

Portainer Extension Software

# Implementation Guide

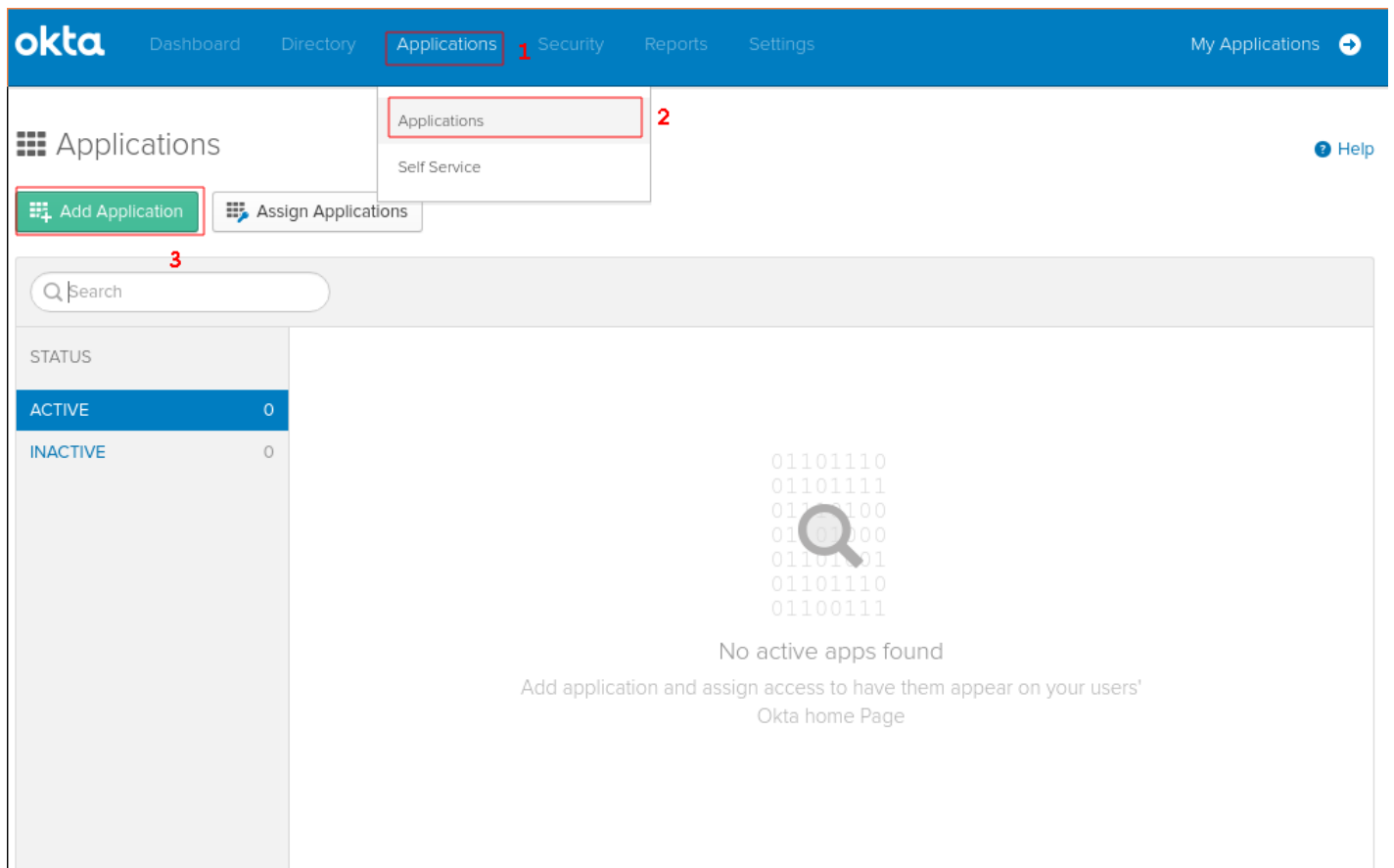
## External Authentication for Okta

July 2019

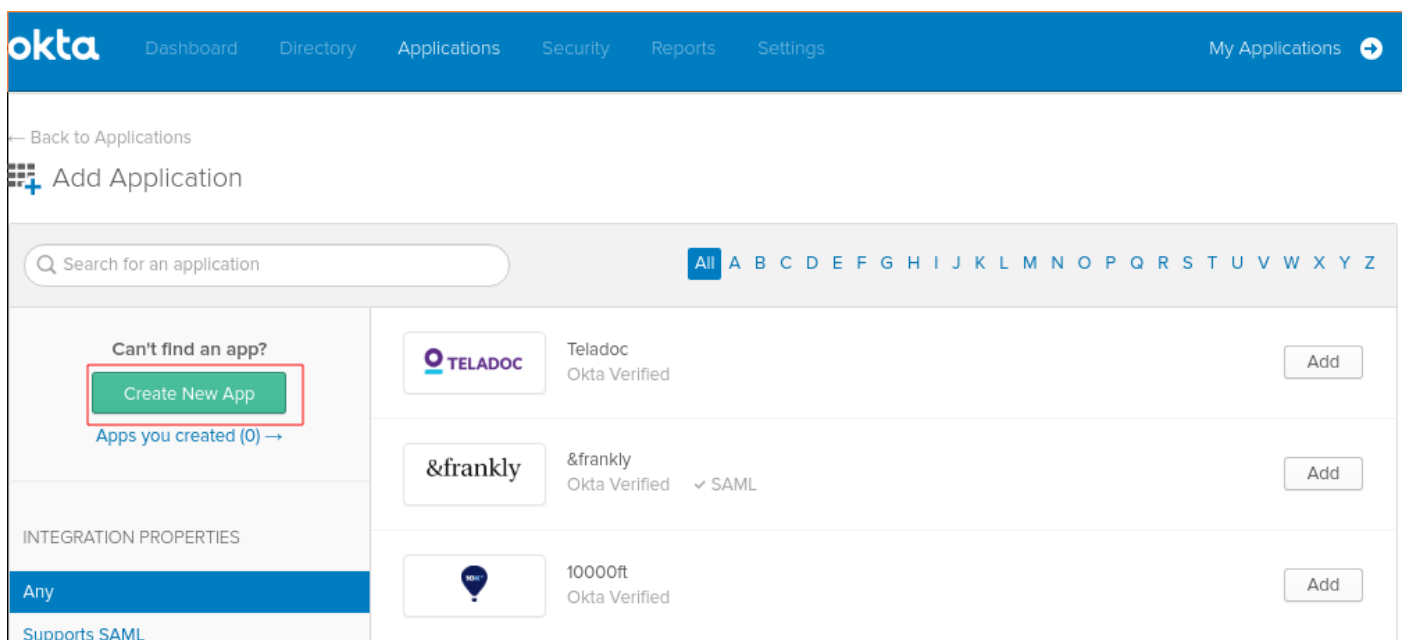
### Implementation Guide External Authentication for Okta

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

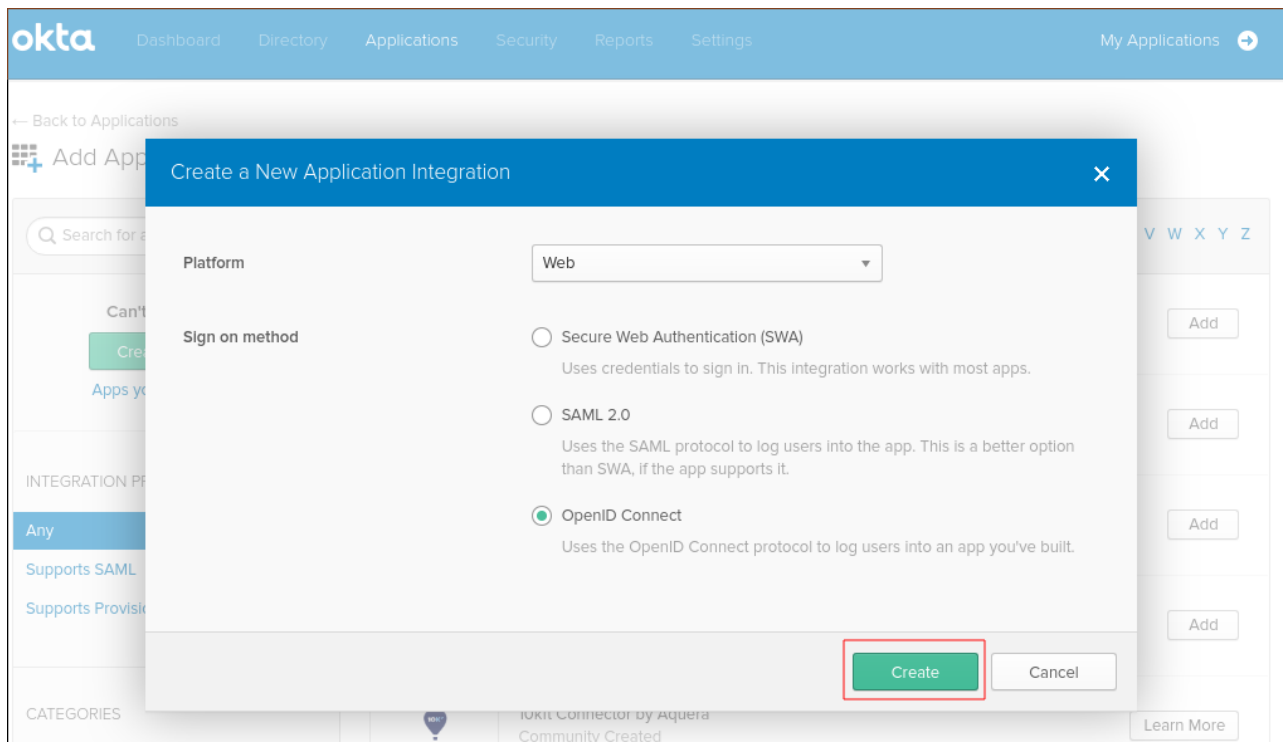
Step 2. Navigate to the Applications page and click **Add Application**



Step 3. Click **Create New App**



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



Okta Dashboard Directory Applications Security Reports Settings My Applications

Back to Applications

Add App

Search for

Can't find what you're looking for? Create a new app.

INTEGRATION PROVIDERS

Any

Supports SAML

Supports Provisioning

CATEGORIES

Okta Connector by Aquera Community Created

Learn More

Create a New Application Integration

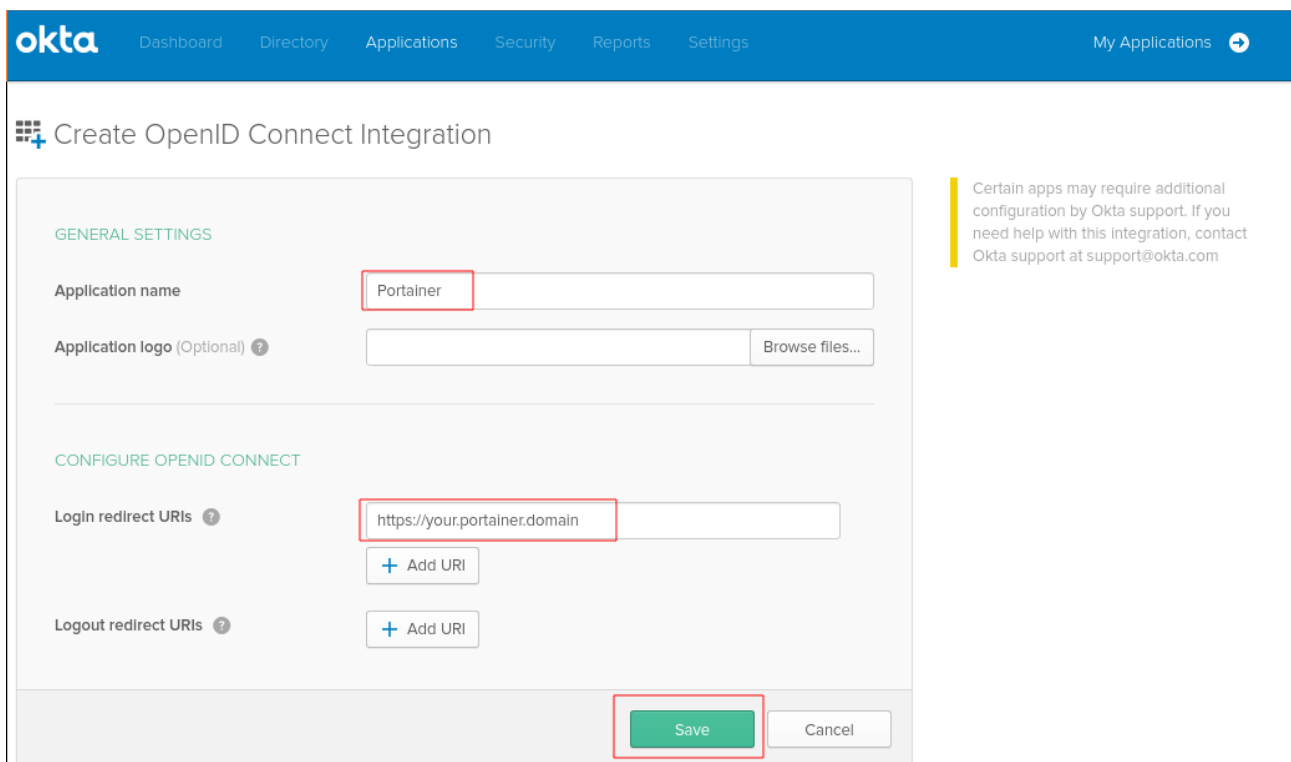
Platform: Web

Sign on method:

- ☐ Secure Web Authentication (SWA)  
Uses credentials to sign in. This integration works with most apps.
- ☐ SAML 2.0  
Uses the SAML protocol to log users into the app. This is a better option than SWA, if the app supports it.
- ☒ OpenID Connect  
Uses the OpenID Connect protocol to log users into an app you've built.

Create Cancel

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



Okta Dashboard Directory Applications Security Reports Settings My Applications

Create OpenID Connect Integration

GENERAL SETTINGS

Application name: Portainer

Application logo (Optional): Browse files...

CONFIGURE OPENID CONNECT

Login redirect URIs: https://your.portainer.domain

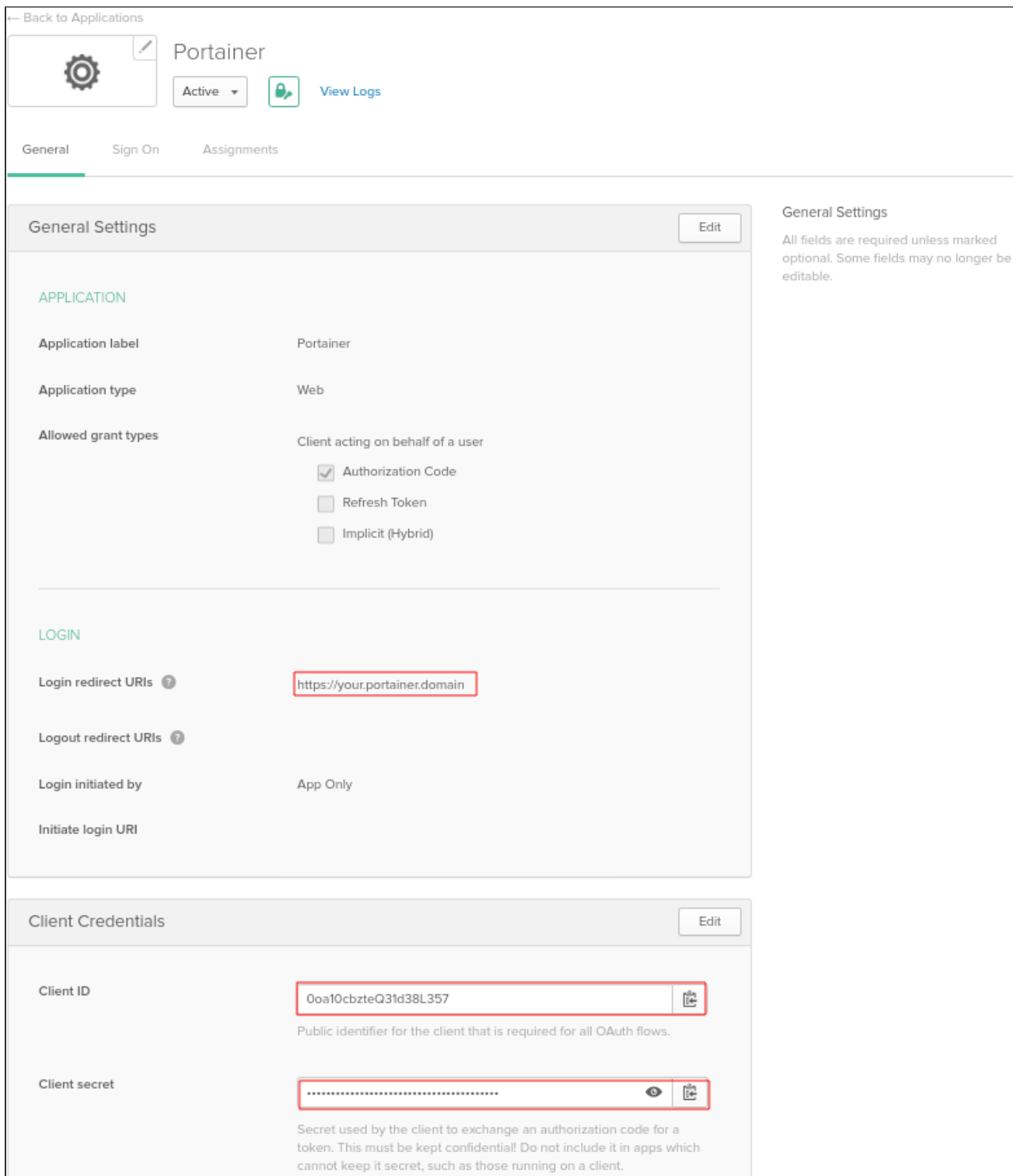
+ Add URI

Logout redirect URIs: + Add URI

Save Cancel

Certain apps may require additional configuration by Okta support. If you need help with this integration, contact Okta support at support@okta.com

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



← Back to Applications

Portainer

Active View Logs

General Sign On Assignments

### General Settings

Edit

All fields are required unless marked optional. Some fields may no longer be editable.

#### APPLICATION

Application label Portainer

Application type Web

Allowed grant types Client acting on behalf of a user

- ☒ Authorization Code
- ☐ Refresh Token
- ☐ Implicit (Hybrid)

#### LOGIN

Login redirect URIs ? https://your.portainer.domain

Logout redirect URIs ?

Login initiated by App Only

Initiate login URI

#### Client Credentials

Edit

Client ID 0aa10cbzteQ31d38L357

Public identifier for the client that is required for all OAuth flows.

Client secret .....

Secret used by the client to exchange an authorization code for a token. This must be kept confidential! Do not include it in apps which cannot keep it secret, such as those running on a client.

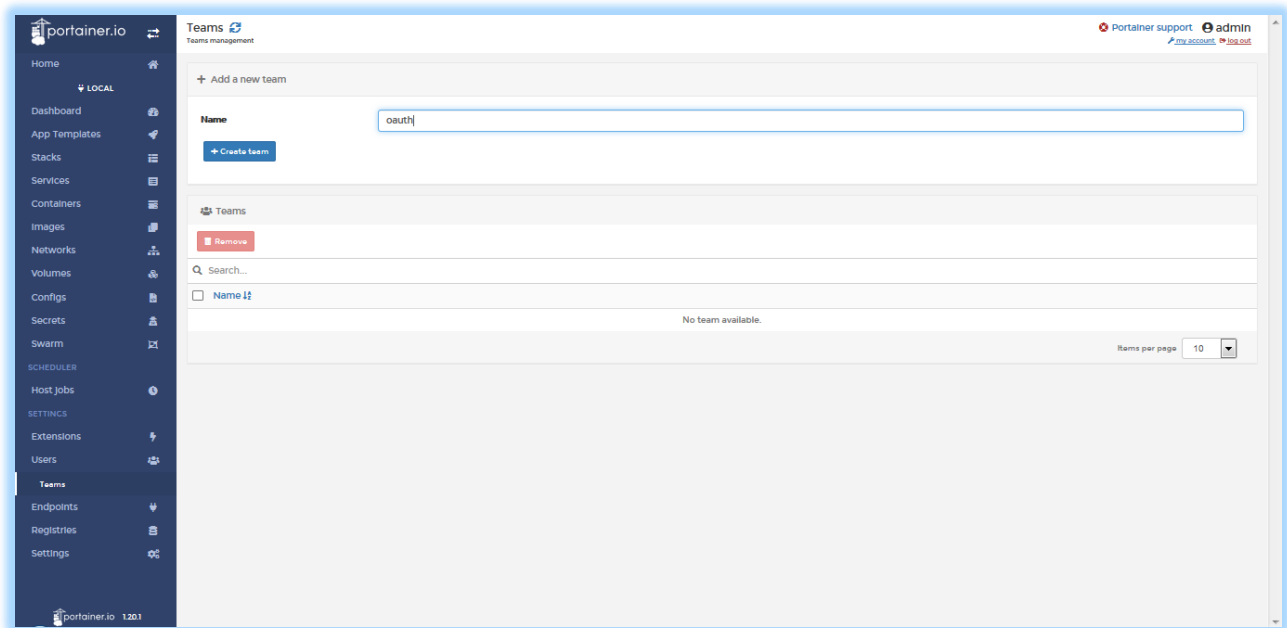
Now, we assume you already have users defined in your system, but if not, click on **Assignments** and assign users as required.

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

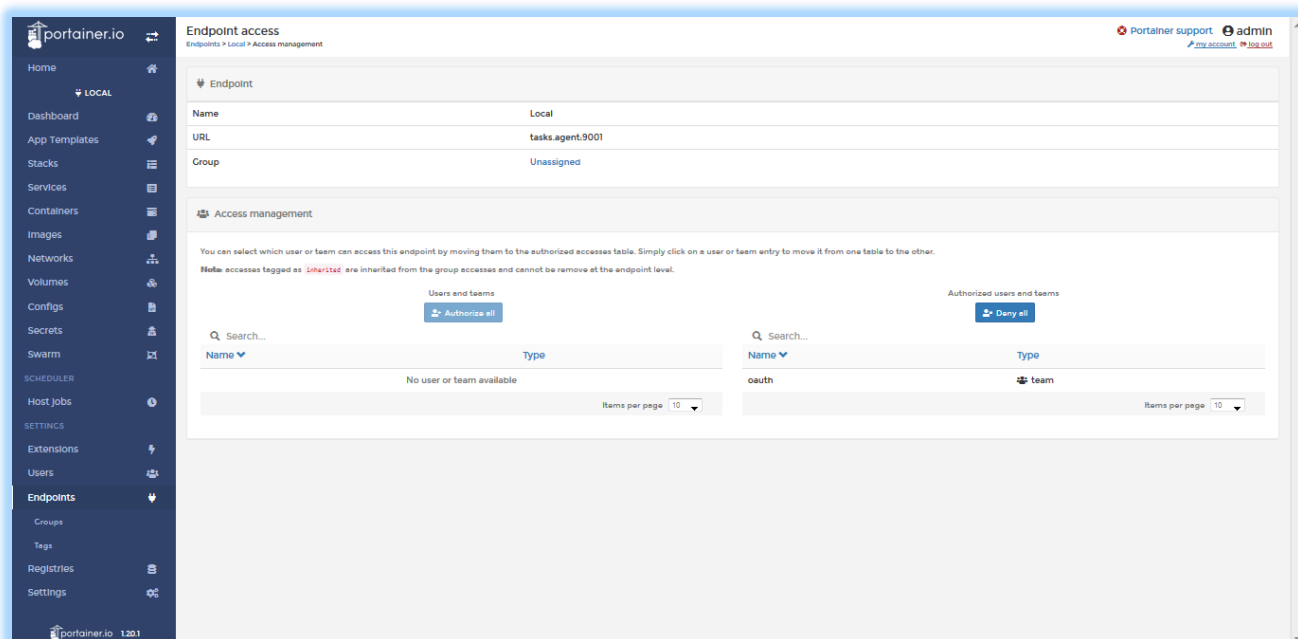
Purchase the **Portainer External Authentication** extension and apply the license key (process not shown here).

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 Authentication.

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](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](https://YOUR_OKTA_DOMAIN.okta.com/oauth2/v1/token)

In the **Resource URL** field, enter [https://YOUR OKTA DOMAIN.okta.com/oauth2/v1/userinfo](https://YOUR_OKTA_DOMAIN.okta.com/oauth2/v1/userinfo)

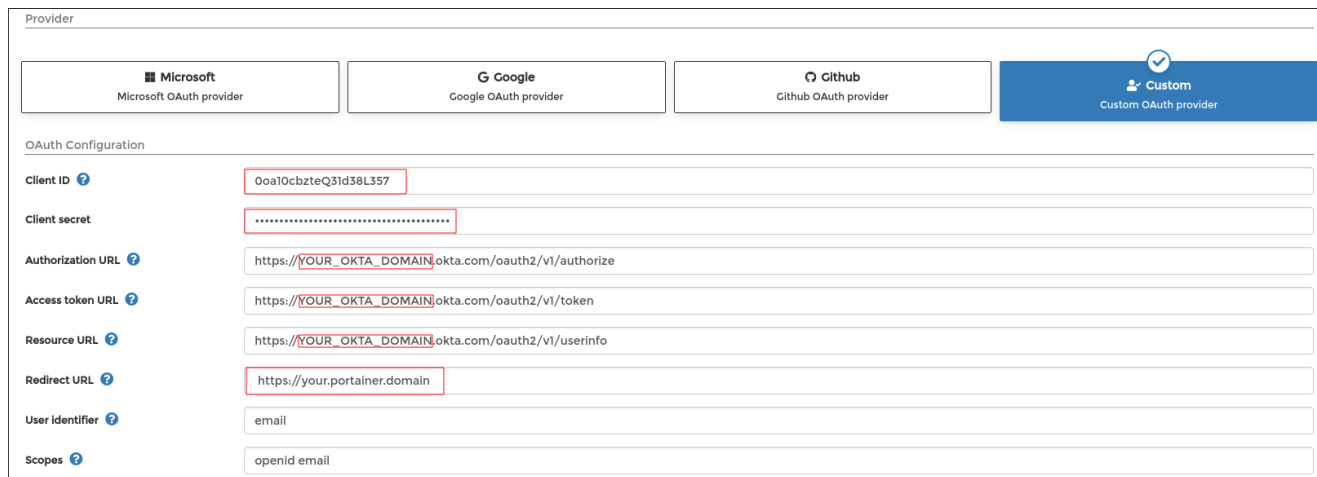
Make sure to replace **YOUR\_OKTA\_DOMAIN.okta.com** with your Okta subdomain (the one on which you created the Okta App).

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**



The screenshot shows the 'Provider' selection interface with four options: Microsoft, Google, Github, and Custom. The 'Custom' provider is selected. Below this is the 'OAuth Configuration' section with the following fields:

| Field             | Value   |
|-------------------|---|
| Client ID         | 00a10cbzteQ31d38L357                                  |
| Client secret     | *****   |
| Authorization URL | https://YOUR_OKTA_DOMAIN.okta.com/oauth2/v1/authorize |
| Access token URL  | https://YOUR_OKTA_DOMAIN.okta.com/oauth2/v1/token     |
| Resource URL      | https://YOUR_OKTA_DOMAIN.okta.com/oauth2/v1/userinfo  |
| Redirect URL      | https://your.portainer.domain                         |
| User identifier   | email   |
| Scopes            | openid email  |

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.