# Okta & OneLogin & Auth0 Setup Instructions

How to configure Okta and Onelogin and Auth0 from the CMC UI

* [Okta Provider](#Okta&OneLogin&Auth0SetupInstructions-Ok)
* [OneLogin (SAML2) Provider](#Okta&OneLogin&Auth0SetupInstructions-On)
* [Auth0 provider](#Okta&OneLogin&Auth0SetupInstructions-Au)

## ****Okta Provider****

**1- Configure Okta App, then download the metadata**

Configure the OKTA APP by following the instructions [here](https://incorta.atlassian.net/wiki/wiki/spaces/INC/pages/1975812174/Configure+Okta+SSO+on+your+local+development+environment), from the step 1 to 25.  
NOTE: Instructions starting step 26 are for old releases only and not supported in current releases.

**2- Prepare the metadata XML**

Update the XML, add the following tags between the md:EntityDescriptor

<configuration>

<default>{entityID}</default>

<applications>

<application>

<md:EntityDescriptor>

.............

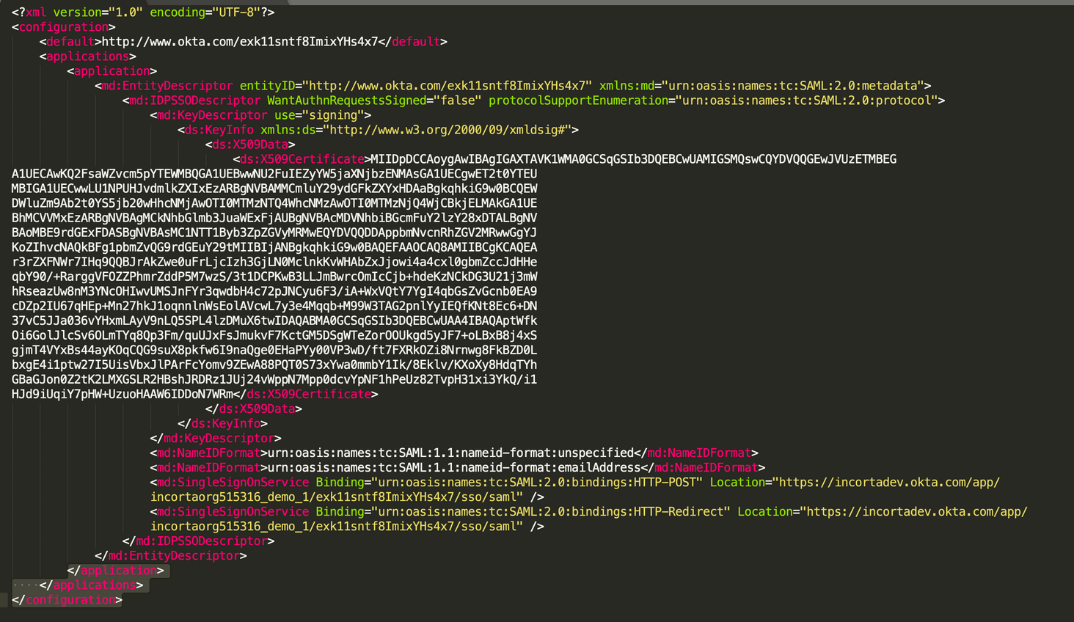
</md:EntityDescriptor>

</application>

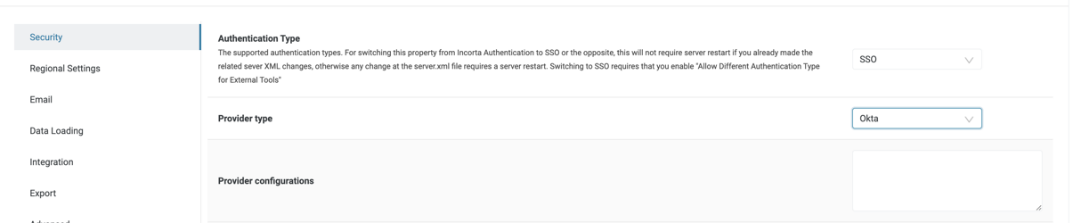
</applications>

</configuration>

make sure that you copy the entityId url in the <md:EntityDescriptor> and replace it with {entityID} in the <default> tag  
Copy the XML and paste it into an online XML formatter. You can use this one for example: <https://www.freeformatter.com/xml-formatter.html>   
  
So eventually your XML should look something like this:

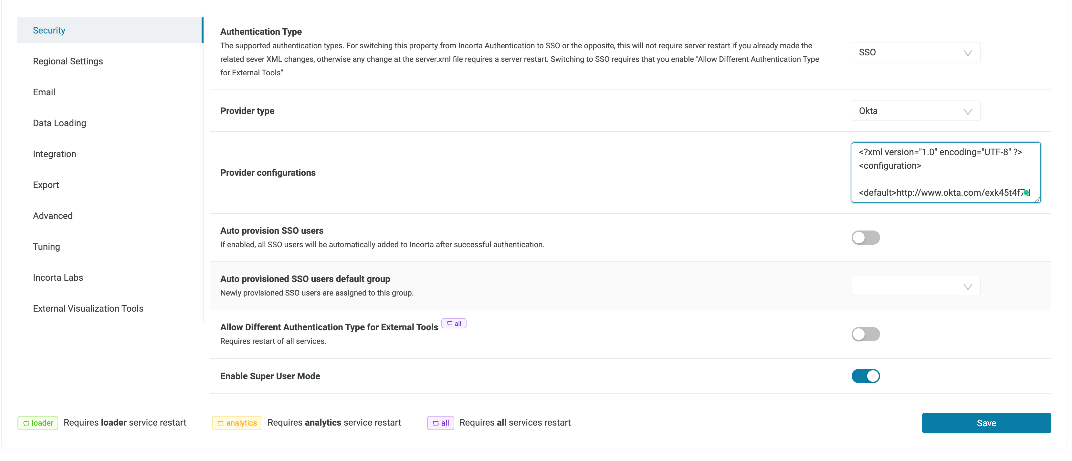


**3- Enable the SSO, then Select the Okta provider from the dropdown list at security tab in the tenant configurations in CMC**



**4-Restart Analytics and Loader services**   
Navigate to CMC → Clusters → localCluster → Nodes  
NOTE: Must restart Analytics and Loader services after changing Authentication Type.

**5- Copy the XML you edited in step 2 and paste it in the** Provider configurations **section, then click the Save button**

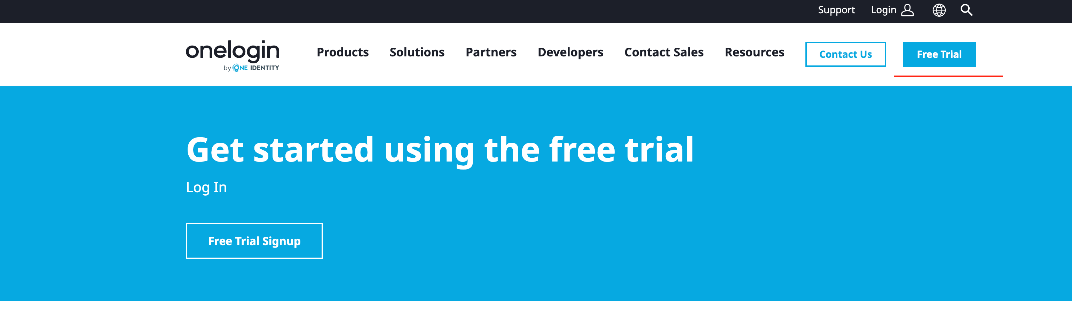


**6-Auto provision:**   
**When on,** SSO user assigned in step 23 [here](https://incorta.atlassian.net/wiki/wiki/spaces/INC/pages/1975812174/Configure+Okta+SSO+on+your+local+development+environment) can login without being assigned in Incorta.  
**NOTE:** If Auto provision is on, and a user is created in Incorta with the same email as the SSO user’s email, the SSO user will not be able to sign in and an error will occur when trying to sign in.  
**When off,** SSO user assigned in step 23 [here](https://incorta.atlassian.net/wiki/wiki/spaces/INC/pages/1975812174/Configure+Okta+SSO+on+your+local+development+environment) can login after creating an SSO user in Incorta by Navigating to Incorta Analytics → Security tab → create a user with same email assigned in step 23 [here](https://incorta.atlassian.net/wiki/wiki/spaces/INC/pages/1975812174/Configure+Okta+SSO+on+your+local+development+environment).  
  
**7- Now, you can log in to Incorta using Incorta’s URL followed by “!<tenant\_name>“ (Example:** [**http://localhost:8080/incorta/!demo/**](http://localhost:8080/incorta/!demo/)**)**

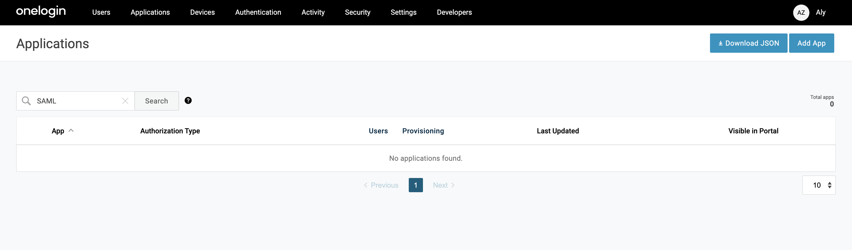
## ****OneLogin (SAML2) Provider****

**1- Configure the Onelogin app, then download the metadata**

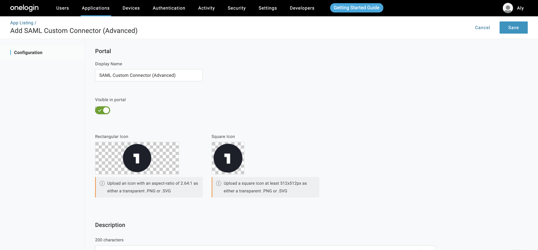
* Navigate to [Onelogin.com](https://www.onelogin.com/) and select “Free Trial”



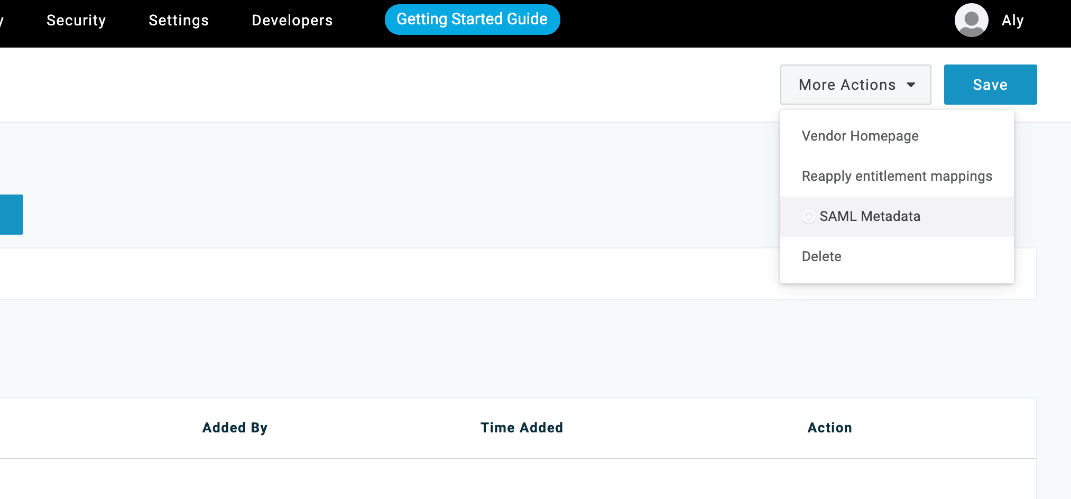
* Fill in your information to start the free trial, and you will receive an email with a link to activate your account.
* Navigate to Applications tab → Add App → search for SAML



* Select “SAML Custom Connector (Advanced)”
* Then select save in this window:



* Navigate to Configuration → ACS (Consumer) URL Validator\* -> and write your <environment link>/!<Tenant\_Link>  
  example: [**https://jan22.cloudstaging.incortalabs.com/incorta/!saml/**](https://jan22.cloudstaging.incortalabs.com/incorta/!saml/)  
  Navigate to Configuration -> ACS (Consumer) URL\* -> -> and write your <environment link>/!<Tenant\_Link>  
  example: [**https://jan22.cloudstaging.incortalabs.com/incorta/!saml/**](https://jan22.cloudstaging.incortalabs.com/incorta/!saml/)
* Navigate to Parameters → Select “Configured by admin”
* Select “+” → Write “loginName” in Field Name → enable “Include in SAML assertion” → Click Save → Write “Email” in Value → Click Save
* Navigate to Users → Make sure your user is added.  
  Note: If not added, search your email you used to sign up with in the search bar and add it
* Navigate to Privileges → search your name in the search bar and click on “check” to add it
* Now to download the Metadata, click on More Actions → SAML Metadata



**2- Map the metadata XML to the following properties file**

* Copy the following properties file into a notepad/editor .

onelogin.saml2.strict = false

onelogin.saml2.debug = true

onelogin.saml2.sp.entityid = https://app.onelogin.com/saml/metadata/d0e2e45f-b581-46da-adeb-98ae0184c16f

onelogin.saml2.sp.assertion\_consumer\_service.url = https://sso-ui-hz.clouddev3.incortalabs.com/incorta/!demo/

onelogin.saml2.sp.assertion\_consumer\_service.binding = urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST

onelogin.saml2.sp.single\_logout\_service.url = https://sso-ui-hz.clouddev3.incortalabs.com/incorta/!demo/#/logout.jsp

onelogin.saml2.sp.single\_logout\_service.binding = urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect

onelogin.saml2.sp.nameidformat = urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified

onelogin.saml2.sp.x509cert =

onelogin.saml2.sp.privatekey =

onelogin.saml2.idp.entityid = https://app.onelogin.com/saml/metadata/d0e2e45f-b581-46da-adeb-98ae0184c16f

onelogin.saml2.idp.single\_sign\_on\_service.url = https://hz-incorta.onelogin.com/trust/saml2/http-redirect/sso/d0e2e45f-b581-46da-adeb-98ae0184c16f

onelogin.saml2.idp.single\_sign\_on\_service.binding = urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect

onelogin.saml2.idp.single\_logout\_service.url = https://hz-incorta.onelogin.com/trust/saml2/http-redirect/slo/1471495

onelogin.saml2.idp.single\_logout\_service.response.url =

onelogin.saml2.idp.single\_logout\_service.binding = urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect

onelogin.saml2.idp.x509cert=

onelogin.saml2.security.nameid\_encrypted = false

onelogin.saml2.security.authnrequest\_signed = false

onelogin.saml2.security.logoutrequest\_signed = false

onelogin.saml2.security.logoutresponse\_signed = false

onelogin.saml2.security.want\_messages\_signed =

onelogin.saml2.security.want\_assertions\_signed = false

onelogin.saml2.security.sign\_metadata =

onelogin.saml2.security.want\_assertions\_encrypted = false

onelogin.saml2.security.want\_nameid\_encrypted = false

onelogin.saml2.security.requested\_authncontext = urn:oasis:names:tc:SAML:2.0:ac:classes:urn:oasis:names:tc:SAML:2.0:ac:classes:Password

onelogin.saml2.security.onelogin.saml2.security.requested\_authncontextcomparison = exact

onelogin.saml2.security.want\_xml\_validation = true

onelogin.saml2.security.signature\_algorithm = http://www.w3.org/2000/09/xmldsig#rsa-sha1

onelogin.saml2.organization.name = SP Java

onelogin.saml2.organization.displayname = SP Java Example

onelogin.saml2.organization.url = http://sp.example.com

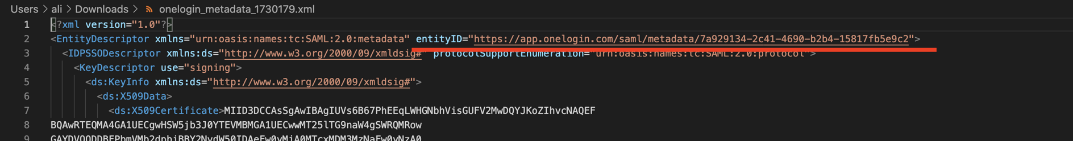
onelogin.saml2.contacts.technical.given\_name = Technical Guy

onelogin.saml2.contacts.technical.email\_address = technical@example.com

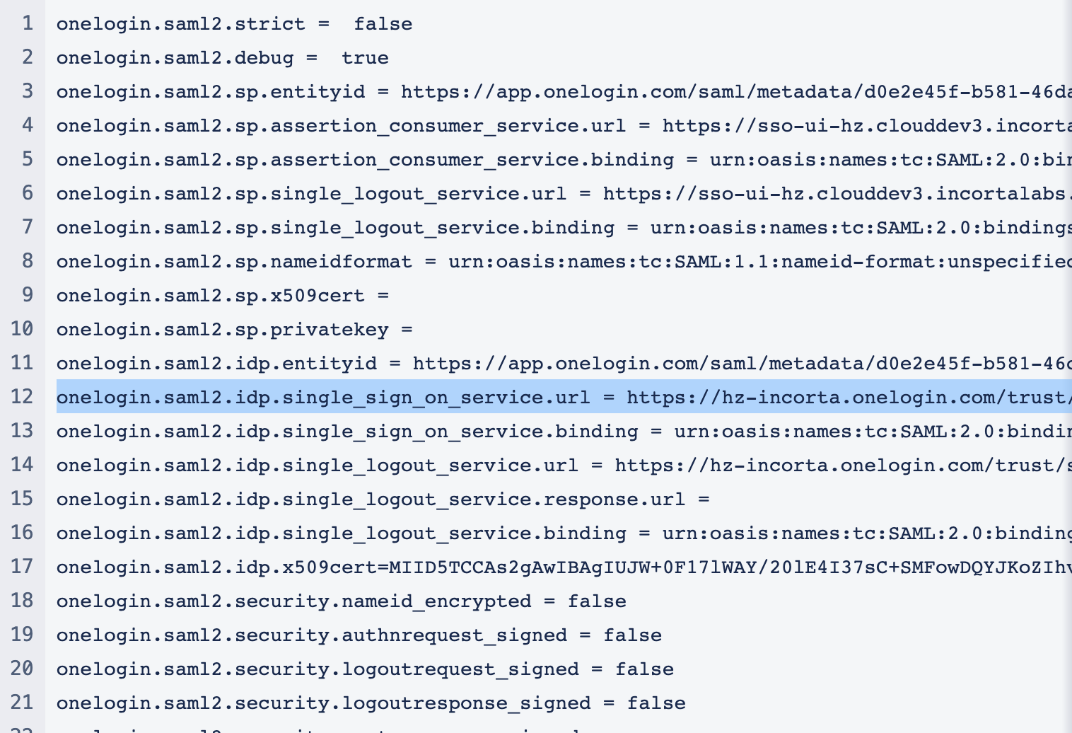
onelogin.saml2.contacts.support.given\_name = Support Guy

onelogin.saml2.contacts.support.email\_address = support@@example.com

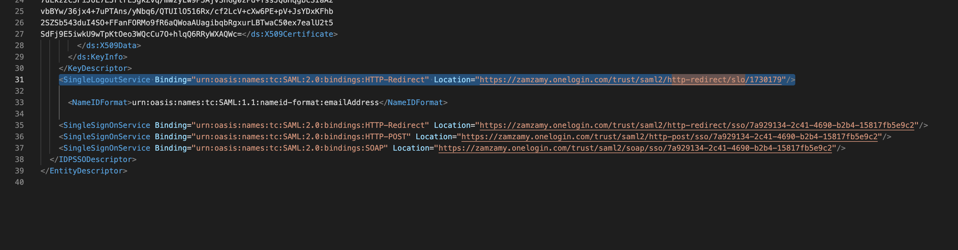
* Copy the entity Id link from metadata and replace it with the links in line 3 and line 11 of the properties file (replace the link only not the whole line).



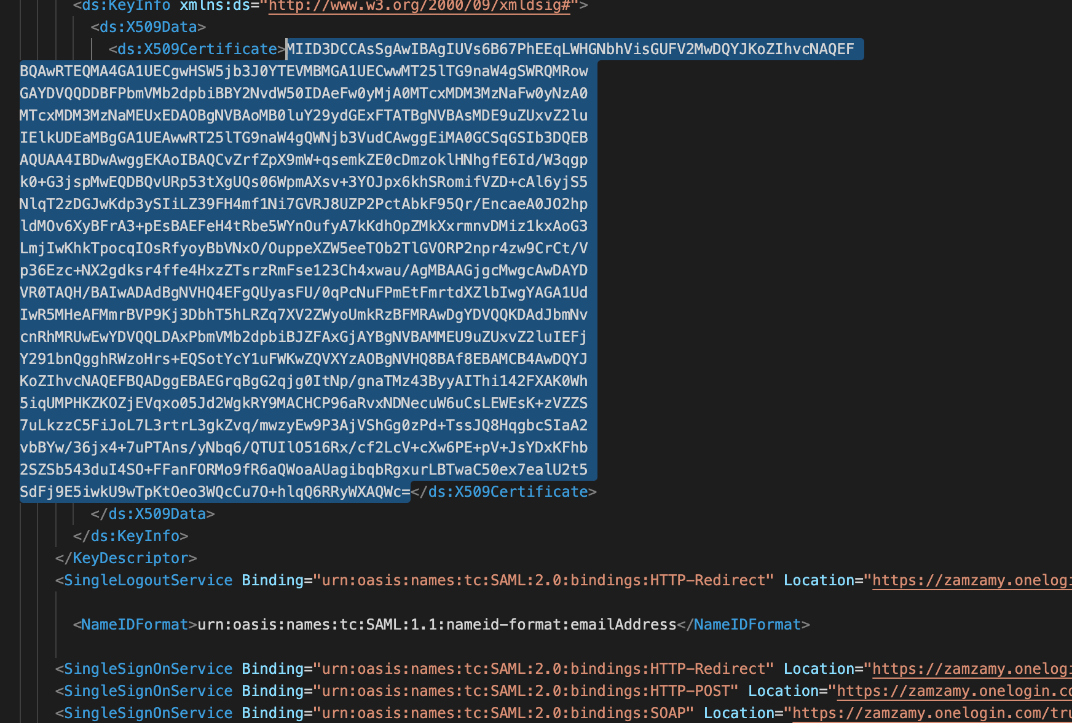
* Write your environment link followed by /!<Tenant\_Name>/ in onelogin.saml2.sp.assertion\_consumer\_service.url in line 4 instead of the current link.  
  example: <https://jan22.cloudstaging.incortalabs.com/incorta/!saml/>
* In line 6, replace the logout link with your environment link: replace this part:  
  https://sso-ui-hz.clouddev3.incortalabs.com/incorta/!demo/  
  with your link and don’t forget to replace “demo” in the link with your tenant name
* Copy the sso http redirect link from the metadata file and paste it line 12 of the properties file (replace the link only not the whole line)



* Copy the slo http redirect link from the metadata file and paste it in line 14 of the properties file   
  (replace the link only not the whole line).

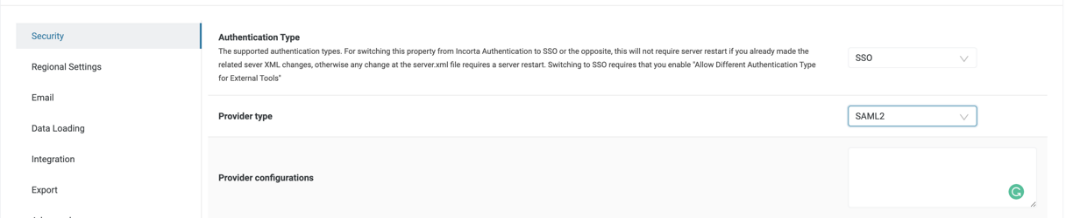


* Copy the certificate from the metadata



Remove all spaces in the certificate using this online editor: [Remove All Whitespace](https://www.browserling.com/tools/remove-all-whitespace) , and paste the edited certificate in line 17 of the properties file. (replace the link only not the whole line).

**3- Enable the SSO, then Select the SAML2 provider from the dropdown list at security tab at CMC**



**4- Set the Onelogin configurations at the** Provider configurations **section by pasting the properties file we edited in step 2, then click the Save button**

**5-Restart Analytics and Loader services**   
Navigate to CMC → Clusters → localCluster → Nodes  
NOTE: Must restart Analytics and Loader services after changing Authentication Type.

**6-Auto provision:**   
**When on,** SSO user assigned in step 23 here can login without being assigned in Incorta.  
**NOTE:** If Auto provision is on, and a user is created in Incorta with the same email as the SSO user’s email, the SSO user will not be able to sign in and an error will occur when trying to sign in.  
**When off,** SSO user assigned in step 23 here can login after creating an SSO user in Incorta by Navigating to Incorta Analytics → Security tab → create a user with same email assigned in step 23 here.

**7- Now, you can log in to Incorta using Incorta’s URL followed by “!<tenant\_name>“ (Example:** [**http://localhost:8080/incorta/!demo/**](http://localhost:8080/incorta/!demo/)**)**

## ****Auth0 provider****

**1- Configure Auth0 App, then prepare the configurations**

you can find the instructions [here](https://incorta.atlassian.net/wiki/spaces/INC/pages/2197127199/Configuring+Incorta+to+integrate+with+Auth0+as+an+SSO+provider#Define-Incorta-as-a-new-application-in-Auth0), Define Incorta as a new application in Auth0 section

**2- Map the App configurations to the following properties**

appDomain=hz-dev-incorta.us.auth0.com

clientId=y9c52Wfp94WL2wjbV4i09oGTk9MjMOTL

clientSecret=r0qOHR73Xp5kSq3L2aXvI\_E5ESEboJLsgheSwz6kk8mQ44yXLAnsYKNsH6qDpmIB

callbackURL=https://sso-ui-hz.clouddev3.incortalabs.com/incorta/!demo/callback

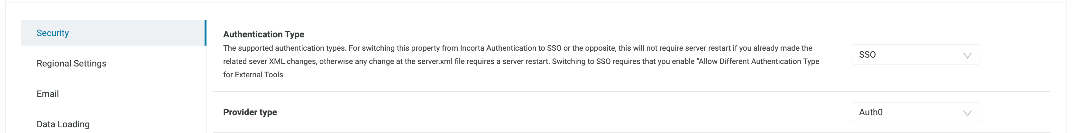
embdeddedURL=https://sso-ui-hz.clouddev3.incortalabs.com/incorta/!demo/embedded

claimName=http://incorta.com/email

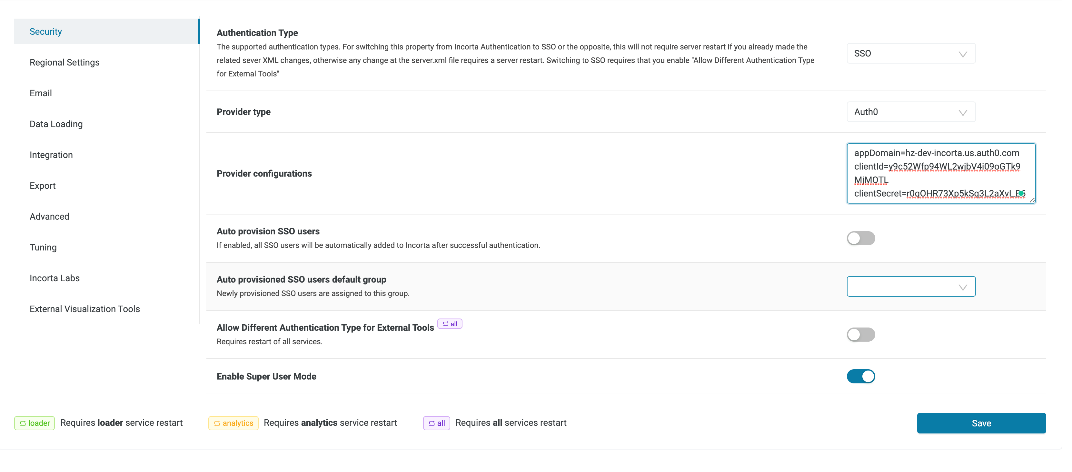
audience=https://sso-ui-hz.clouddev3.incortalabs.com/incorta/!demo

logoutReturnToURL=https://sso-ui-hz.clouddev3.incortalabs.com/incorta/!demo

**3- Enable the SSO, then Select the Auth0 provider from the dropdown list at security tap at CMC**



**4- Set the properties at the** Provider configurations **section, then click the Save button**



**5- Now, you can log in to Incorta using Incorta’s URL followed by “!<tenant\_name>“ (Example:** [**http://localhost:8080/incorta/!demo/**](http://localhost:8080/incorta/!demo/)**)**