# Integrating Azure Active Directory (AzureAD) as SAML2 SSO IdP

## Overview

This document will walk us through configuring Azure Active Directory as a SAML2 SSO identity provider (IdP) and enabling SSO settings in Incorta.

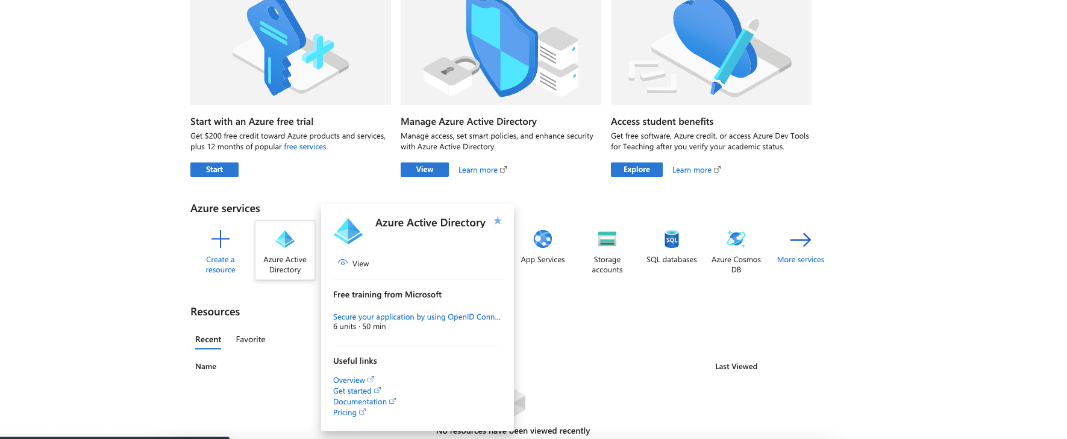
Incorta has “Azure AD“ as an authentication type. However, it is different in the login experience; If “Azure AD“ is selected as an authentication type, they user will always be prompt to enter their tenant/username/password credentials in Incorta’s login screen. But if we configure Azure AD as a SAML2 IdP the user will login directly to Incorta as long as they are logged in to their IdP.

For more information, please refer to the following ticket. [Azure AD Support](https://incorta.atlassian.net/browse/INC-34387)

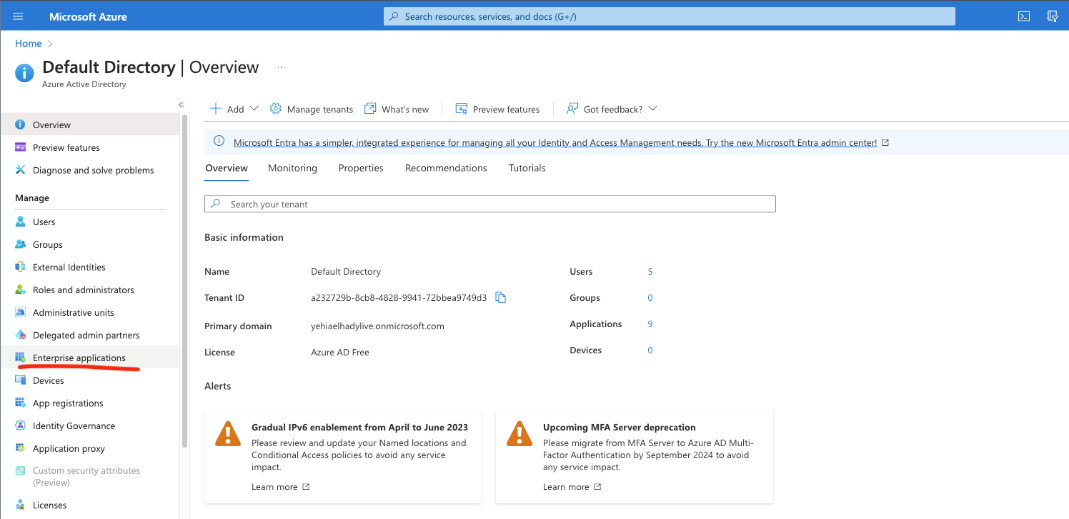
The screenshots in this document might change from the time this document is written.

### Azure AD Configurations

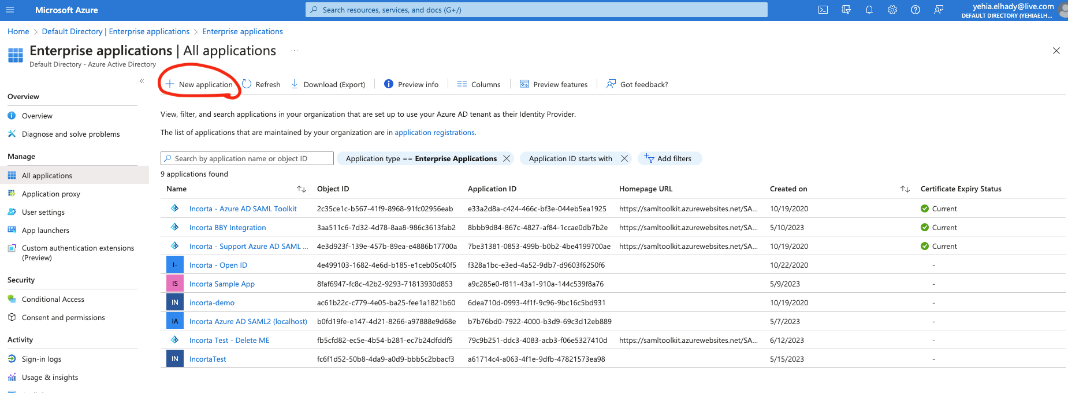
* log in to the Azure portal ([Home - Microsoft Azure](https://portal.azure.com/#home)) and make sure you have one of the following roles (Global Administrator, or Application Administrator) to access the Azure active directory and create and configure enterprise applications. You should be able to see something like the following screenshot(s)



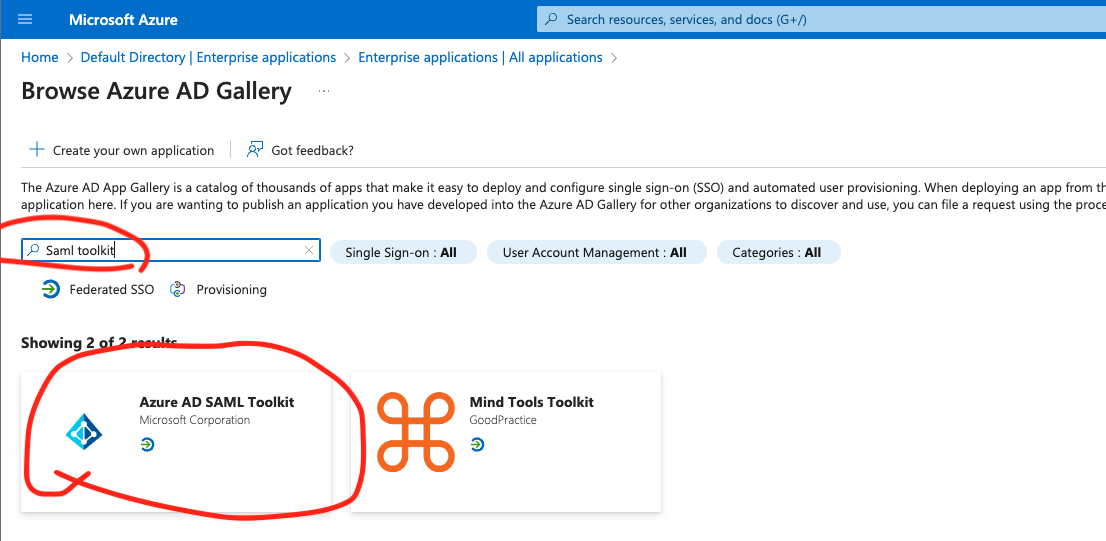
* click on “Azure Active Directory“ and from the right, select “Enterprise applications“



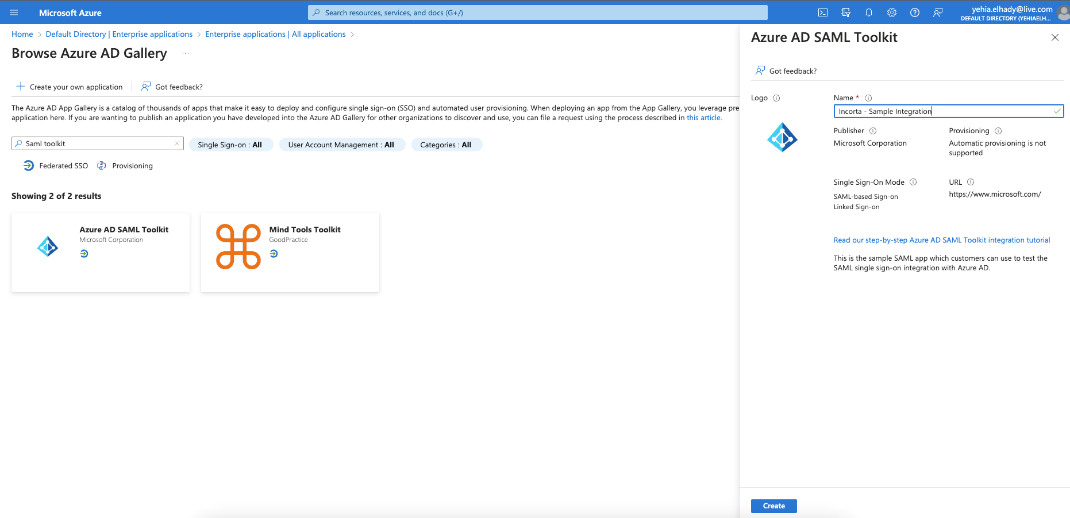
* From “Enterprise applications“ click on “New application“



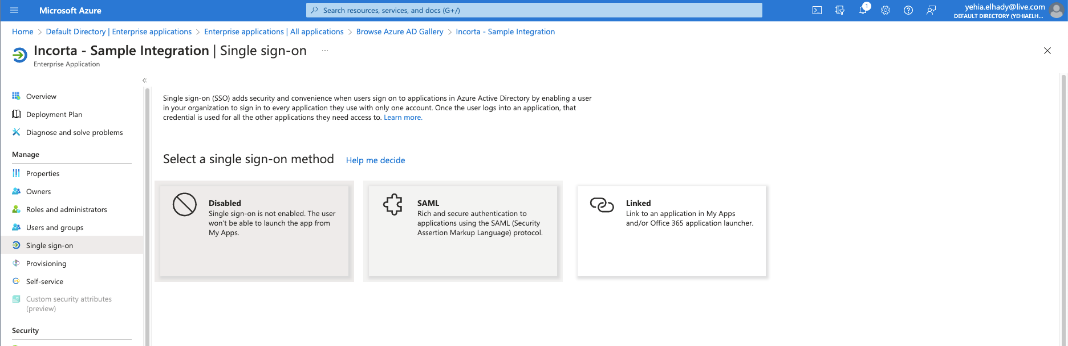
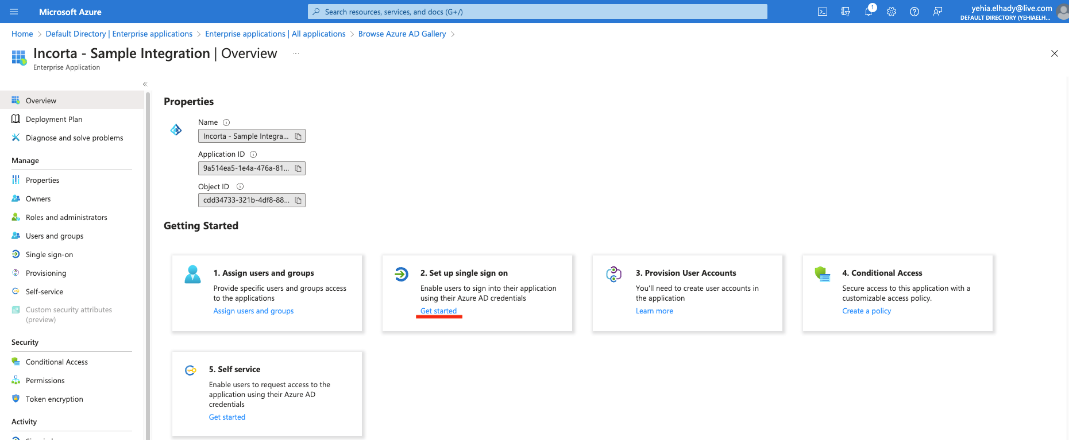
* in the Gallery, type “Saml toolkit“ and select “Azure AD SAML Toolkit“



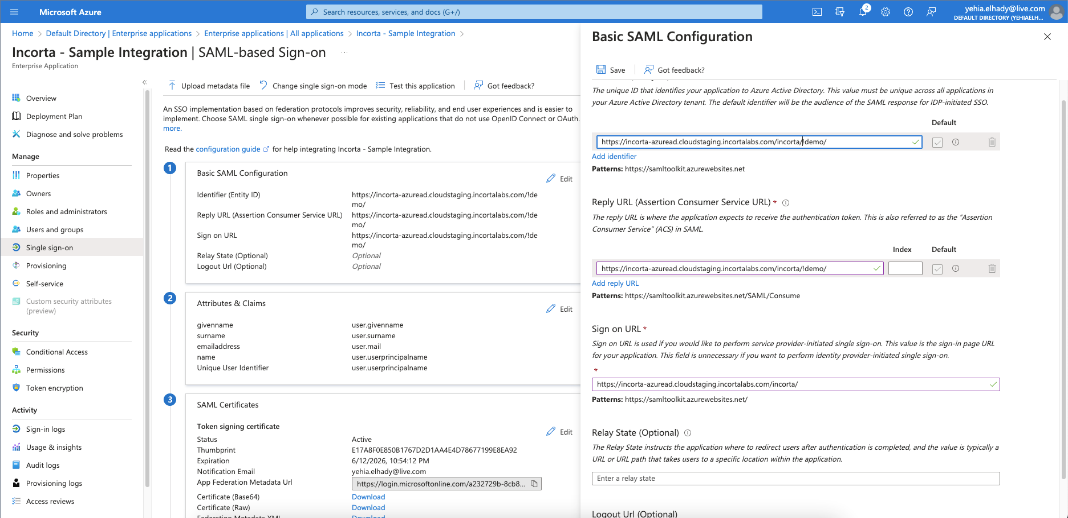
* Give a readable name for your application



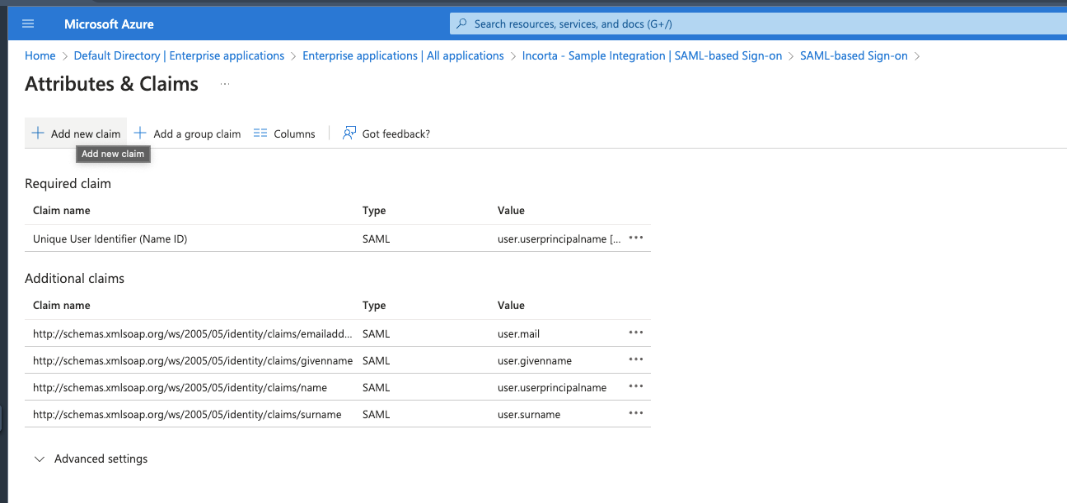
* The application should be created successfully and you should be able to see something like the following screenshot. Click on “get started“ link in “Setup Single sign on” and choose SAML

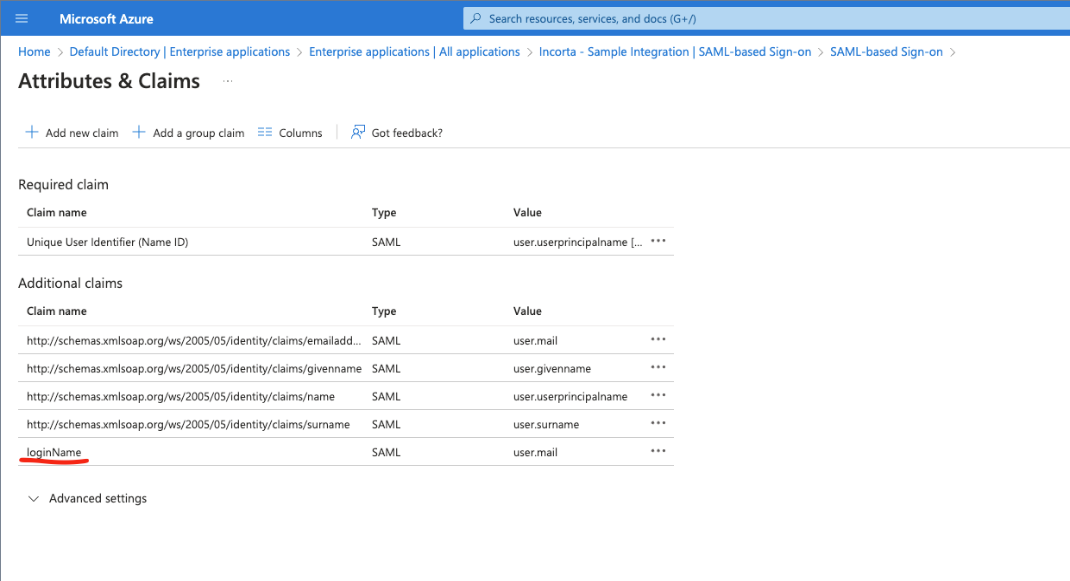
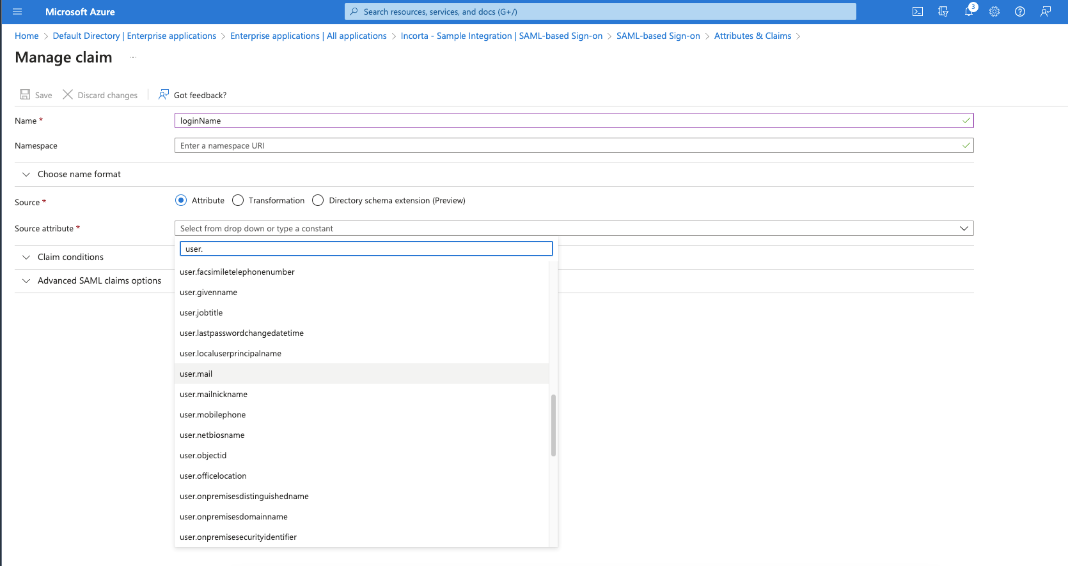


* Edit the “Basic SAML configuration” section by adding the proper URLs as indicated below. Replace the provided URLs with the actual Incorta ones, including the tenant name.

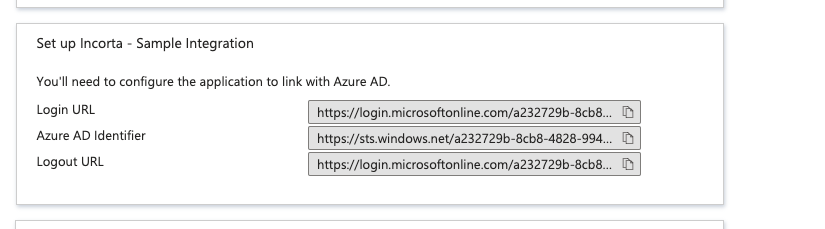


* Edit the “Attributes and claims” section to add a custom claim named “loginName“ like the following screenshots. Make sure that the “Source attribute“ matches the login name field for the Incorta user



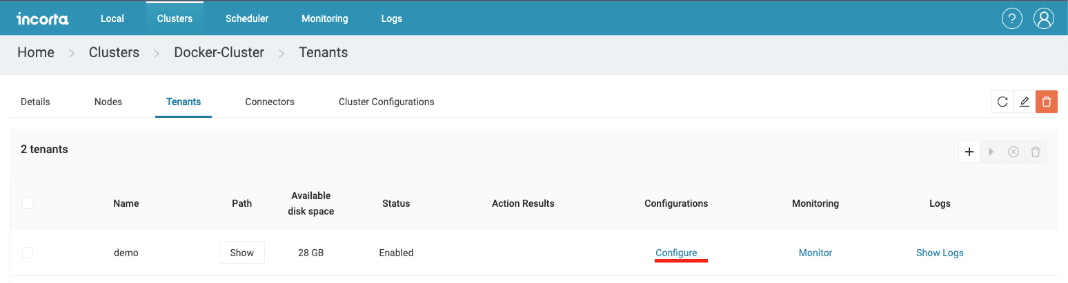


* Download the certificate (the Base64) on and save it, as we will need it when we apply the configuration on Incorta side. Any text editor can open the downloaded certificated and should look as follows:
  + cat Incorta\_Sample\_Integration\_base64.cer
  + -----BEGIN CERTIFICATE-----
  + Omiitteddd......
  + EylNaWNyb3NvZnQgQXp1cmUgRmVkZXJhdGVkIFNTTyBDZXJ0aWZpY2F0ZTAeFw0yMzA2MTIxOTU0
  + MTNaFw0yNjA2MTIxOTU0MTJaMDQxMjAwBgNVBAMTKU1pY3Jvc29mdCBBenVyZSBGZWRlcmF0ZWQg
  + U1NPIENlcnRpZmljYXRlMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAp31KAYgKnbyx
  + f4K2cweRbu4eQwnTW7ntut0SRtX9NHmqtY1gC/mRAPc1raus9s1FclyPyaTo2iBu6WB42fQrNjB5
  + ItVivEYOcS4tSVzuQ/WplrXcz8NkT2Zi87v+6WVm9e+R1wPSMDwIbPOoNuAKhUFTh6zEVvxwsIkk
  + .....Omitted...
  + -----END CERTIFICATE-----
* Copy the following URLs, as we are going to need them when configuring Incorta

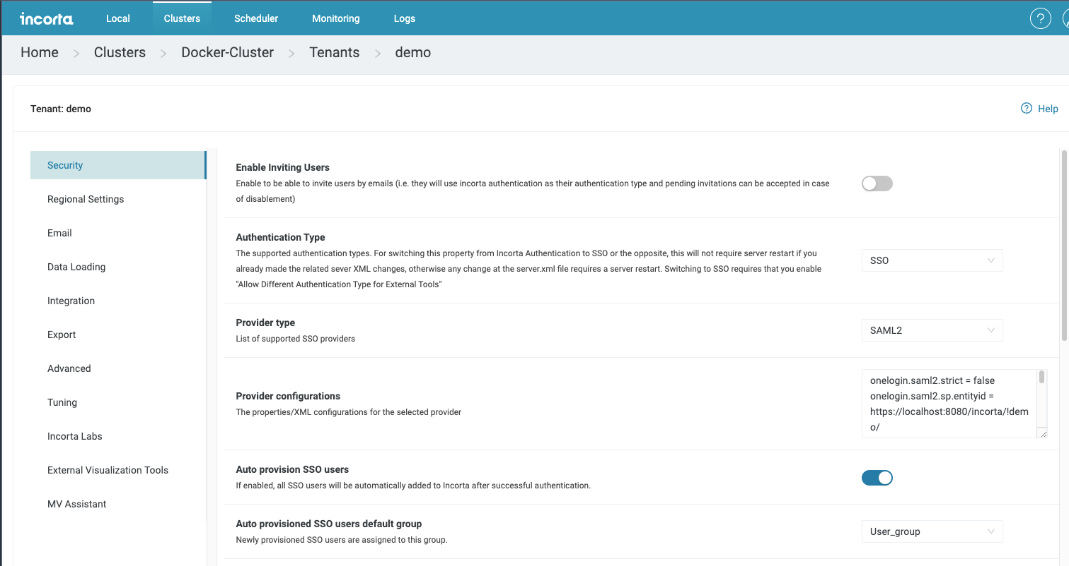


### Configuring Incorta

* You must prepare the following properties on a text editor
  + for the value of the onelogin.saml2.idp.x509cert copy the content of the downloaded certificate without the “BEGIN CERTIFICATE“ and “END CERTIFICATE“ lines. Also, make sure that the certificate text is on a single line
  + onelogin.saml2.strict = false
  + onelogin.saml2.sp.entityid = <the configured entity Id>
  + onelogin.saml2.sp.assertion\_consumer\_service.url = <the configured assertion consumer URL>
  + onelogin.saml2.sp.assertion\_consumer\_service.binding = urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect
  + onelogin.saml2.sp.single\_logout\_service.url = <incorta-url>/logout.jsp?redirectUrl=.
  + onelogin.saml2.sp.single\_logout\_service.binding = urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect
  + onelogin.saml2.idp.entityid = <Azure AD Identifier copied form the previous step>
  + onelogin.saml2.idp.single\_sign\_on\_service.url = <login URL copied form the previous step>
  + onelogin.saml2.security.want\_nameid = false
  + 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 = <logout URL copied from the previous step>
  + onelogin.saml2.idp.single\_logout\_service.binding = urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect
  + onelogin.saml2.idp.x509cert= <the value of the certificated downloaded>
  + The following is a sample configuration:
    - #### local configurations
    - onelogin.saml2.strict = false
    - onelogin.saml2.sp.entityid = https://localhost:8080/incorta/!demo/
    - onelogin.saml2.sp.assertion\_consumer\_service.url = http://localhost:8080/incorta/!demo/
    - onelogin.saml2.sp.assertion\_consumer\_service.binding = urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect
    - onelogin.saml2.sp.single\_logout\_service.url = http://localhost:8080/incorta//logout.jsp?redirectUrl=.
    - onelogin.saml2.sp.single\_logout\_service.binding = urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect
    - onelogin.saml2.idp.entityid = https://sts.windows.net/a232729b-8cb8-4828-9941-72bbea9749d3/
    - onelogin.saml2.idp.single\_sign\_on\_service.url = https://login.microsoftonline.com/a232729b-8cb8-4828-9941-72bbea9749d3/saml2
    - onelogin.saml2.security.want\_nameid = false
    - 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://login.microsoftonline.com/a232729b-8cb8-4828-9941-72bbea9749d3/saml2
    - onelogin.saml2.idp.single\_logout\_service.binding = urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect
    - onelogin.saml2.idp.x509cert= 
* Login to CMC and select the tenant’s configuration



* Make sure that the Authentication type is “SSO“ and the “Provider Type“ is “SAML2“. Paste the configurations from the previous step into “Provider configurations“



### Additional configurations (Optional)

* You can enable “Auto provision SSO users“ and select the “Auto provisioned SSO users group“ if you want users logging in from SSO to be automatically added to Incorta. If “Auto provision SSO users“ is disabled, you will need to manually create users in Incorta in order to let them sign in.