# APIM OAuth 2.0 Token based authentication.

## Prerequisite azure service for the implementation.

1. App Service (Running)
2. API Management service
3. App Registration (Azure App).

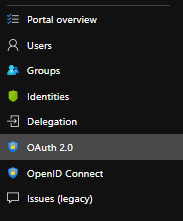
## Implementation

### Create App service

Need app service for which in running status.

### APIM setting for OAuth 2.0

#### Configure new OAuth2.0 for APIM service.



1. Authorization endpoint URL:

https://login.microsoftonline.com/ <<Tenant-Id >>/oauth2/authorize

1. Token endpoint URL

https://login.microsoftonline.com/<<Tenant-Id >>/oauth2/token

1. Additional body parameters using application/x-www-form-urlencoded format

Name: Resource

Value : Client Id

1. Client Credentials

* Client id
* Client Secrete

1. Authorization code grant flow

Auto generated URL while configuring OAuth 2.0 for APIM. This URL will be used to add in App registration authentication redirect URL

1. Implicit grant flow

Auto generated URL while configuring OAuth 2.0 for APIM

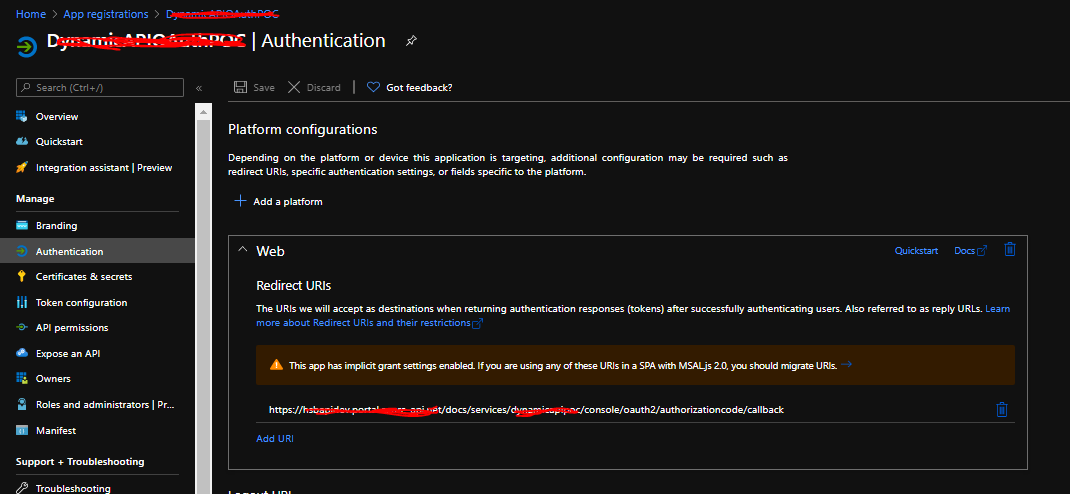
### Create App Registration for the API

#### First needs to create an App Registration in azure portal by providing all details.

#### Create secrete key for App Registration and record the secrete key before it will become not readable.

#### Add Redirect URL:

To Add Redirect URL



You can fetch redirect URL from APIM OAuth configuration and add it in App registration Authentication.

**Path** : APIM🡪 OAuth 2.0 🡪 <<OAuth configuration>> 🡪 Redirect URI (legacy portal) 🡪 Authorization code grant flow

#### Create Token API operation.

This API operation is used to generate the API Token.

Below setting need to add for creating token API.

1. Setting 🡪 Web service URL

https://login.microsoftonline.com/<<Tenant-Id>>/oauth2

#### Add policy for APIM API.

Validate policy need to add for API operations for which want token base access.

Format is mentioned as bellow.

<policies>

<inbound>

<validate-jwt header-name="Authorization" failed-validation-httpcode="401" failed-validation-error-message="Unauthorized. Access token is missing or invalid.">

<openid-config url="https://login.microsoftonline.com/<<ClientID>>/.well-known/openid-configuration" />

<required-claims>

<claim name="<<name>>">

<value>api://<<ClientID>></value>

</claim>

</required-claims>

</validate-jwt>

<base />

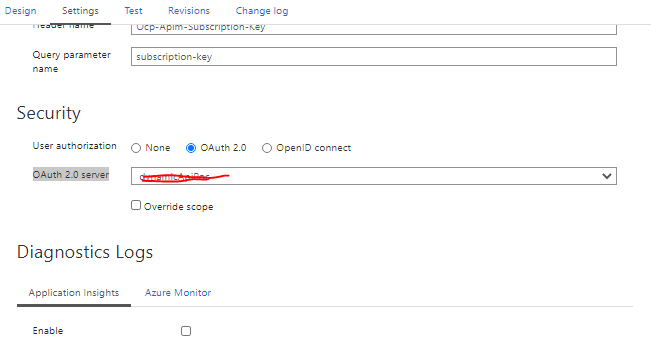
</inbound>

</policies>

#### Setting Changes for APIM API operation.

##### Select APIM🡪Setting🡪User Authentication OAuth2.0

##### OAuth 2.0 server : Select name of OAuth configuration you have created priorly.



## How to use APIM OAuth2.0

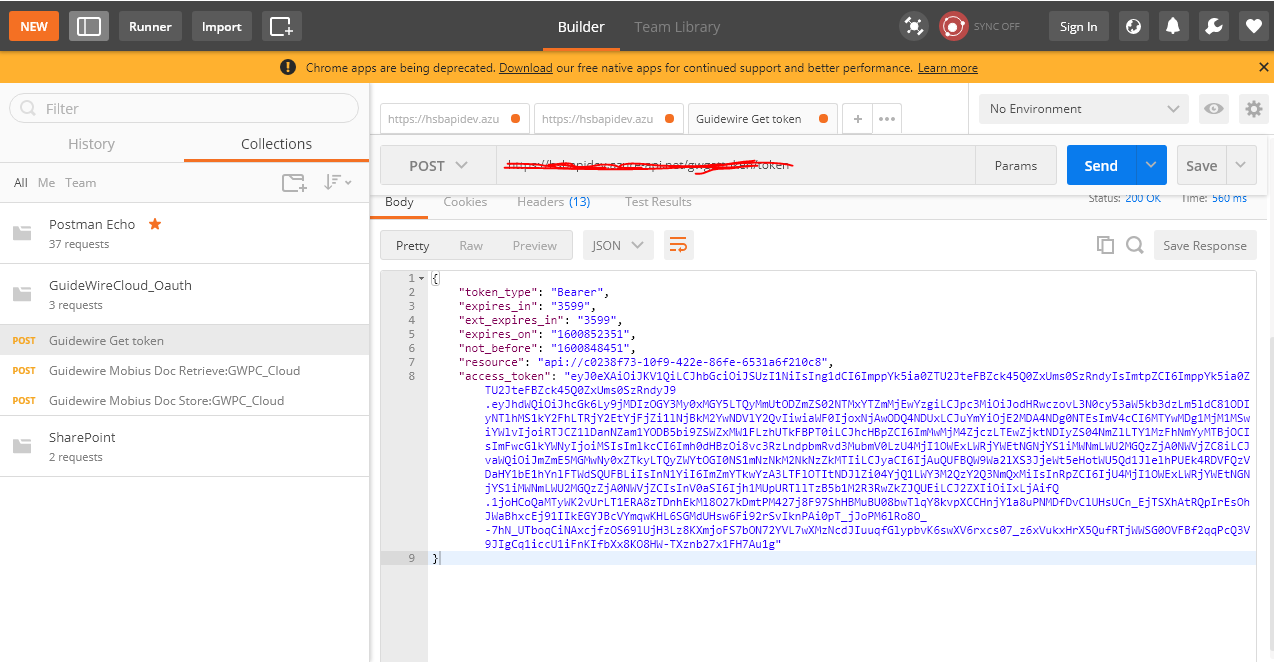
### Invoke token endpoint to generate token.

#### Create plain text input string which sent in the body of Token API.

Format of the sting:

grant\_type=client\_credentials&client\_id=<<client\_id\_value>>&client\_secret=<<client\_secrete\_value>>&resource=api:// <<client\_id\_value>>

#### Add Ocp-Apim-Subscription-Key in header of the token API call.



### Invoke other API operation by using access token from above token API response.

