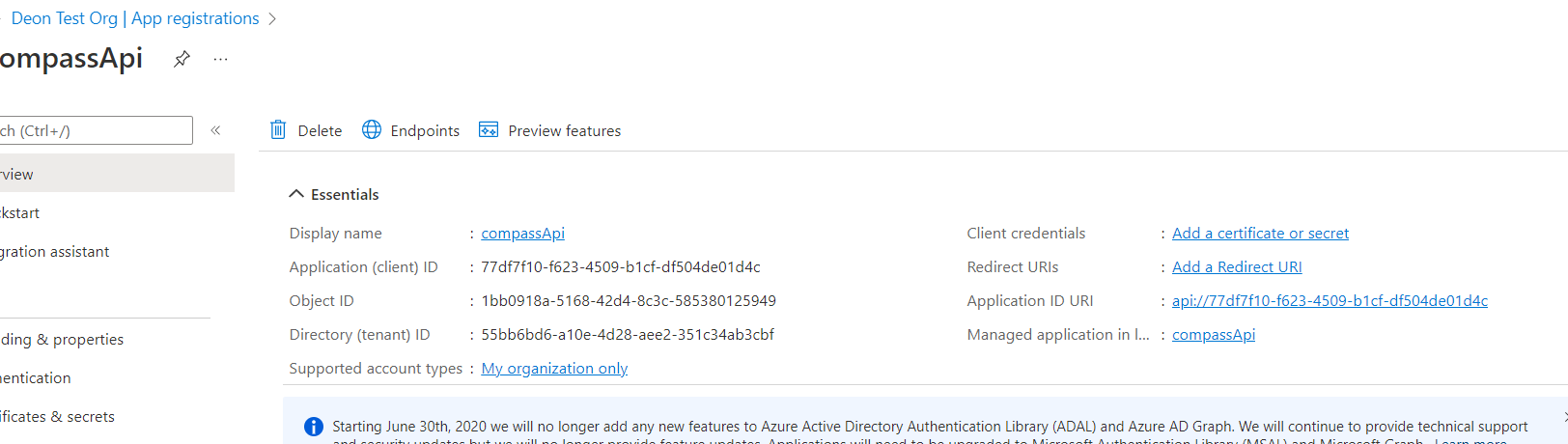
Protect web API and access them via Oauth2

# 1. set up Azure org

# 2. App Registration for the API

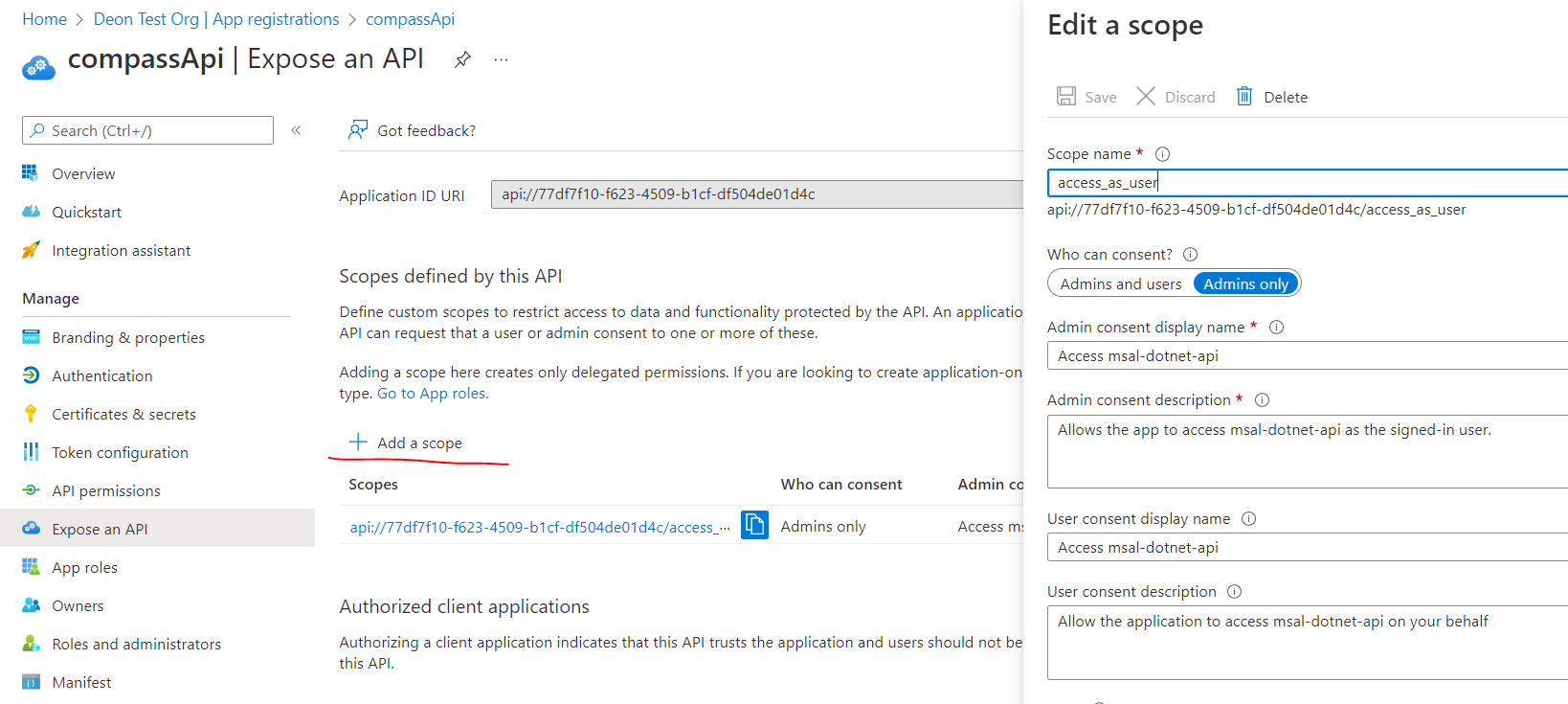
## 2.1 create App Registration for the API



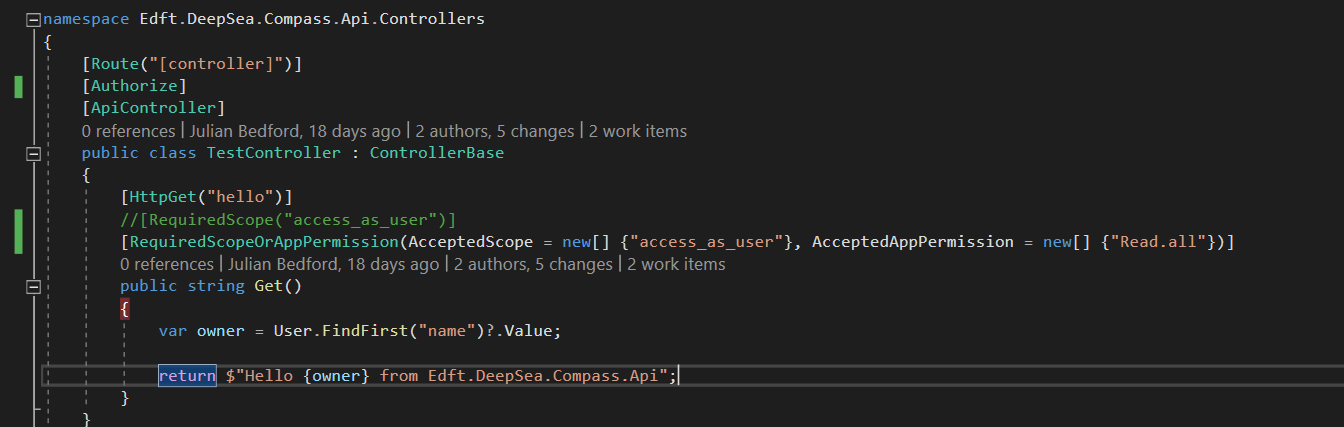
## 2.2. Expose an API

A scope needs to be defined to expose the API

### Add a scope:



Scope name is defined by you but will be used in the API solution code (for verification to check if the received token has the right scope)

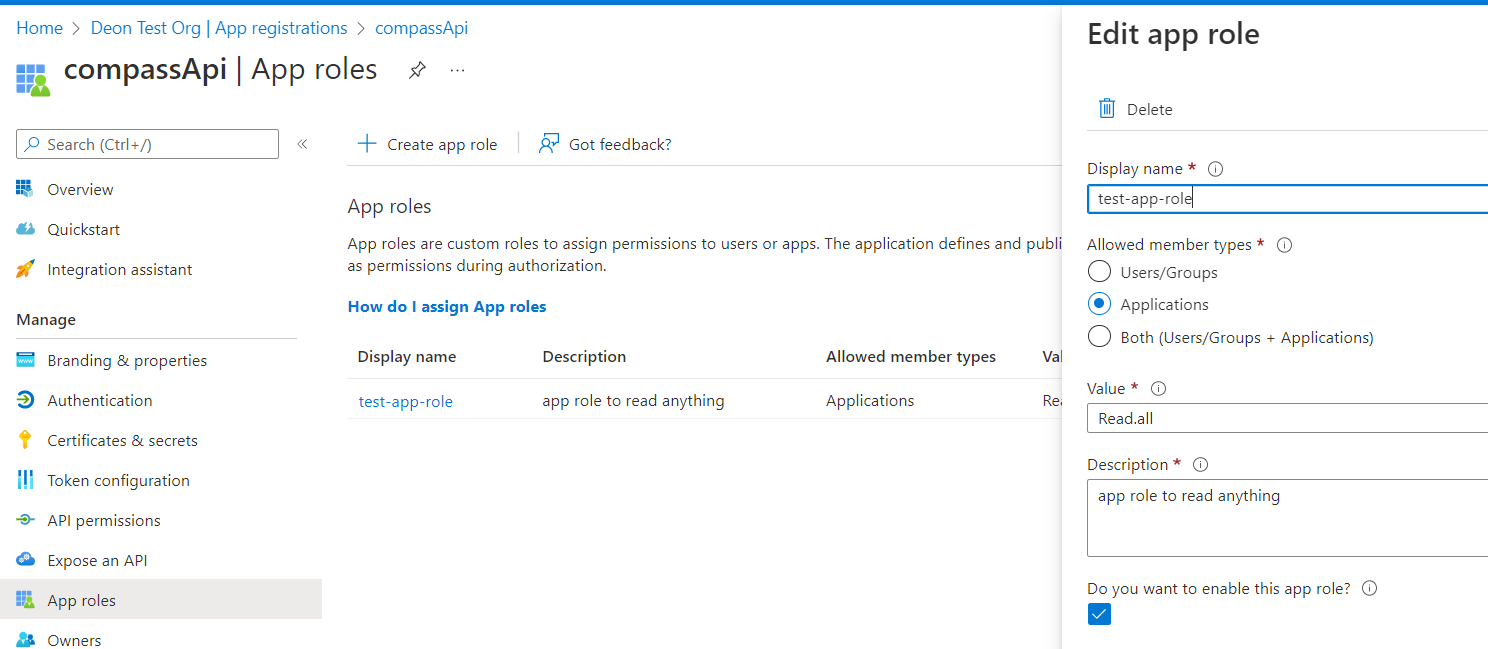


### Note: the Authorised client application list

It should make the API trust clients in the list, however it did not work for me

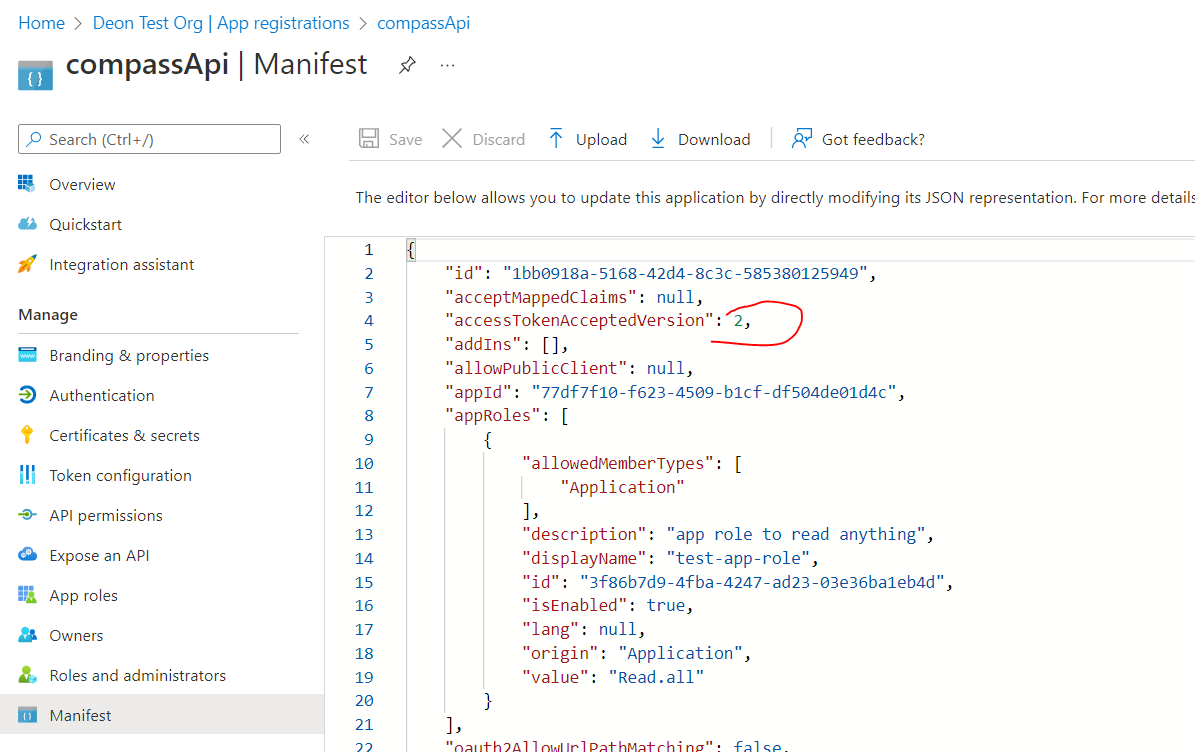
### App roles

This is also referred as App Permissions. Because we are trying to configure an application to access the API not on behalf of a particular user (use case: test automation framework, Postman, or background daemon services)



Again, the value “Read.all” is defined by me – but it needs to be used in the API code. This role will be included in the access token and the API code will need to verify if the token contains this role.

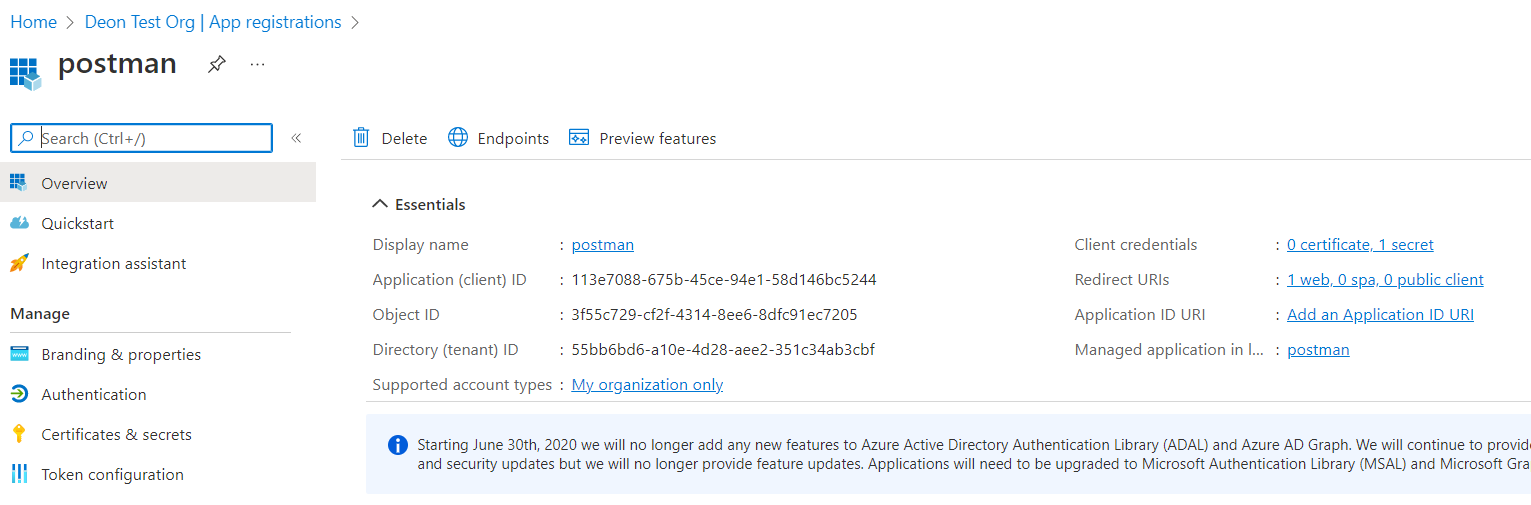
## 2.3 Update Manifest to use accessToken version 2



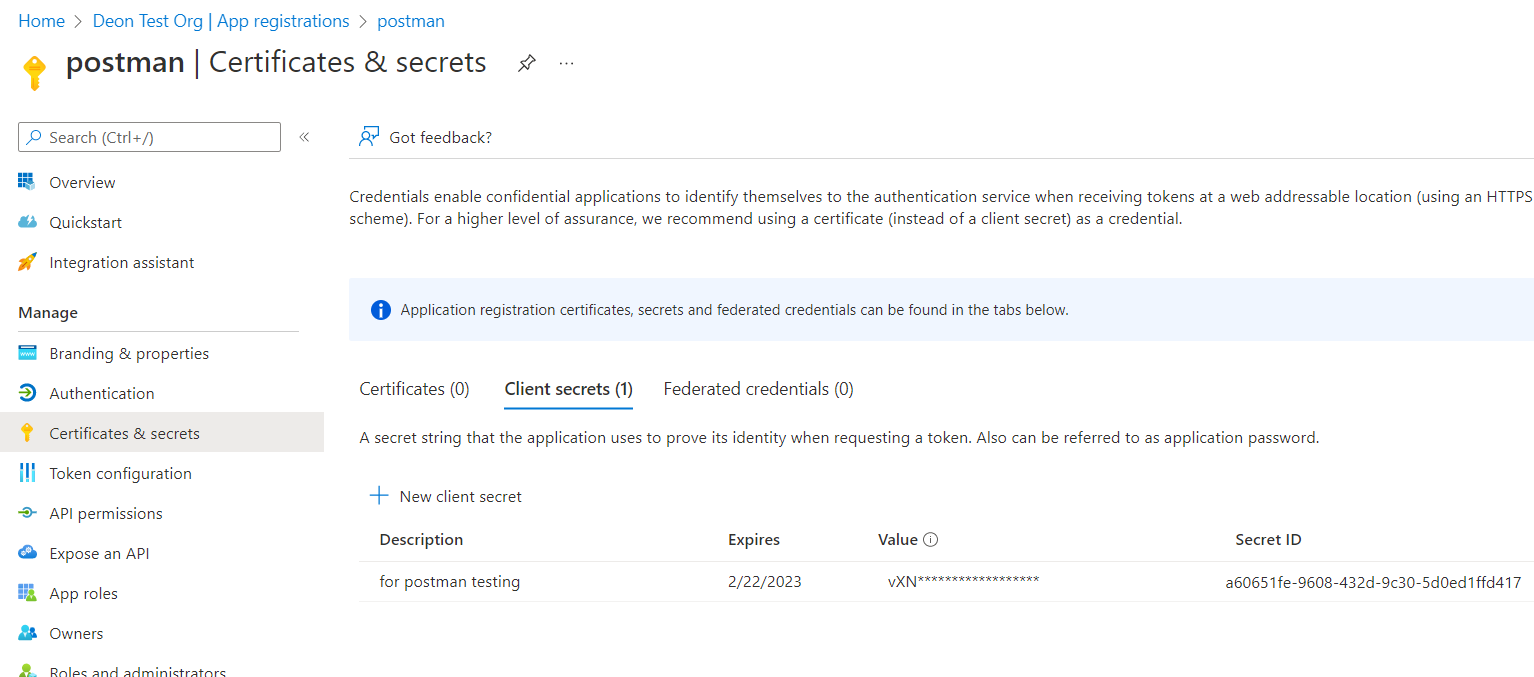
# 3. App Registration for the client

The client is our application that wants to access the API, e.g.: test automation framework, Postman

## 3.1 create the app registration



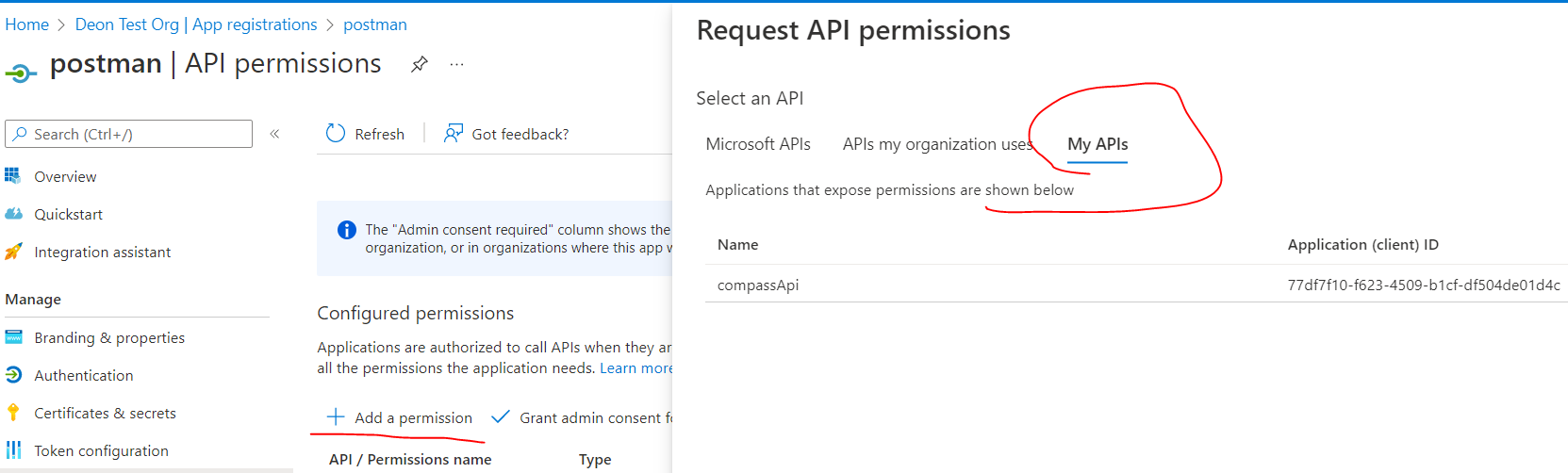
## 3.2 Create a client secret

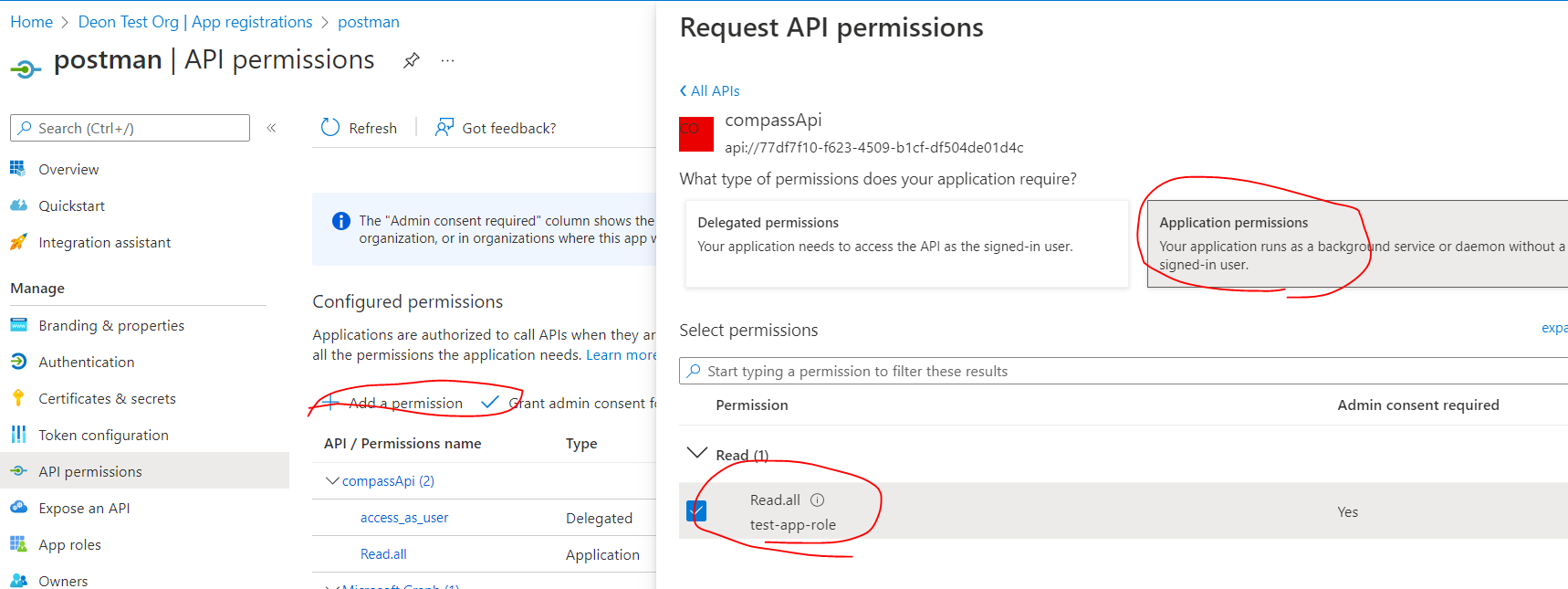


Note: must note down the secret during creation as it wont be displayed again

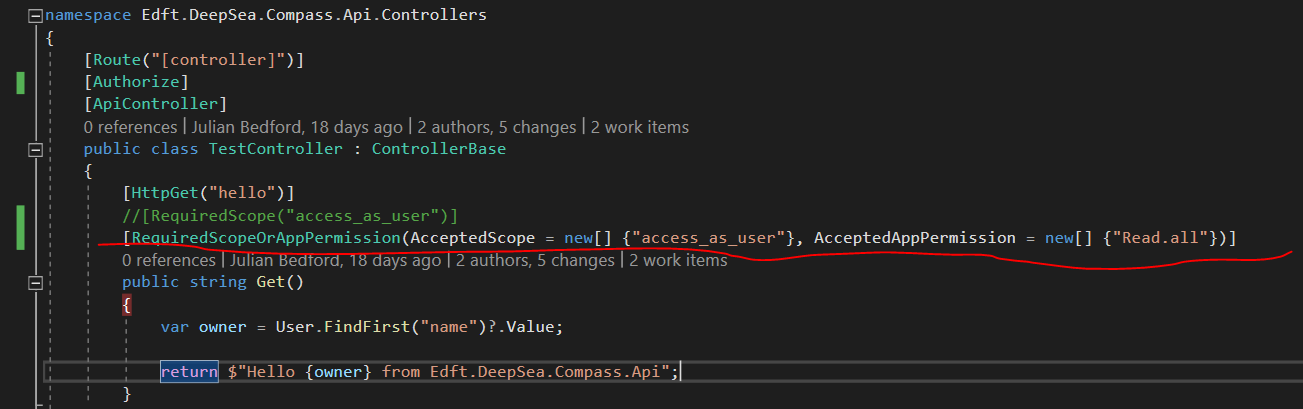
## 3.3 Add API permission

These are the permissions granted to this app for this app to access APIs



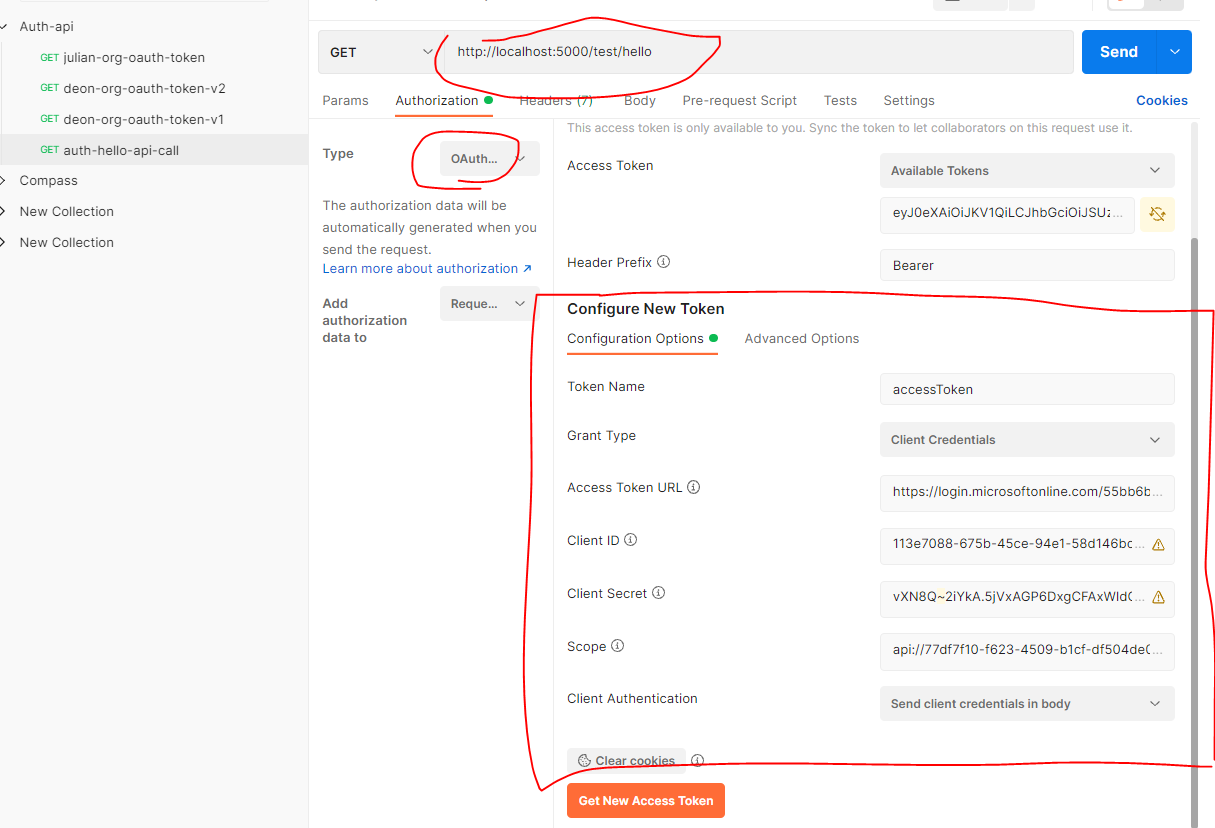


# 4. Configure .net API project route



This means it should accept scope or AppPermission, in our case it’s the Read.all app permission we configured in the client’s app registration.

# 5. Configure Postman



## URL:

the end point of the API – here I’m running it locally

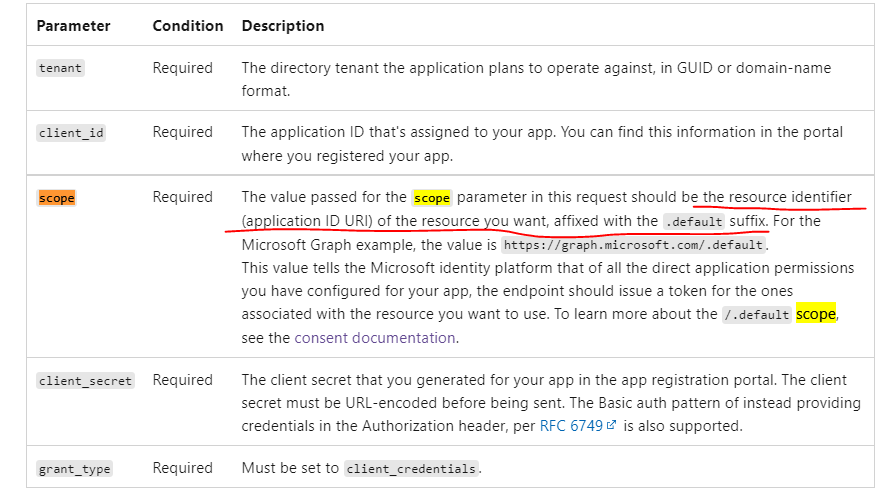
## Type: Oauth2

## Grant type: client credentials

## Access Token URL:

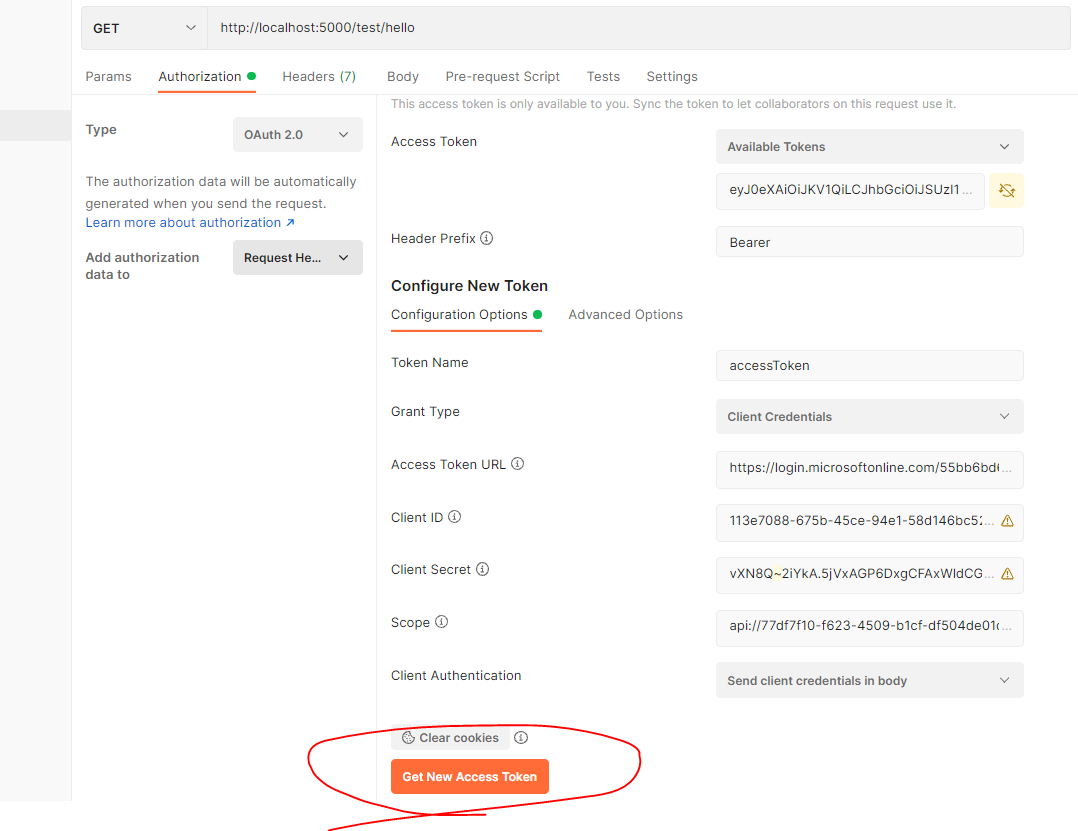
## Client ID & Client secret:

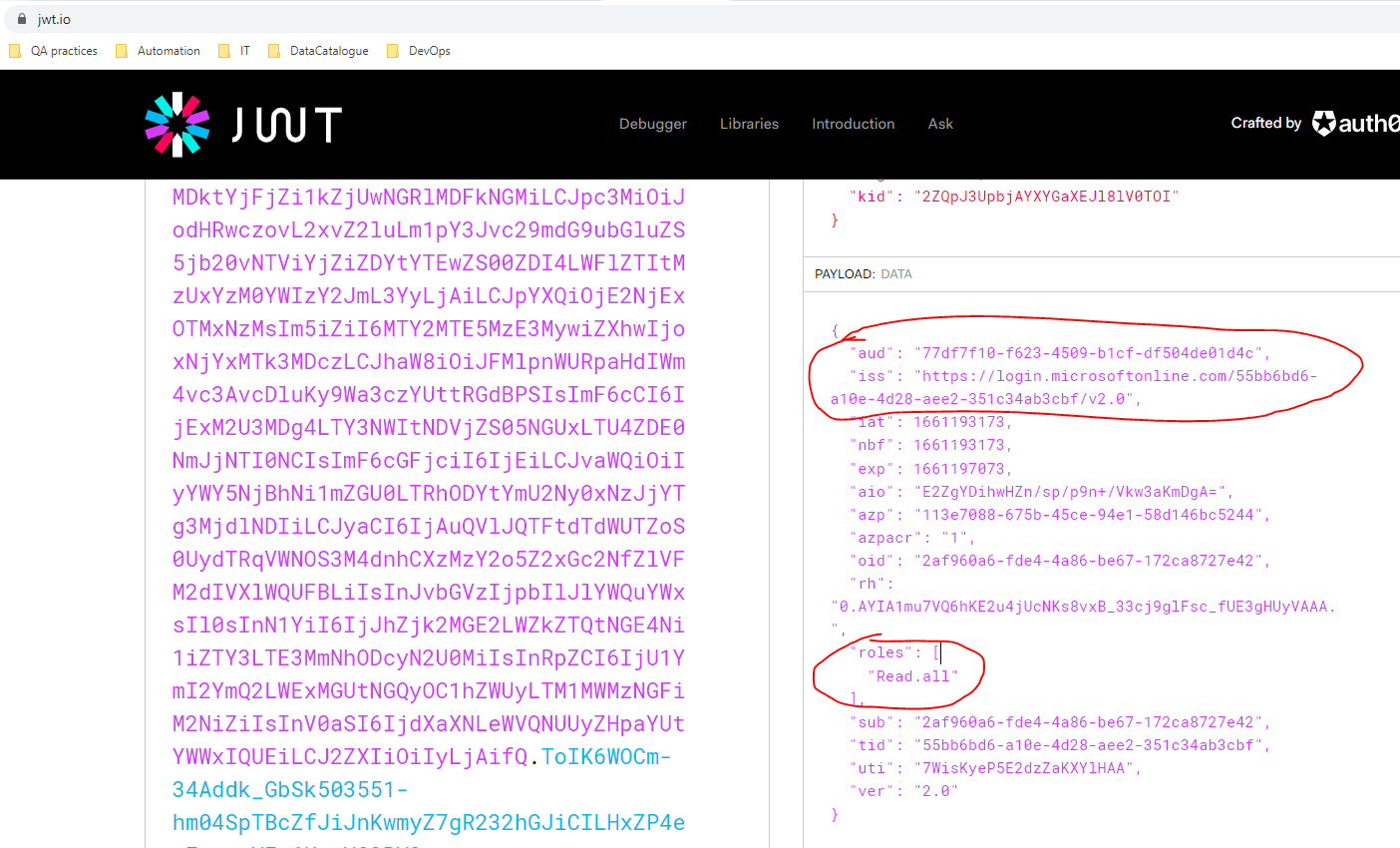
## Scope:

Scope needs to be affixed with .default suffix 

So, for this case, it should be: api://77df7f10-f623-4509-b1cf-df504de01d4c/.default

# 6. Access token



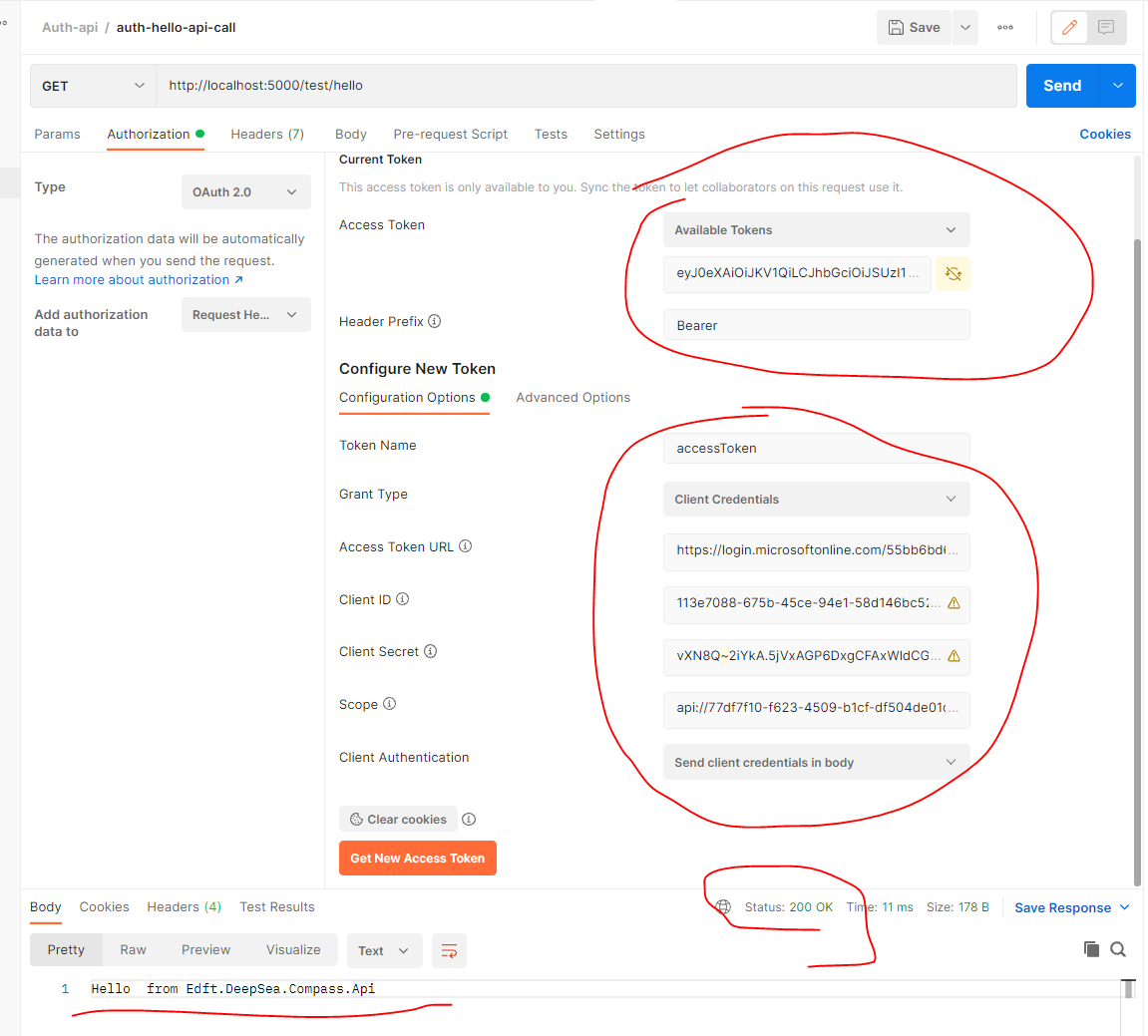


Aud: API client ID

Iss: contains tenant ID

Roles: Read.all – the app permission we granted to the client

# 7. Access the API



# 8. Use .net code instead of Postman

Use this example using MAL.NET library

<https://github.com/Azure-Samples/active-directory-dotnetcore-daemon-v2/tree/master/2-Call-OwnApi>