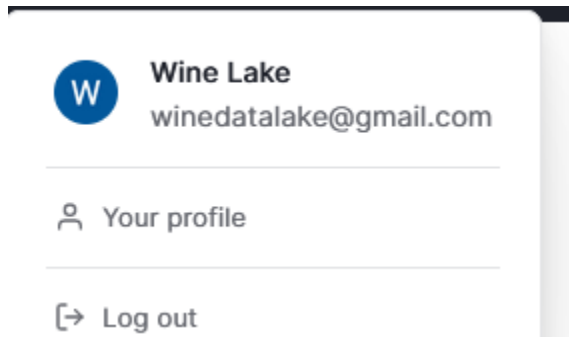
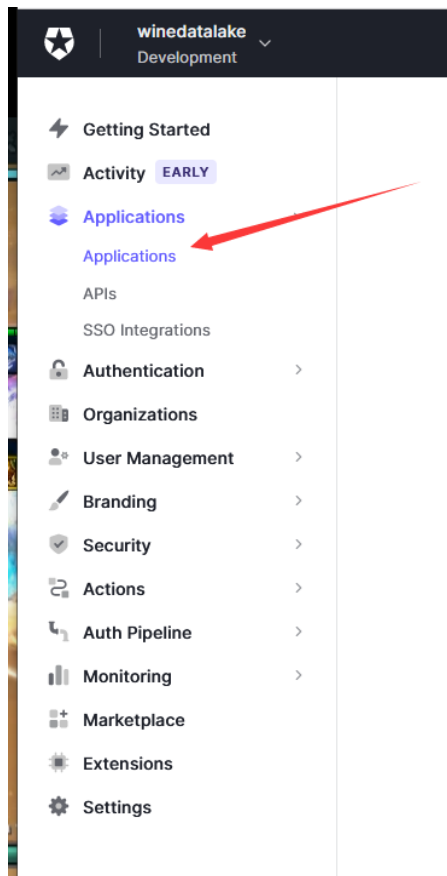






1.Login the auth0 with the email



2.Click on applications



3. Click on wine data lake

	Wine Data Lake Single Page Application	Client ID: <code>Nncz6b9skBCCAkyR4AFUyEdct3URx5Kd</code> 
	WineDataLakeAPI Machine to Machine	Client ID: <code>pfwNa8Hsg9VuJnKCcmsoLFLgAzxQbCna</code> 

4. After you deploy the webpage with google cloud, add your url to the following:

Application URIs

Application Login URI

In some scenarios, Auth0 will need to redirect to your application's login page. This URI needs to point to a route in your application that should redirect to your tenant's `/authorize` endpoint. [Learn more](#)

Allowed Callback URLs

After the user authenticates we will only call back to any of these URLs. You can specify multiple valid URLs by comma-separating them (typically to handle different environments like QA or testing). Make sure to specify the protocol (`https://`) otherwise the callback may fail in some cases. With the exception of custom URI schemes for native clients, all callbacks should use protocol `https://`. You can use [Organization URL](#) parameters in these URLs.

Allowed Logout URLs

A set of URLs that are valid to redirect to after logout from Auth0. After a user logs out from Auth0 you can redirect them with the `returnTo` query parameter. The URL that you use in `returnTo` must be listed here. You can specify multiple valid URLs by comma-separating them. You can use the star symbol as a wildcard for subdomains (`*.google.com`). Query strings and hash information are not taken into account when validating these URLs. Read more about this at <https://auth0.com/docs/authenticate/login/logout>

Allowed Web Origins

Comma-separated list of allowed origins for use with [Cross-Origin Authentication](#), [Device Flow](#), and [web message response mode](#), in the form of `<scheme> "://" <host> [":" <port>]`, such as `https://login.mydomain.com` or `http://localhost:3000`. You can use wildcards at the subdomain level (e.g.: `https://*.contoso.com`). Query strings and hash information are not taken into account when validating these URLs.

Allowed Origins (CORS)

5. You will see the login/sign up function enable on your webpage:

