# Auth0 Integration

## ****Overview:****

This is an overview of the high-level flow for authenticating Incorta users using **Auth0** as an authentication / Identity provider.

There are two main flows which are discussed below in detail:

* A user with a valid JWT token.
* A user with no or invalid JWT token.

### ****A user with a valid JWT token:****

1. Incorta intercepts the request and checks for a specific cookie that contains the JWT token.
2. The token is decoded and validated based on the below criteria:
   1. Its the issuer, Incorta will be configured to be aware of **Auth0** as a valid issuer, maybe we could add a special signature to add extra security.
   2. It's an expiry date, in case the token is expired the user will be redirected to **Auth0**to be re-authenticated.
   3. The presence of a pre-configured claim i.e. a user id, user email.
3. If all the required criteria are present the user is granted access to Incorta.

### ****A user with no or invalid JWT token:****

In this case, Incorta intercepted the request coming to Incorta and couldn't find a cookie containing the JWT token or the JWT token was invalid.

1. The user is redirected to **Auth0**in order to be authenticated and grant Incorta as application access to a subset of the user's personal information.
2. **Auth0** redirects the user back to an intermediate URL with specific values (code and state) the will be used in a later request by Incorta to **Auth0** to get a new JWT token.
3. The new JWT token is stored in a cookie to be used for later requests to Incorta.