MIRACLE
SOFTWARE SYSTEMS

JSON WEB TOKENS
Generete and Validate Policies

PavanKumar Meduri
Api Connect Developer
Miracle Software Systems, Inc.

09-02-2017

JWT Generate And Validate policy

What is JWT?

It is the open standard that defines the way of Securely Transmitting the Json objects between the Clients or parties.

When should we use JWT?

JWT can be used for Authentication,And for Information Exchange.

Structure of JWT:

JWT consists of 3 parts
1.HEADER
It contains two parts,they are

- type of token we are used
- which Hashing Algorithem we are follwing

2.PAYLOAD
The Payload contains three types of claims

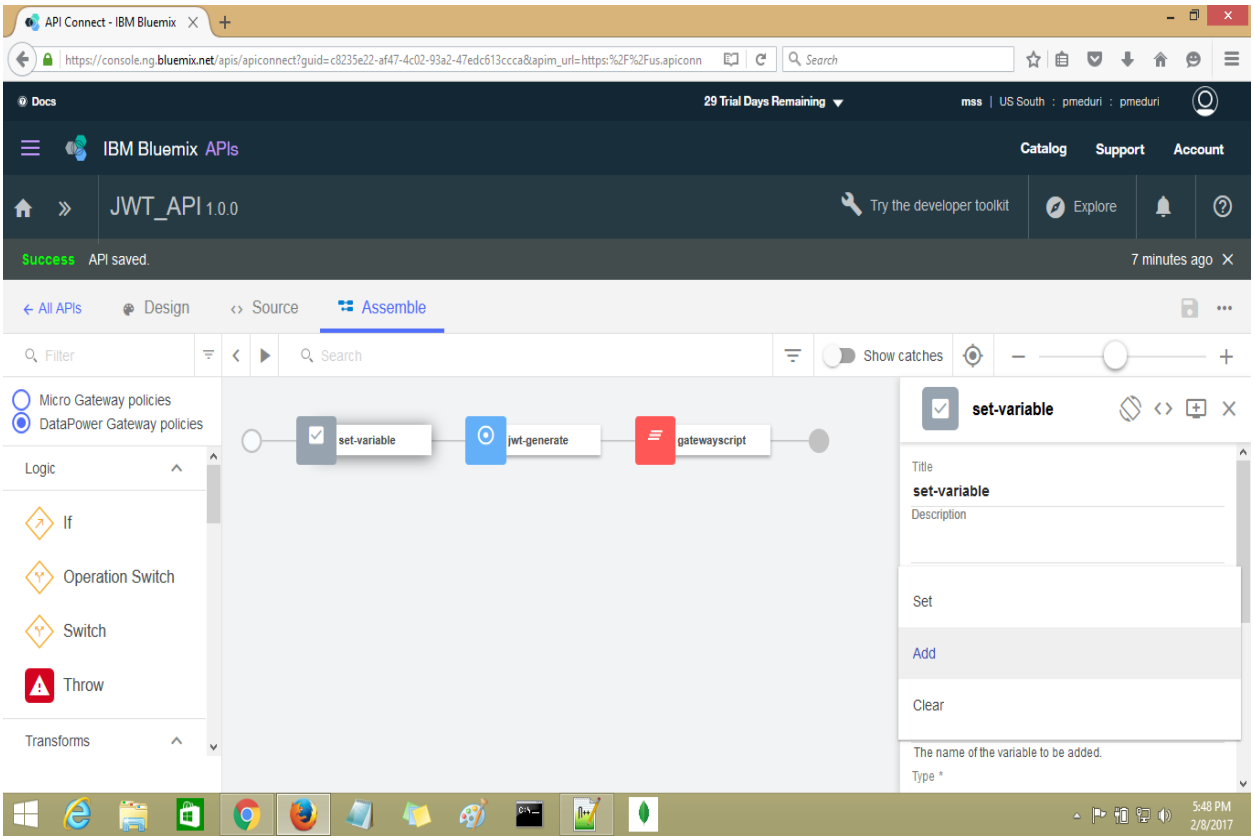
- Reserved Claims
- Public Claims
- Pravite Claims

3.SIGNATURE

Before going to the Generating and Validating the JWT first We need to refer the SET VARIABLE policy and GATEWAY SCRIPT POLICY.

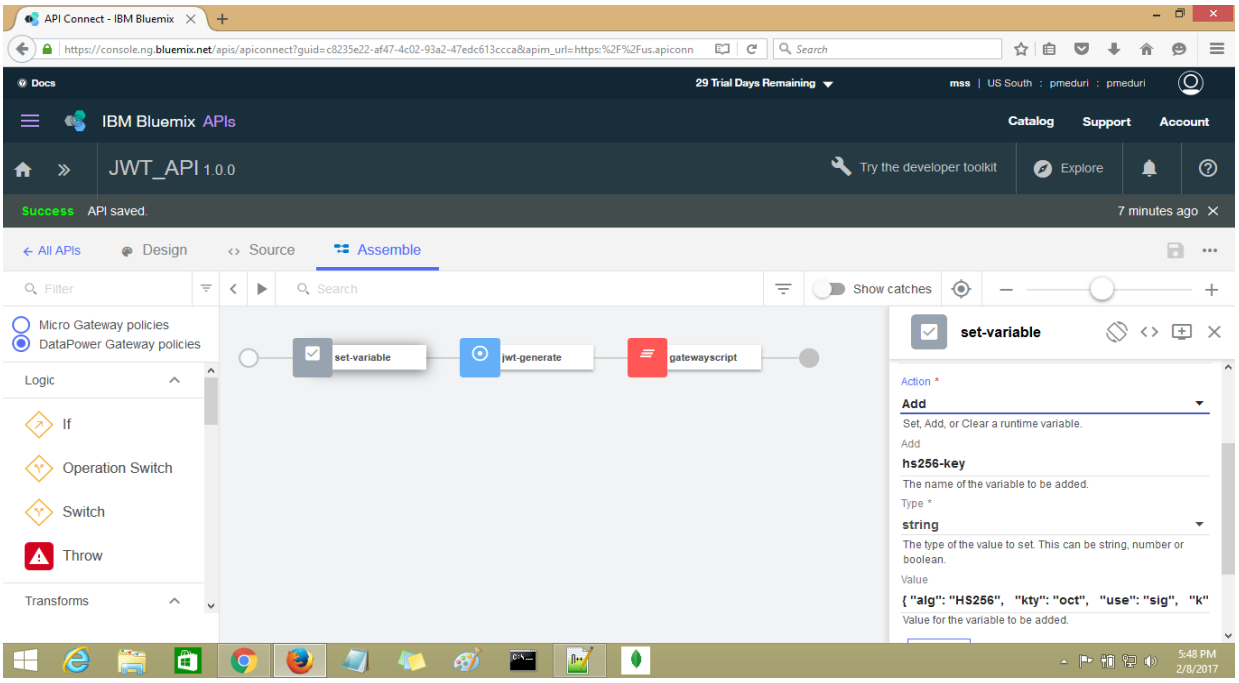
SET VARIABLE POLICY:

USE:
we can use set variable policy to set a runtime variable a string value, or to add or clear a runtime variable.



In the Set Variable policy there is action type which is requeried to SET or to ADD or to Clear[to delete].

For Generate or validate JWT we can use Add as the Action type.



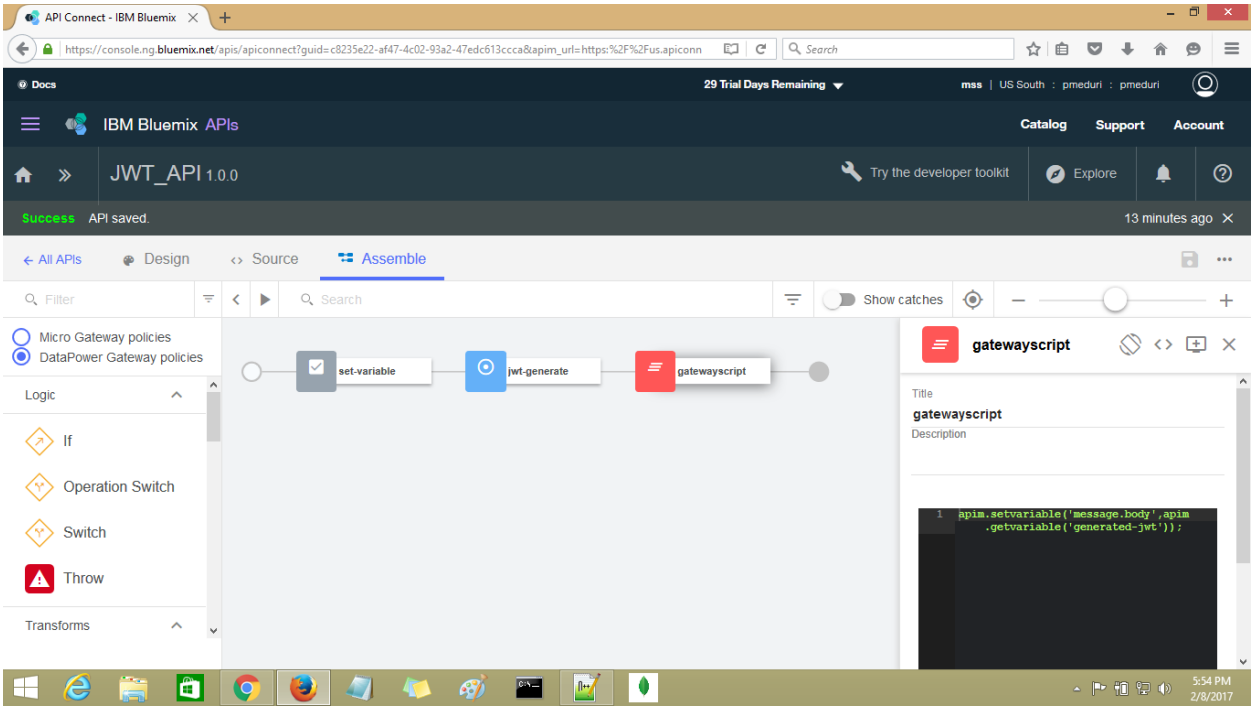
Here we can Spicify the Name of the variable to be added,
Select the type of the data we are adding to the payload,
We can use the value which is generated from the HS 256 Algorithem.

This Set Variable policy is used to Store the Data which is used store the particular Algorithem we are using.

Note:This set variable policy same for generate and Validate JWT key.

GatewayScript policy:

We can use gateway script policy to execute spicified Datapower GatewayScript program.
For Every operation we need to write the Spicified Scripting.
For Eg:



Now we can move to Generate JWT Policy.

Generate JWT policy:

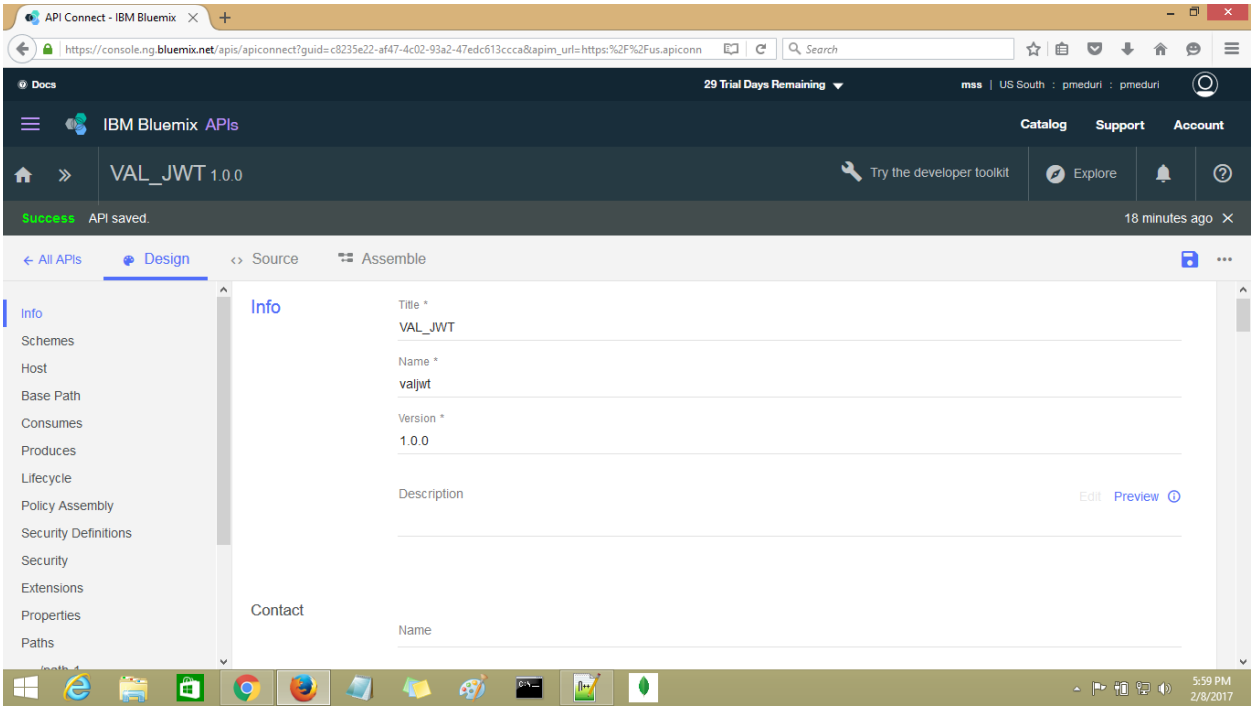
Generating JWT policy can be used to both REST and SOAP api's,Here I am Using the REST api.

Composing REST api:

For that we need to sign in to bluemix account,

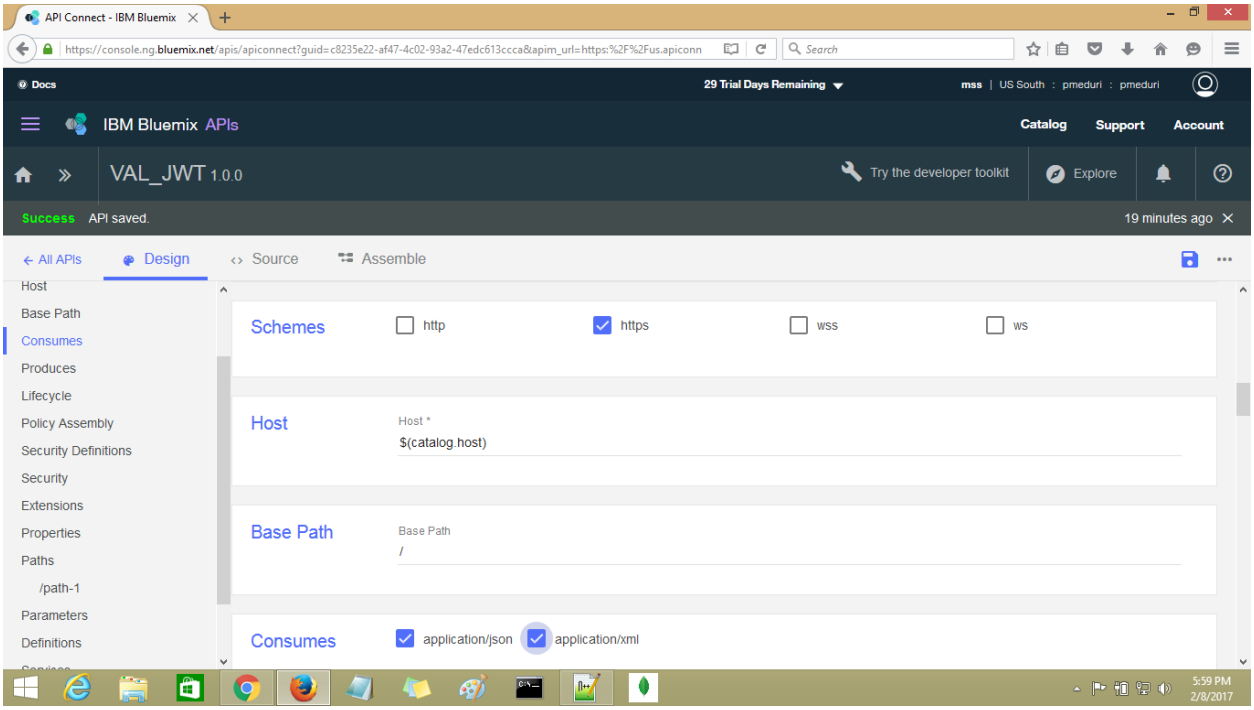
GO for +API,and select the New API

then the promt will be open

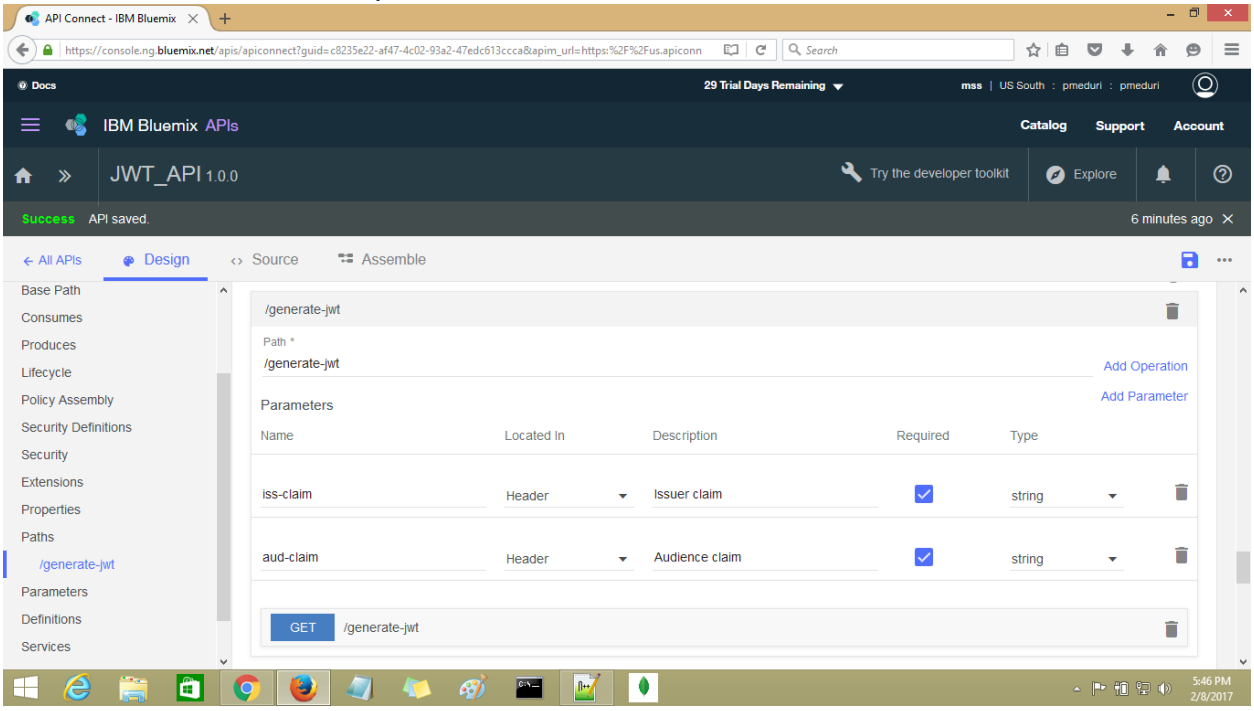


Here we can give the TITLE of the API,and make sure that Basepath will be Empty.

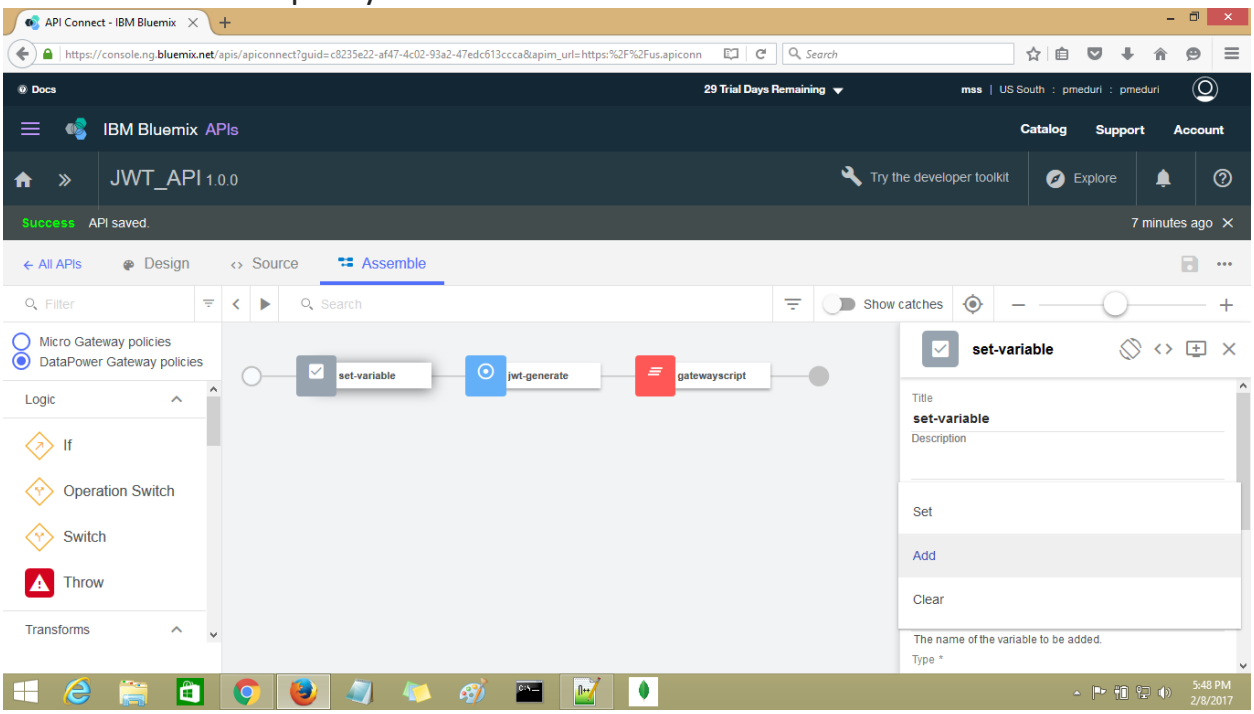
Select the Schemas as https and content type of the Api can be both JSOn and XML.

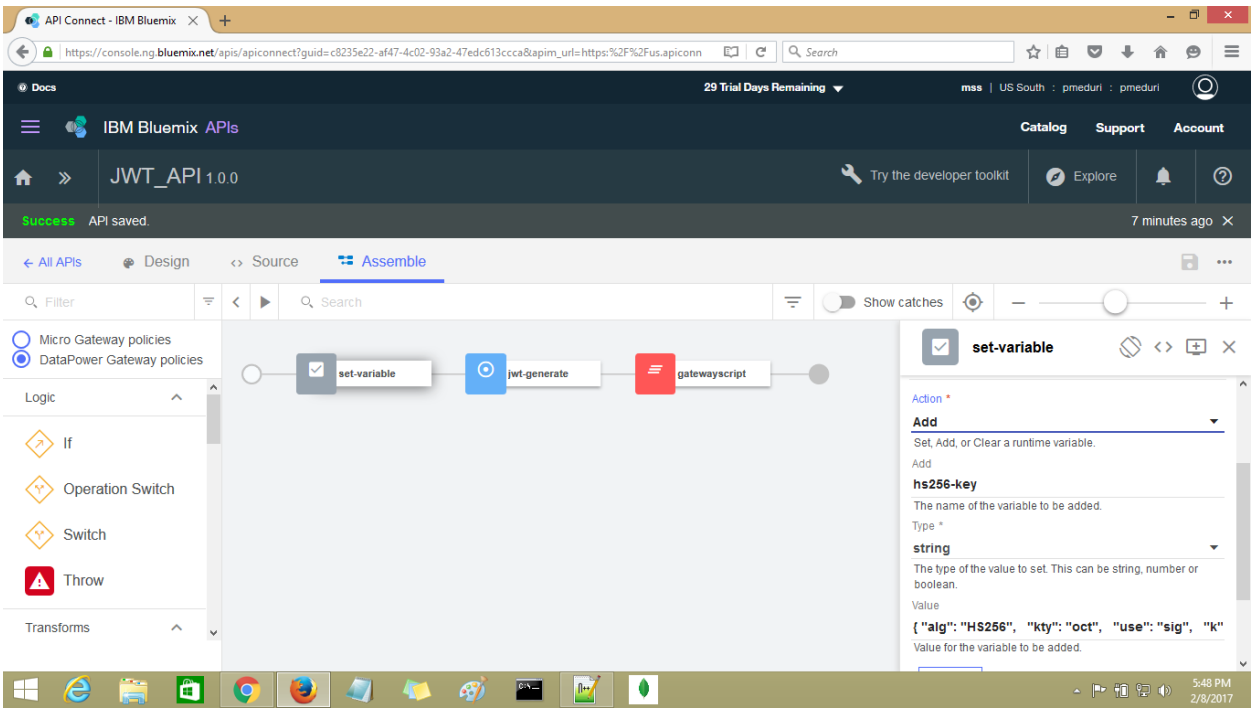


In the paths field we need to create the GET/generate_JWT
After that I we need to create the parameters for ISSUER claim and Audience Claim and make it as Required.



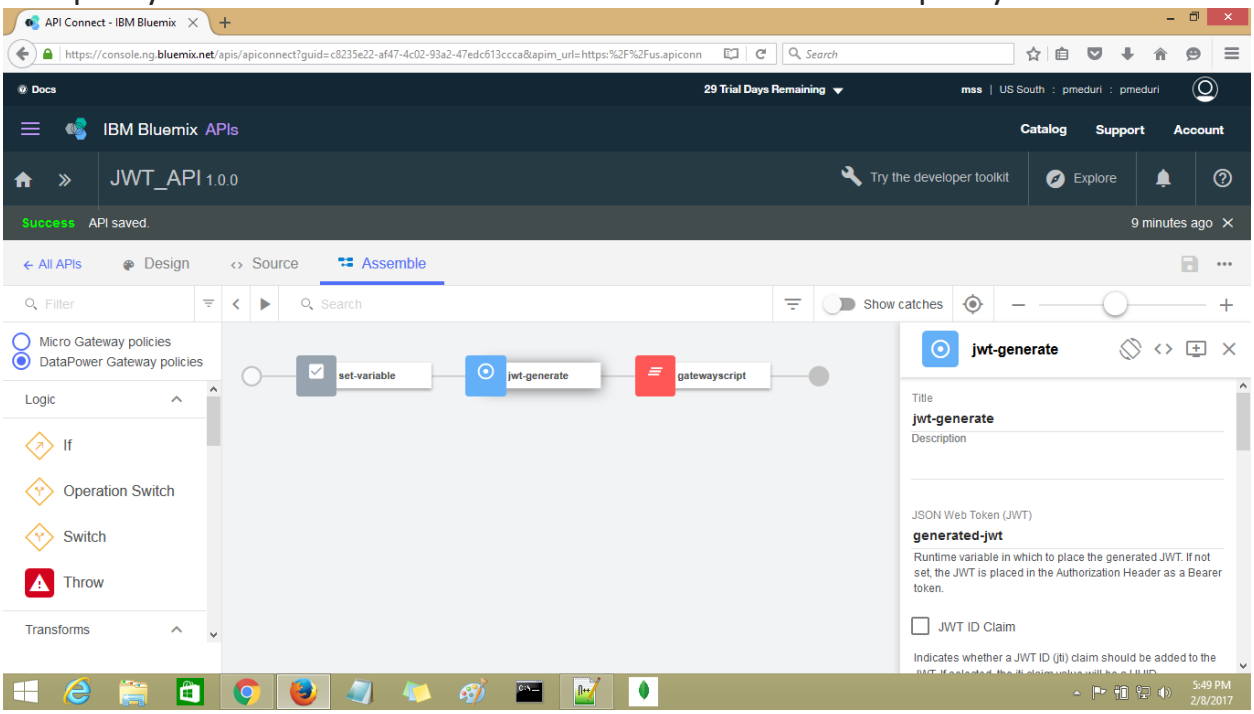
For generating the JWT we need to set the data regarding encodeing algorithem in the SET variable policy as we mentioned above.



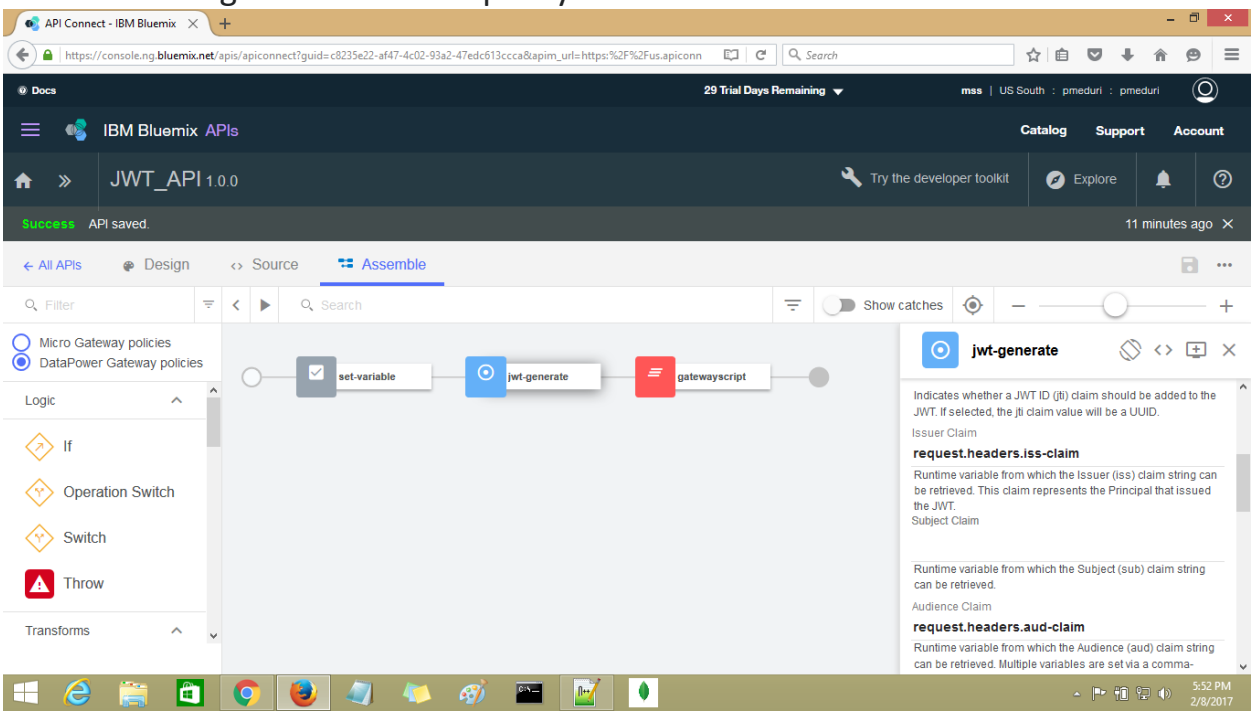


Generate JWT:

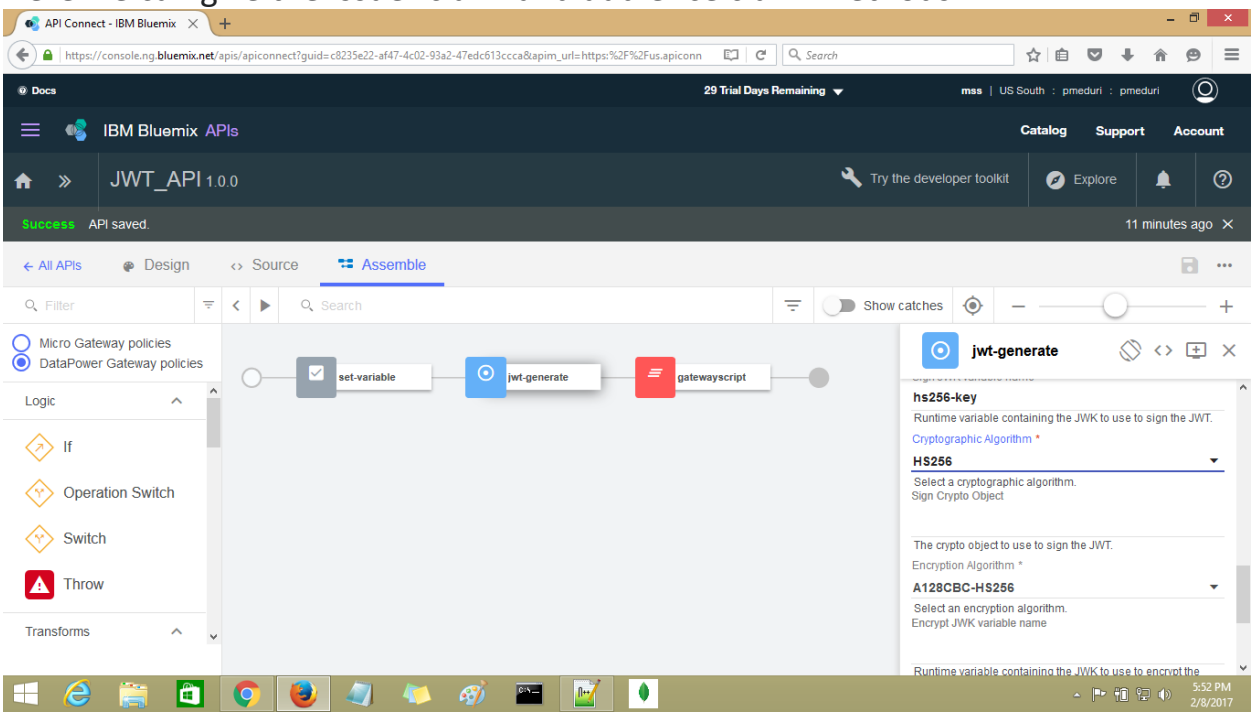
This policy can be attached to the flow after the SetVariable policy.



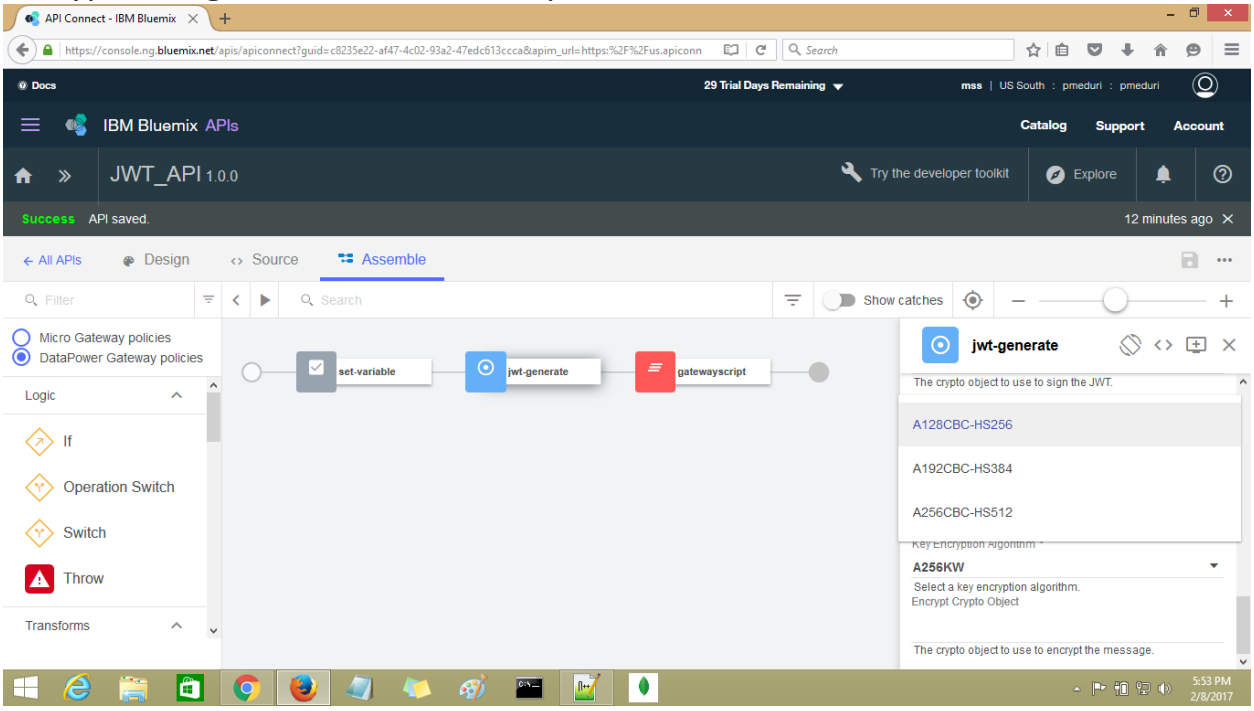
In this we can give name of the policy and JSON Web Token Name.

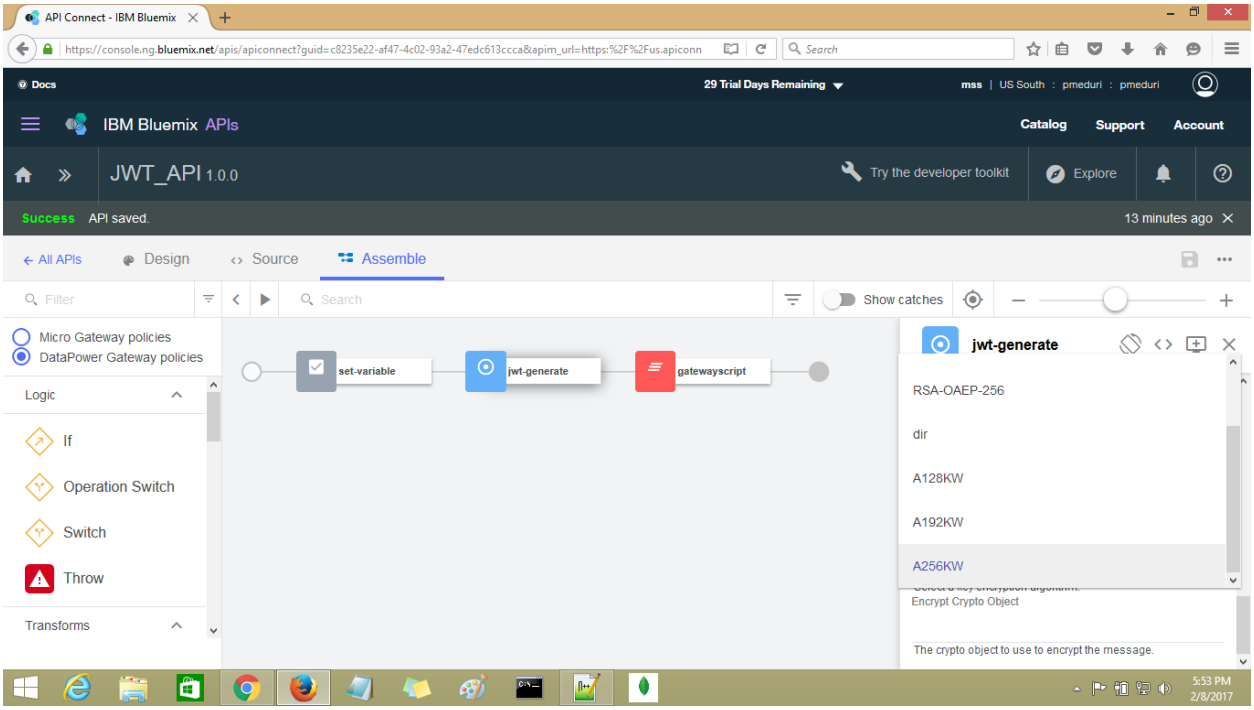


Here we can give the Issuer claim and audience claim methods.

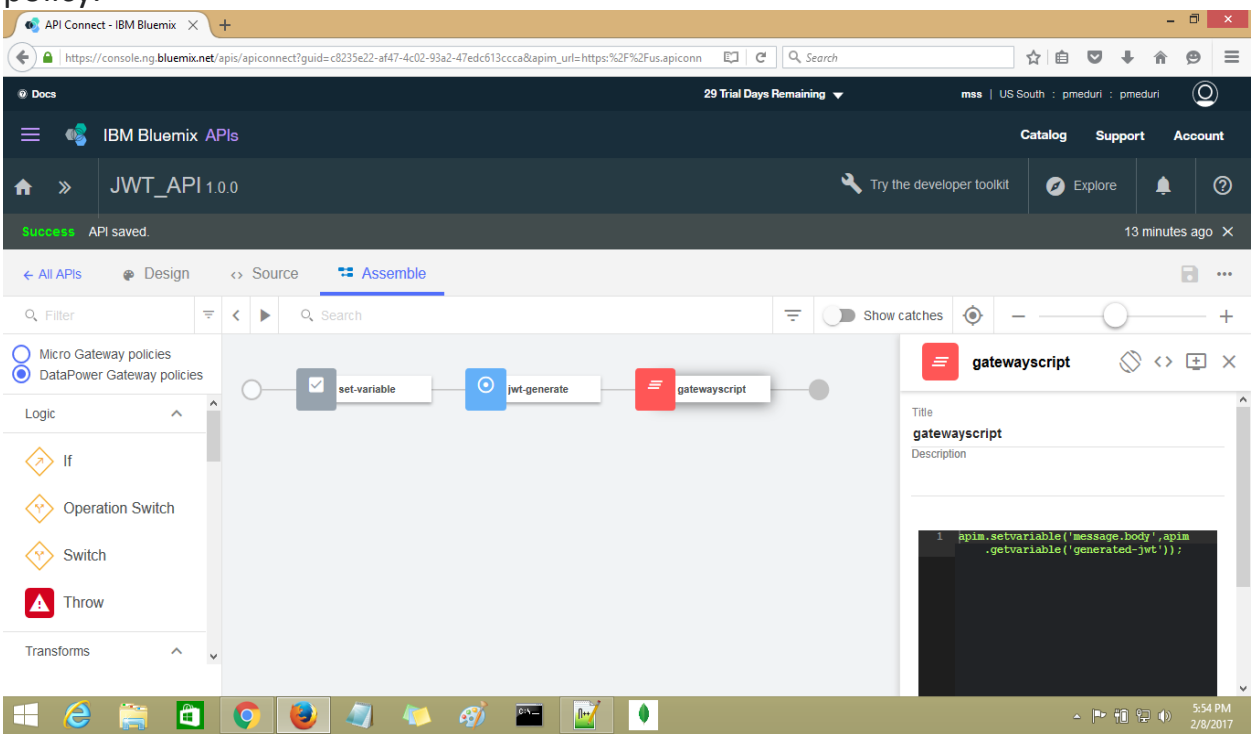


After that we need to select the required Cryptographic Algorithem and Encryption Algorithem from the dropdown menu.





The genereted Encrypted token can be displayed by using the GatewayScript policy.



In the Gateway Script policy we can write java script to retrive the generated jwt from the Mesage body.

After completion of these steps click on SAVE button,and republish the product.

After that select the GET/validate_jwt definition

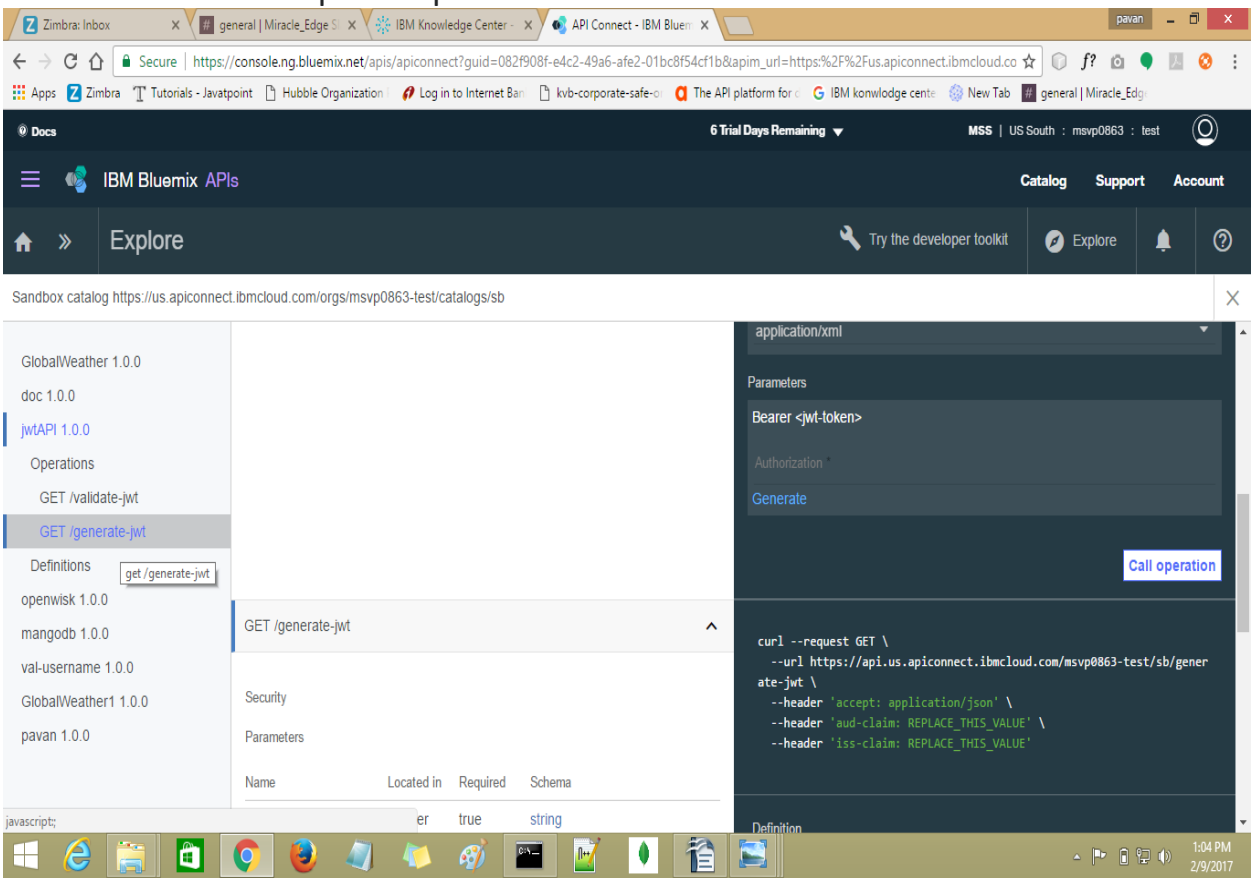
here Iam using **apic** as issuer claim and **id** as Audience claim.

Now click on INVOKE button.

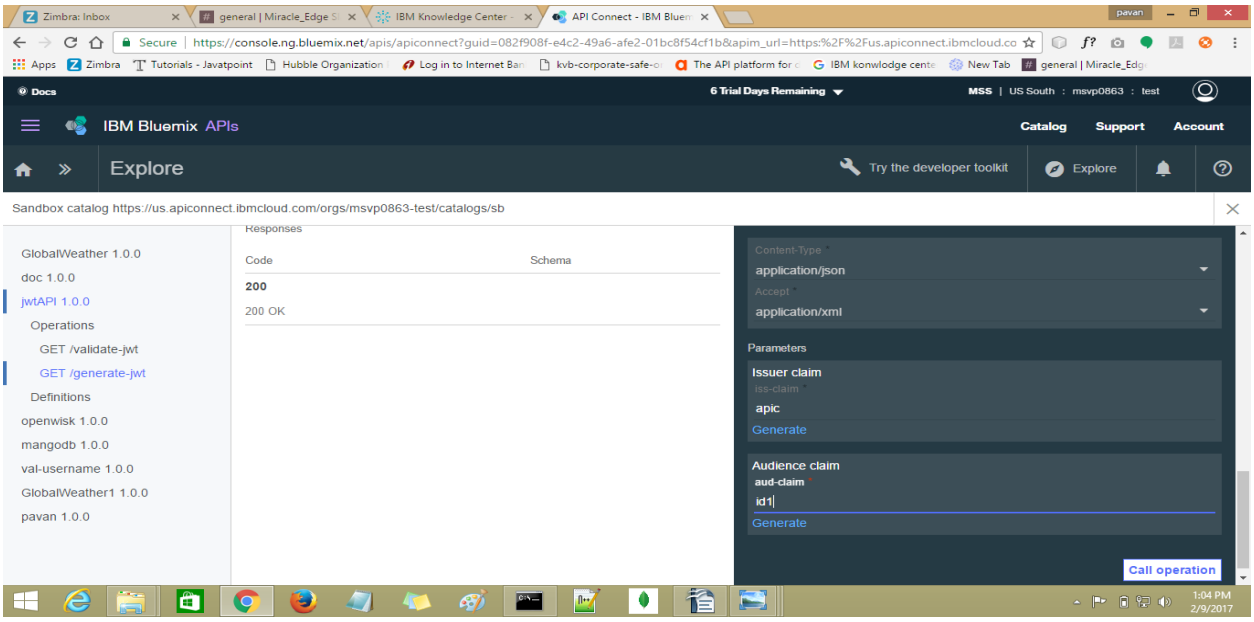
Then the respnse will be shown . or

Select the EXPLORE button click on Sandbox

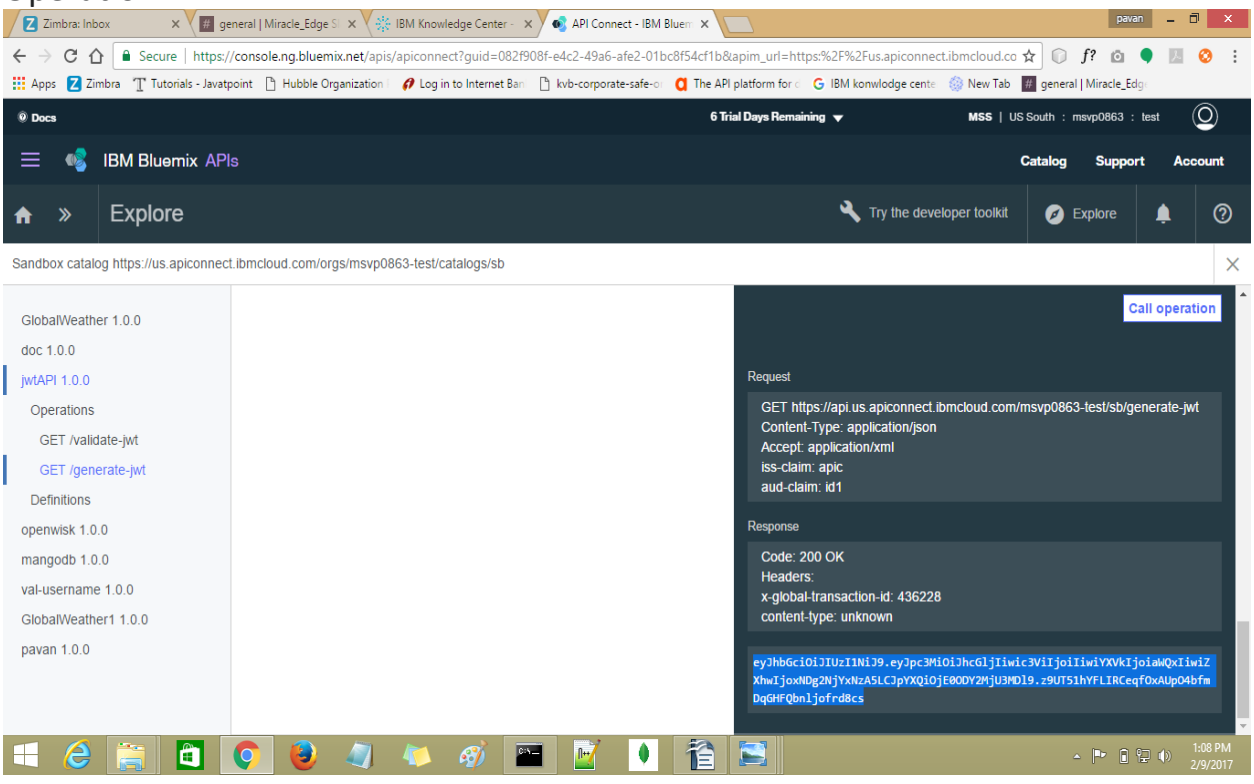
in that select the required api from the list.



Select the required definition from the list.



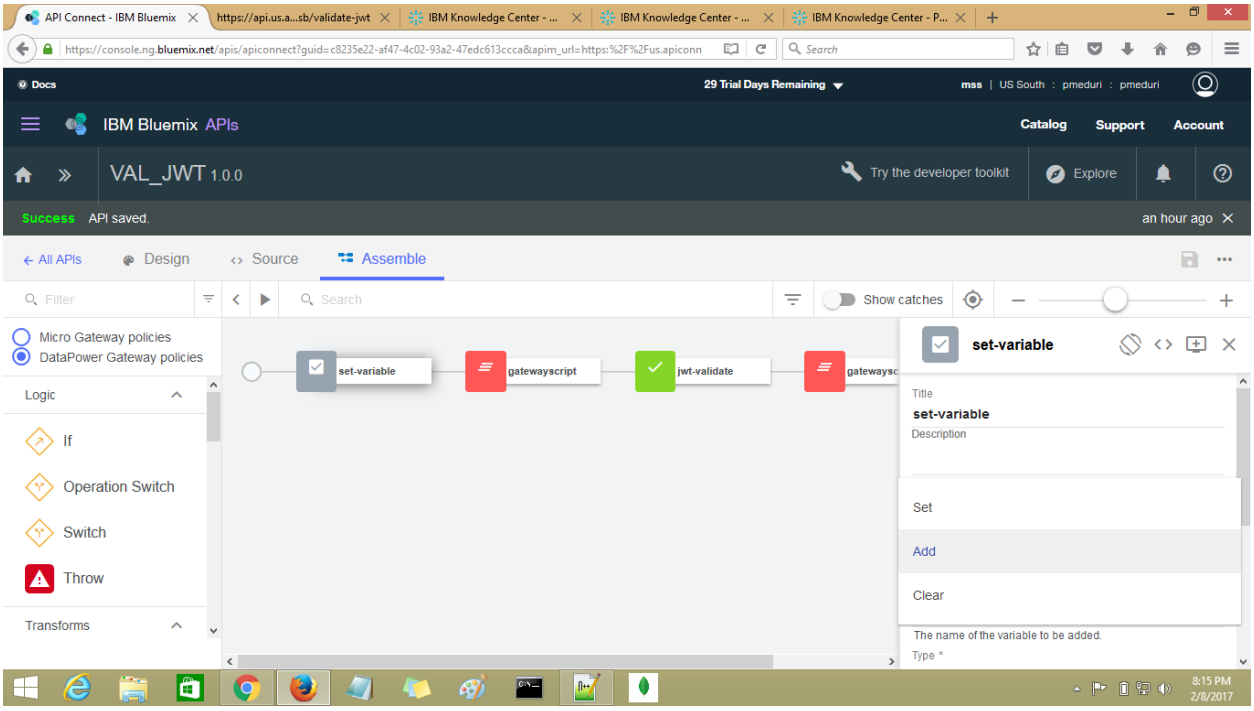
In the Issuer Claim give value as **apic** and Audience Claim as **id1**,and click on Call Operation.

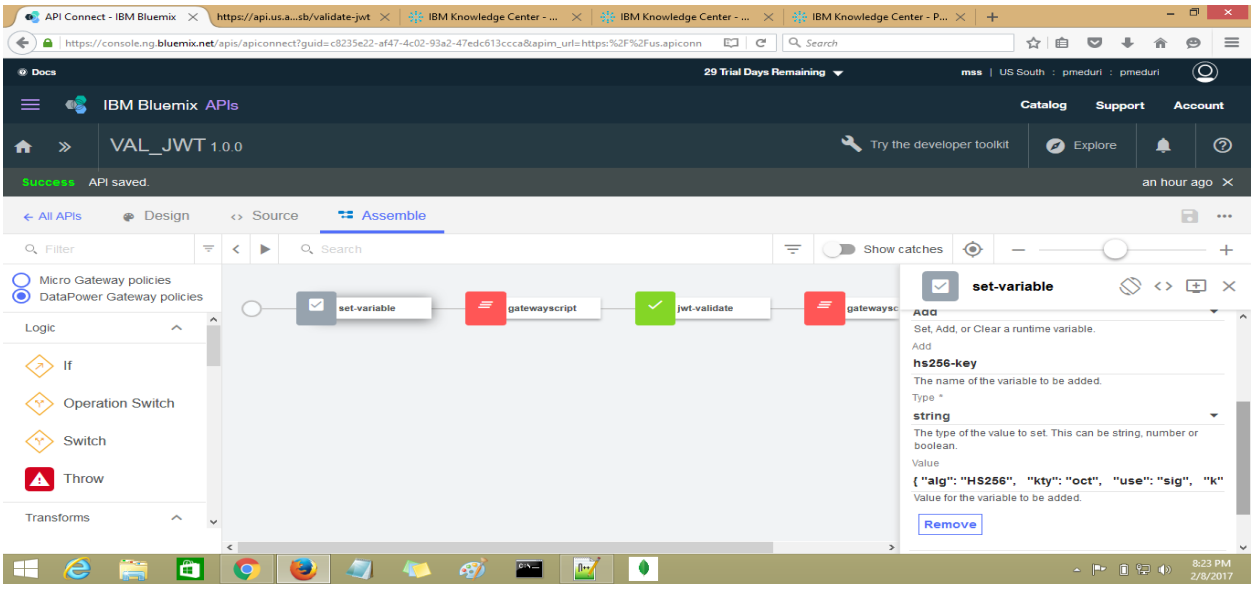


Validate_JWT:

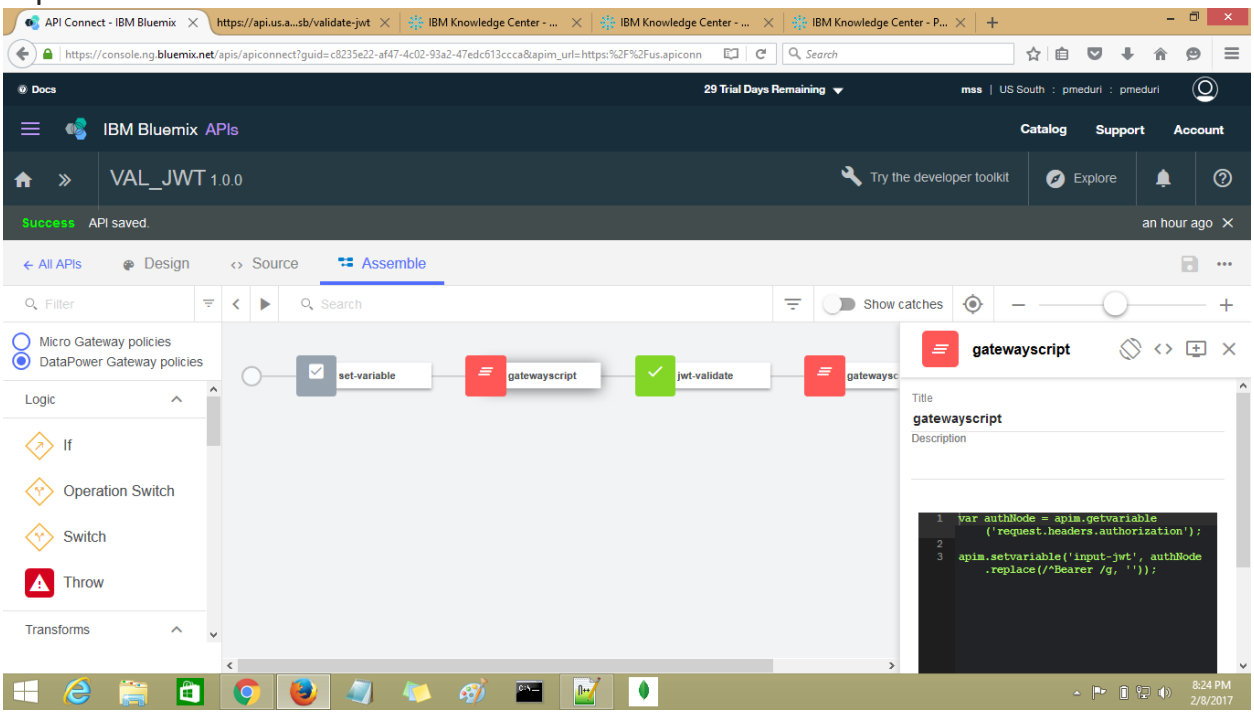
To perform the JWT validations first we need to add the variables or data to SetVariable based on the HS256 algorithem.

SetVariable which I was configured in the Generated JWT is same.





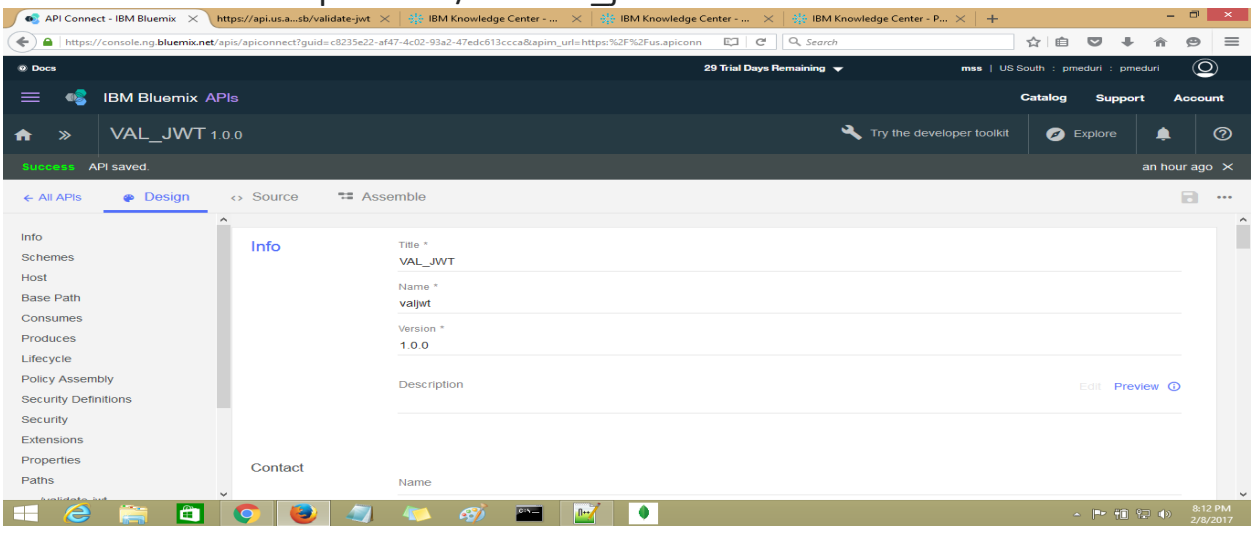
After that we can create the GatewayScript policy to retrive the genrate_jwt and replace with the **Bearer**.

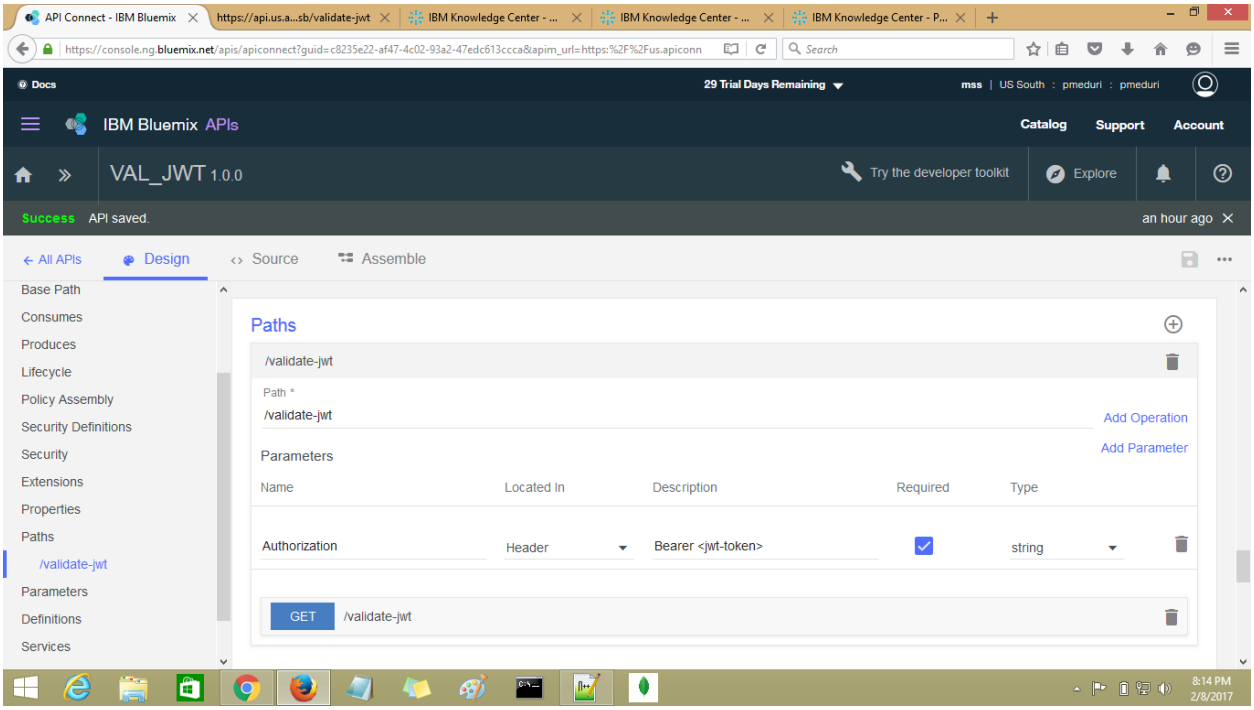


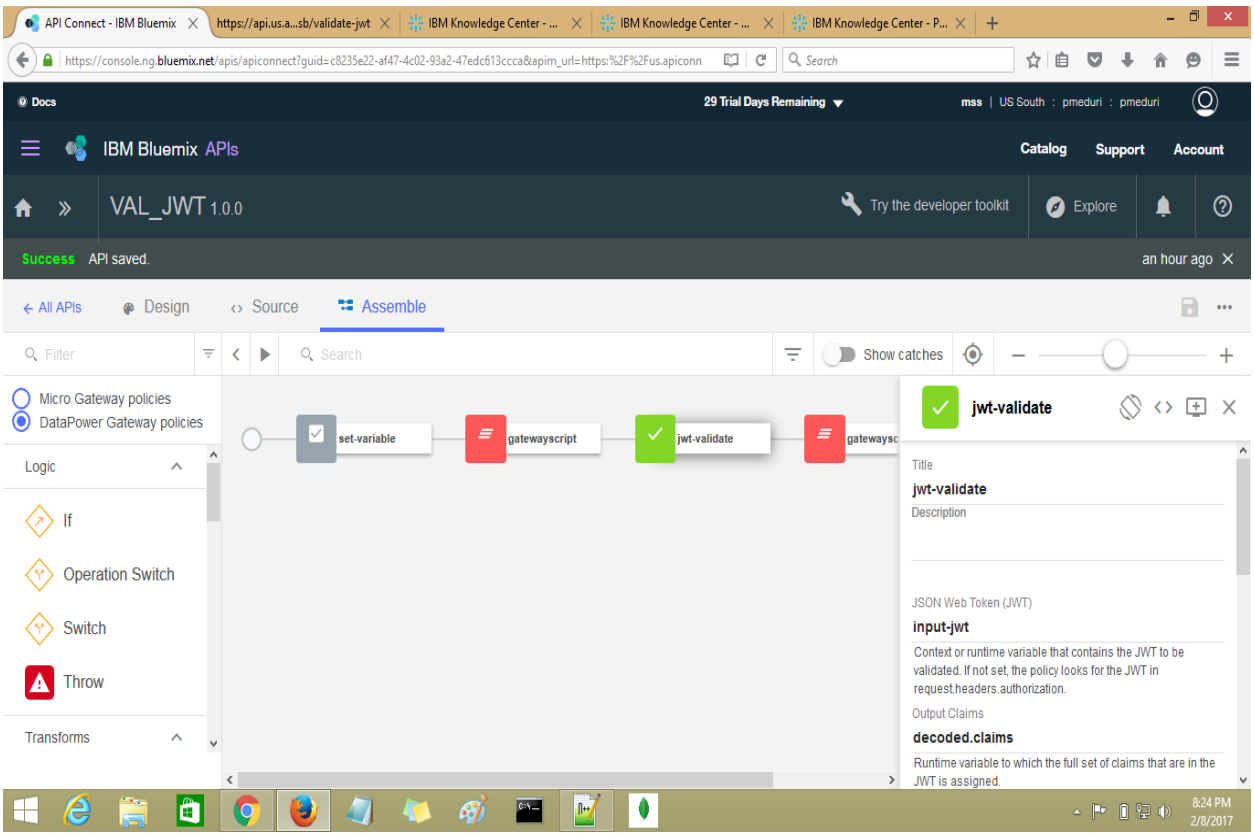
After getting the variable from the gatewayscript plicy it can be transferred to the jwt_validate policy.

Composing validate_jwt:

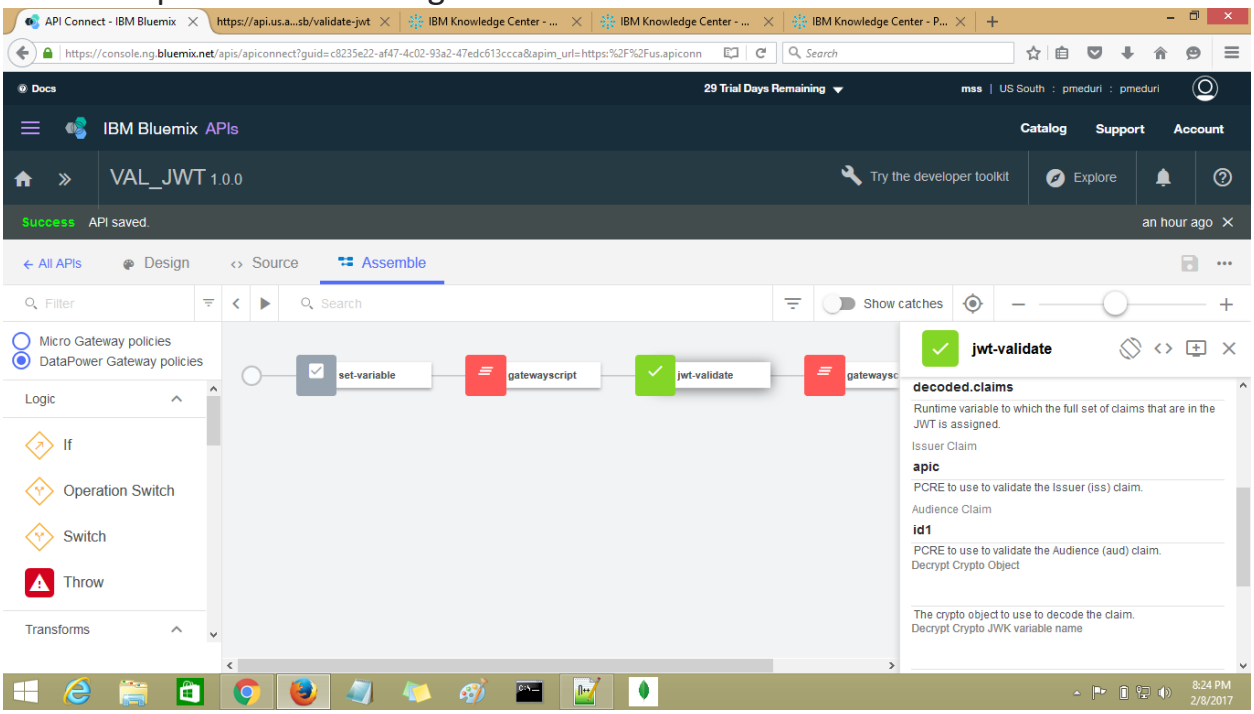
In the generated_jwt policy we composed REAT api,like that in the definitions field we can add the path GET/validate_jwt.



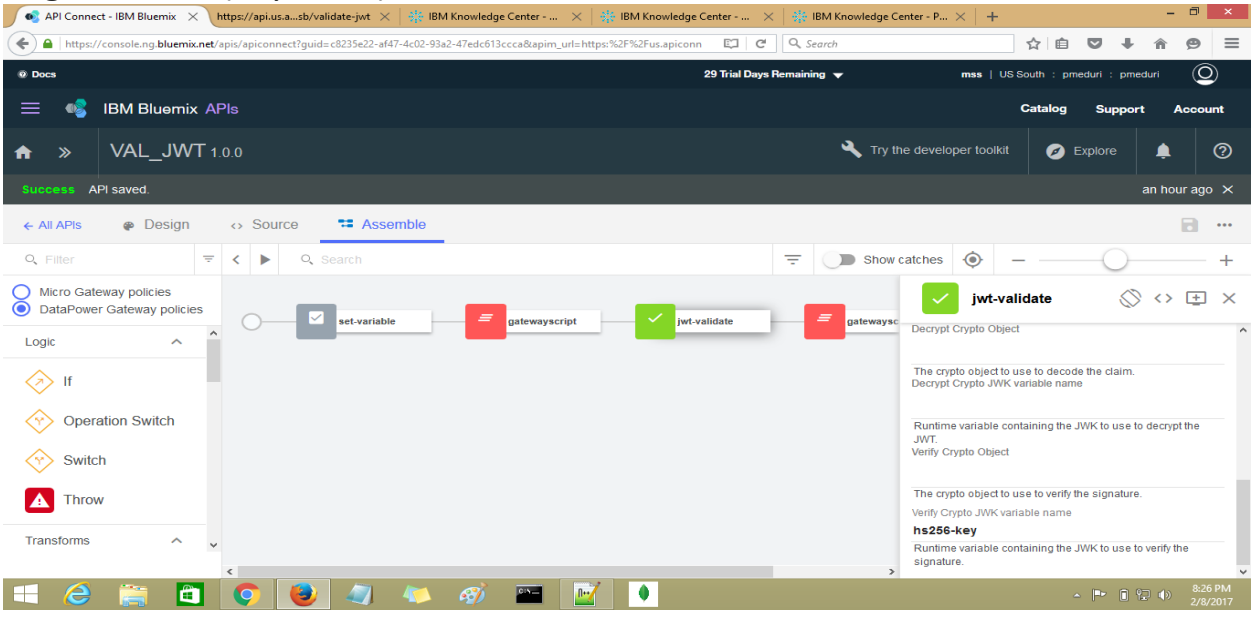




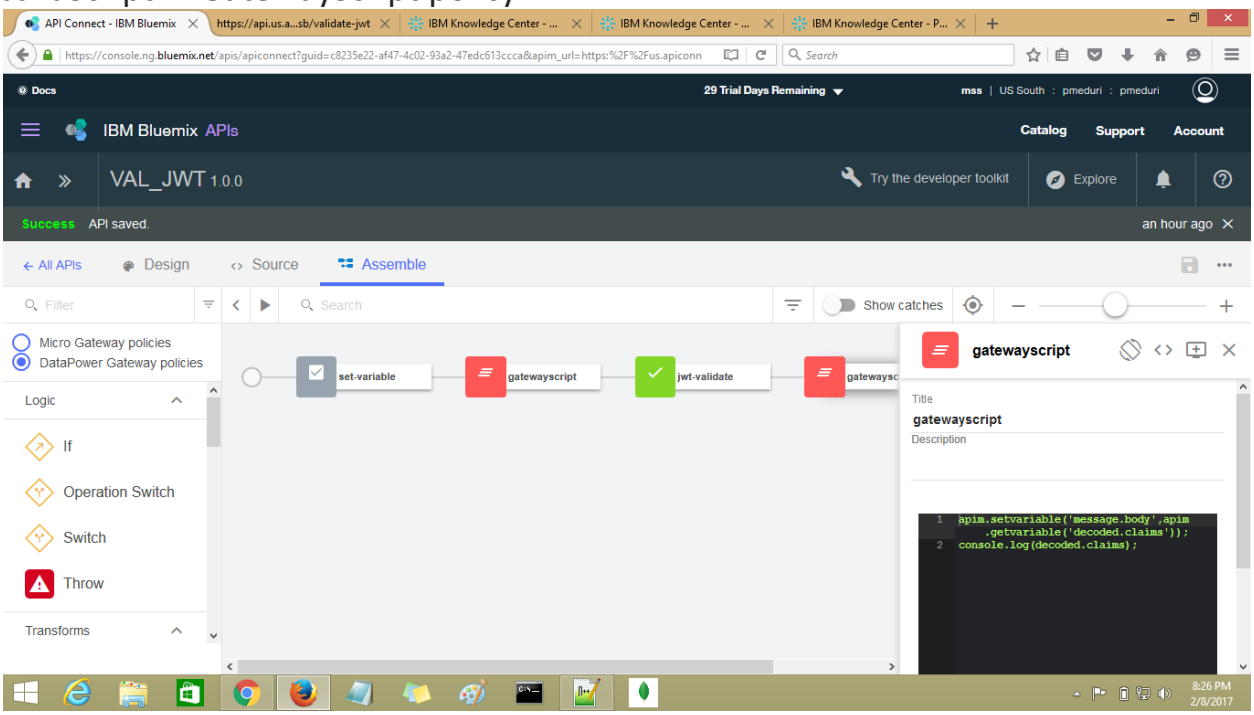
In the JSON web Token we need to give the name to store the value in the enctypted format which need to be Decoded.
In the Output claims will be given as decoded-claims .



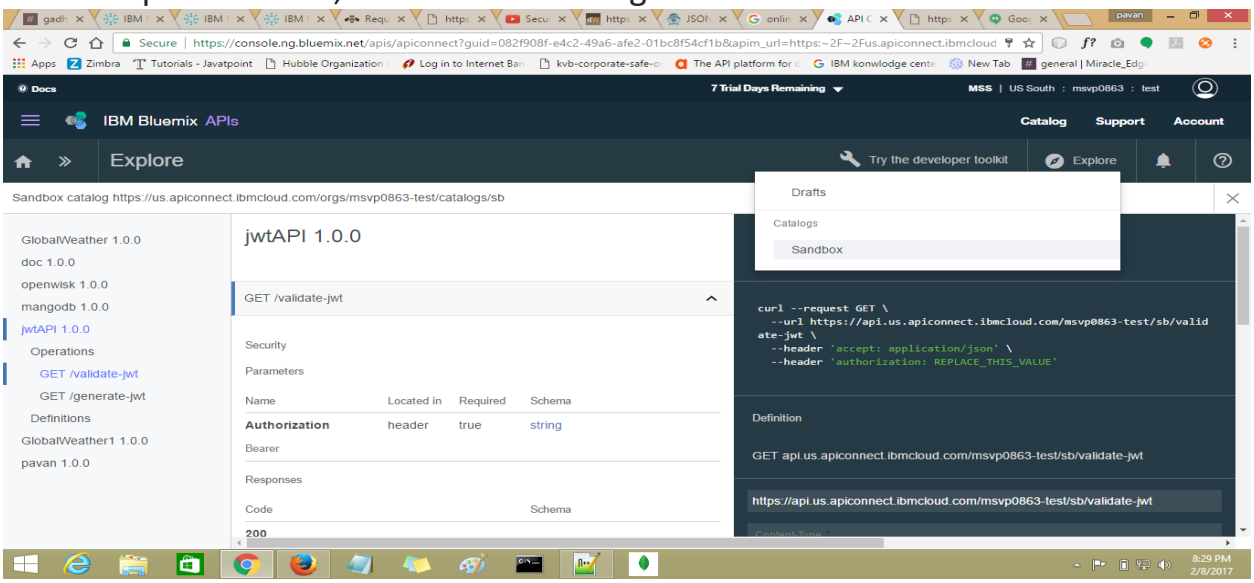
In the Issuer Claim we can give value **apic** (any value)and Audience Claim we need to give the **id1**(any value).



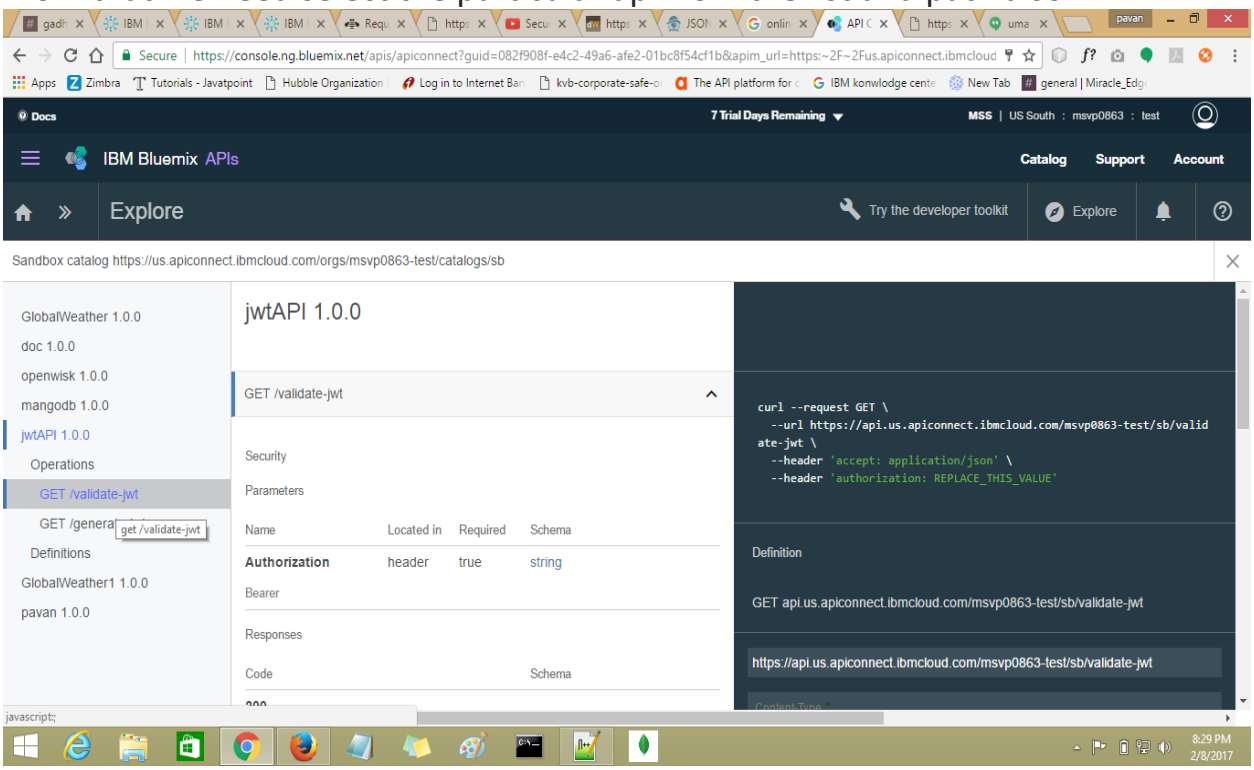
Verify crypto variable name can be given as the hs256-key.
The validated message body can be stored in gatewayscript policy.From that message we need to retrive the decoded-claims.For that we need to write JavaScript in GatewayScript policy.

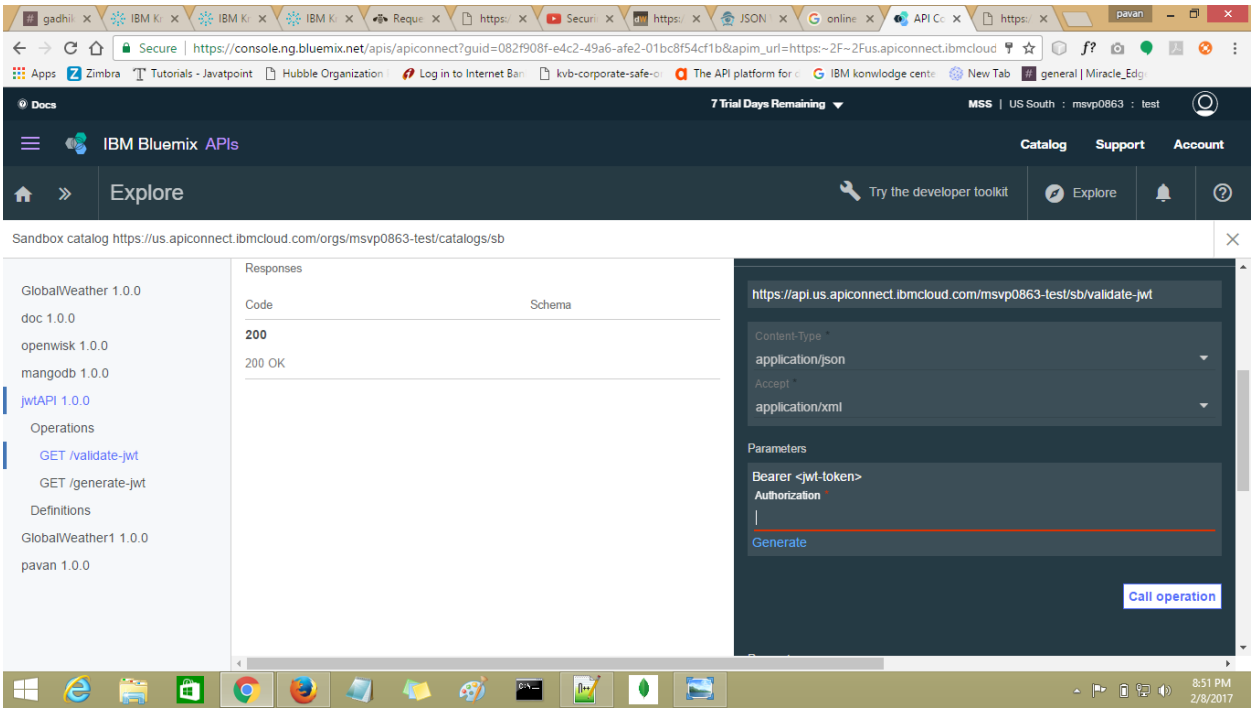


After complition of these steps click on SAVE button.
Go for Explore Button,in that we need to go for Sandbox.

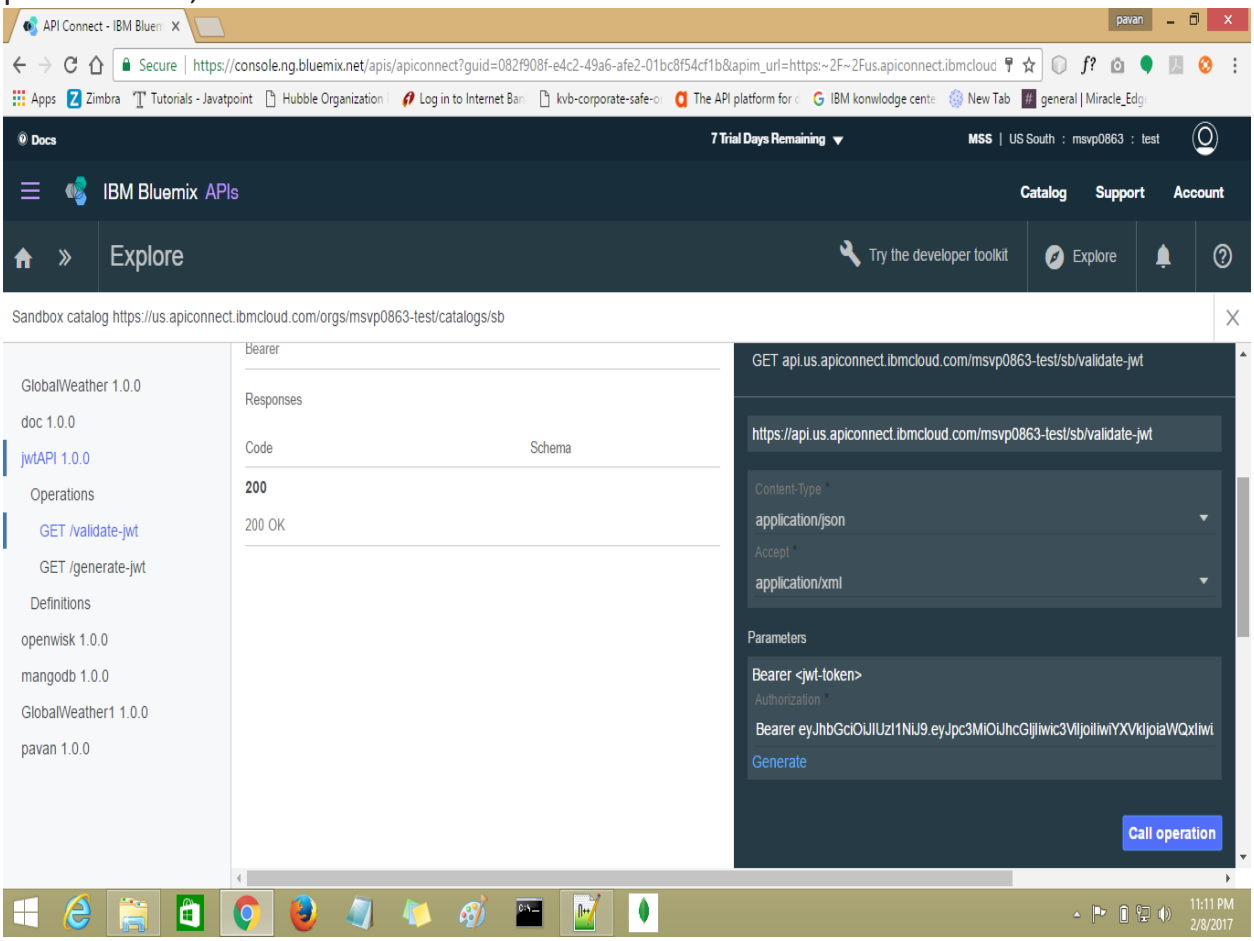


From that we need select the particular api from the list and path also.





From that to call that operation we need to give Generated JWT code from the privious one,it can like



Then click on Call operation.

Then the output will be