

JSON WEB TOKENS

Generete and Validate Policies

PavanKumar Meduri

09-02-2017

Api Connect Developer
Miracle Software Systems, Inc.

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 Algorithm we are following

2.PAYLOAD

The Payload contains three types of claims

- Reserved Claims
- Public Claims
- Private Claims

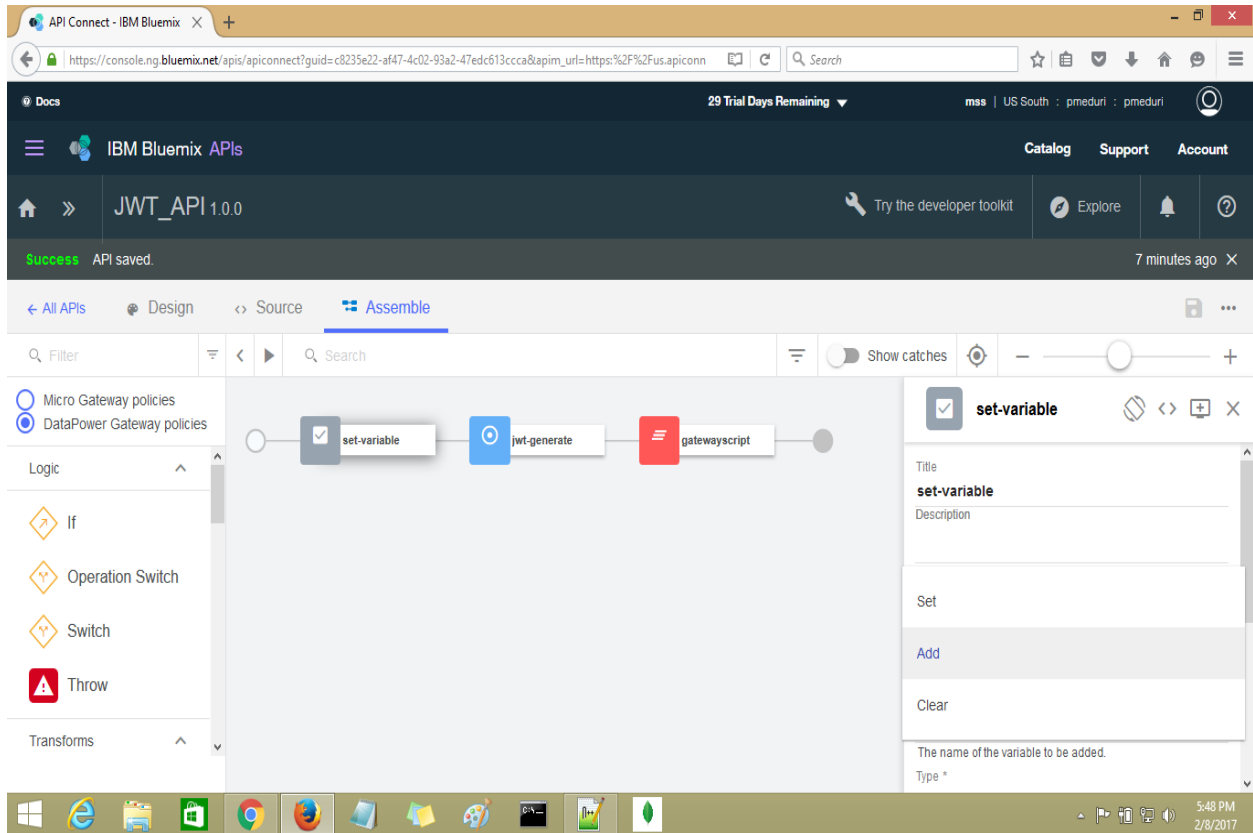
3.SIGNATURE

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:

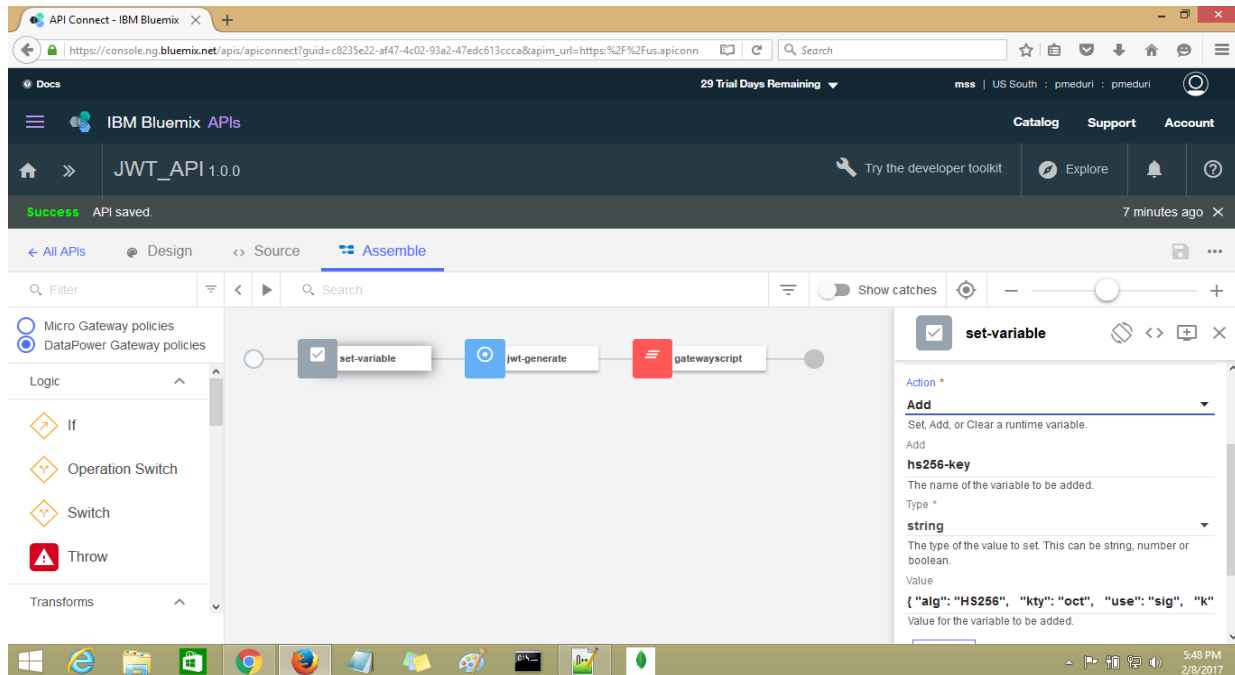
USE:

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 required 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 Specify 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 Algorithm.

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

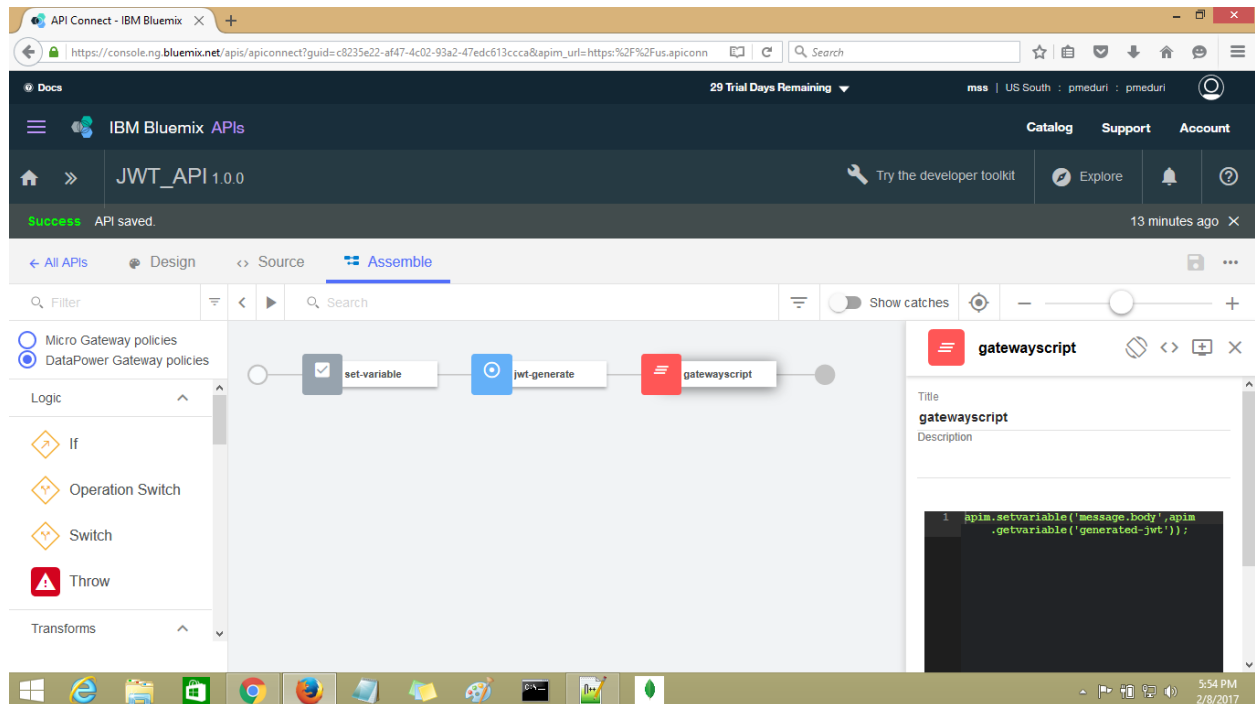
Note: This set variable policy same for generate and Validate JWT key.

GatewayScript policy:

We can use gateway script policy to execute specified Datapower GatewayScript program.

For Every operation we need to write the Specified Scripting.

For Eg:



Generate JWT policy:

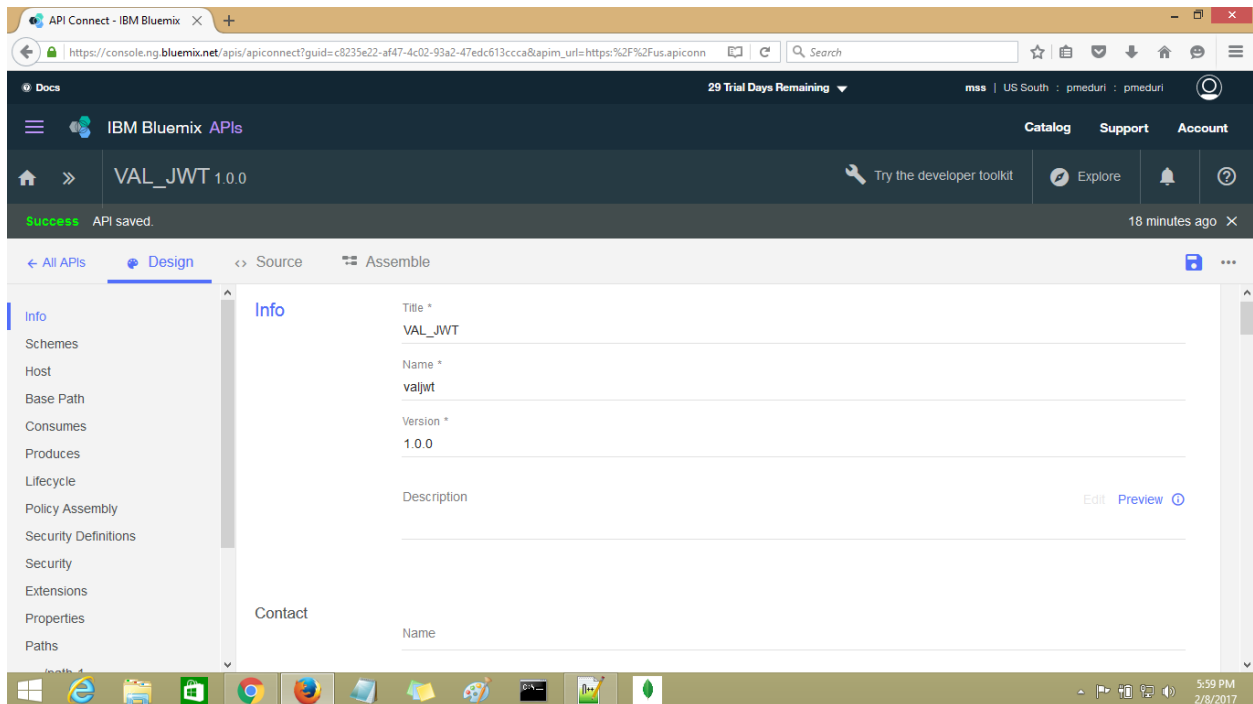
Generating JWT policy can be used to both REST and SOAP api's, Here I am Using the REST api.

Composing REST api:

For that we need to sign in to Bluemix account,

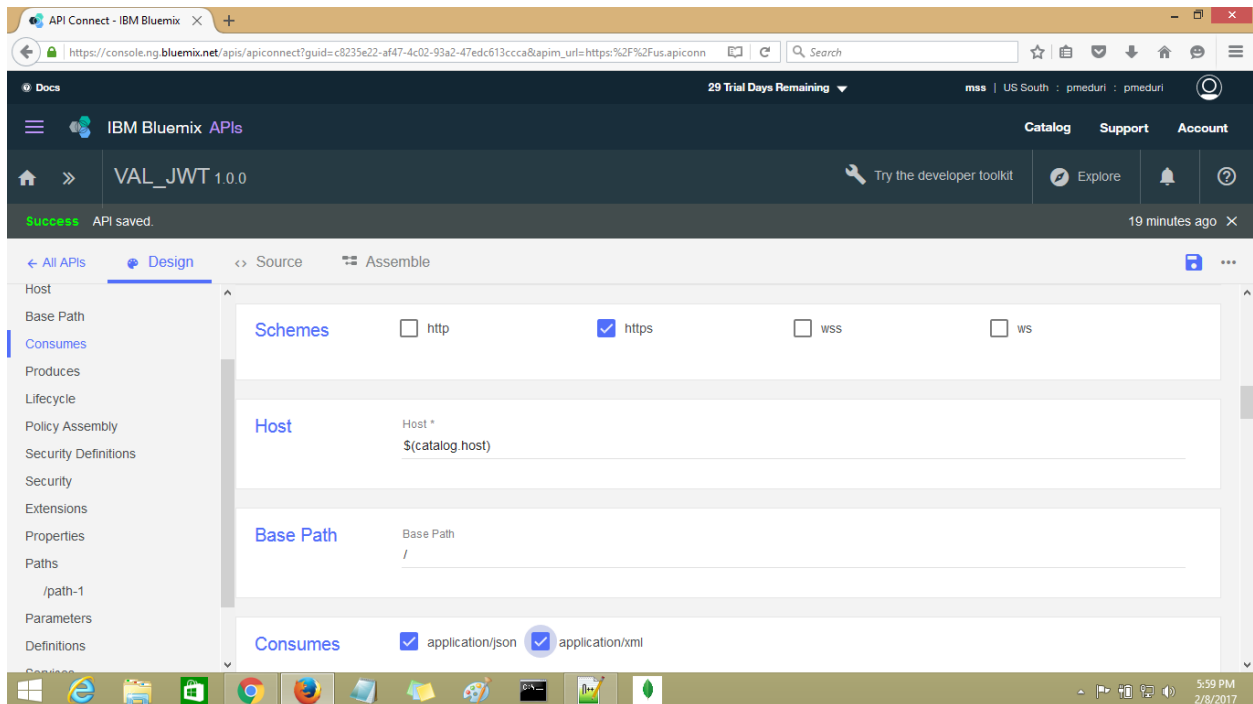
GO for +API, and select the New API

then the prompt will be open

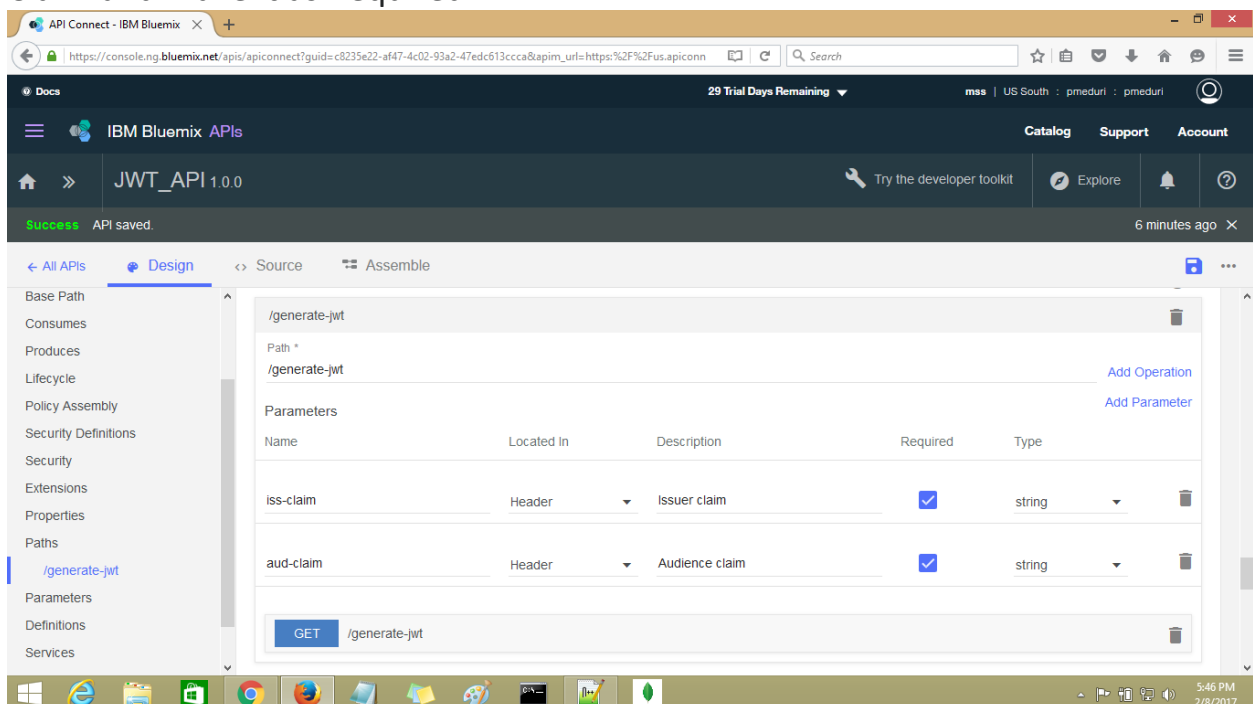


Here we can give the TITLE of the API, and make sure that Basepath will be Empty.

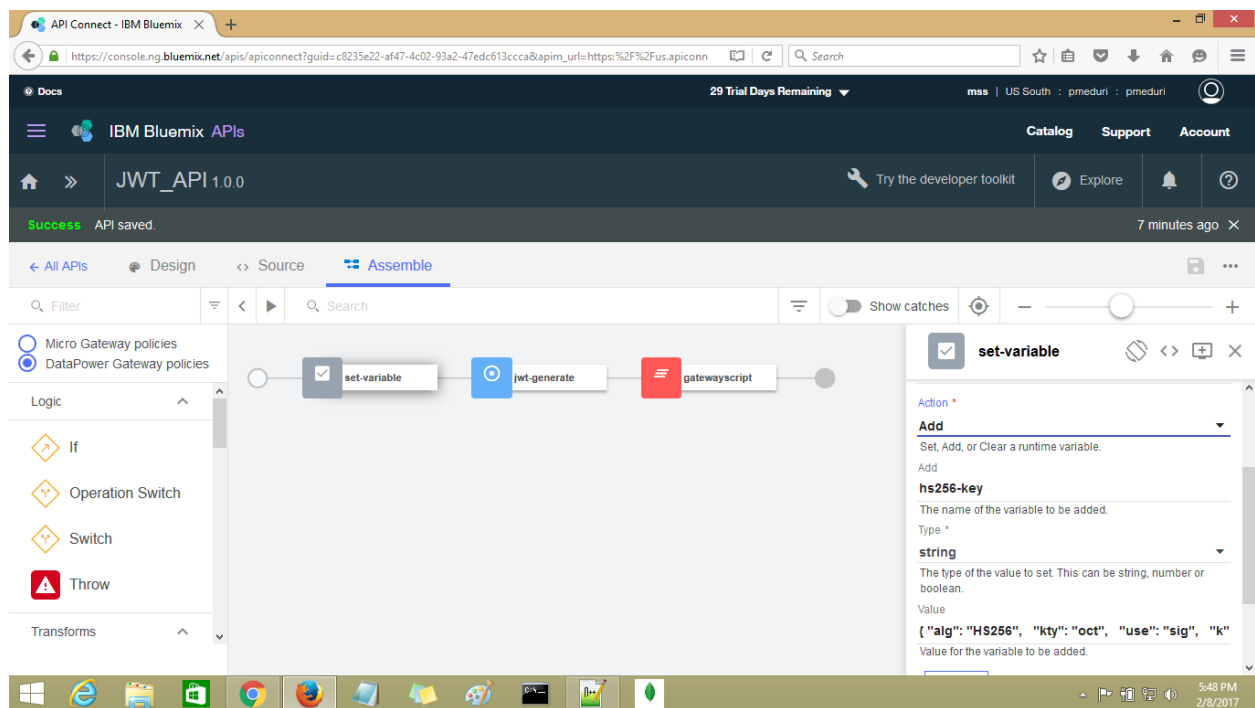
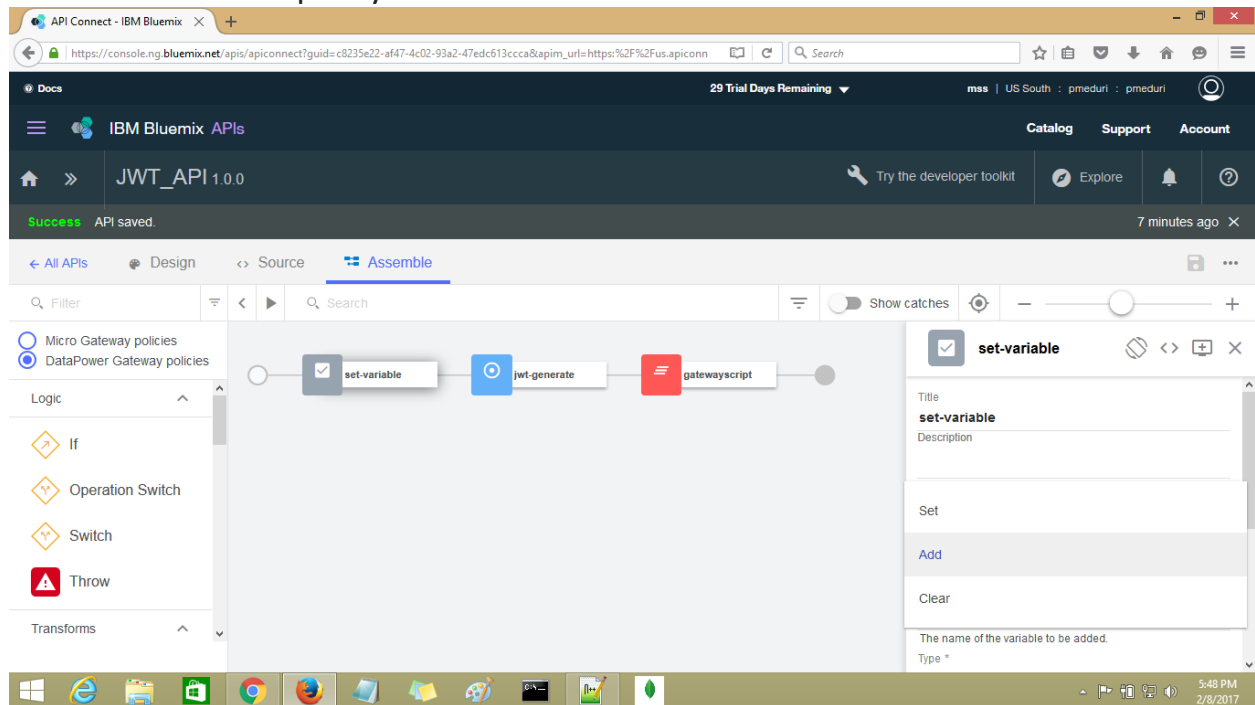
Select the Schemas as https and content type of the Api can be both JSON and XML.



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.

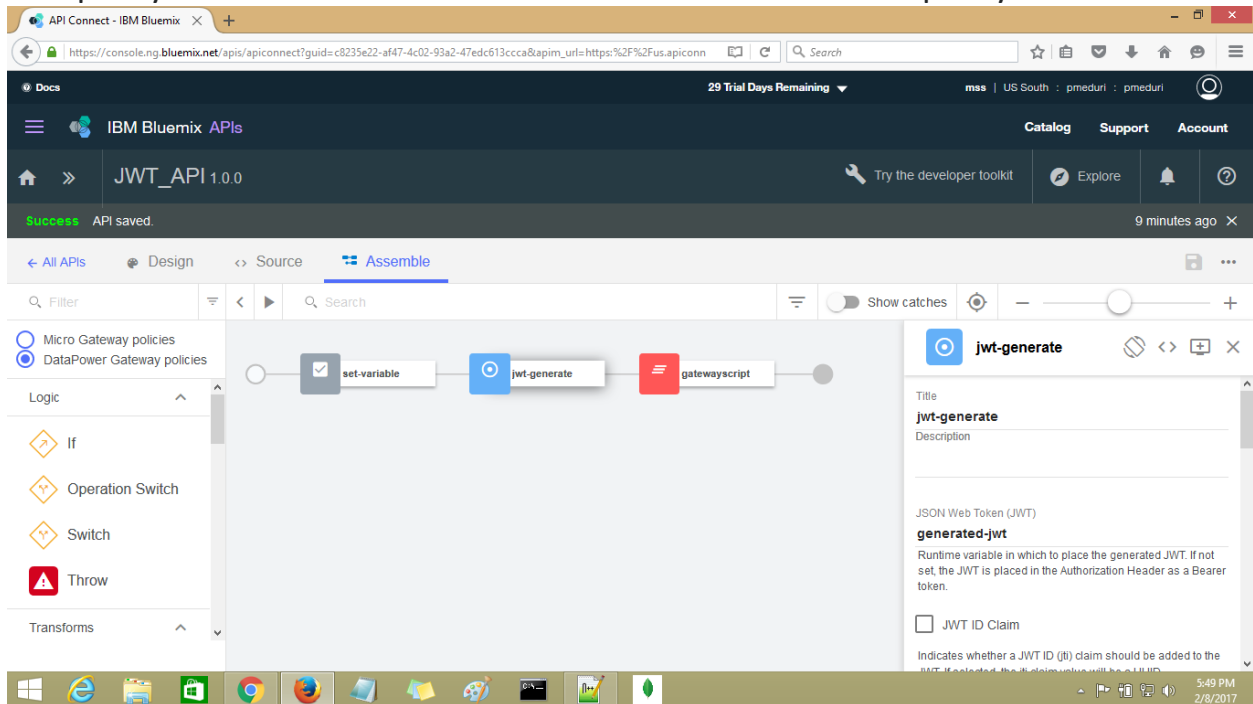


For generating the JWT we need to set the data regarding encoding algorithm in the SET variable policy as we mentioned above.

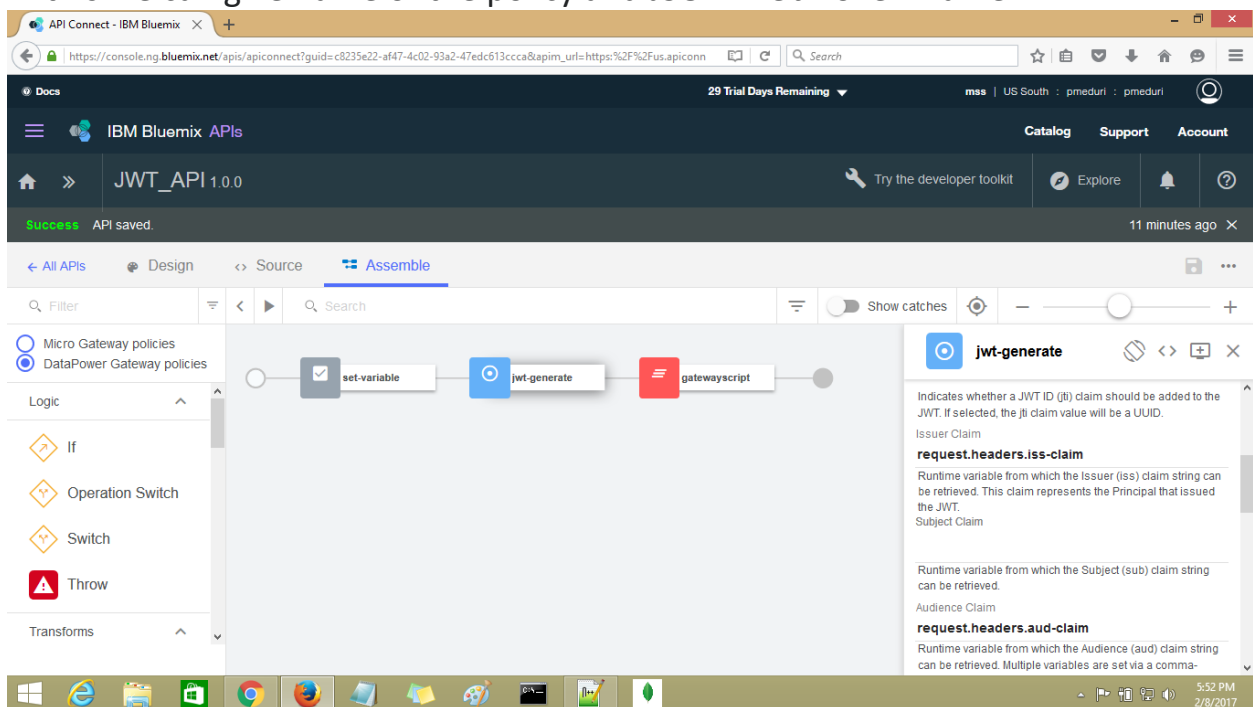


Generate JWT:

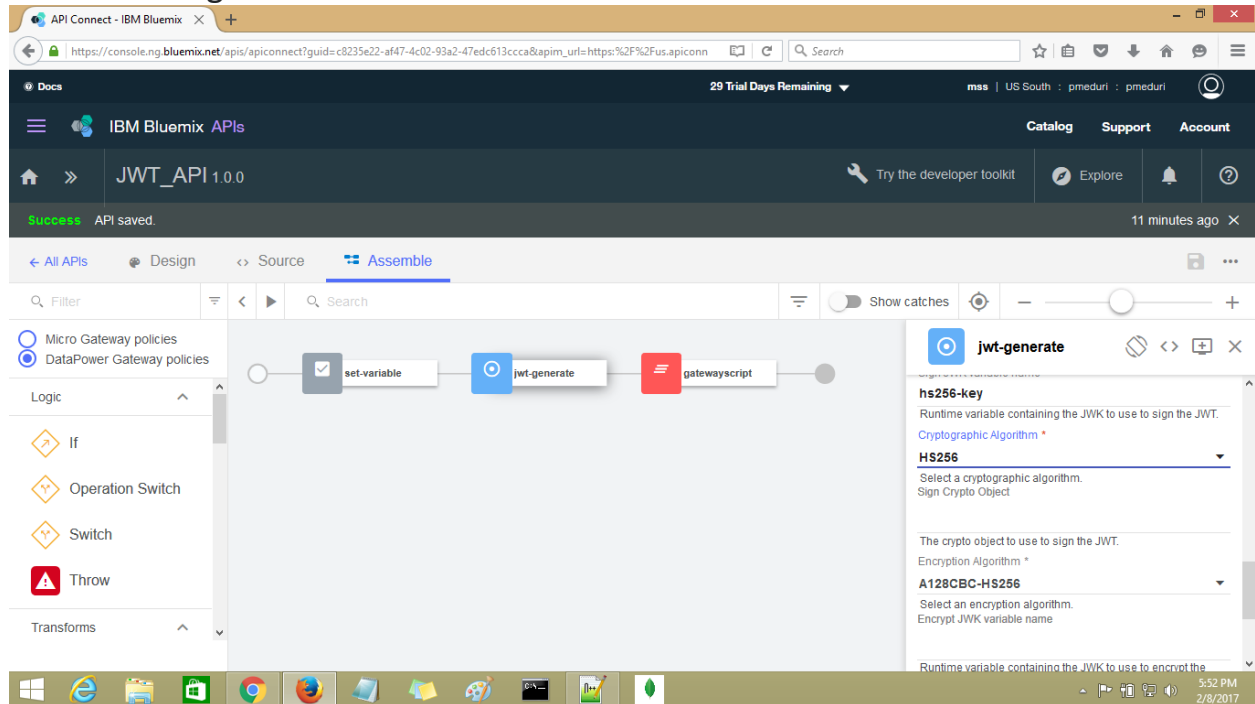
This policy can be attached to the flow after the SetVariable policy.



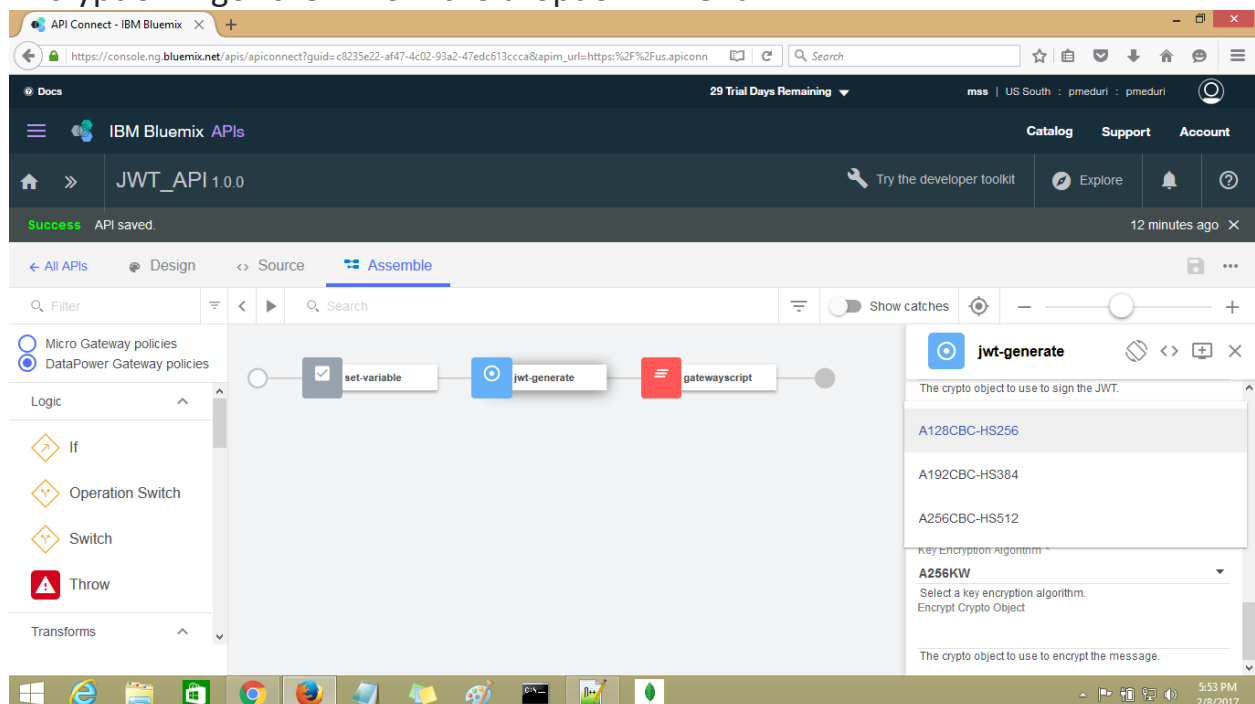
In this we can give name of the policy and JSON Web Token Name.

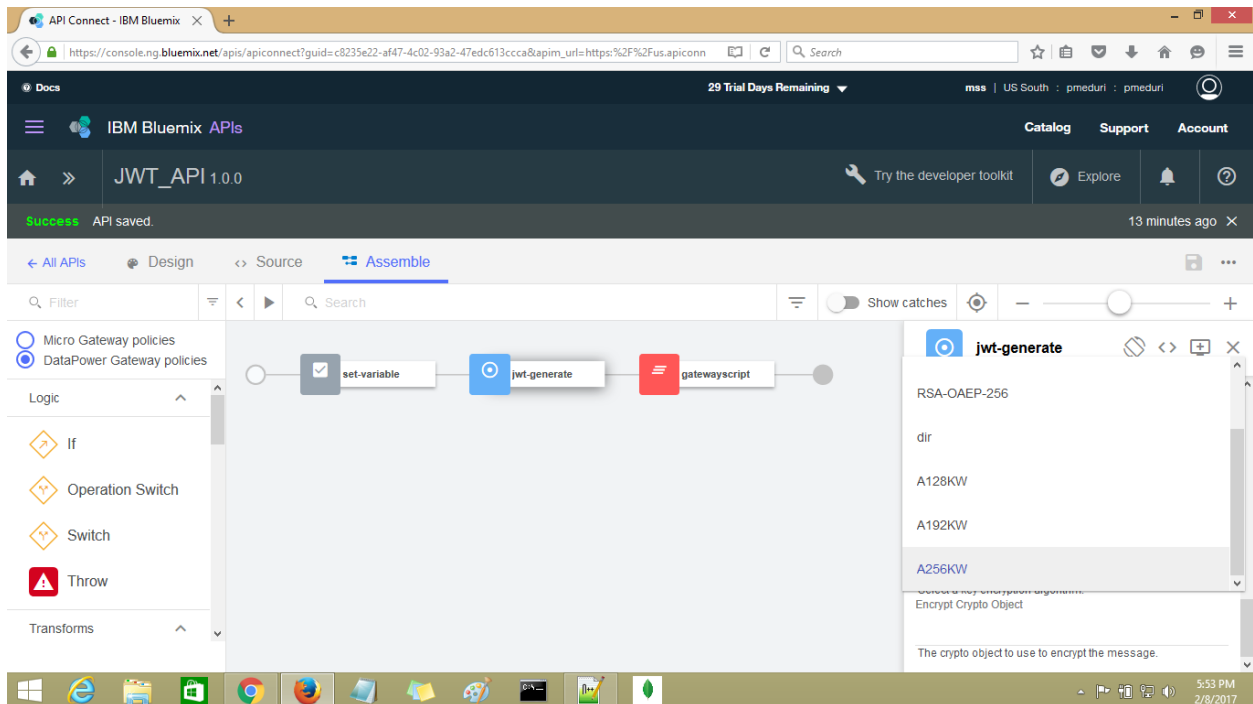


Here we can give the Issuer claim and audience claim methods.

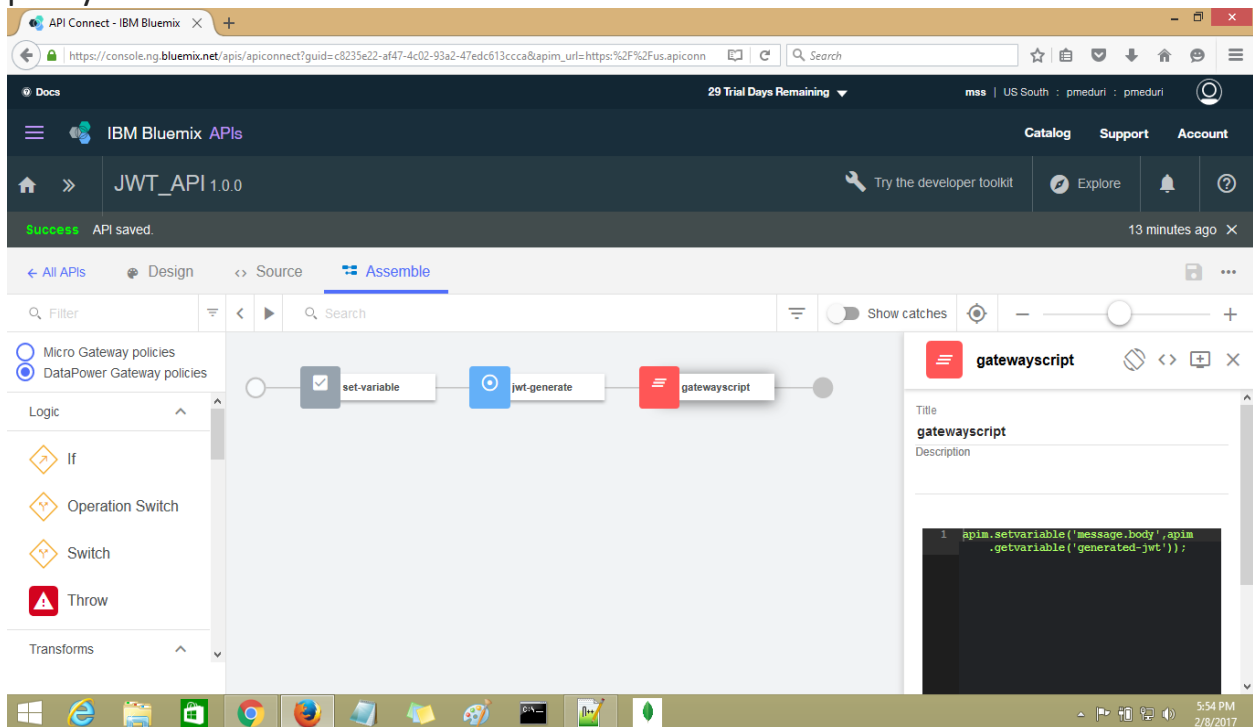


After that we need to select the required Cryptographic Algorithm and Encryption Algorithm from the dropdown menu.





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



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

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

After that select the GET/validate_jwt definition

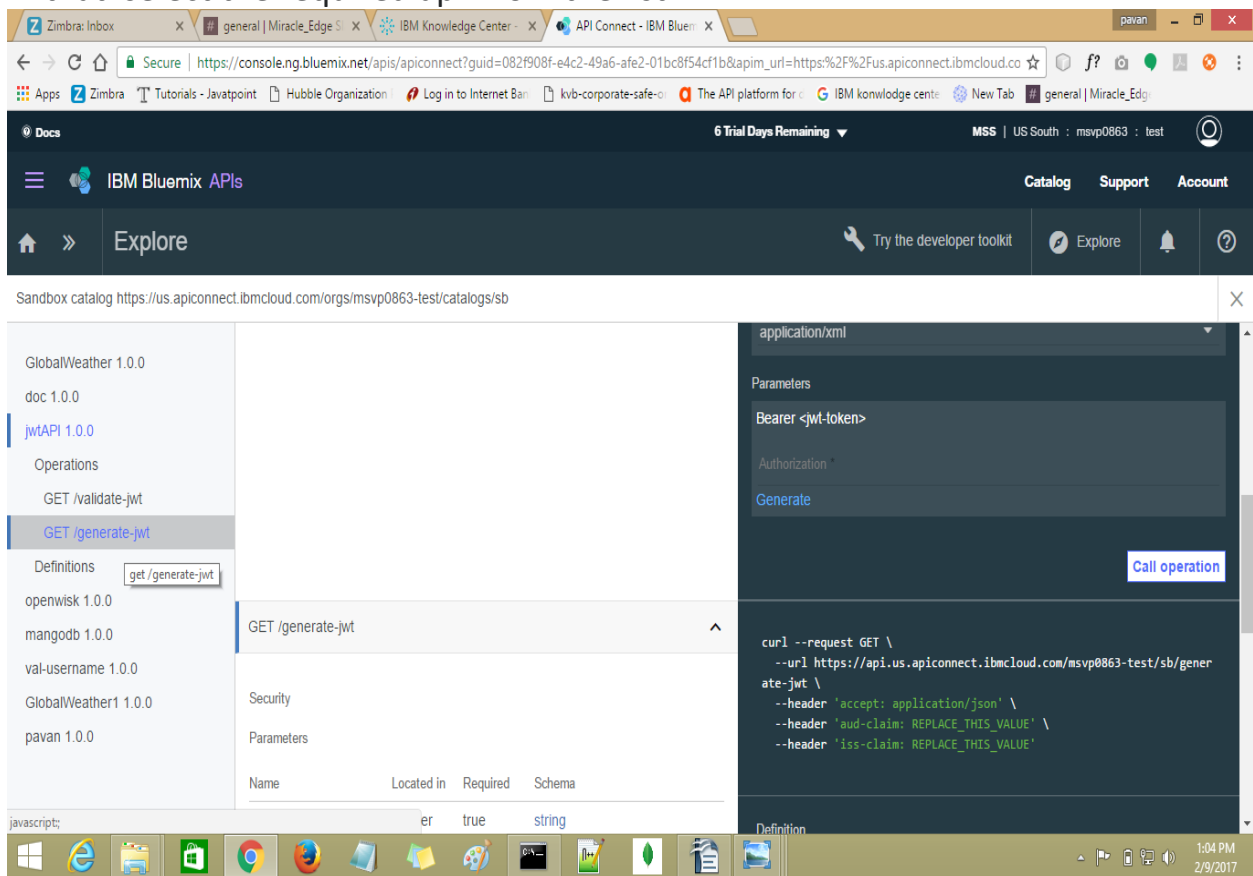
here I am using **apic** as issuer claim and **id** as Audience claim.

Now click on INVOKE button.

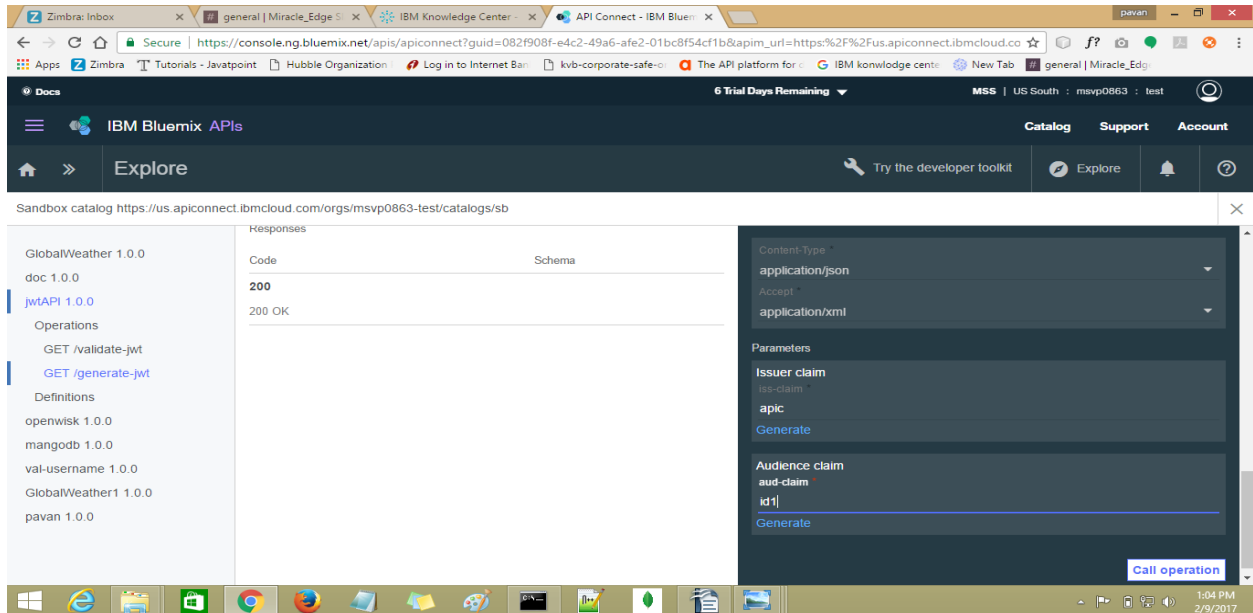
Then the response will be shown . or

Select the EXPLORE button click on Sandbox

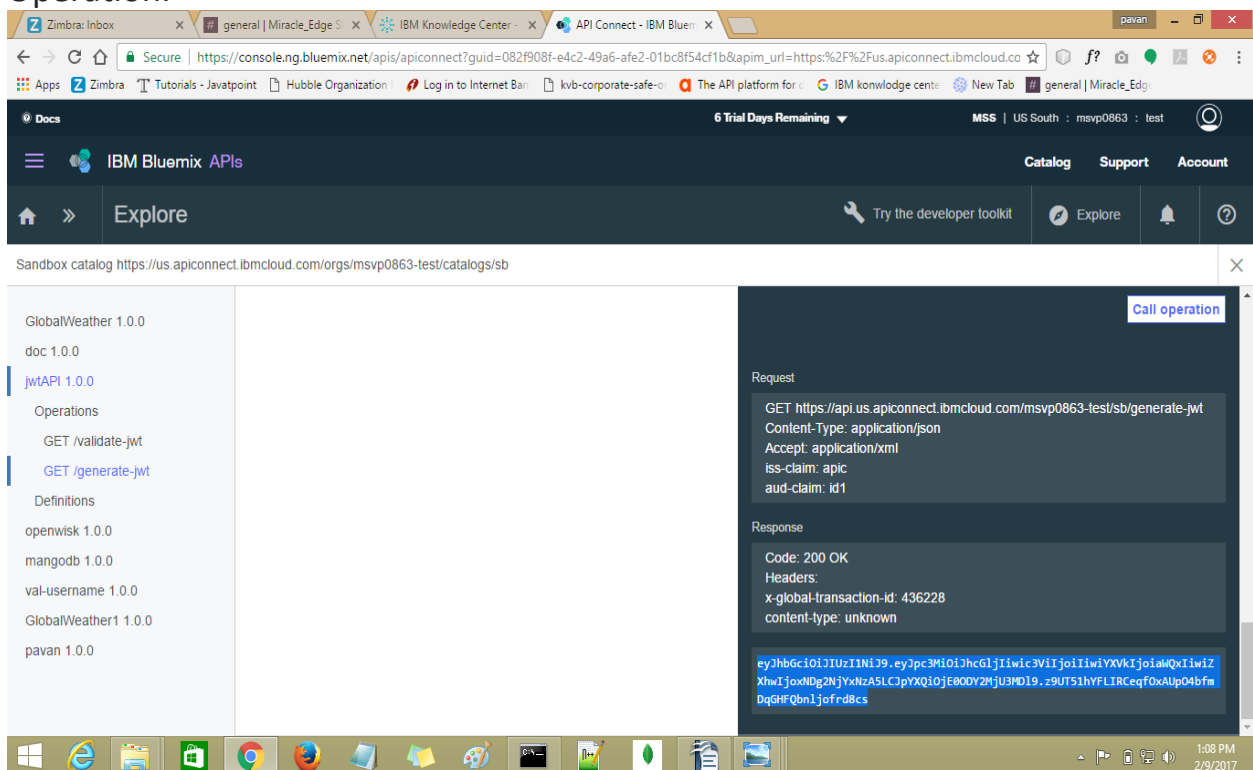
in that select the required api from the list.



Select the required definition from the list.



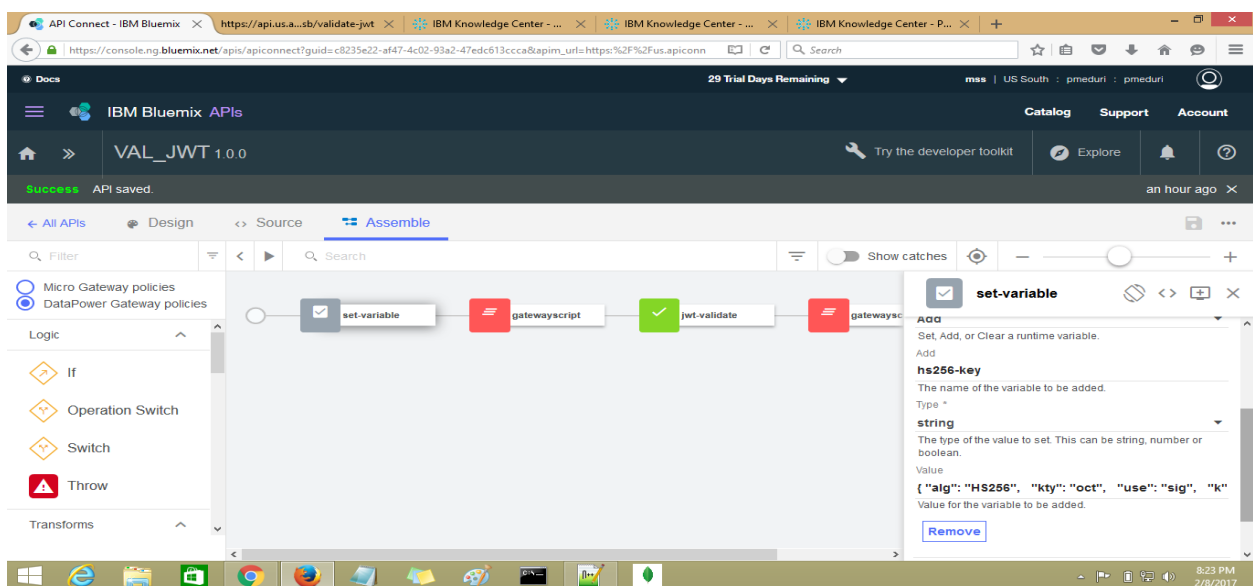
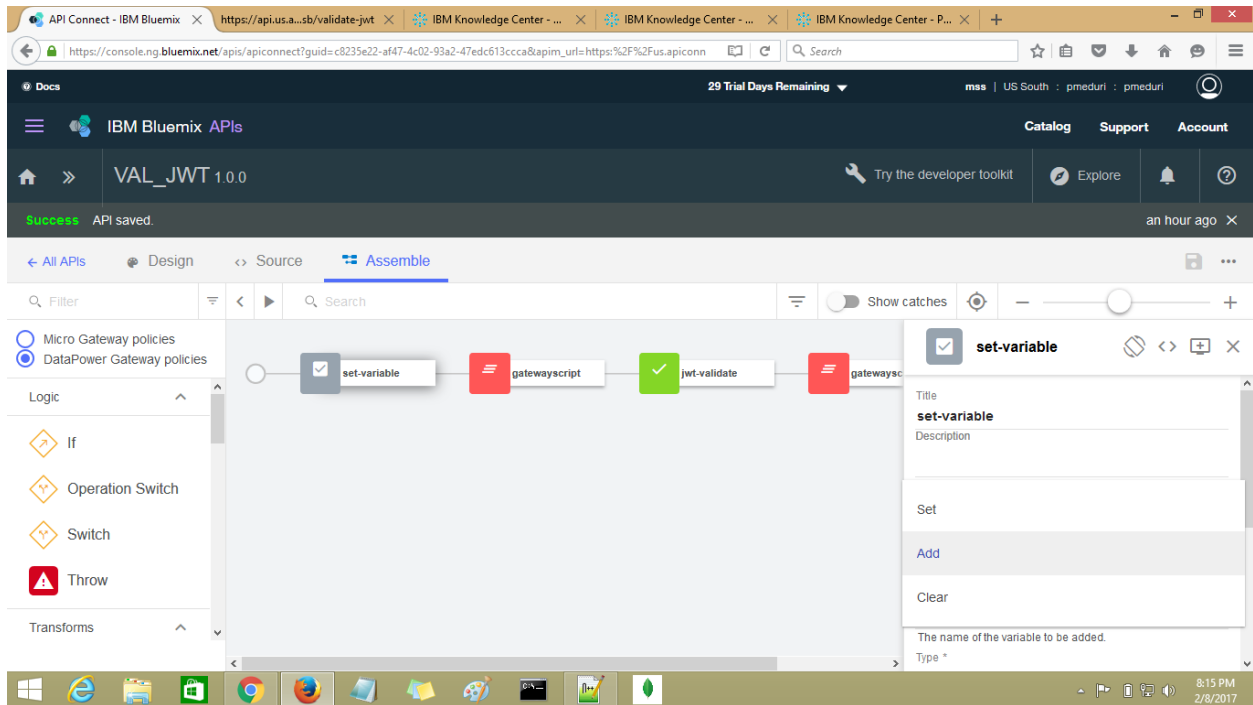
In the Issuer Claim give value as **apic** and Audience Claim as **id1**, and click on Call Operation.



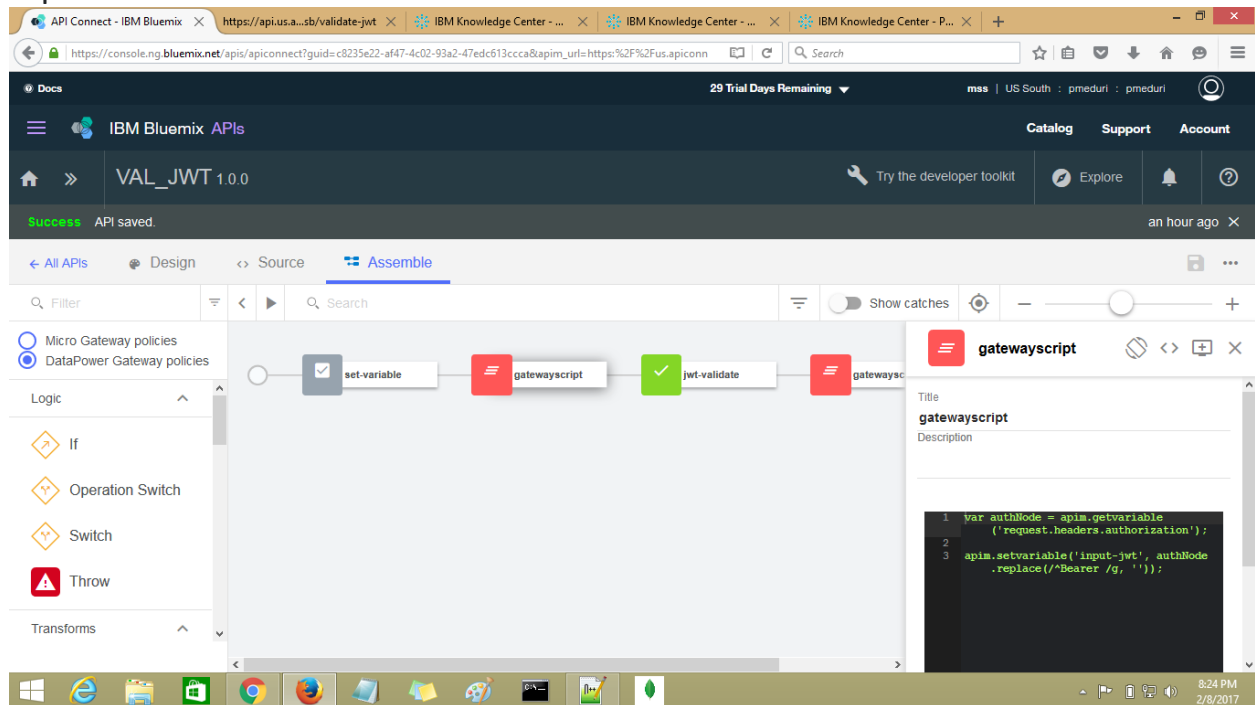
Validate_JWT:

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

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



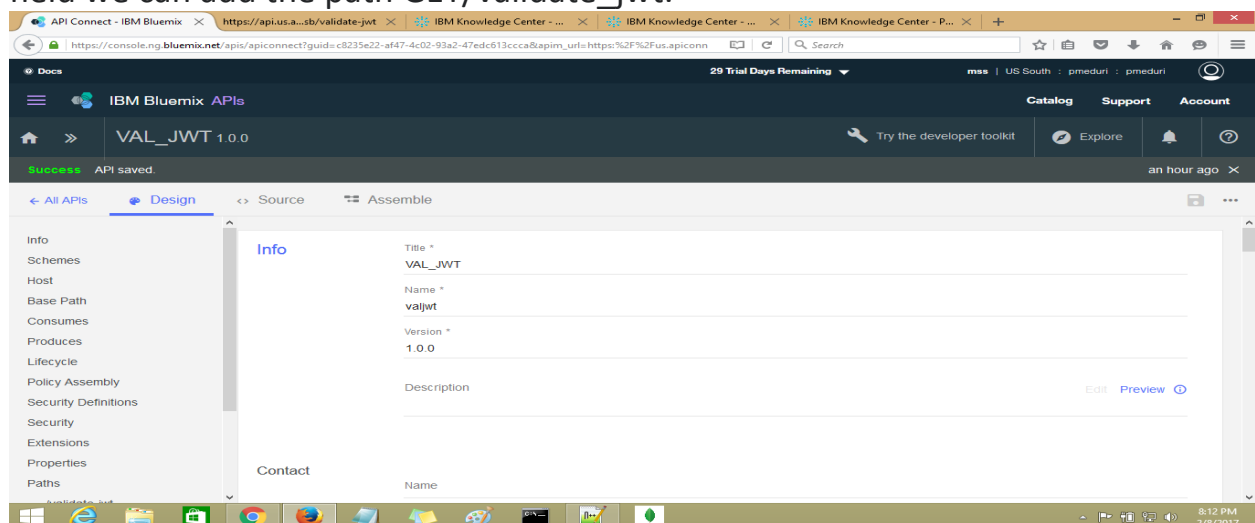
After that we can create the GatewayScript policy to retrieve the generate_jwt and replace with the Bearer.



After getting the variable from the gatewayscript policy 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.



API Connect - IBM Bluemix

https://api.us.a...sb/validate-jwt

IBM Knowledge Center - ...

IBM Knowledge Center - P...

IBM Knowledge Center - P...

https://console.ng.bluemix.net/apis/apiconnect?guid=c8235e22-af47-4c02-93a2-47edc613ccca&apim_url=https:%2F%2Fus.apiconn

Search

Docs

29 Trial Days Remaining

mss | US South : pmeduri : pmeduri

IBM Bluemix APIs

Catalog Support Account

VAL_JWT 1.0.0

Try the developer toolkit

Explore

an hour ago

Success API saved.

All APIs Design Source Assemble

Base Path

Consumes

Produces

Lifecycle

Policy Assembly

Security Definitions

Security

Extensions

Properties

Paths

/validate-jwt

Parameters

Definitions

Services

Paths

/validate-jwt

Path *

/validate-jwt

Add Operation

Add Parameter

Parameters

Name	Located In	Description	Required	Type
Authorization	Header	Bearer <jwt-token>	<input checked="" type="checkbox"/>	string

GET /validate-jwt

API Connect - IBM Bluemix

https://api.us.a...sb/validate-jwt

IBM Knowledge Center - ...

IBM Knowledge Center - ...

IBM Knowledge Center - P...

https://console.ng.bluemix.net/apis/apiconnect?guid=c8235e22-af47-4c02-93a2-47edc613ccca&apim_url=https:%2F%2Fus.apiconn

Search

Docs

29 Trial Days Remaining

mss | US South : pmeduri : pmeduri

IBM Bluemix APIs

Catalog Support Account

VAL_JWT 1.0.0

Try the developer toolkit

Explore

an hour ago

Success API saved.

All APIs Design Source Assemble

Filter

Search

Show catches

Micro Gateway policies

DataPower Gateway policies

Logic

If

Operation Switch

Switch

Throw

Transforms

set-variable

gatewayscript

jwt-validate

gatewayscript

jwt-validate

Title

jwt-validate

Description

JSON Web Token (JWT)

input-jwt

Context or runtime variable that contains the JWT to be validated. If not set, the policy looks for the JWT in request.headers.authorization.

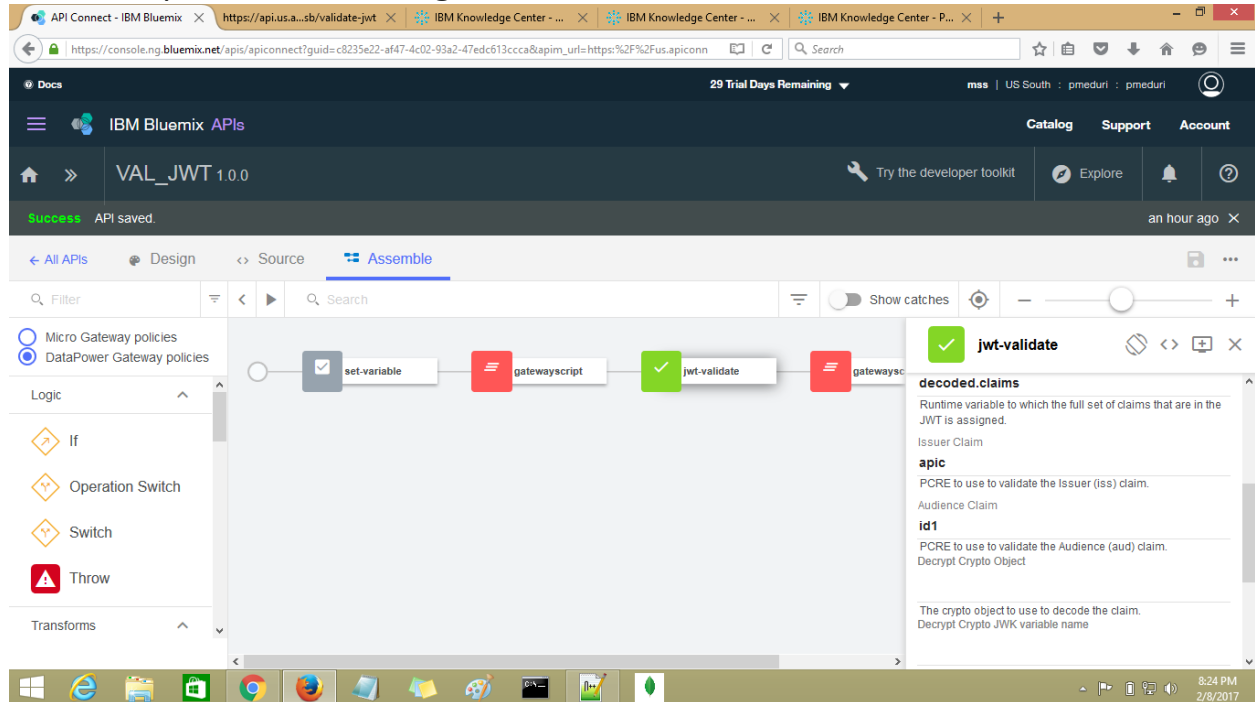
Output Claims

decoded.claims

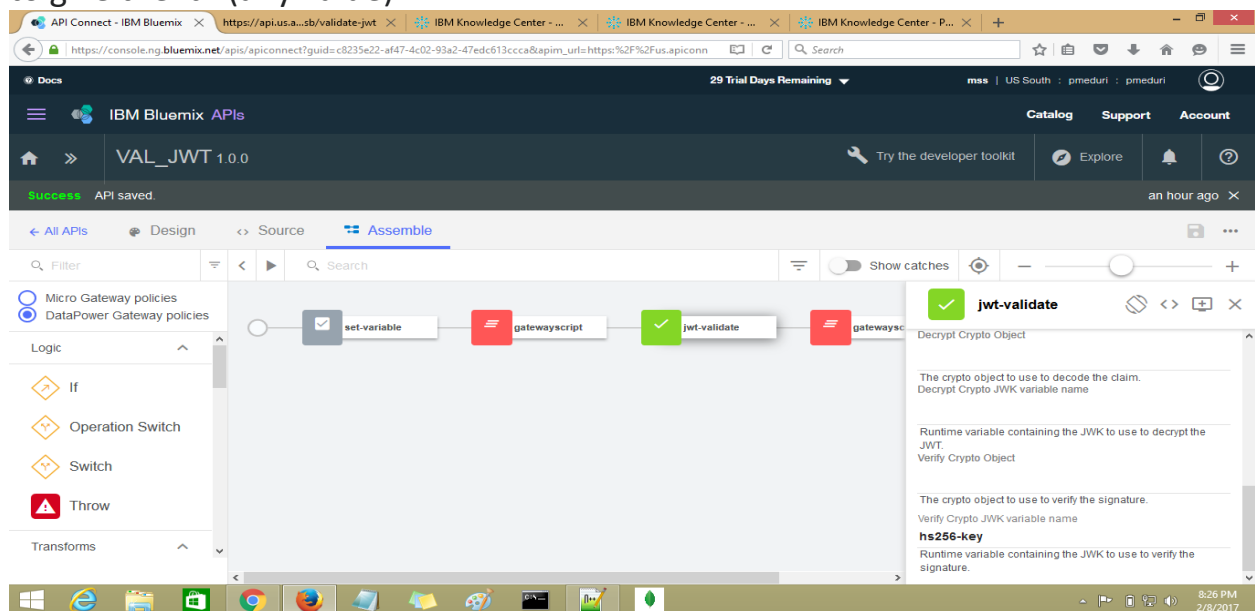
Runtime variable to which the full set of claims that are in the JWT is assigned.

In the JSON web Token we need to give the name to store the value in the encrypted format which need to be Decoded.

In the Output claims will be given as decoded-claims .

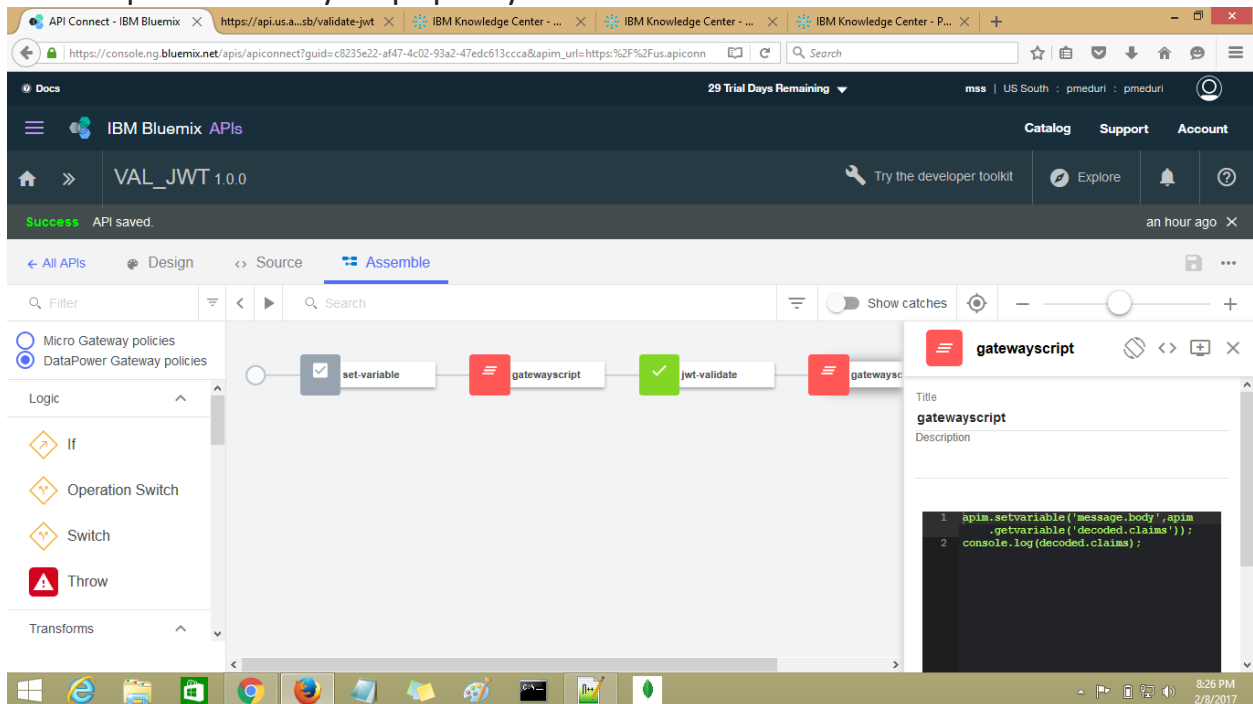


In the Issuer Claim we can give value **apic** (any value) and Audience Claim we need to give the **id1** (any value).



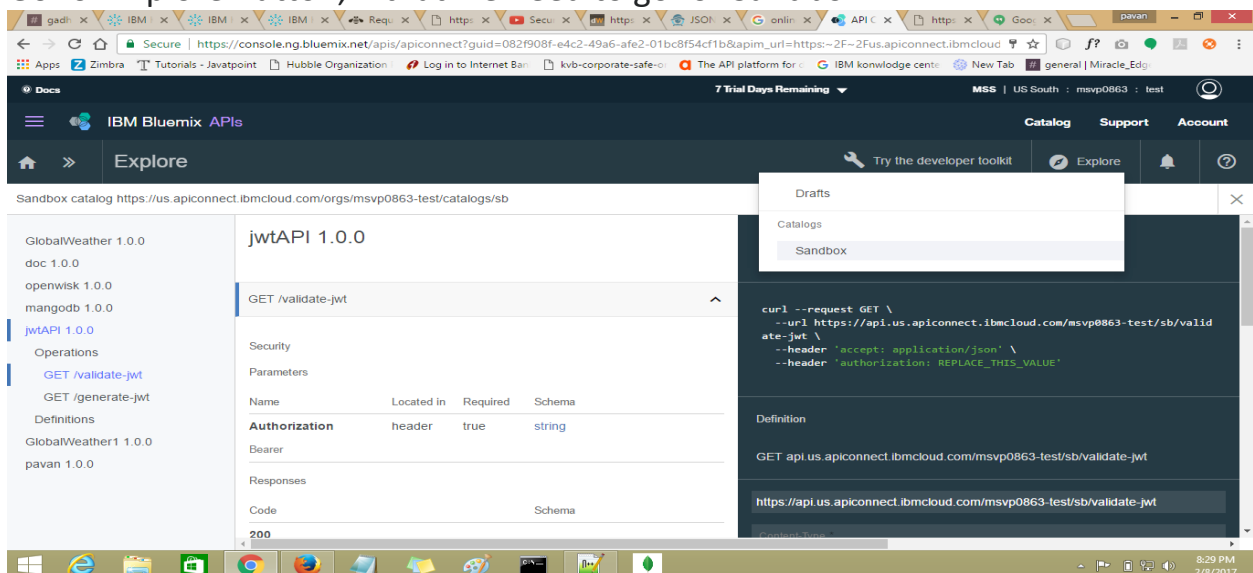
Verify crypto variable name can be given as the hs256-key.

The validated message body can be stored in gatewayscript policy. From that message we need to retrieve the decoded-claims. For that we need to write JavaScript in GatewayScript policy.



After completion 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.

The screenshot shows the IBM Bluemix APIs console interface. The left sidebar lists various APIs, with 'jwtAPI 1.0.0' selected. The main panel displays details for the 'GET /validate-jwt' endpoint. The 'Parameters' section shows a table with columns: Name, Located in, Required, and Schema. The 'Responses' section shows a table with columns: Code and Schema. The 'Definition' section contains a curl command and the endpoint URL.

Name	Located in	Required	Schema
Authorization	header	true	string

Code	Schema
200	


```
curl --request GET \
--url https://api.us.apiconnect.ibmcloud.com/msvp0863-test/sb/validate-jwt \
--header 'accept: application/json' \
--header 'authorization: REPLACE_THIS_VALUE'
```

Definition
GET api.us.apiconnect.ibmcloud.com/msvp0863-test/sb/validate-jwt

https://api.us.apiconnect.ibmcloud.com/msvp0863-test/sb/validate-jwt

The screenshot shows the IBM Bluemix APIs console interface. The left sidebar lists various APIs, with 'jwtAPI 1.0.0' selected. The main panel displays details for the 'GET /validate-jwt' endpoint. The 'Responses' section shows a table with columns: Code and Schema. The 'Parameters' section shows a form with a 'Bearer <jwt-token>' field and an 'Authorization' field. The 'Generate' button is visible.

Code	Schema
200	
200 OK	

Parameters

Bearer <jwt-token>
Authorization
|
Generate

Call operation

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

The screenshot shows the IBM Bluemix API console interface. The browser address bar displays the URL: `https://console.ng.bluemix.net/apis/apiconnect?guid=082f908f-e4c2-49a6-afe2-01bc8f54cf1b&apim_url=https://2f~2f.us.apiconnect.ibmcloud.com`. The console header includes a 'Docs' tab, a '7 Trial Days Remaining' indicator, and user information 'MSS | US South : msvp0863 : test'. The main navigation bar shows 'IBM Bluemix APIs', 'Catalog', 'Support', and 'Account'. The 'Explore' section is active, displaying a 'Sandbox catalog' for the URL `https://us.apiconnect.ibmcloud.com/orgs/msvp0863-test/catalogs/sb`. On the left, a sidebar lists various APIs, with 'jwtAPI 1.0.0' selected. Under 'Operations', the 'GET /validate-jwt' operation is highlighted. The main panel shows the operation details, including the endpoint `GET api.us.apiconnect.ibmcloud.com/msvp0863-test/sb/validate-jwt`, the URL `https://api.us.apiconnect.ibmcloud.com/msvp0863-test/sb/validate-jwt`, and the 'Parameters' section. The 'Parameters' section shows a 'Bearer <jwt-token>' field with the value `Bearer eyJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJhcGllIiwic3ViOiJ0aWwYXVtjoiaWQxliwi`. A 'Generate' button is visible next to the token. At the bottom right of the operation details, there is a blue 'Call operation' button. The Windows taskbar at the bottom shows the time as 11:11 PM on 2/8/2017.

Then click on Call operation.

Then the output will be

[illegible]