portainer.io

Portainer Extension Software

Implementation Guide

External Authentication for Okta

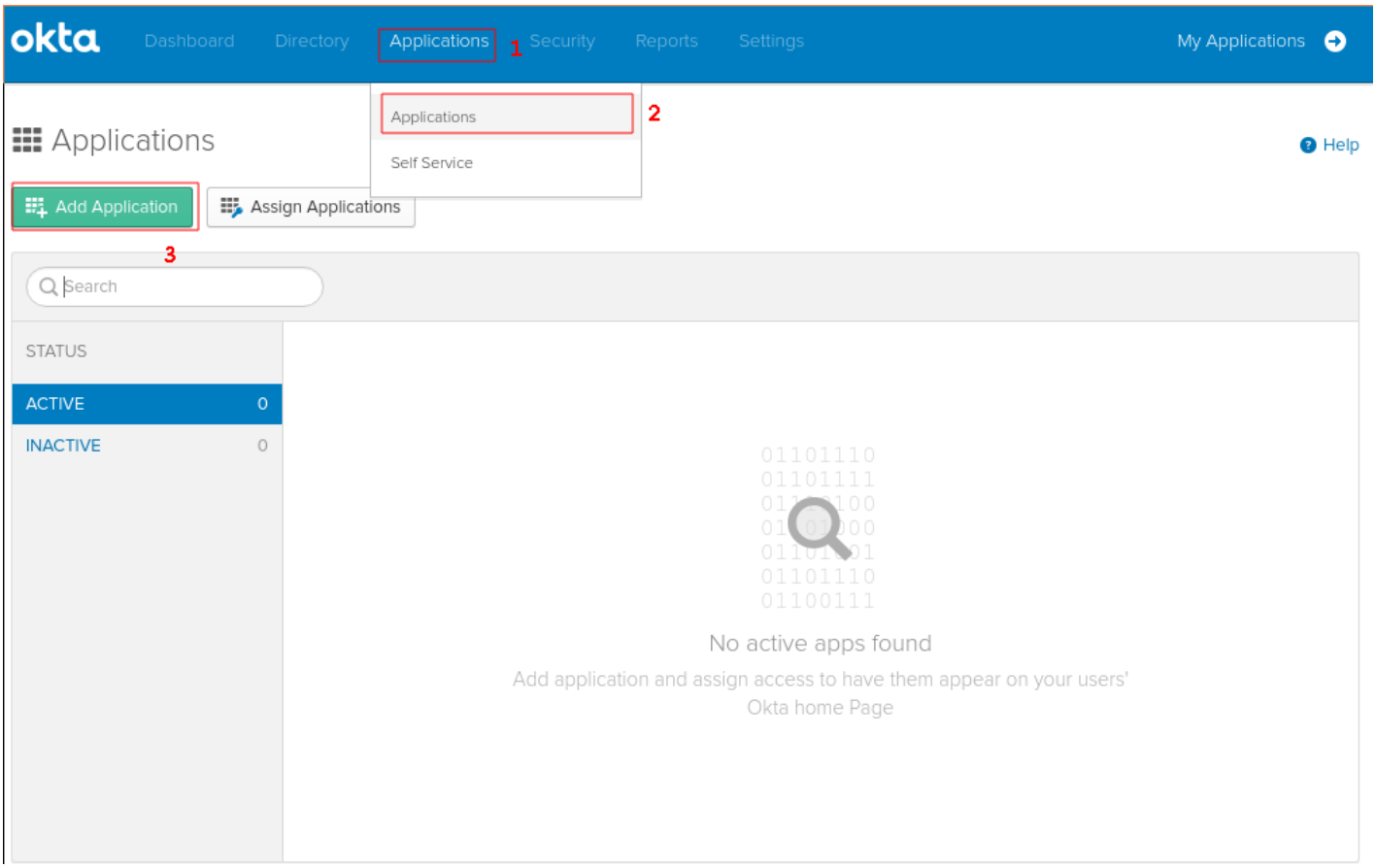
July 2019

Implementation Guide

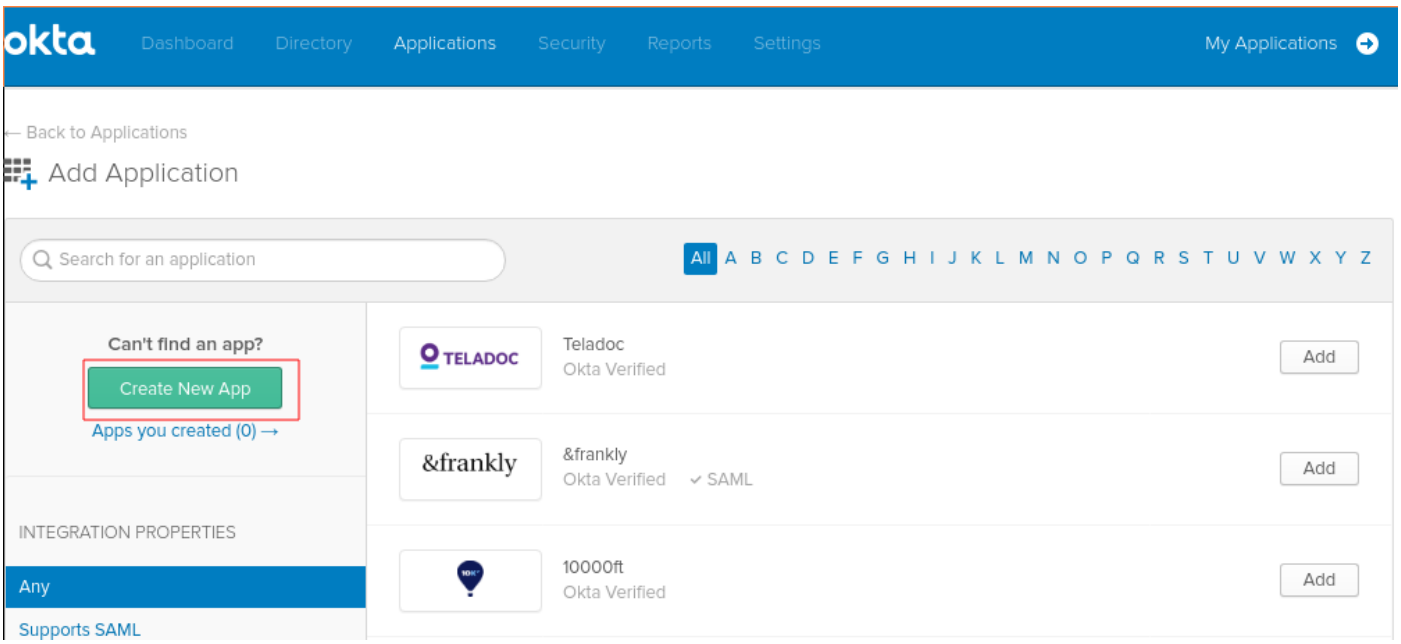
External Authentication for Okta

Step 1. Login to Okta Administration Console as an Admin.

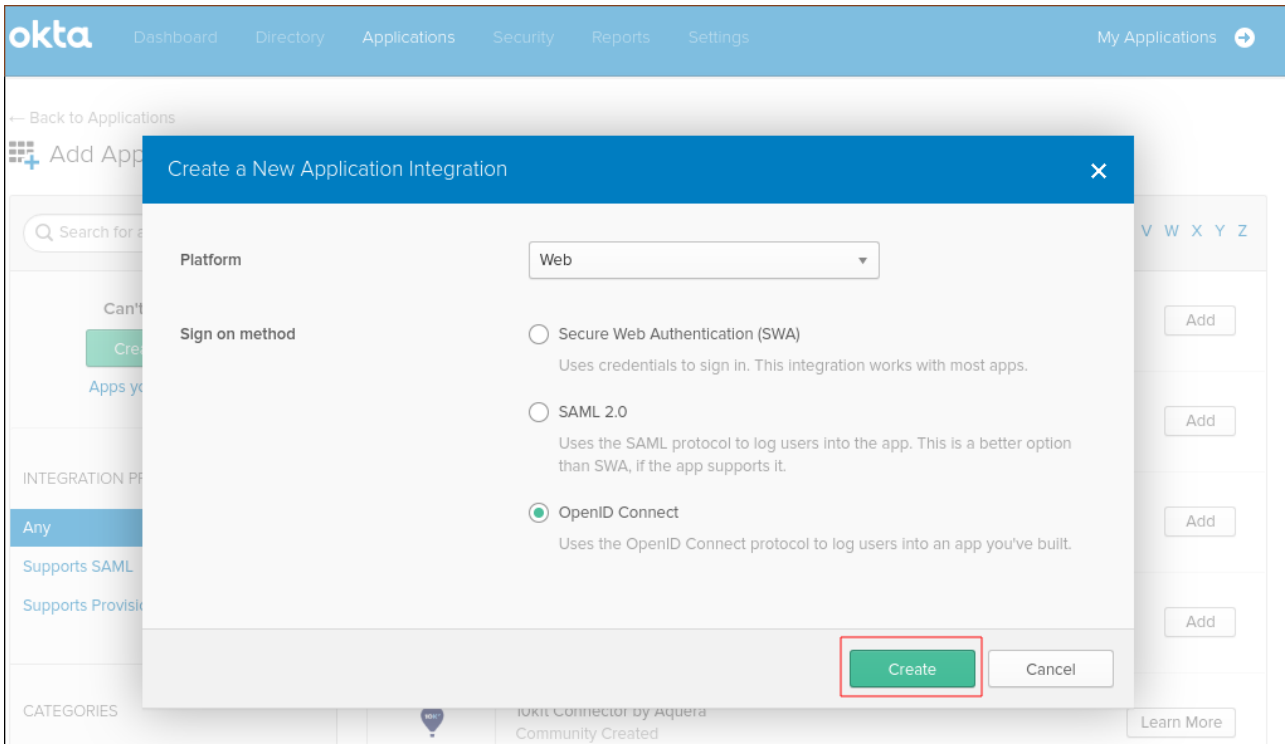
Step 2. Navigate to the Applications page and click **Add Application**



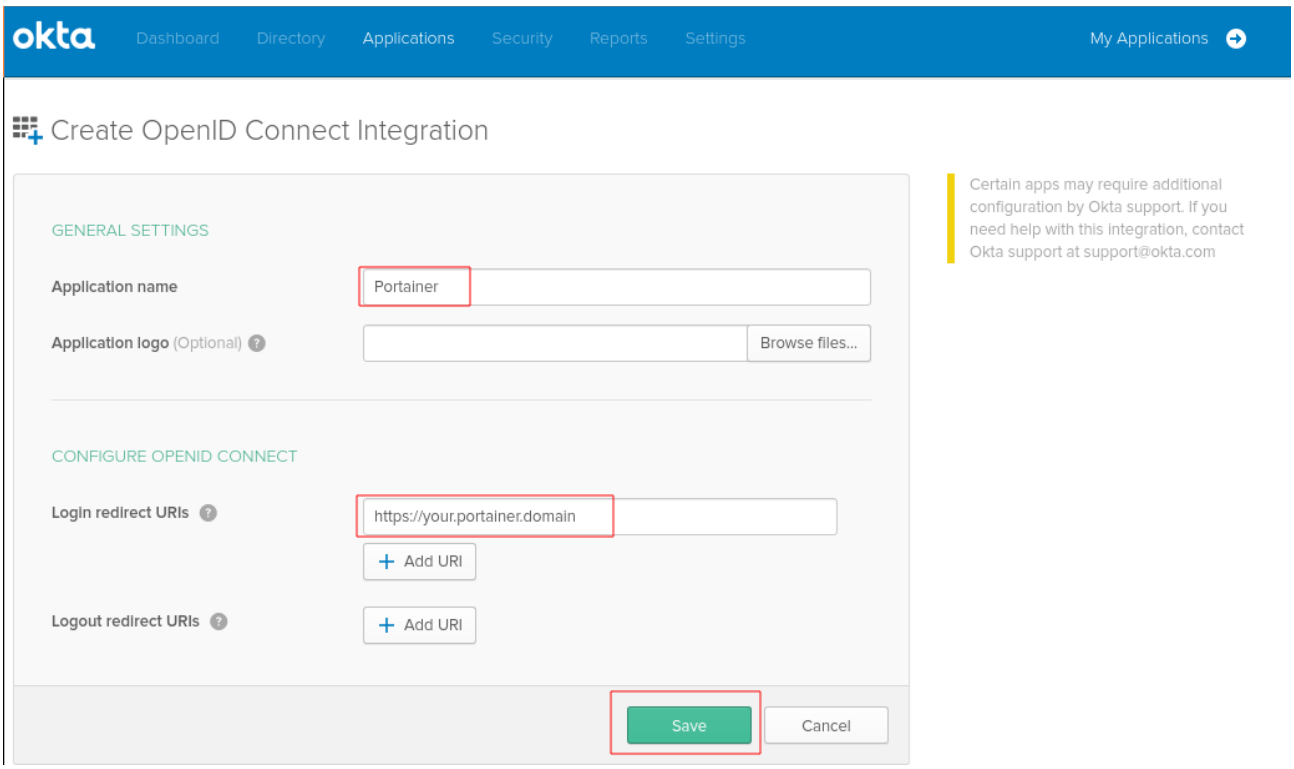
Step 3. Click **Create New App**



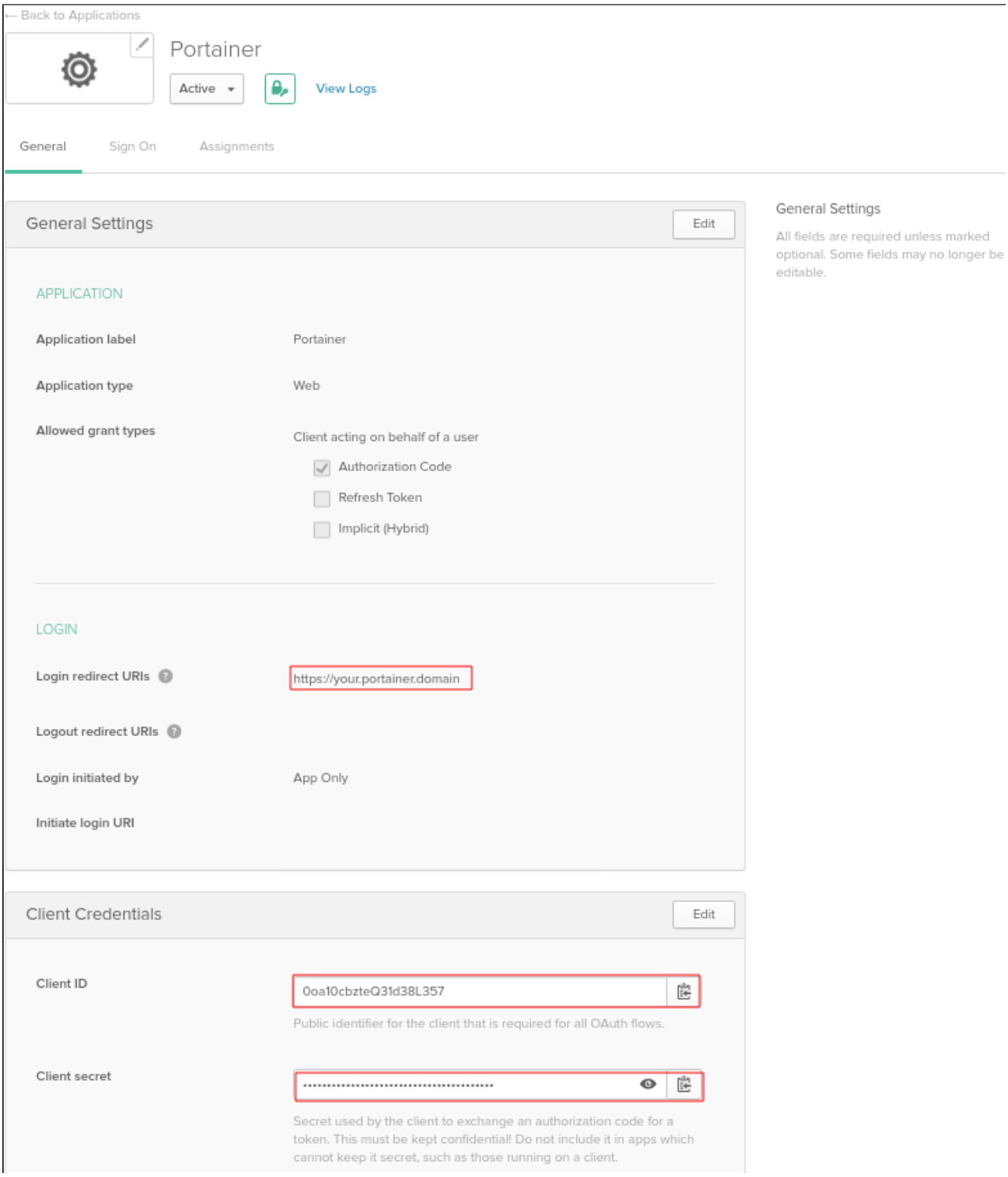
Step 4. Select **Web** and **OpenID Connect**. Then click **Create**



Step 5. Fill the Okta **Application Name** (this one is only for you) and the **Login redirect URI** field. Then click **Save**.



Step 6. Once application has been created, save the following information: **Login redirect URI**, **Client ID**, **Client Secret**



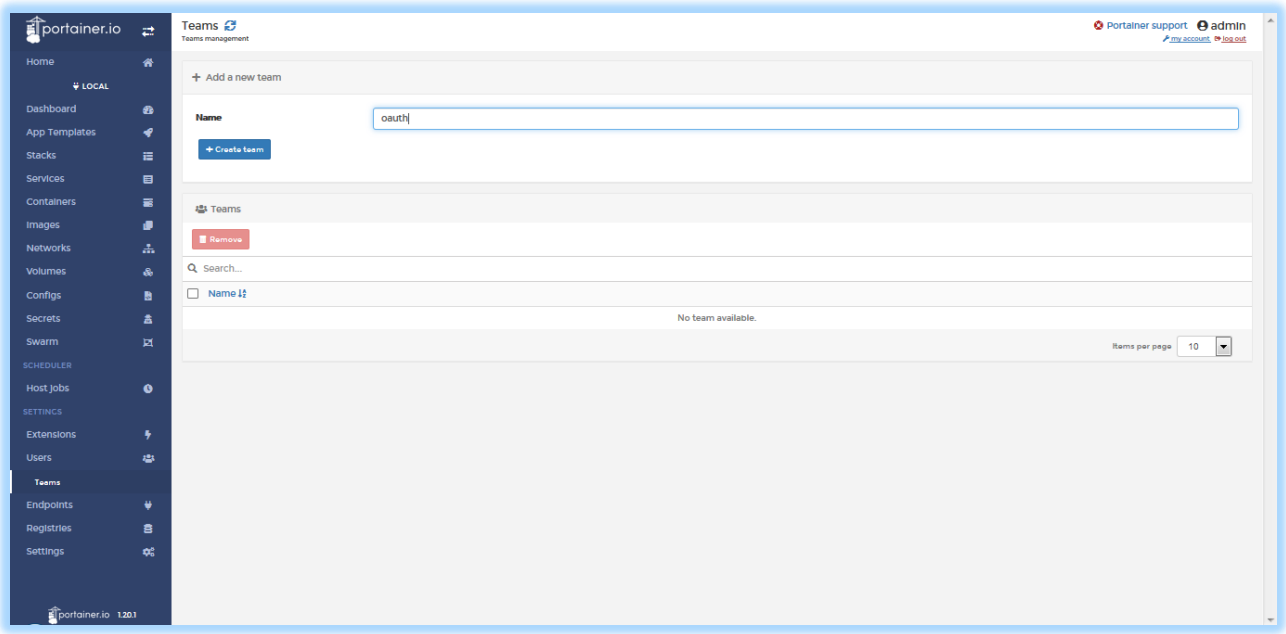
Now, we assume you already have users defined in your system, but if not, click on **Assignments** and assign users as required.

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

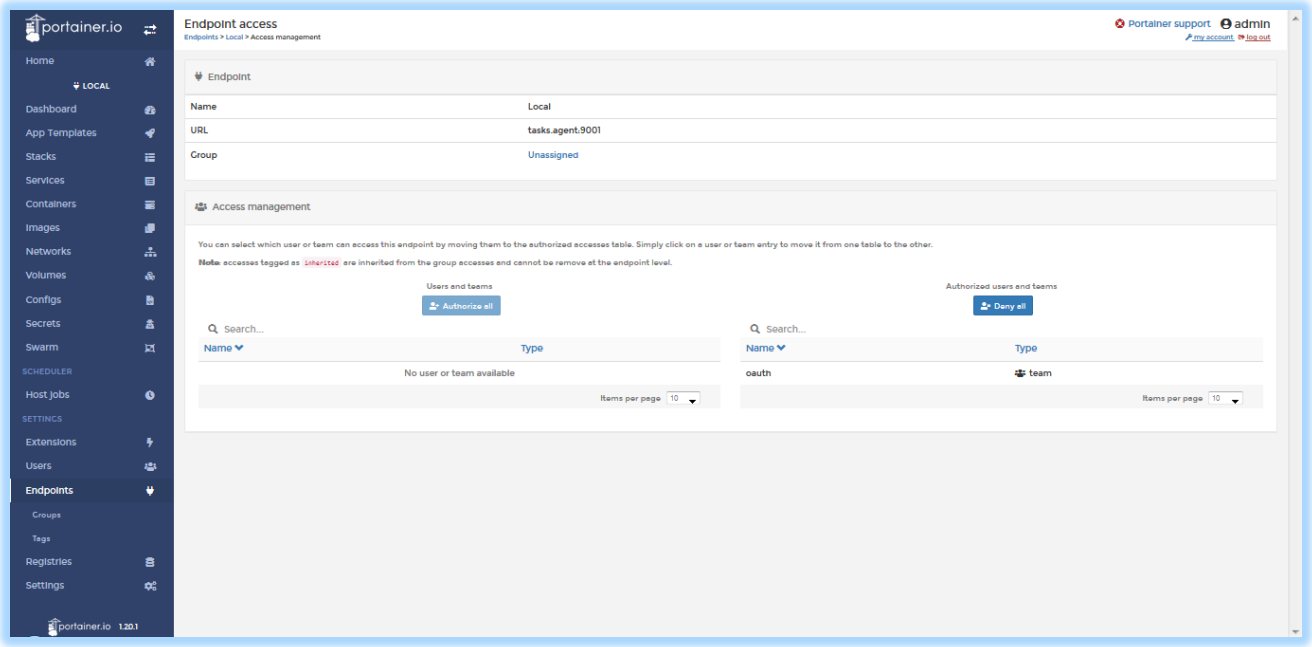
Purchase the **Portainer External Authentication** extension and apply the license key (process not shown here).

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 8. Let's configure Portainer External Authenication.

Click on **Settings**, then **Authentication**

Select **OAuth**, then select **Custom**

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

In the **Client ID** field enter the Client ID as previously obtained in the Okta application page.

In the **Client Secret** field enter the Client Secret as previously obtained in the Okta application page.

In the **Authorisation URL** field, enter https://YOUR_OKTA_DOMAIN.okta.com/oauth2/v1/authorize

In the **Access token URL** field, enter https://YOUR_OKTA_DOMAIN.okta.com/oauth2/v1/token

In the **Resource URL** field, enter https://YOUR_OKTA_DOMAIN.okta.com/oauth2/v1/userinfo

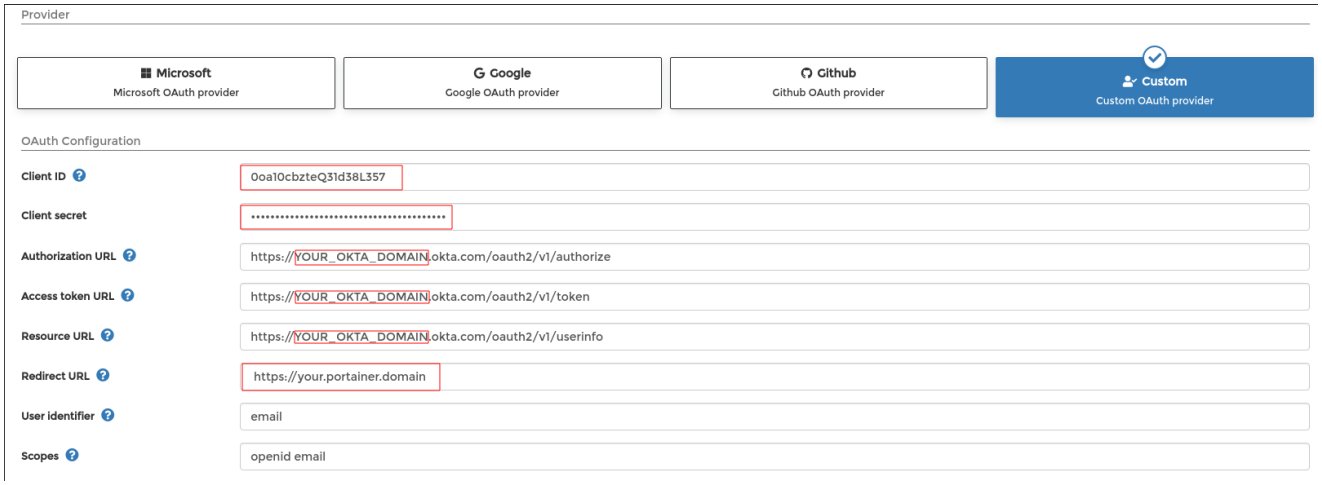
Make sure to replace **YOUR_OKTA_DOMAIN.okta.com** with your Okta subdomain (the one on which you created the Okta App).

In the **Redirect URL** field, enter the FDQN/URL of your Portainer instance (should match the one you entered on step 5).

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

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

Click **Save**



Logout as the Admin

Step 9. Login using OAuth

At the Login Page, click the **Login with OAuth** box for OAuth login.

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

You are now logged into Portainer using OAuth from Okta.

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.