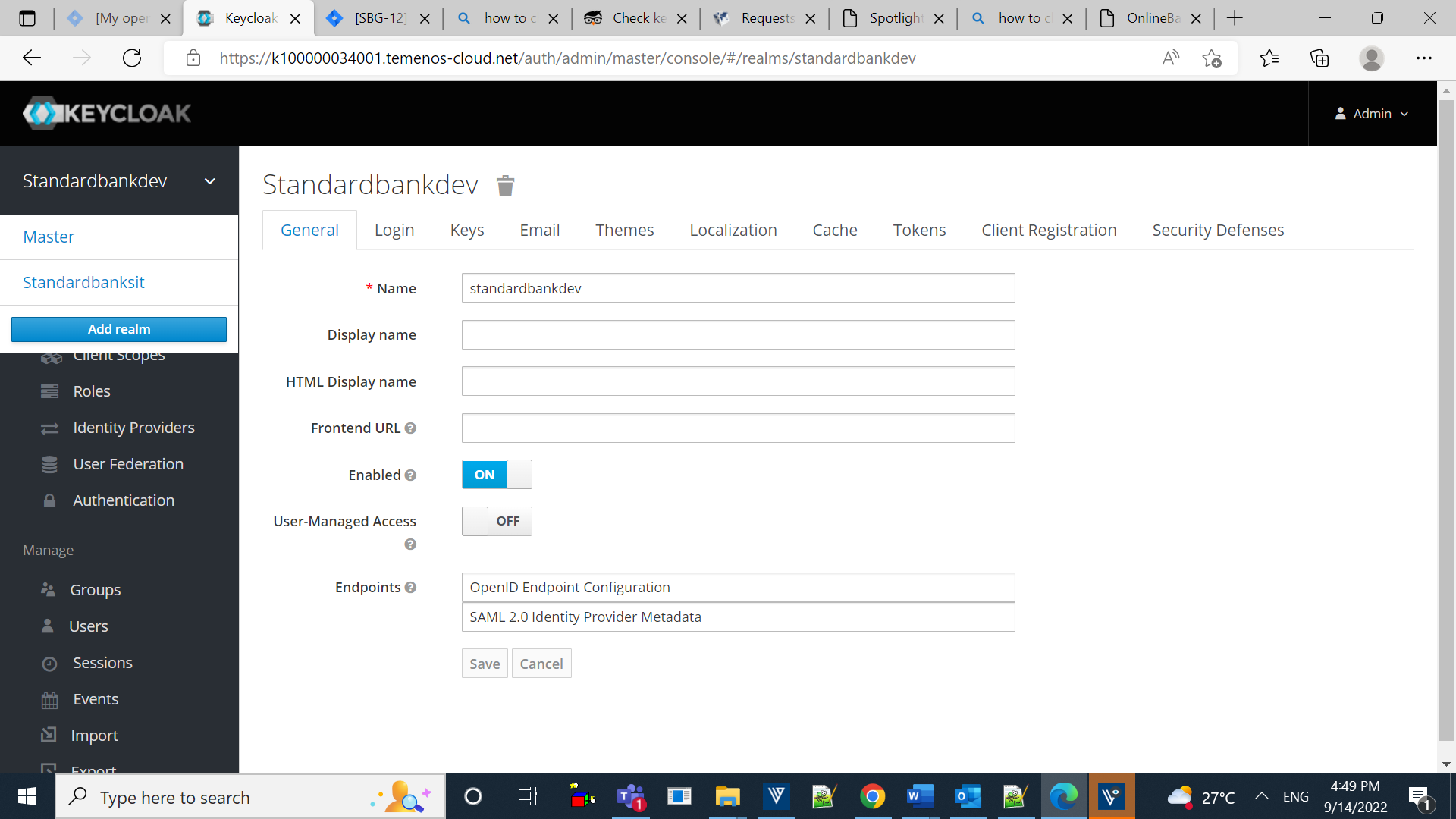
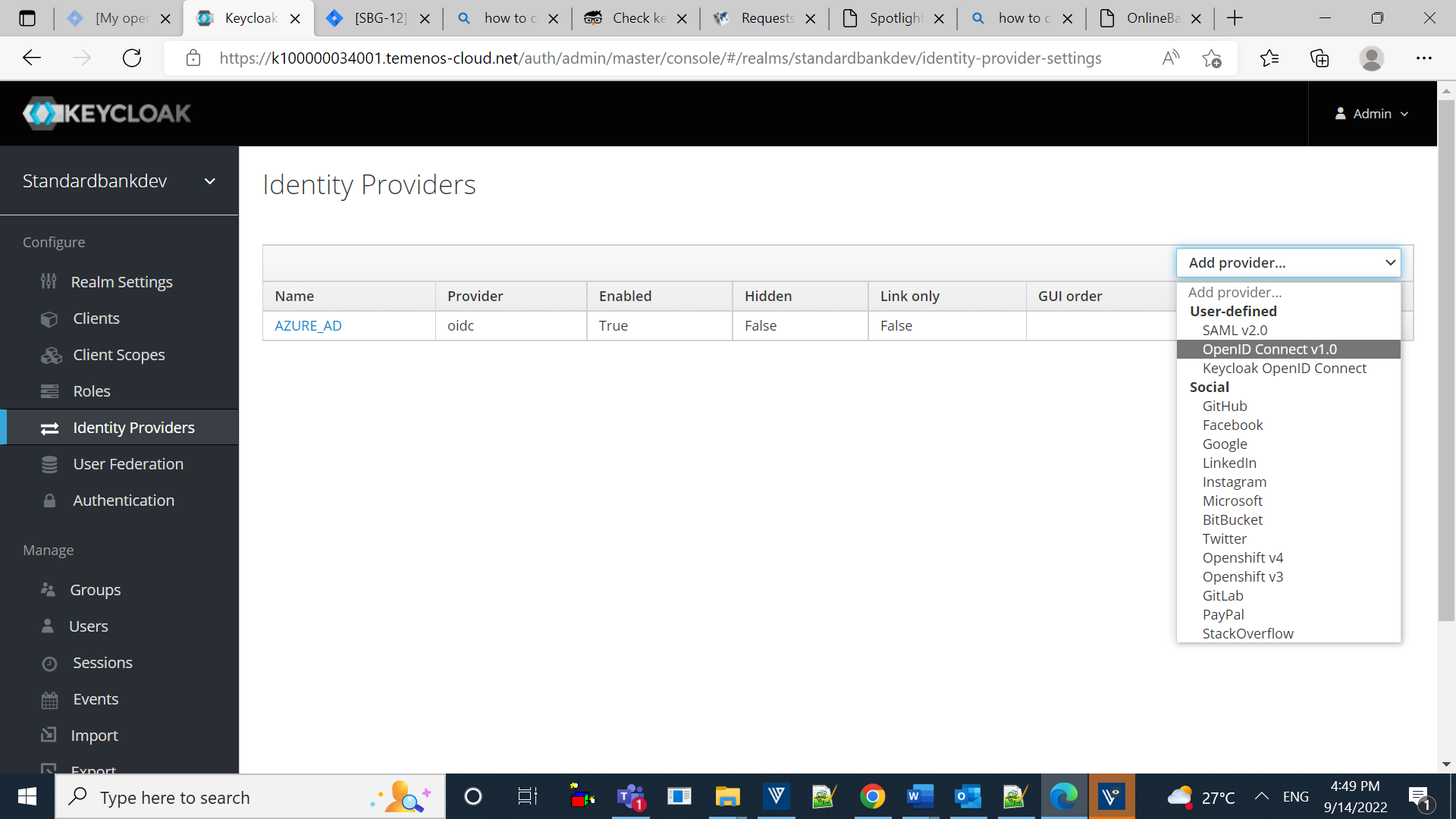
**ADFS INTEGRATION WITH KEYCLOCK**

Keycloak Version used – 12.0.2

**Step 1-**

**In Keycloak**-> Realm





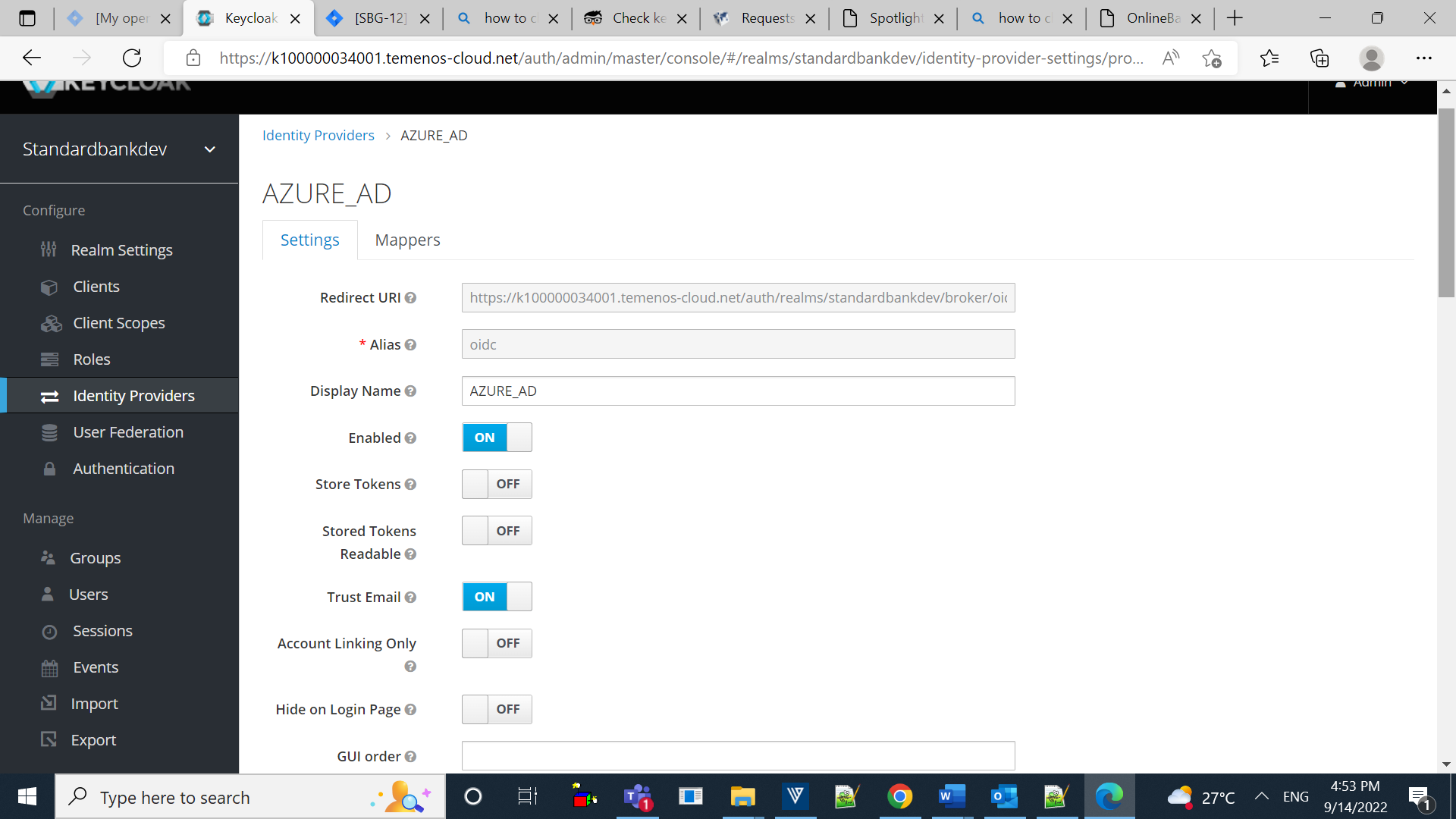
Select Identity Providers and add provider OpenID Connect v1.0

**Step 2-**

In Add Identity Provider

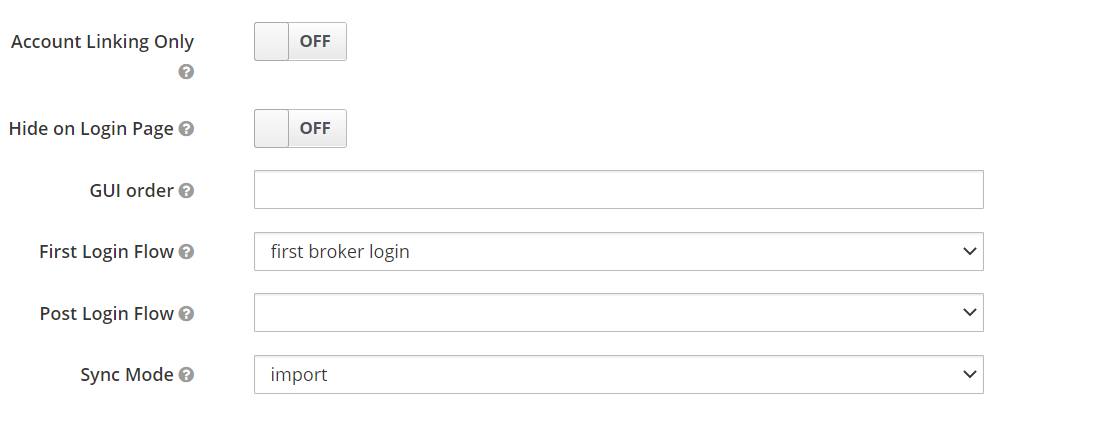
Copy the Redirect URI and paste it in notepad.

Update display name as **AZURE\_AD**



**Step 3-**

Replicate the below changes in the keycloak.



**Step 4-**

From the registered app Click on Endpoints.

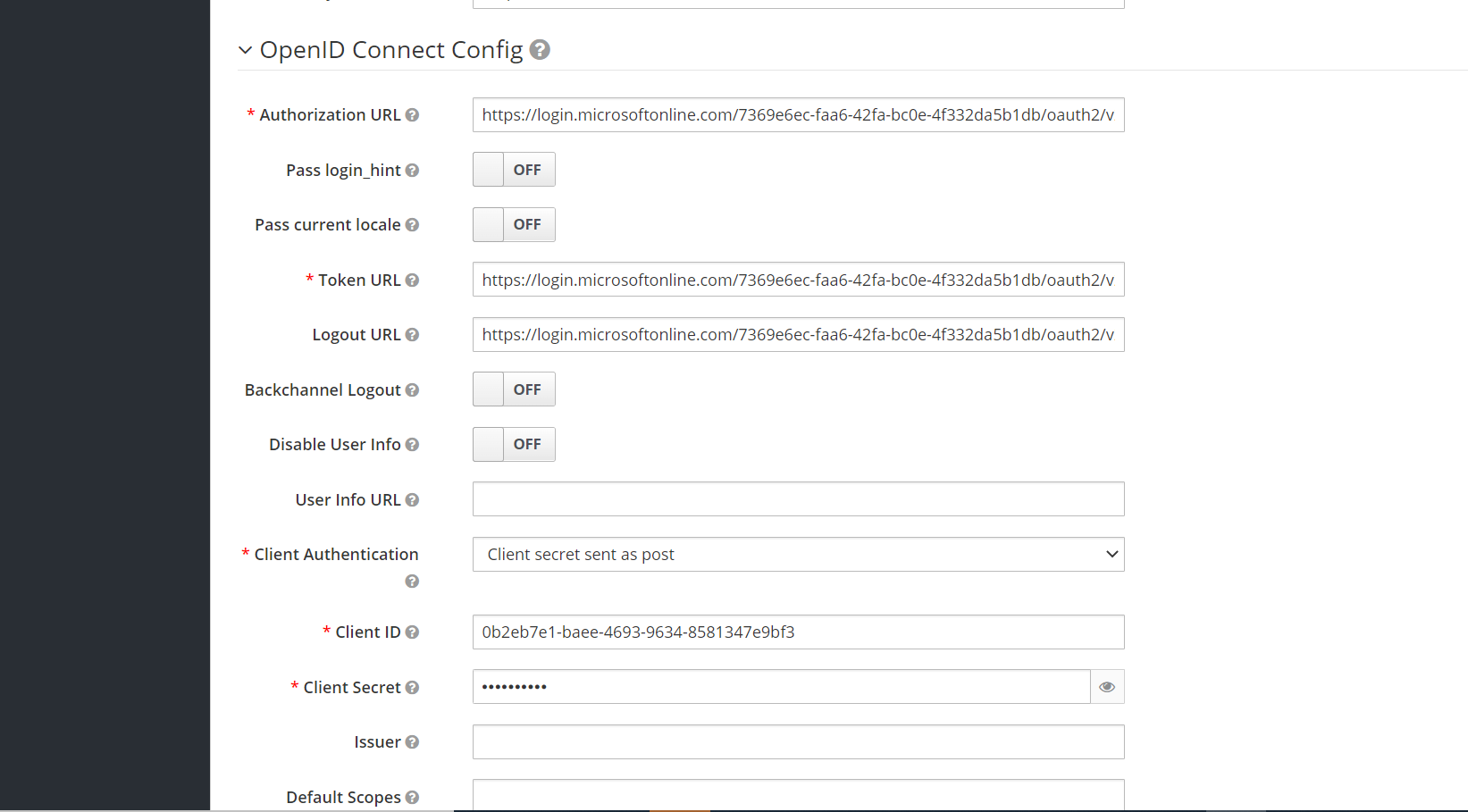
Copy Endpoints authorization endpoint and token Endpoints.

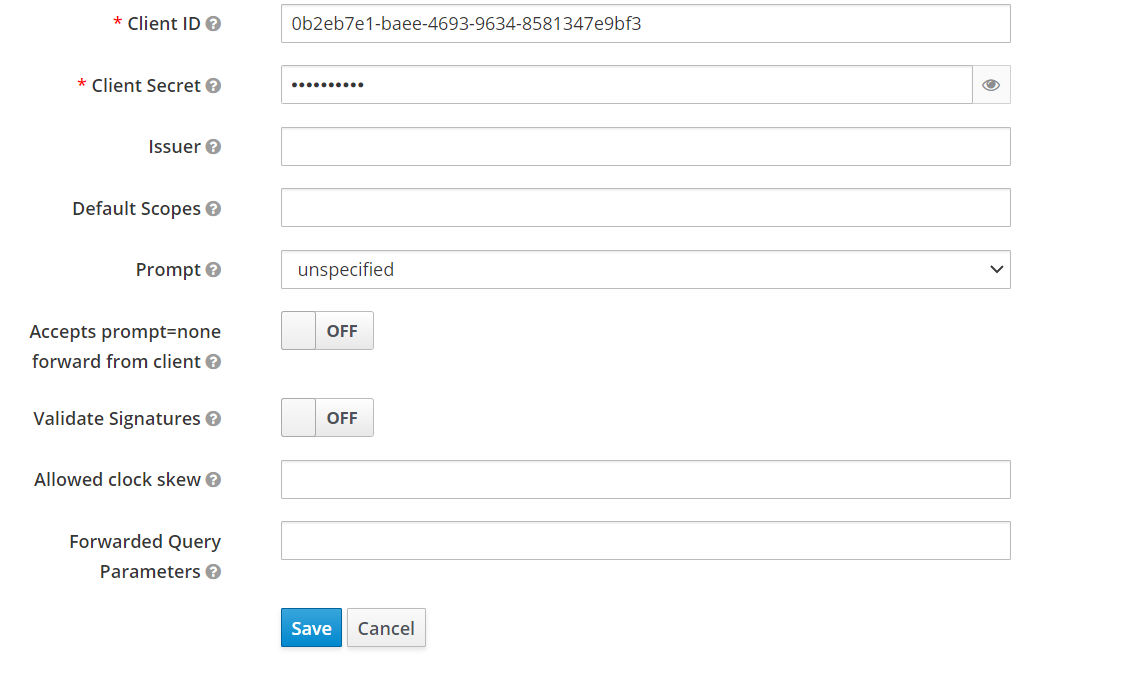
Paste the copied Endpoints

Authorization Endpoint in Authorization Url and Token Endpoint in Token URL

From AZURE:

Copy Application (client) ID from the App that have been registered recently.





After following the below steps click on save.

**Username Fix: Add Default Scopes as: “openid email profile”.**

****

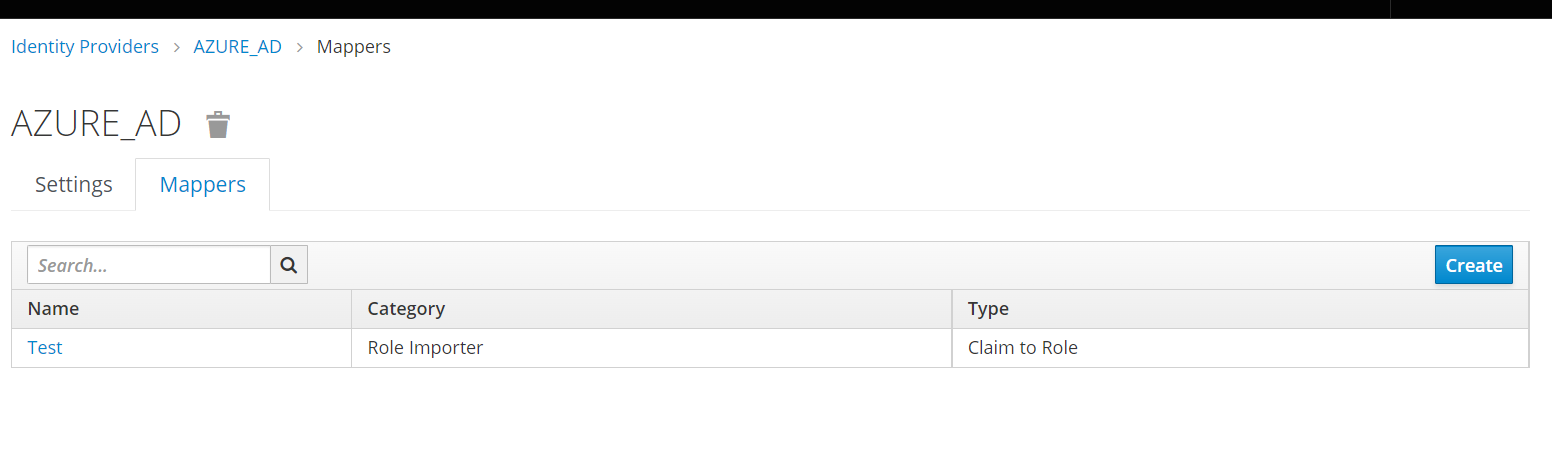
**Step 5-**

Assign some members to the newly created groups.

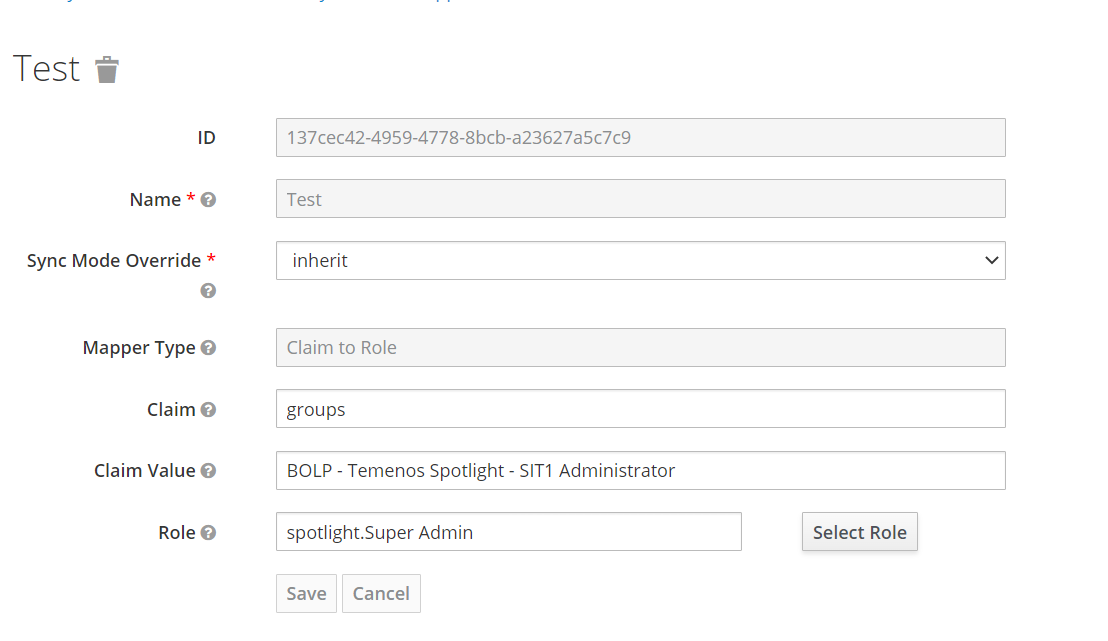
We created a group name

BOLP - Temenos Spotlight - SIT1 Administrator

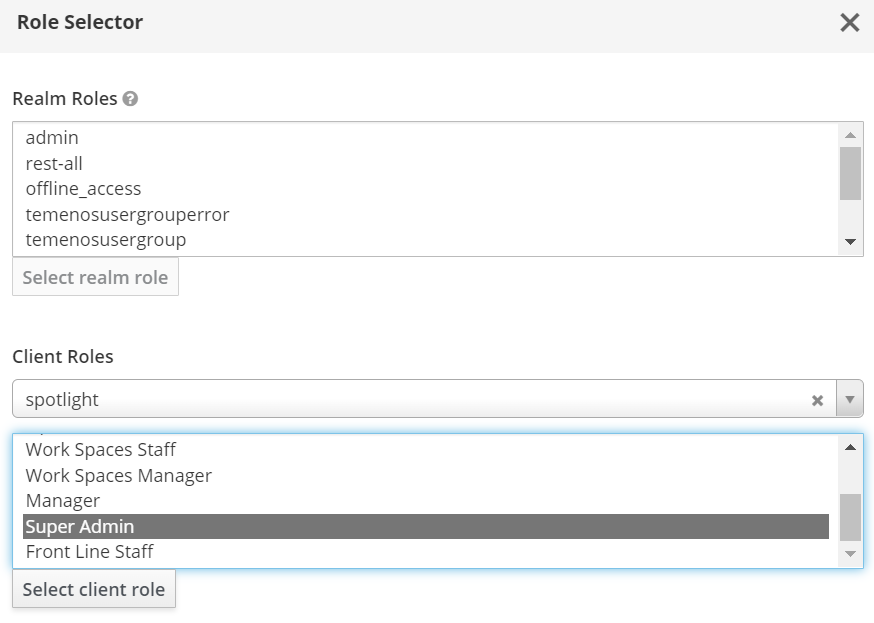
Go to this identity provider and go to Mappers. Create a new one.



Replicate the steps:



For role selection we used super admin



Step-6:

Launch Spotlight and login with AZURE.

**URL’S we used in configuration of Azure in UAT Environment:**

Application name: **BOLP\_Temenos\_Spotlight\_UAT1**

**Authorization URL:**

**https://login.microsoftonline.com/7369e6ec-faa6-42fa-bc0e-4f332da5b1db/oauth2/v2.0/authorize**

**Token URL:**

**https://login.microsoftonline.com/7369e6ec-faa6-42fa-bc0e-4f332da5b1db/oauth2/v2.0/token**

**Logout URL:**

**https://login.microsoftonline.com/7369e6ec-faa6-42fa-bc0e-4f332da5b1db/oauth2/v2.0/logout**

**Client ID:**

**6c41112e-2635-484b-bead-67e13da5f79d**

**Client Secret:**

**IgL8Q~yLSxFzmsldNSR1~HwHOgtz.WNi9CXi4cG-**

**Note:**

**for redirect URI should be configured by SBG, after getting Access from SBG. respectively to specified groups users can login with there role.**

**USER GROUPS:**

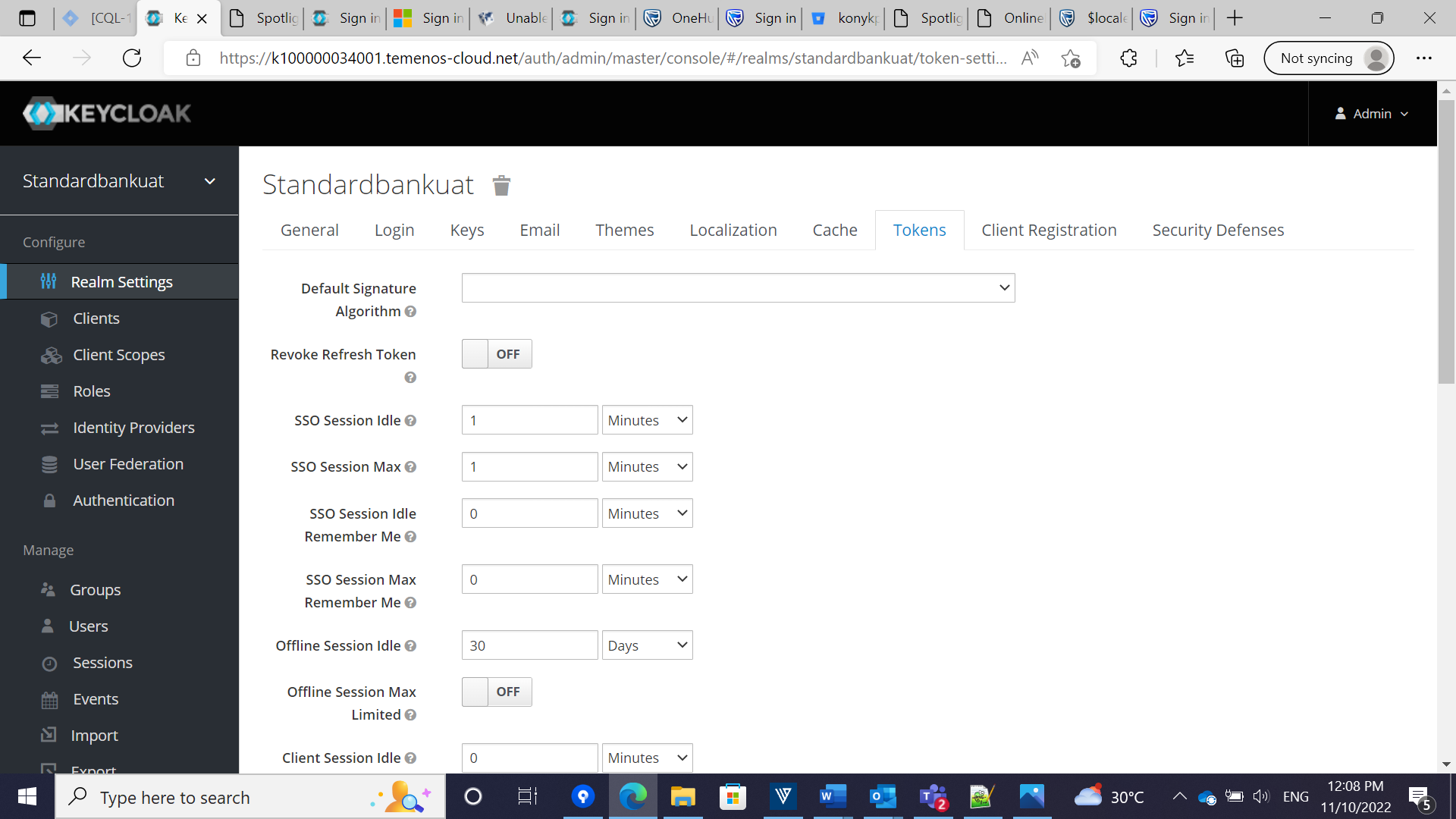
**For Admin:**

**BOLP - Temenos Spotlight - UAT1 Administrator**

**For Front Line staff:**

**BOLP - Temenos Spotlight – UAT1 Front Line Staff**

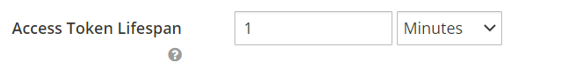
For session timeout in Azure we configured below :



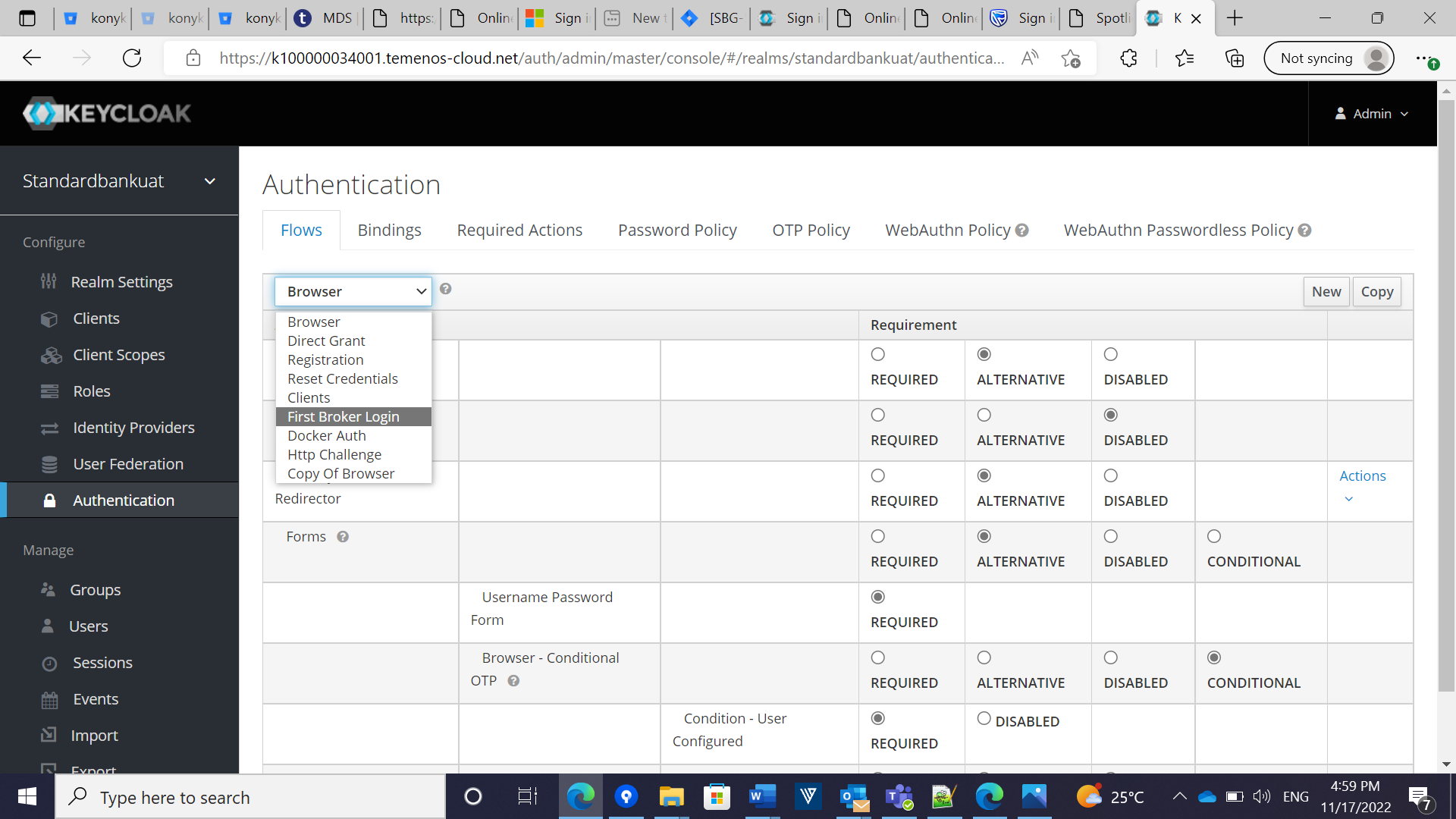
**In Realm setting --------> tokens, we need to change this 3 to solve the session timeout issue in ADFS**

**SSO SESSION IDLE, SSO SESSION MAX and ACCESS TOKEN LIFESPAN.**





And for disabling the intermittent page (update user information) while LOGIN. We have done one change.



In Authentication -> First broker login -> review profile page-> select the disabled button.