OAUTH 2.0 Troubleshooting POSTMAN

Use Case: Sometimes we end up with a compose connection failing with OAUTH.

To narrow down the problem, we try to isolate it piece by piece.

by testing workflow

Alation -->IDP (Here we POSTMAN to test, can be done via curl too , but POSTMAN makes easy..and other security point of view)

Alation-->Snowflake

Background

When we configure OAUTH in Alation Compose, we involve at least three parties.

Integration Story:

1. Alation
2. Snowflake(Can be any datasource taken for example)
3. IDP (Can be any like AzureAD, OKTA or Snowflake itself)

Alation asks for IDP (Azure AD or OKTA) to create a client app. with callback address to Alation end point https://ACSorONprem/api/datasource_auth/oauth/callback

This generates a client ID and client password (secret).

Now using the client details, IDP endpoints (authorise and token), and scope, we get a token (the value that we need to extract from the token is used as a username in Snowflake), and this token is passed to Snowflake.

We use POSTMAN to validate this token and claim mapping.

Prerequiste:

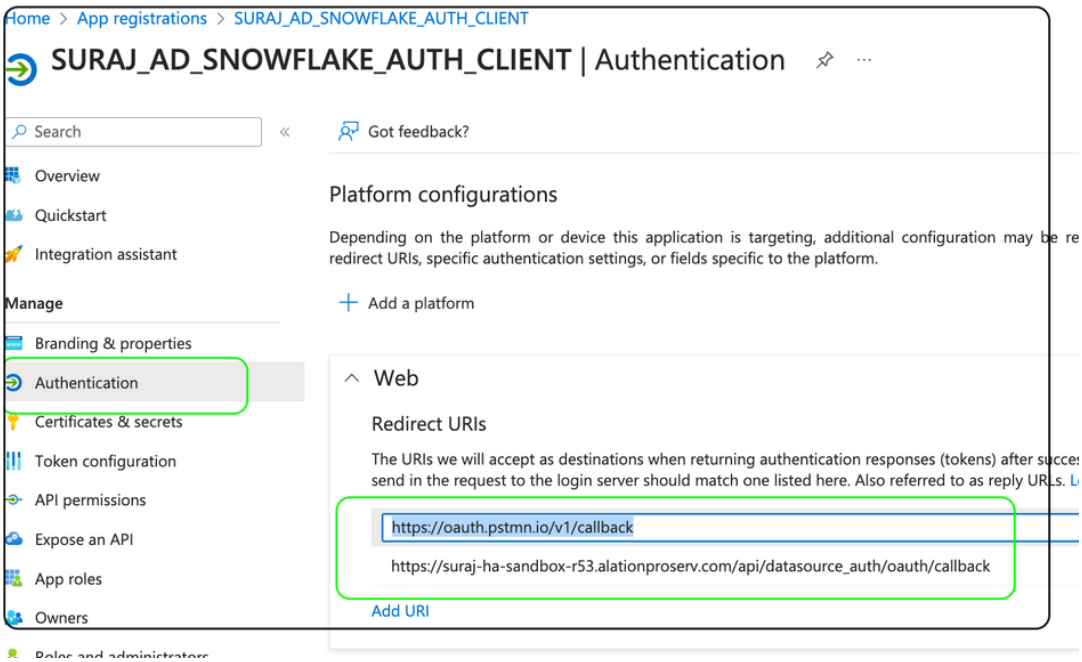
1. The POSTMAN tool is required (the web version also works). This can be installed on IDP admin, Alation admin (preferred), or Snowflake admin. Anyone can do this.
2. Details from OAUTH for Alation from IDP(Azure or OKTA or Ping or Another)

Steps:

Step1:

On the IDP side, just add the public POSTMAN callback url (https://oauth.pstmn.io/v1/callback)along with the Alation callback url.

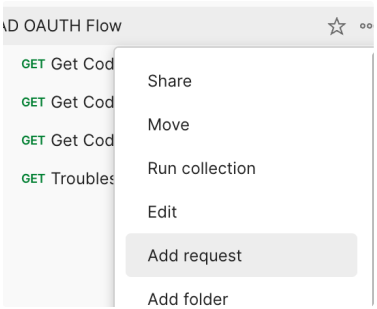
example Azure



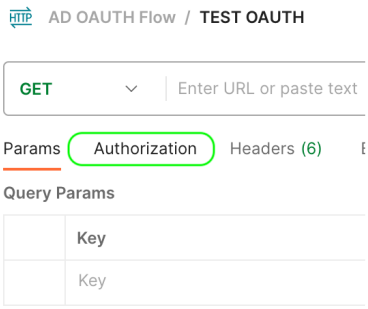
Step2:

Launch Postman and fill in the same details as in Alation side

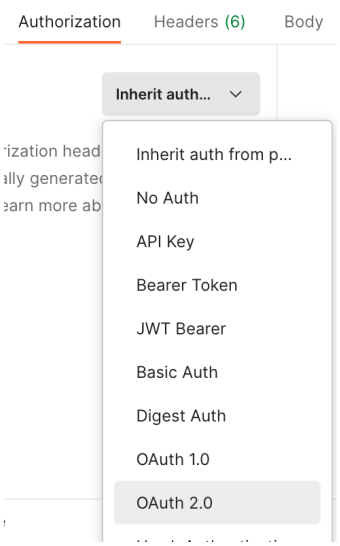
Once you launch postman , Just add a new request, give any name



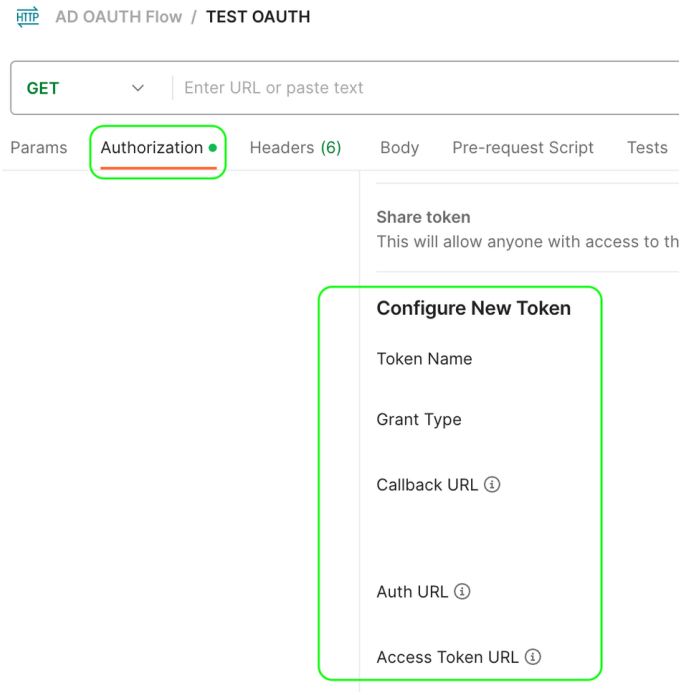
Switch to Authorization tab



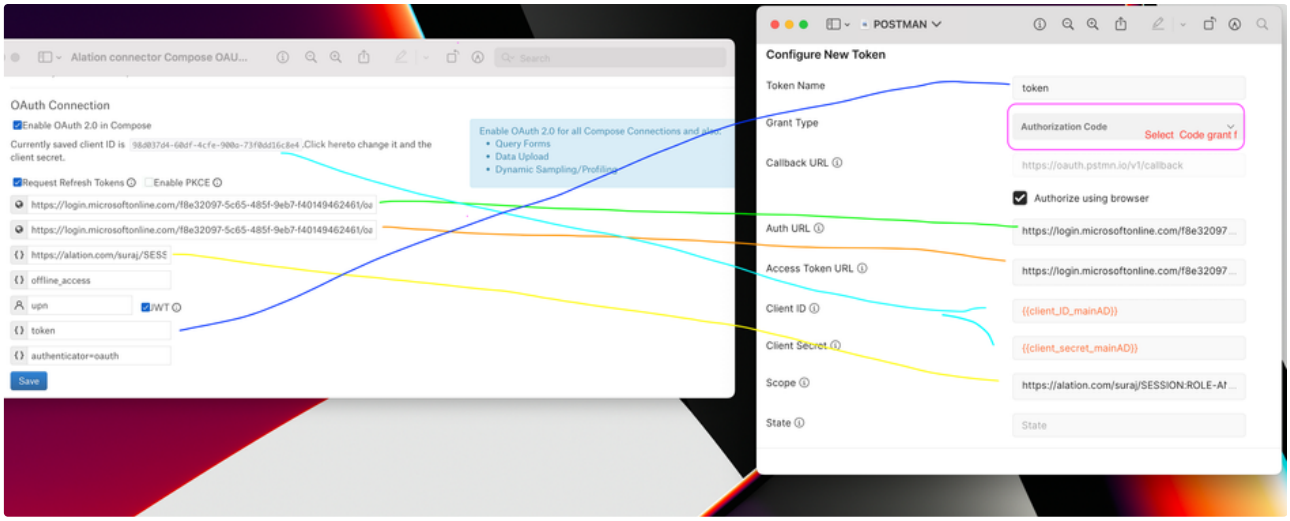
Select OAuth 2.0



Start filling the middle panel with configuration details

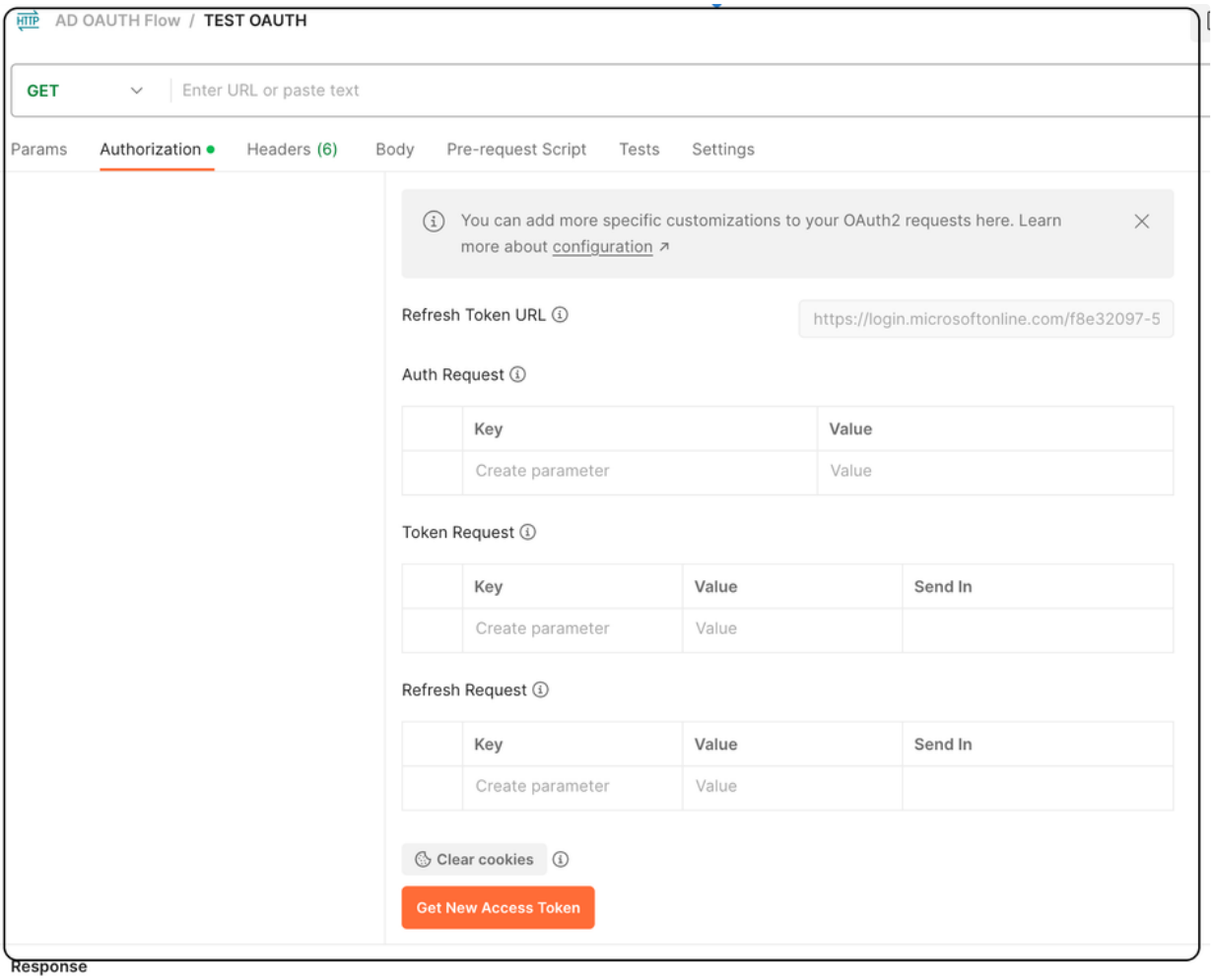


Map with same values use in Alation choose the Grant type as Code in PostMan



Step3: Testing

Scroll Down and click **Get new Access Token**

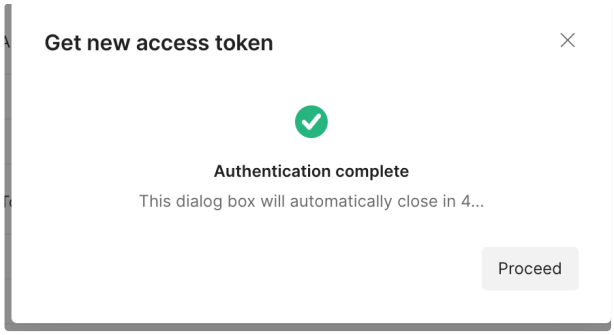


Note1:On click Get New Access Token

It will ask to authenticate via Azure , if this fails ask to give correct clientID and secret

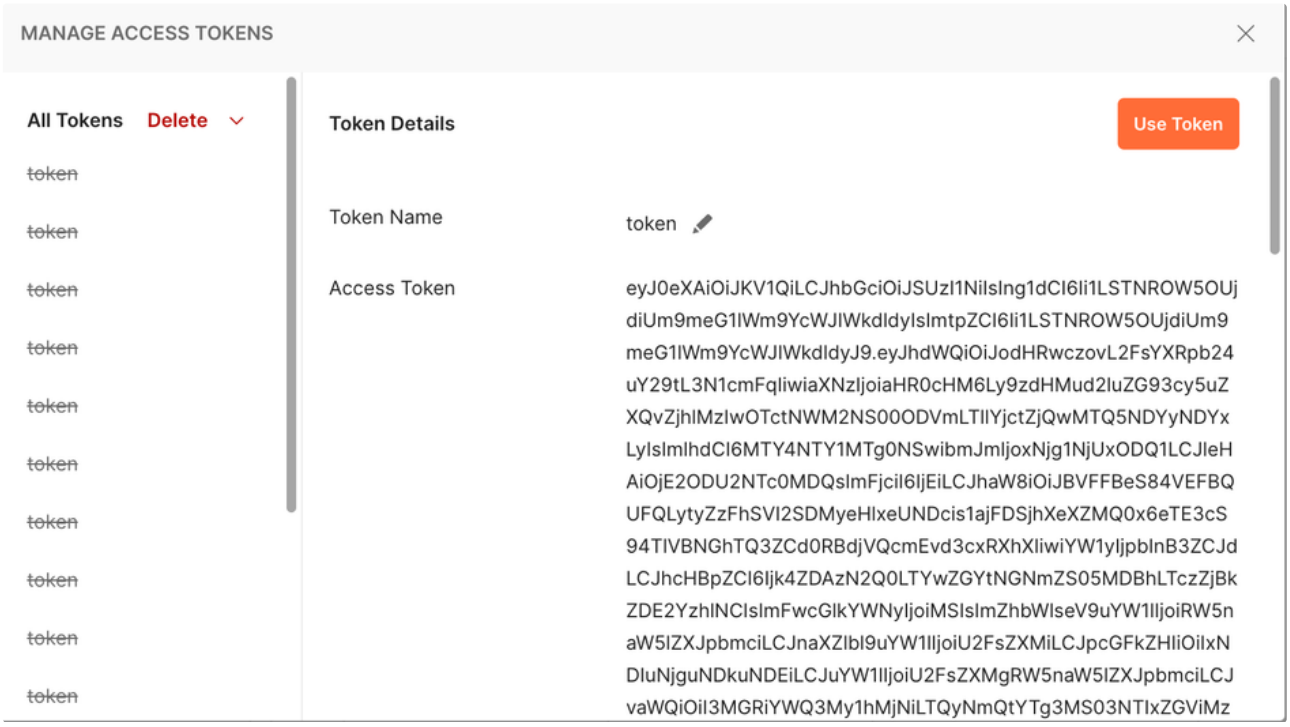
some time your browser will block url , see if any any warning if so allow that.

if this passes

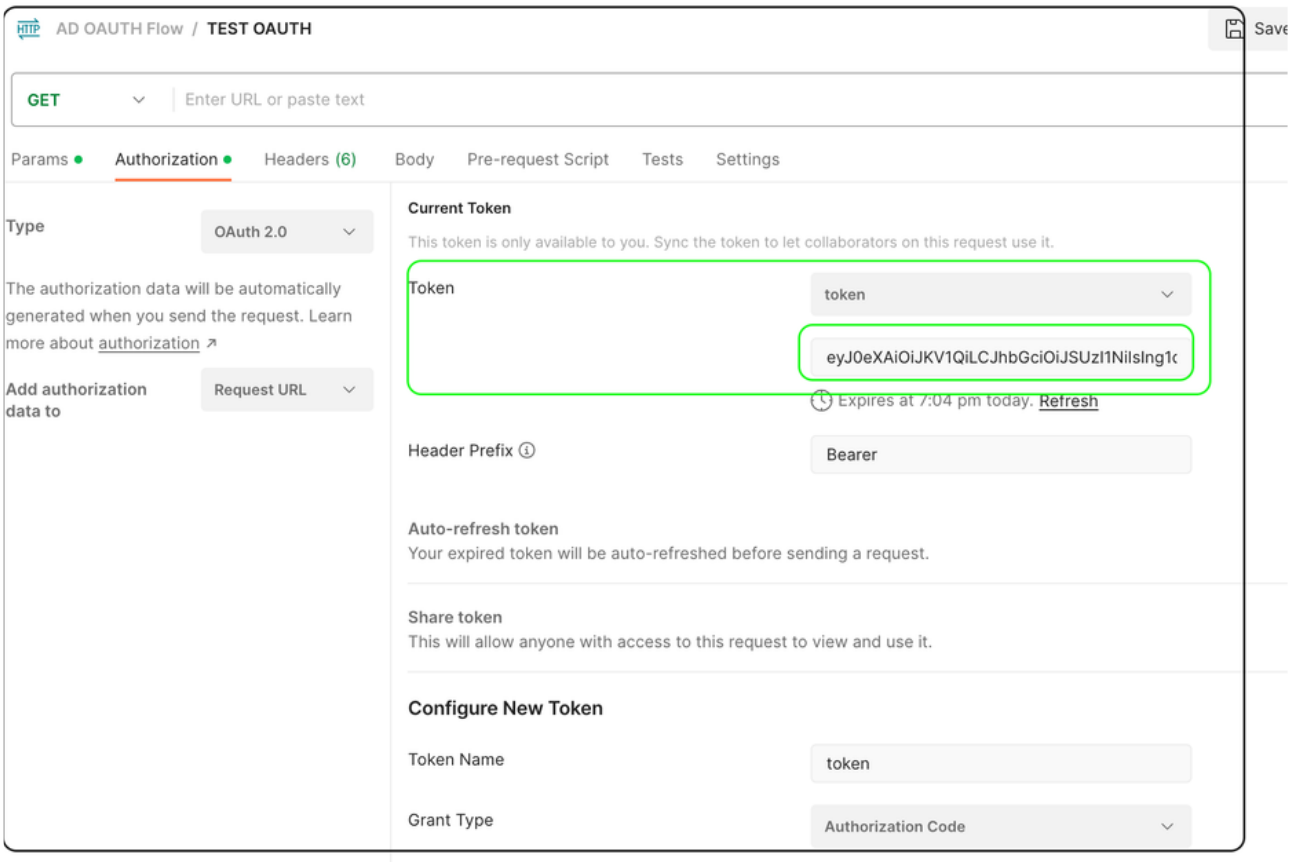


now click proceed

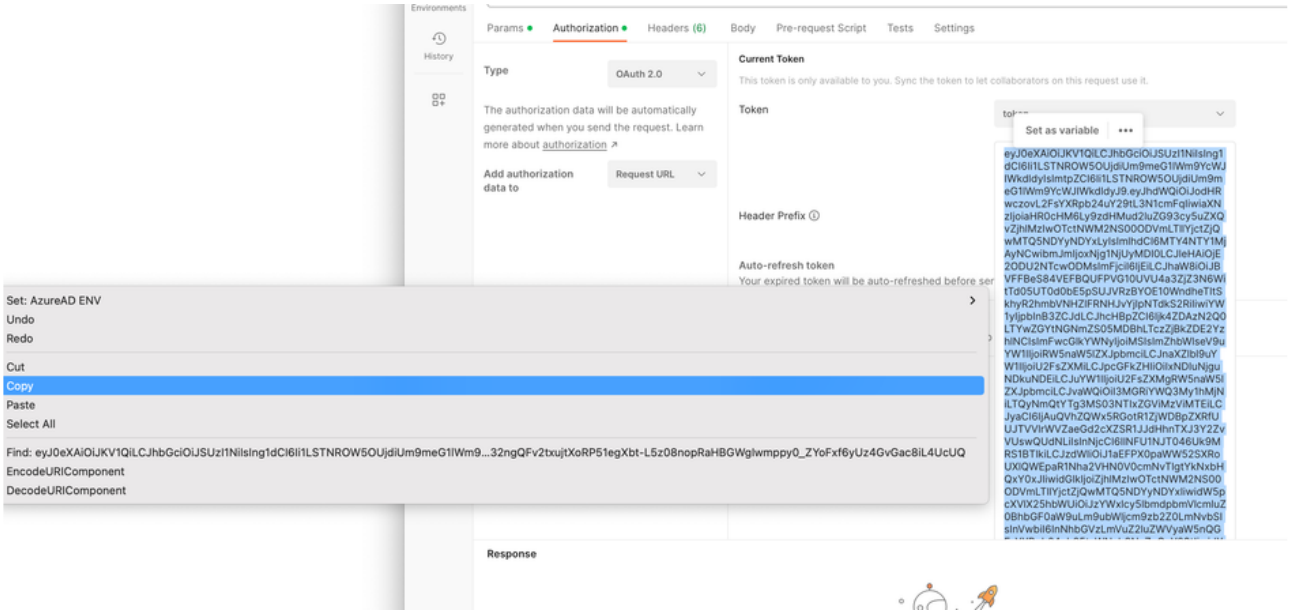
You would see Access Token, Click use Token



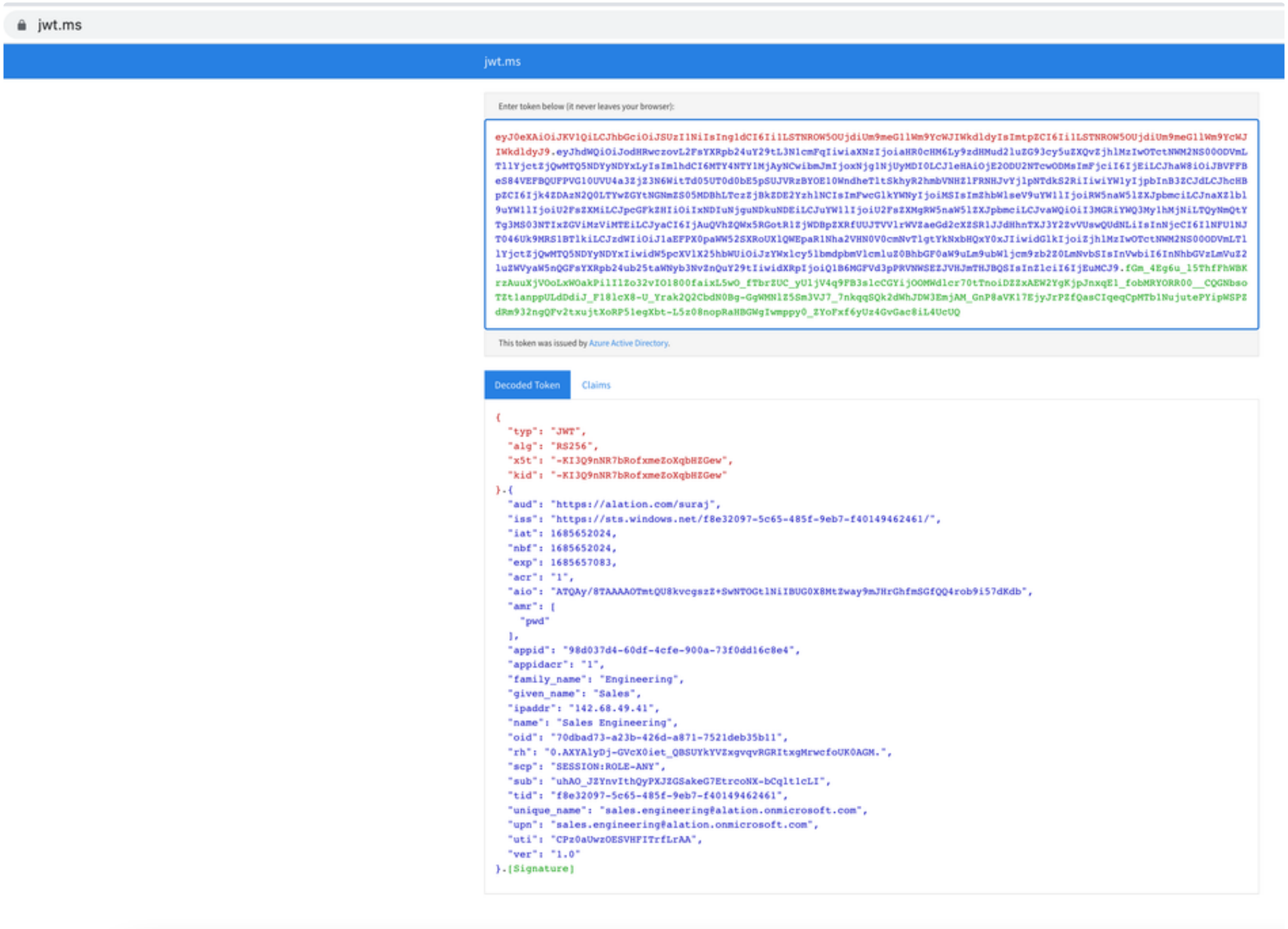
Navigate to top of the Request > you will find Token value



Now copy the Token



and open in any JWT decoder site like jwt.ms or jwt.io and Paste the access token to get decoded



Test at Snowflake side:

Same token you can test : replace your token value

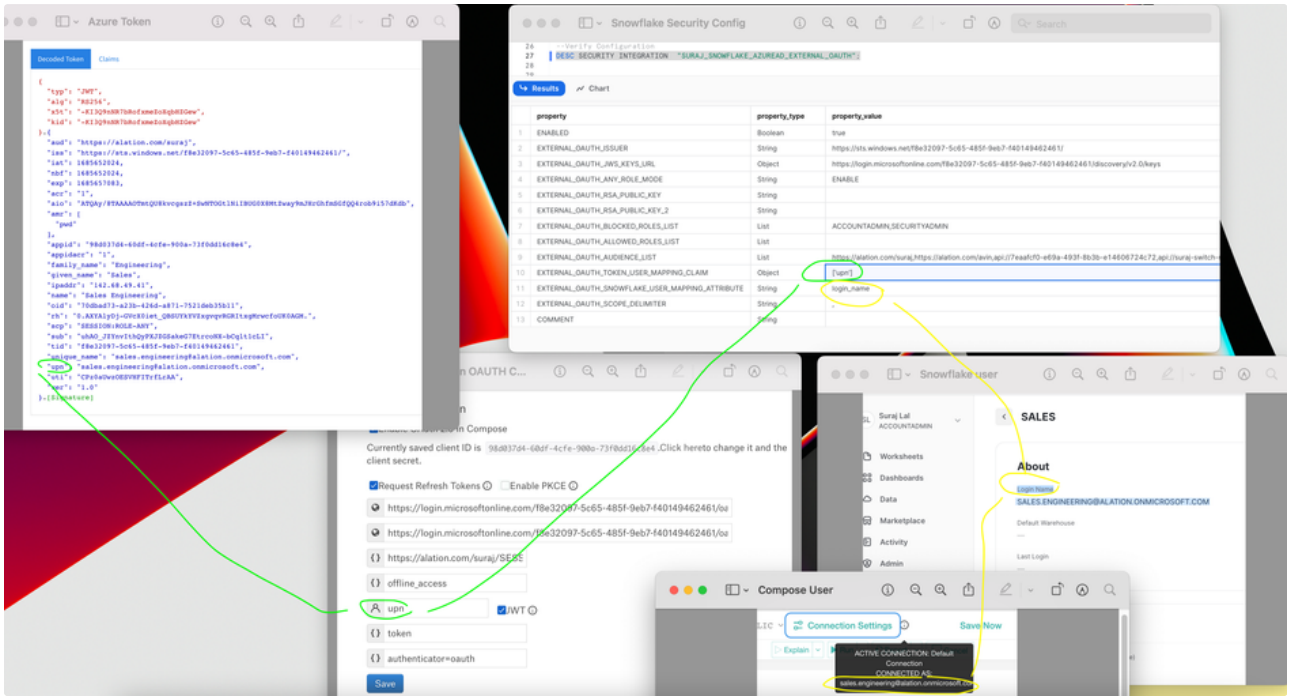
```
SELECT SYSTEM$VERIFY_EXTERNAL_OAUTH_TOKEN('eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIng1dCI6Ii1LSTNROW5OUjdiUm9meG1lWm
```

Final User Mapping between IDP & Alation Compose user & Snowflake:

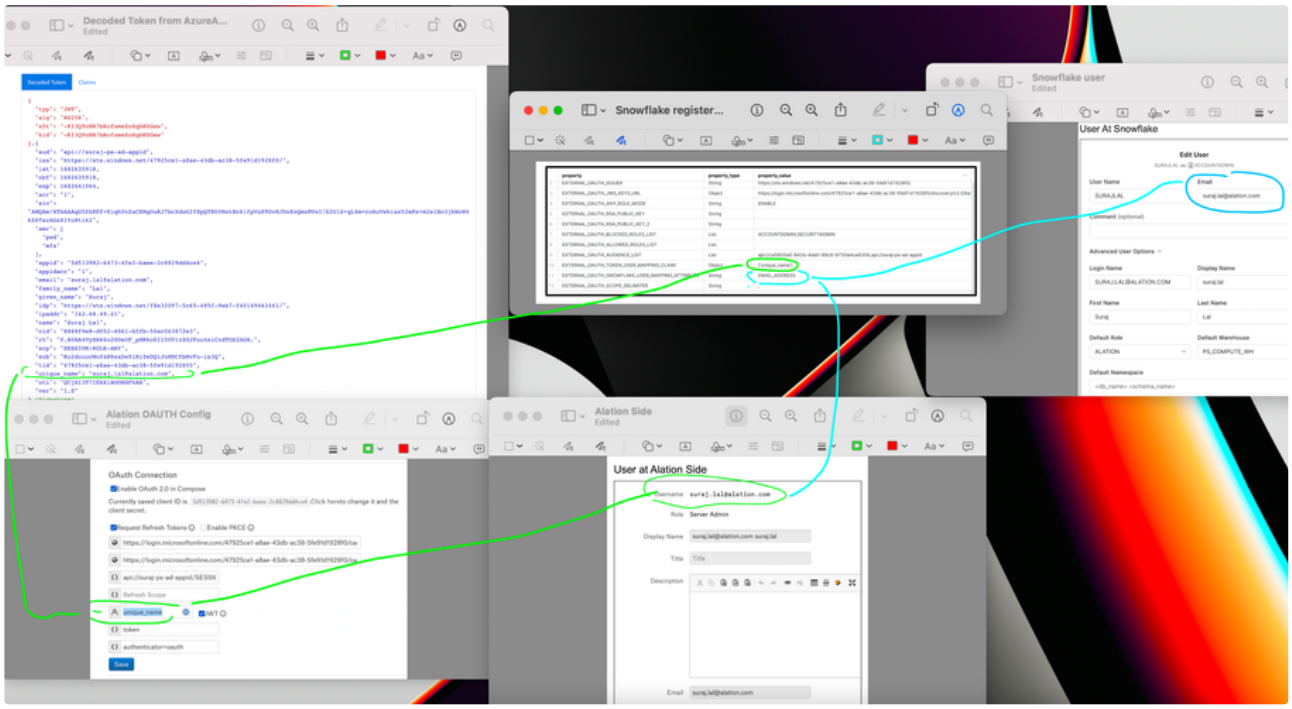
upn in Azure token

upn in Alation user profile OAuth config

upn in Snowflake `EXTERNAL_OAUTH_TOKEN_USER_MAPPING_CLAIM`

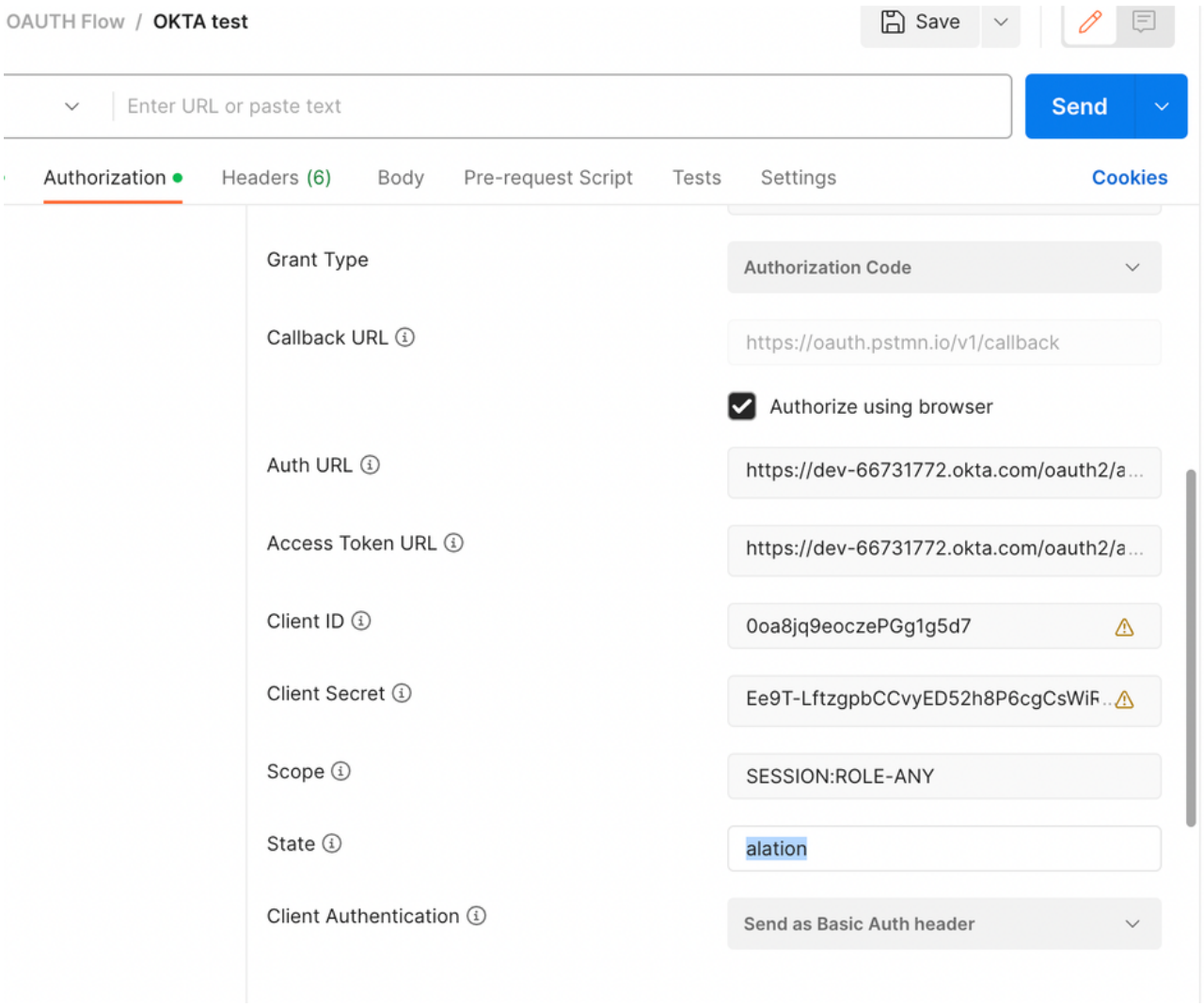


For B2B customer, you need to use unique_name as AzureD is External Directory for those users

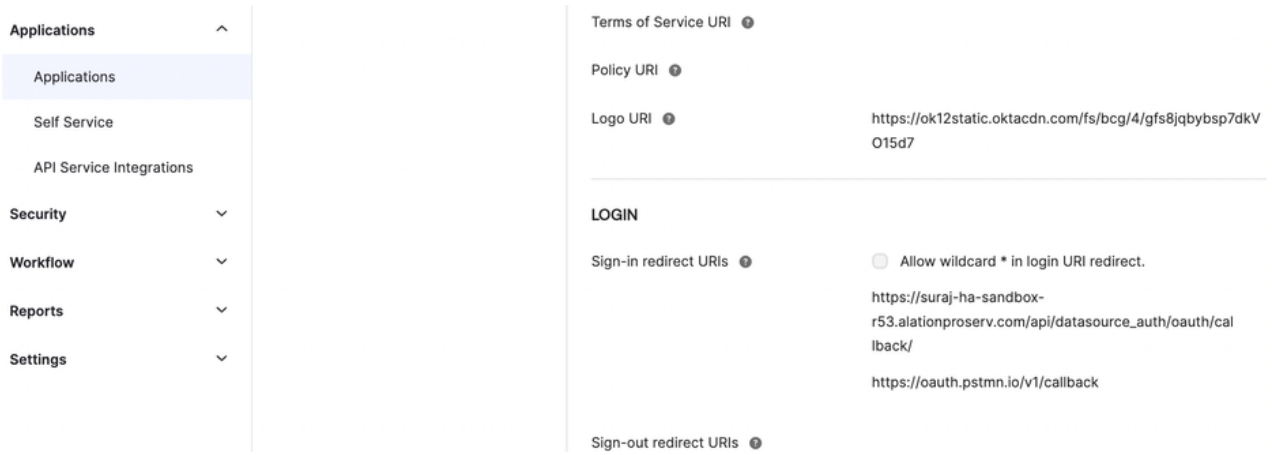


POSTMAN for OKTA

In STATE give any string example alation



In OKTA Client Application Add Redirect URI https://oauth.pstmn.io/v1/callback



Error Recording at Snowflake Side

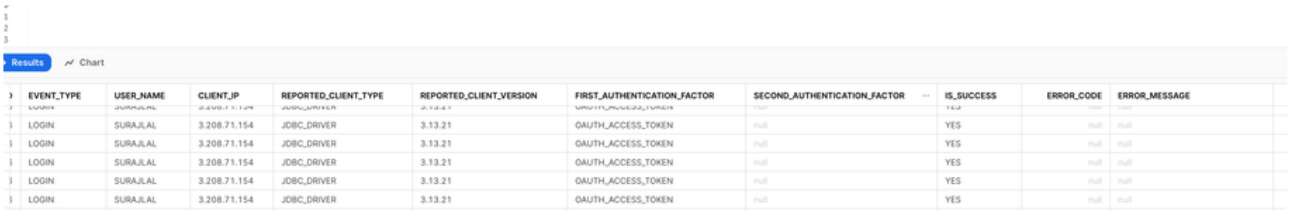
```
select * from SNOWFLAKE.ACCOUNT_USAGE.login_history order by event_timestamp;


select *
from table(SNOWFLAKE.information_schema.login_history_by_user())
order by event_timestamp;

--For Last One Hour
select *
from table(SNOWFLAKE.information_schema.login_history(TIME_RANGE_START => dateadd('hours',-1,current_timestamp()
order by event_timestamp;


--For Last Four Hour
select *
from table(SNOWFLAKE.information_schema.login_history(TIME_RANGE_START => dateadd('hours',-4,current_timestamp()
order by event_timestamp;
```

Check the Error message



EVENT_TYPE	USER_NAME	CLIENT_IP	REPORTED_CLIENT_TYPE	REPORTED_CLIENT_VERSION	FIRST_AUTHENTICATION_FACTOR	SECOND_AUTHENTICATION_FACTOR	IS_SUCCESS	ERROR_CODE	ERROR_MESSAGE
LOGIN	SURAJLAL	3.208.71.154	JDBC_DRIVER	3.13.21	OAUTH_ACCESS_TOKEN	null	YES	null	null
LOGIN	SURAJLAL	3.208.71.154	JDBC_DRIVER	3.13.21	OAUTH_ACCESS_TOKEN	null	YES	null	null
LOGIN	SURAJLAL	3.208.71.154	JDBC_DRIVER	3.13.21	OAUTH_ACCESS_TOKEN	null	YES	null	null
LOGIN	SURAJLAL	3.208.71.154	JDBC_DRIVER	3.13.21	OAUTH_ACCESS_TOKEN	null	YES	null	null
LOGIN	SURAJLAL	3.208.71.154	JDBC_DRIVER	3.13.21	OAUTH_ACCESS_TOKEN	null	YES	null	null

Check Token at Alation Side:

1. sudo service alation shell
2. alation_django_shell
3. OAuthTokens.objects.order_by('-id')[0].access_token

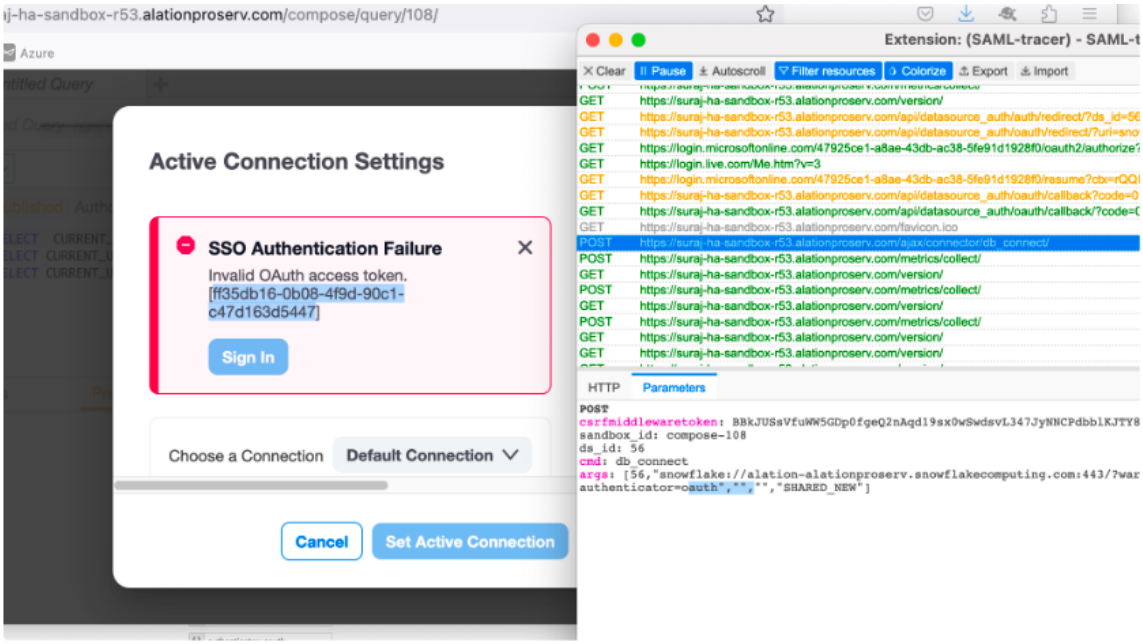
Copy the token and check in Snowflake as Account admin (replace token as per requirement)

```
SELECT SYSTEM$VERIFY_EXTERNAL_OAUTH_TOKEN('eyJraWQiOiJjS3JQWXBZRmJhUElOVG95R1lpY0U5bE4xZHVfRUJYVy1HUWNxTS1XZGxJIi
```

Check Error Codes from Snowflake to Alation

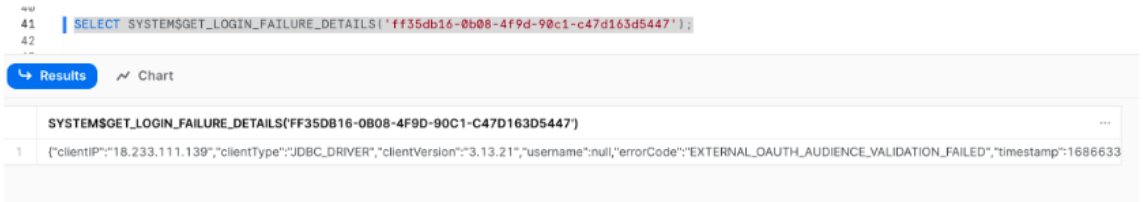
Try: step1 **Check Token at Alation Side if it is success and claim attribute is same as expected then try this steps Check Error Codes from Snowflake to Alation**

Some time Snowflake sends error message and with code , we do not know what is the exact reason.



Connector Log:

Snowflake Validation of Error Message:



Sample : change the value to your own error code

```
SELECT SYSTEM$GET_LOGIN_FAILURE_DETAILS('44d9d1bd-0bd5-4c73-a95f-dcb41f0c4f36');
```

```
--OAUTH Errors
SELECT JSON_EXTRACT_PATH_TEXT(SYSTEM$GET_LOGIN_FAILURE_DETAILS('44d9d1bd-0bd5-4c73-a95f-dcb41f0c4f36'), 'errorCode');
```

Results | Chart

JSON_EXTRACT_PATH_TEXT(SYSTEM$GET_LOGIN_FAILURE_DETAILS('44D9D1BD-0BD5-4C73-A95F-DCB41F0C4F36'), 'ERRORCODE')
EXTERNAL_OAUTH_AUDIENCE_VALIDATION_FAILED

```
SELECT SYSTEM$GET_LOGIN_FAILURE_DETAILS('44d9d1bd-0bd5-4c73-a95f-dcb41f0c4f36');
SSO Authentication Failure
```

Results | Chart

SYSTEM$GET_LOGIN_FAILURE_DETAILS('44D9D1BD-0BD5-4C73-A95F-DCB41F0C4F36')
1 {"clientIP":"18.233.111.139","clientType":"JDBC_DRIVER","clientVersion":"3.13.21","username":null,"errorCode":"EXTERNAL_OAUTH_AUDIENCE_VALIDATION_FAILED","timestamp":1686627339}