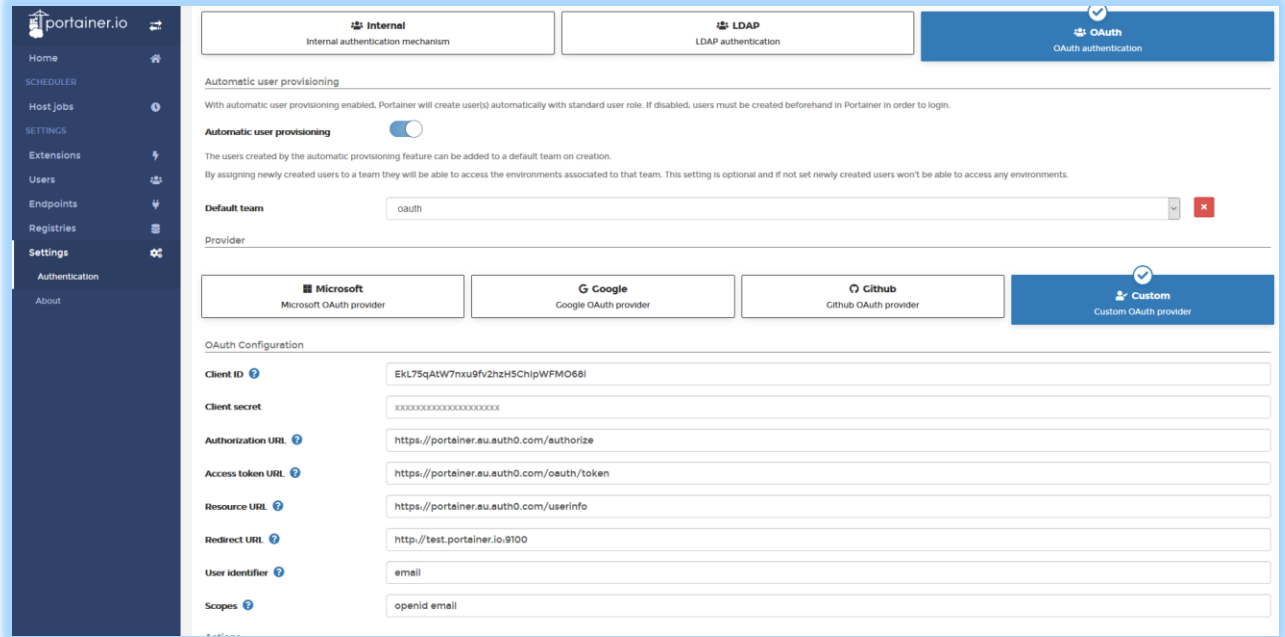
In the "Resource URL" field, enter <https://portainer.au.auth0.com/userinfo>. Make sure to replace "portainer.au.auth0.com" with the "domain" you previously obtained in the Auth0 application page.

In the "Redirect URL" field, enter the FDQN/URL of your Portainer instance, e.g. <http://test.portainer.io:9100>

In the "User Identifier" field, enter "email".

In the "Scopes" field, enter "openid email".

Click Save.



portainer.io

Home

SCHEDULER

Host Jobs

SETTINGS

Extensions

Users

Endpoints

Registries

Settings

Authentication

About

Internal
Internal authentication mechanism

LDAP
LDAP authentication

OAuth
OAuth authentication

Automatic user provisioning

With automatic user provisioning enabled, Portainer will create user(s) automatically with standard user role. If disabled, users must be created beforehand in Portainer in order to login.

Automatic user provisioning ☐

The users created by the automatic provisioning feature can be added to a default team on creation.

By assigning newly created users to a team they will be able to access the environments associated to that team. This setting is optional and if not set newly created users won't be able to access any environments.

Default team

Provider

Microsoft
Microsoft OAuth provider

Google
Google OAuth provider

Github
Github OAuth provider

Custom
Custom OAuth provider

OAuth Configuration

Client ID

Client secret

Authorization URL

Access token URL

Resource URL

Redirect URL

User identifier

Scopes

Click Save.

Logout as the Admin

Step 6. Login using oAUTH

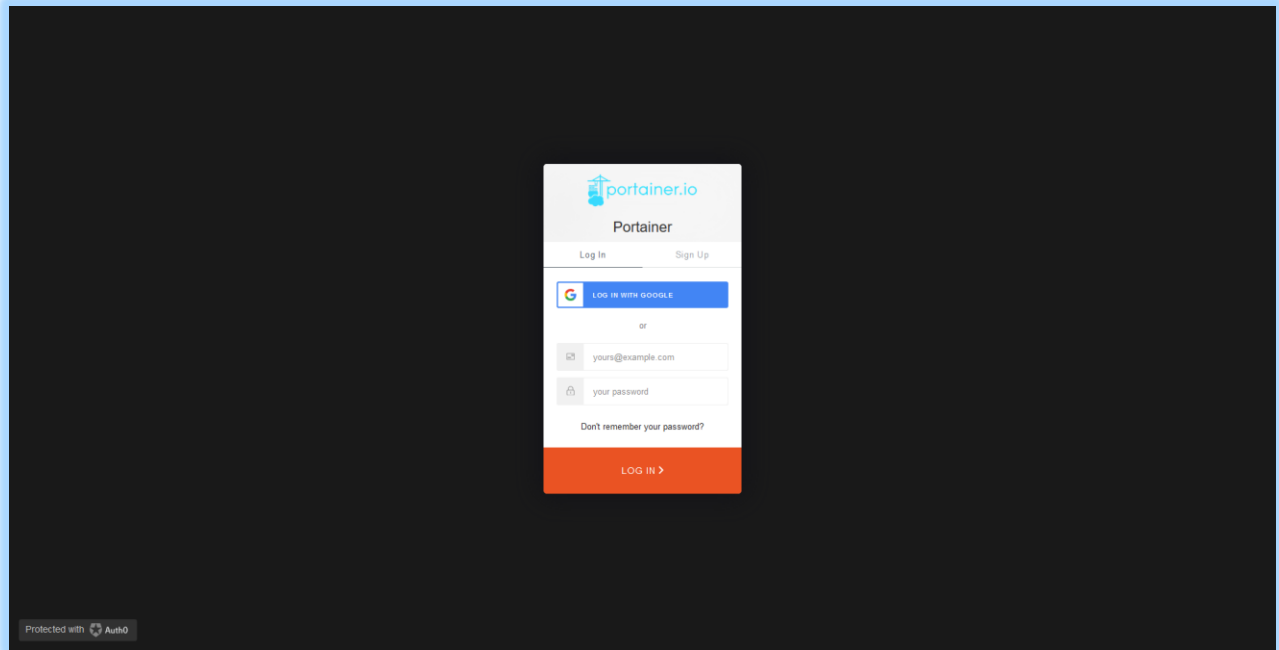
At the Login Page, click the “Login with oAUTH” box for oAUTH login.



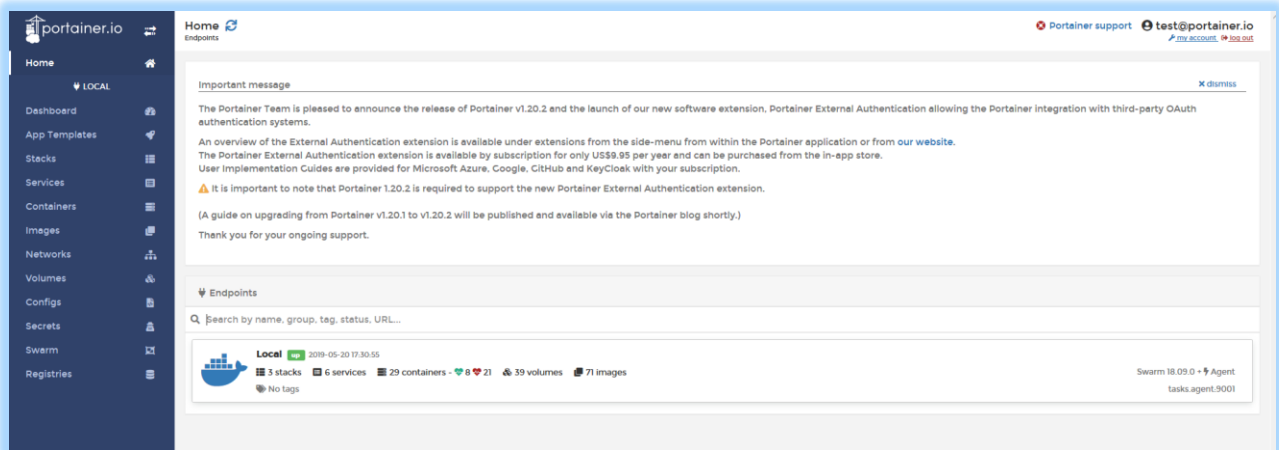
portainer.io

Login with OAuth **Login**

Enter your oAuth username and password where prompted (note you are redirected to your Auth0 instance for Auth).



You are now logged into Portainer using oAUTH from Auth0.



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.