# Configuring Incorta to integrate with Auth0 as an SSO provider

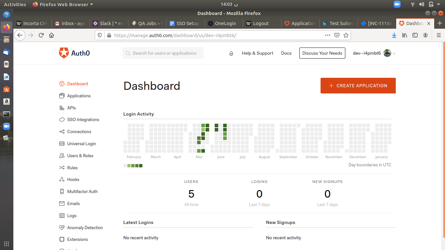
* [Define Incorta as a new application in Auth0](#ConfiguringIncortatointegratewithAuth0a)
* [Enabling SSO Authentication in Incorta](#ConfiguringIncortatointegratewithAuth0a)

## Define Incorta as a new application in Auth0

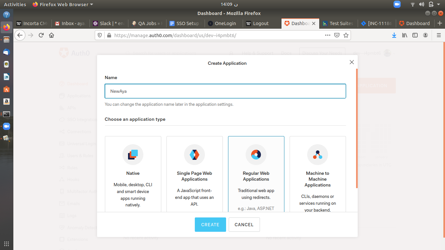
Auth0 dashboard layout may be different from the time this document is written.

1- Create a new Auth0 developer’s account from [here](https://auth0.com/)

2- When you logon to Auth0 from your dashboard, click on “Create Application. “



 3- Choose “Regular Application“ and click “Create. “



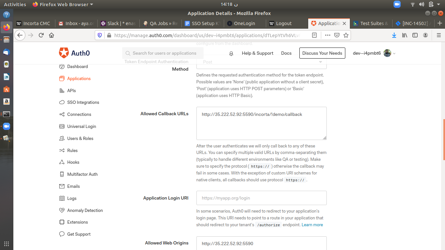
4-Go to the “Settings“ tab ( We will use “Domain,” “client,” and “ClientSecret”)

5- in the “Allowed Callback URLs“ section add “[http://<hostname>:<port>/incorta/!<tenant\_name>/callback](http://localhost:8080/incorta/!demo/callback)“ (Example: http://localhost:8080/incorta/!demo/callback)

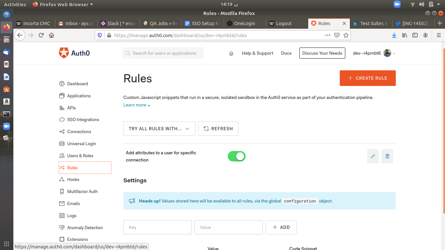
6- In the “Allowed Web Origins” section add “http://<hostname>:<port>“ (Example: <http://localhost:8080>)

7- In the “Allowed Logout URLs” section add “http://<hostname>:<port>/incorta/!<tenant\_name>“ (Example: <http://localhost:8080/incorta/!demo>)

8- Save your changes

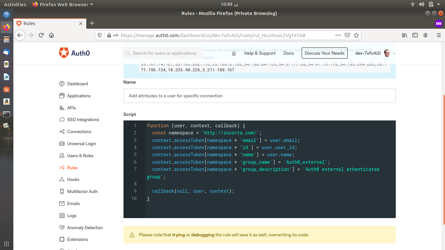


9- Click on the “Rules“ menu item in the left menu and choose “Create Rule. “



10- Choose from the “Enrich profile” section “add attributes to a user for a specific connection.”

11- Add the below code, then save changes



function (user, context, callback) {

const namespace = 'http://incorta.com/';

context.accessToken[namespace + 'email'] = user.email;

context.accessToken[namespace + 'id'] = user.user\_id;

context.accessToken[namespace + 'name'] = user.name;

// The below code is not required

context.accessToken[namespace + 'group\_name'] = 'Auth0\_external';

context.accessToken[namespace + 'group\_description'] = 'Auth0 external authorized group';

callback(null, user, context);

}

12- Click on the “APIs” menu item from the left menu and choose “Create API. “

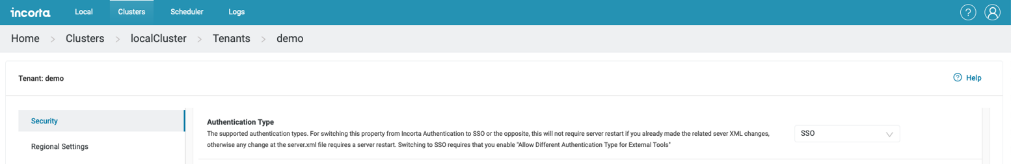
13- Give it a friendly name in the “Name“ section (Example: Incorta)

14- In the “identifier“ add “http://<hostname>:8080/incorta/!<tenant\_name>“ (Example: <http://localhost:8080/incorta/!demo)>

15- Click on “Create. “

## Enabling SSO Authentication in Incorta

1- From the tenant configurations in CMC, set the authentication type to SSO



   2- Update “server.xml” of your Incorta analytics service instance with the below Valve tag.

the Valve tag should be added directly under the Host tag

<Valve className="com.incorta.sso.valves.auth0.Auth0Valve"

             appDomain="dev-7ofu4i2i.auth0.com"

             clientId="zsnQb4dBSI738yN6oLFy438yFsbzAK7C"

             clientSecret="QRPgXKmHT\_3ZBK\_POGurUa-ANWKxjPesG53ebZxCkYeFu9fIjPWJbOBvz0QslVYr"

             callbackURL="http://localhost:8080/incorta/!demo/callback"

             embdeddedURL="http://localhost:8080/incorta/!demo/embedded"

             claimName="http://incorta.com/email"

             audience="http://localhost:8080/incorta/!demo/"

             LoggingEnabled="true"

       />

3- Go to “IncortaNode/runtime/lib”

 4- Remove “incorta.onelogin.valv-1.0.jar.”

 5- Restart the analytics service and log in using Incorta’s URL followed by “!<tenant\_name>“ (Example: http://localhost:8080/incorta/!demo/)

6- You will be directed to Auth0 to authenticate, and then you will be redirected to Incorta’s home page