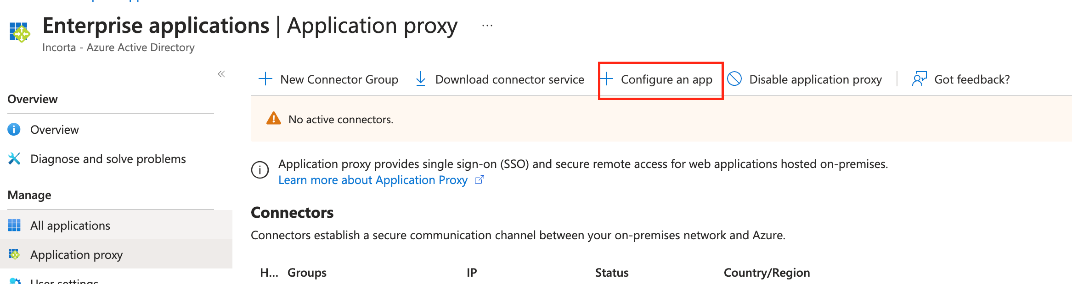
# Azure Active Directory SAML SSO with Application Proxy

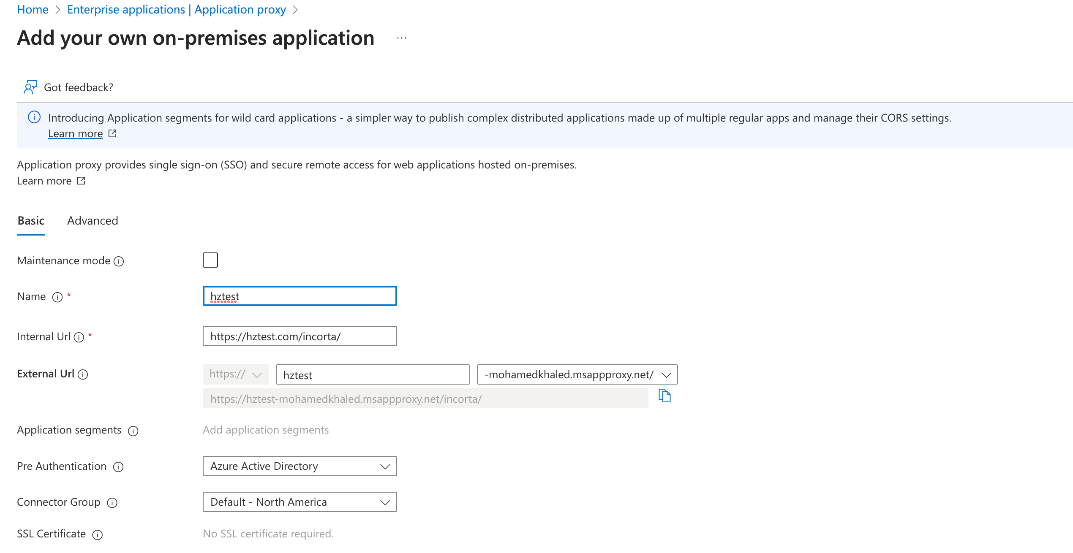
1- Go to [Enterprise applications](https://portal.azure.com/#blade/Microsoft_AAD_IAM/StartboardApplicationsMenuBlade) > Application proxy > Configure an app



2- Set your **App Name**, and set the **Internal URL** with the actual Incorta URL.

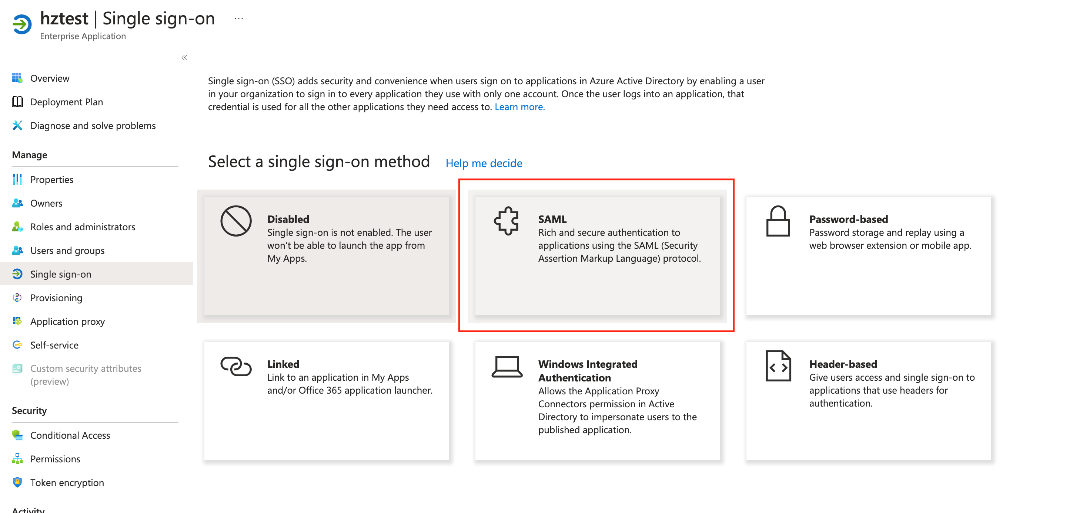
Set the Internal URL in this structure [https://hostName/incorta/](https://hostname/incorta/), without the tenant name

3- Select **Azure Active Directory** as the **Pre Authentication** method for your application.

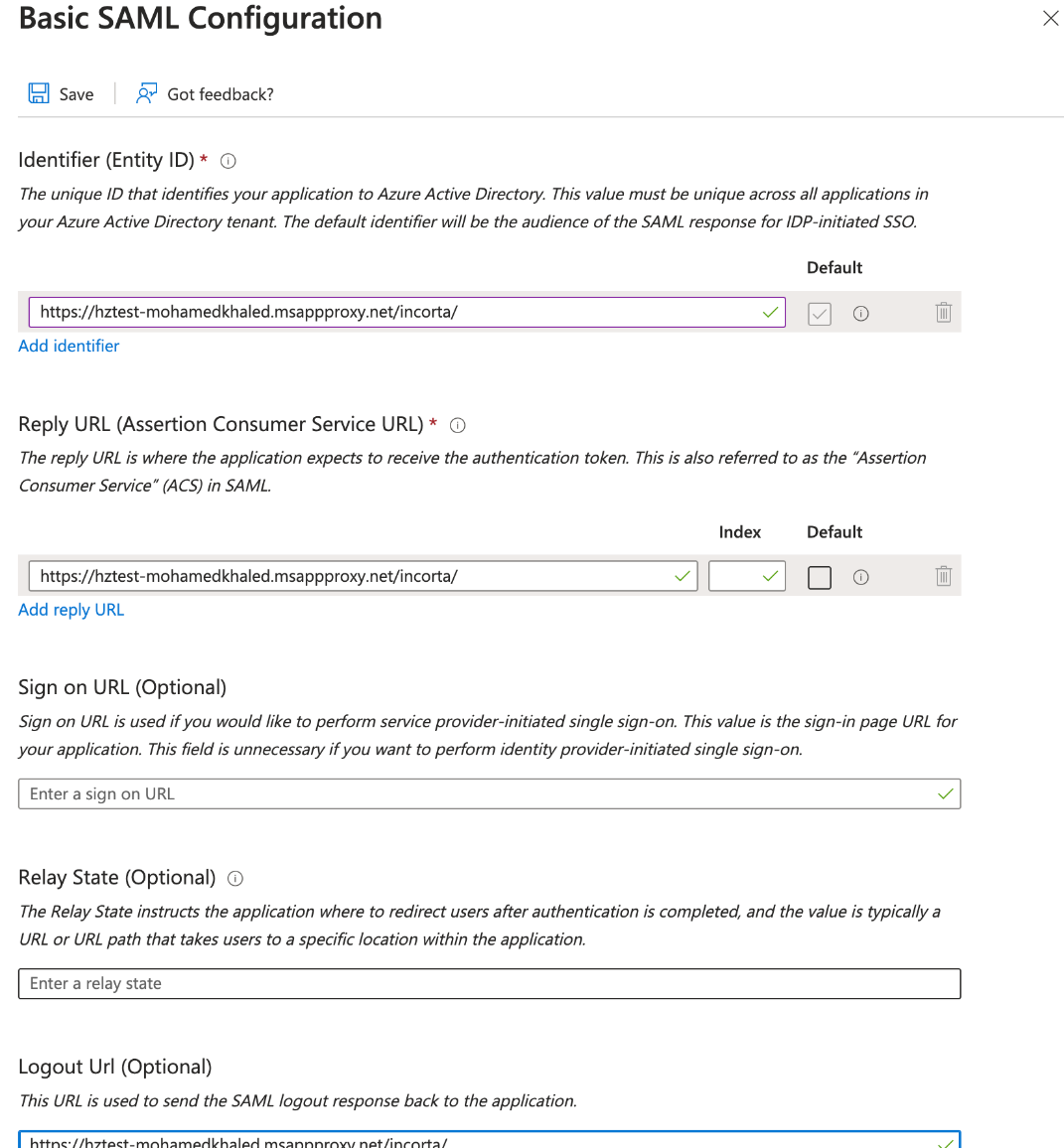


4- Copy the **External URL** for the application. You'll need this URL to complete the SAML configuration.

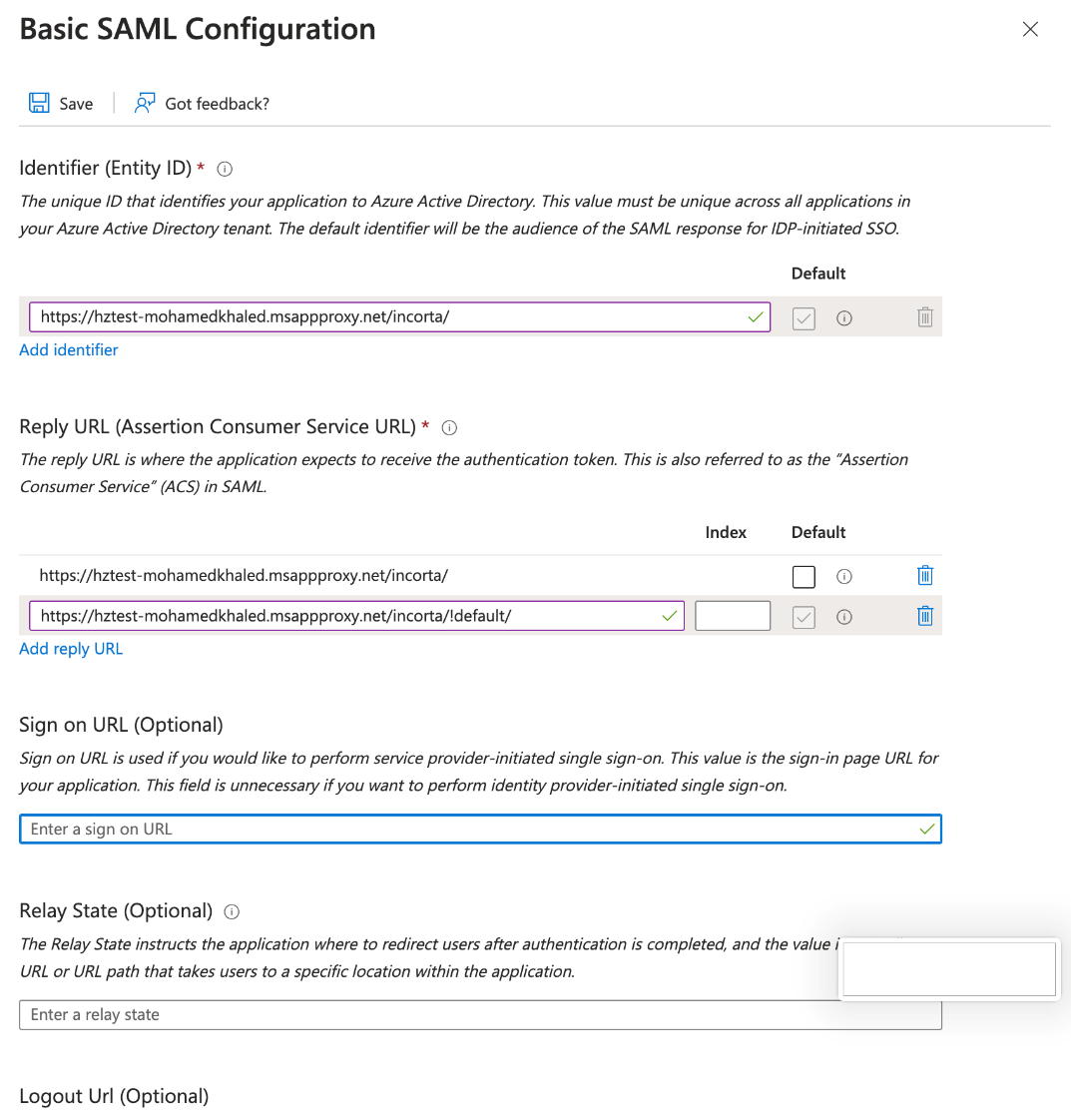
5- Go to your app, then select **Single sign-on > SAML**



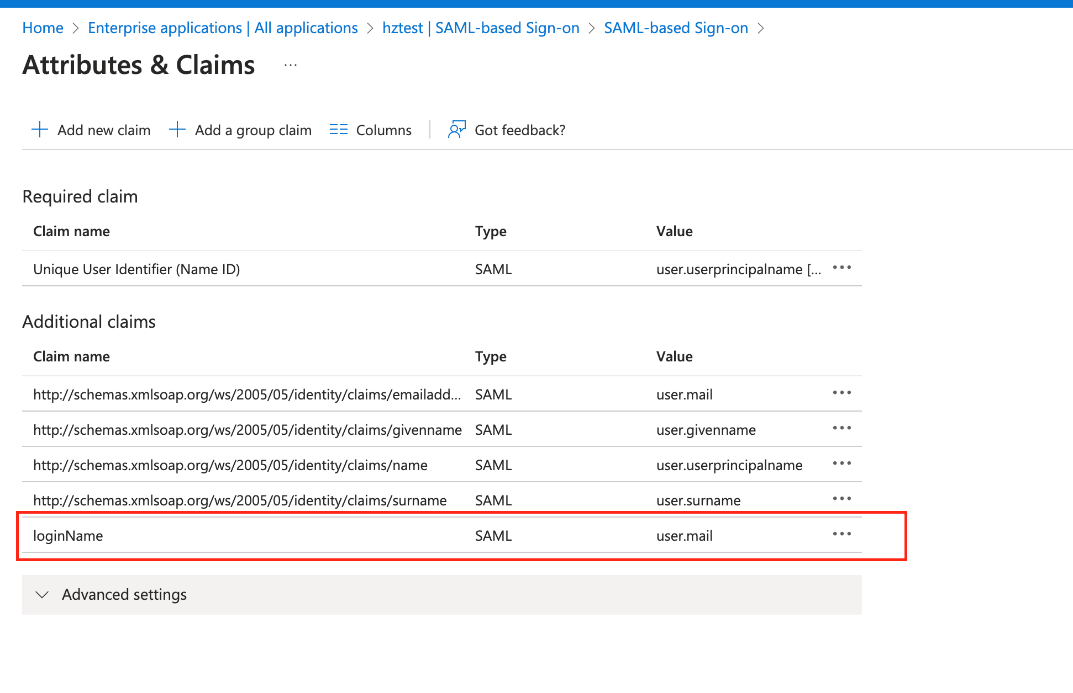
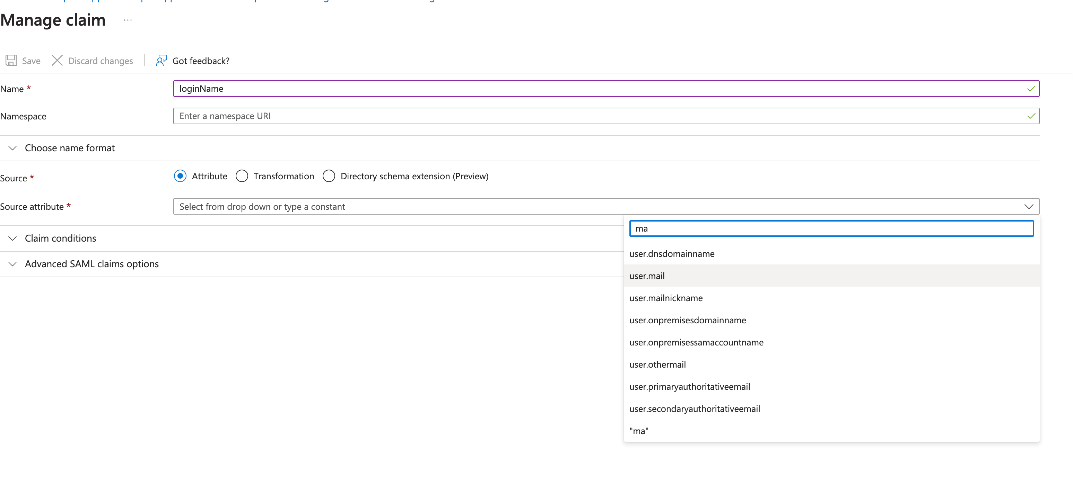
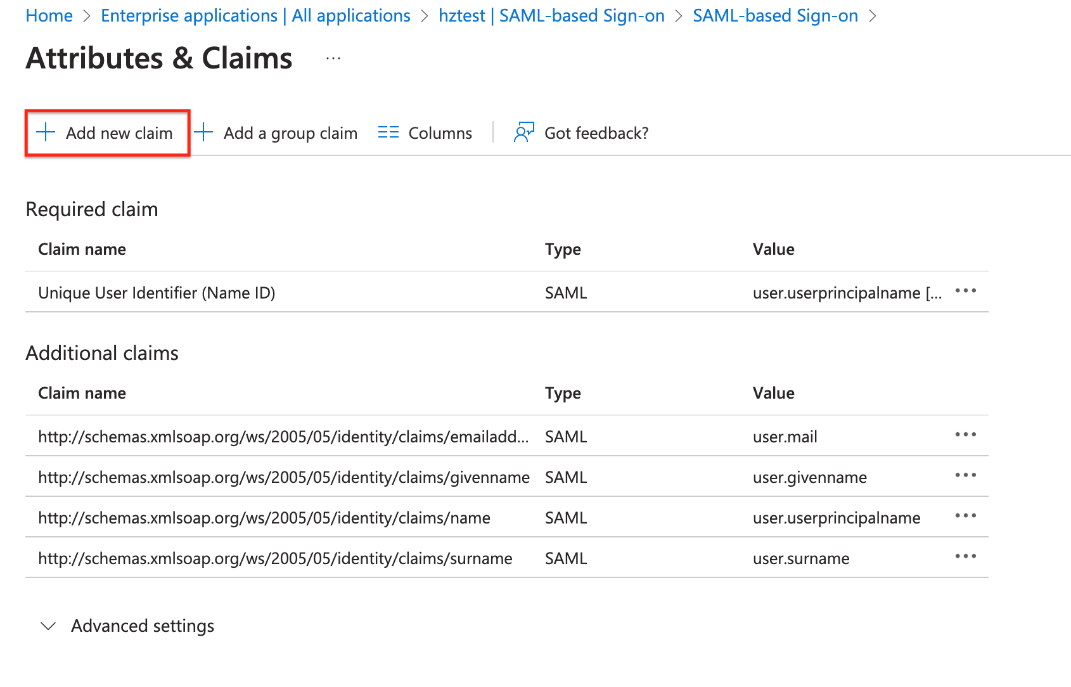
6- Edit the **Basic SAML configuration** section by adding the External proxy URL as indicated below.



7- Add another **Reply URL** with the tenant name, and set it as a Default



8- 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



9- Go to **Users and Groups**, and assign the users to your app.

10 - Now, you can configure the Incorta SSO tenant, and log in to Incorta using Incorta's URL followed by   
**!<tenant\_name>** [Example: [http://hostname/incorta/!default/](http://localhost:8080/incorta/!demo/) ]