1.Register the Product App in AAD

2.Then get the app ID,TenantID,authority

3.Expose it as an API

then Create the Scopes by which someone will access this API

then create the Roles based on users and Groups (Products.ReadOnly,Orders.ReadOnly)

Then By using Connected Apps Create the Authentication codes in the Program.cs

then add your Postman as a client app to this API(in AAD go to the ProductAPI app and add the Client App which has been registered as Postman in the Expose API section with proper scope permissions)

Give the postman Client App Authorized for One of the Scopes in ProductAPI .(This needs to be done as one scope has to be present while Creating the JWT token0)

-for an Example suppose you have three scopes (ScopedForOrders,ScopedForCatalgoue,ScopedForSavedToKart,Common) in ProductAPI,

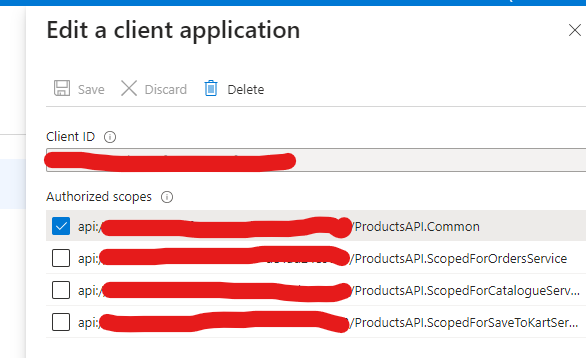
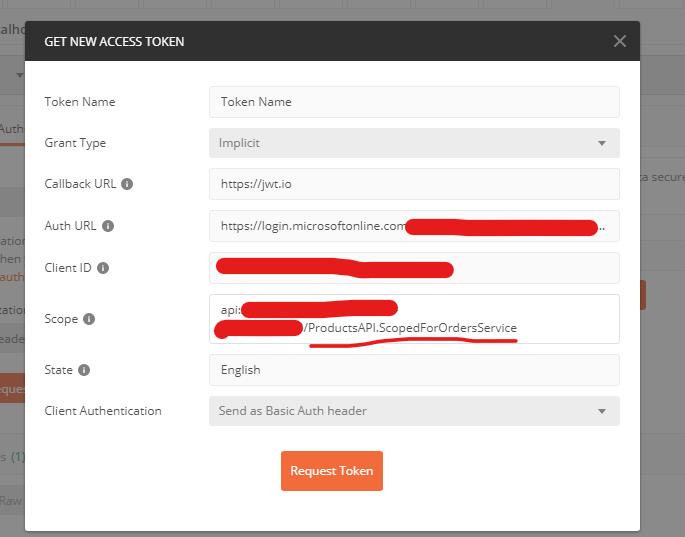
-suppose I want to have a JWT token for 'ScopeForOrders' only , If you have not assigned your clientApp(Postman) with atleast one scope , By default it will return all the scopes ((ScopedForOrders,ScopedForCatalgoue,ScopedForSavedToKart,Common)) even though you have asked for one specific scope

-So its a good practice to add a scope (Common)to the client app and then generate authorize token with only scope 'ScopeForOrders' if this is JWT token is being called from Orders service to interact with Product Service only

-CLick on the "Expose API" , define a scope for ProductAPI as 'ProductAPI.Common'

-Then Add a client Application and add the PostMan Client App by using the AppID(which has been registered as the App registration). then Give the "Product.Common" as authorized Scope only

- Then in Postman request for Authorization

1. Register the Product Api in AAD
2. Then get the app ID, TenantID, authority (Instance)
3. Expose it as an API
4. then Create the Scopes by which someone will access this API, then create the Roles based on users and Groups (Products.ReadOnly, Orders.ReadOnly)
5. Then By using Connected Apps Create the Authentication codes in the Program.cs
6. then add your Postman as a client app to this API (in AAD go to the ProductAPI app and add the Client App which has been registered as Postman in the Expose API section with proper scope permissions)
7. Give the postman Client App Authorized for One of the Scopes in ProductAPI .(This needs to be done as one scope has to be present while Creating the JWT token)
   * For an Example suppose you have three scopes (ScopedForOrders, ScopedForCatalgoue, ScopedForSavedToKart, Common) in ProductAP.
   * Suppose I want to have a JWT token for 'ScopeForOrders' only , If you have not assigned your clientApp(Postman) with atleast one scope, By default it will return all the scopes ((ScopedForOrders,ScopedForCatalgoue,ScopedForSavedToKart,Common)) even though you have asked for one specific scope
   * -So its a good practice to add a scope (Common)to the client app and then generate authorize token with only scope 'ScopeForOrders' if this is JWT token is being called from Orders service to interact with Product Service only
   * -Click on the "Expose API" , define a scope for ProductAPI as 'ProductAPI. Common'
   * Then Add a client Application and add the PostMan Client App by using the AppID(which has been registered as the App registration). then Give the "Product.Common" as authorized Scope only
   * 
8. Then request an Authorization token from the Postman App (which is behaving like client App- Later it will be replaced with the ServiceOneApp(OrderService))
9. 
10. I am only trying to get a scoped Token for OrderService only
11. 
12. IF you can see we are getting only 2 Scope (Common, ScopedOrderService) .Now we can achieve scope based Authorisation by checking if This request comes from OrderService or Not .
13. Giving Roles to Product API

* Go to ProductAPI App in AAD . click on APP Roles and then give the roles specific to ProductAPI
* Asign Users to specific Roles -> enterprise Applications -> assign users and Groups and Select the user and give the user a certain permission only
* Then Try to get a token from Postman and then try to call the API , If Roles are been provided , then only it will authorize the API and give the details of products