

# OAUTH 2.0 Troubleshooting POSTMAN

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

- Test at Snowflake side:
- Final User Mapping between IDP & Alation Compose user & Snowflake:
- For B2B customer, you need to use unique\_name as AzureD is External Directory for those users
- POSTMAN for OKTA
- Error Recording at Snowflake Side
- Check Token at Alation Side:
- Check Error Codes from Snowflake to Alation

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](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.

## Prerequisite:

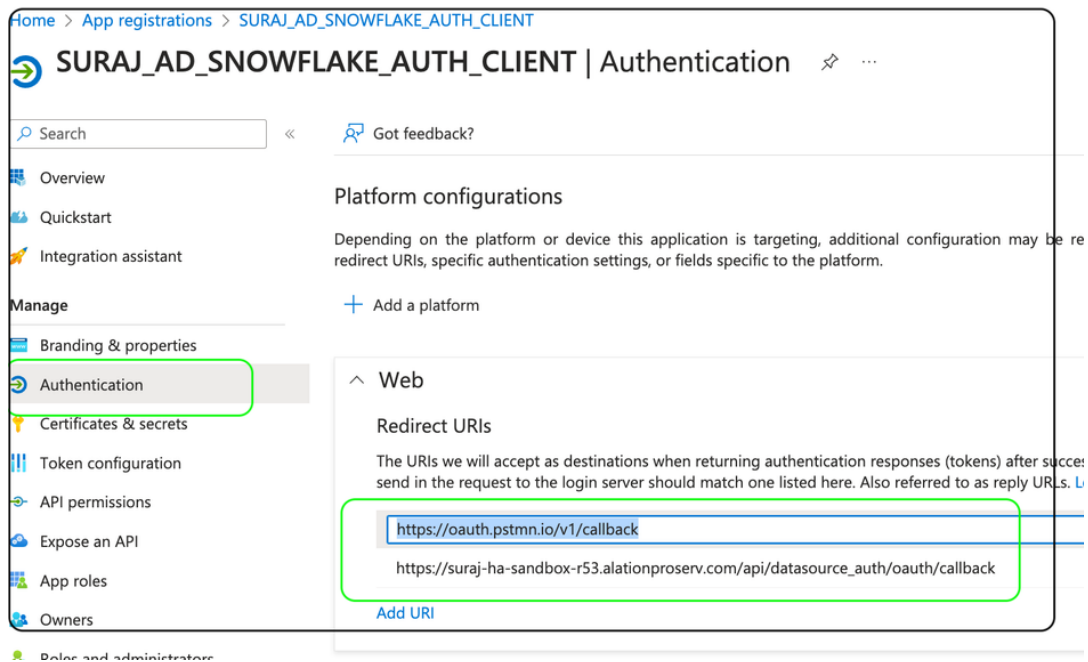
1. The POSTMAN tool is required (the web version also works). This can be installed on IDP admin, Alation admin (preferred), or Snowflake admin. Anyone can do this.
2. Details from OAUTH for Alation from IDP(Azure or OKTA or Ping or Another)

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.

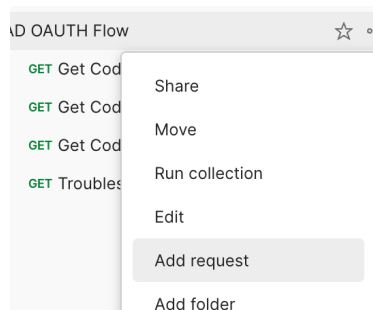
example Azure



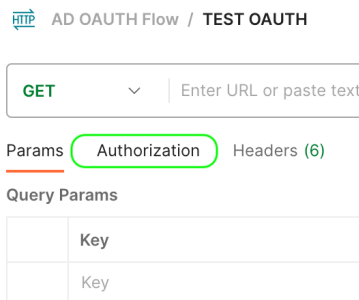
Step2:

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

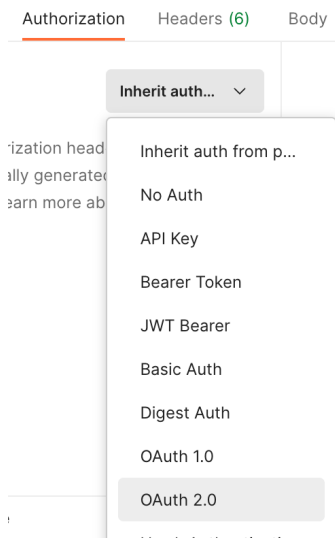
Once you launch postman , Just add a new request, give any name



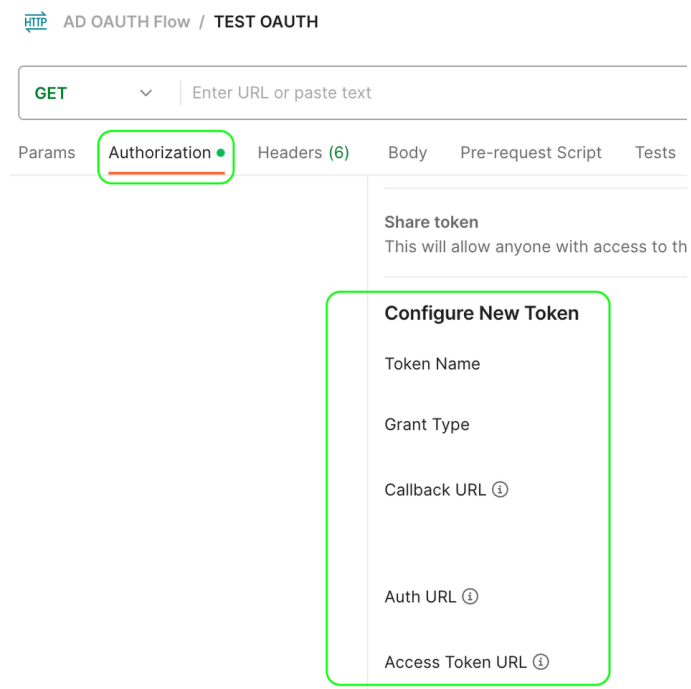
Switch to Authorization tab



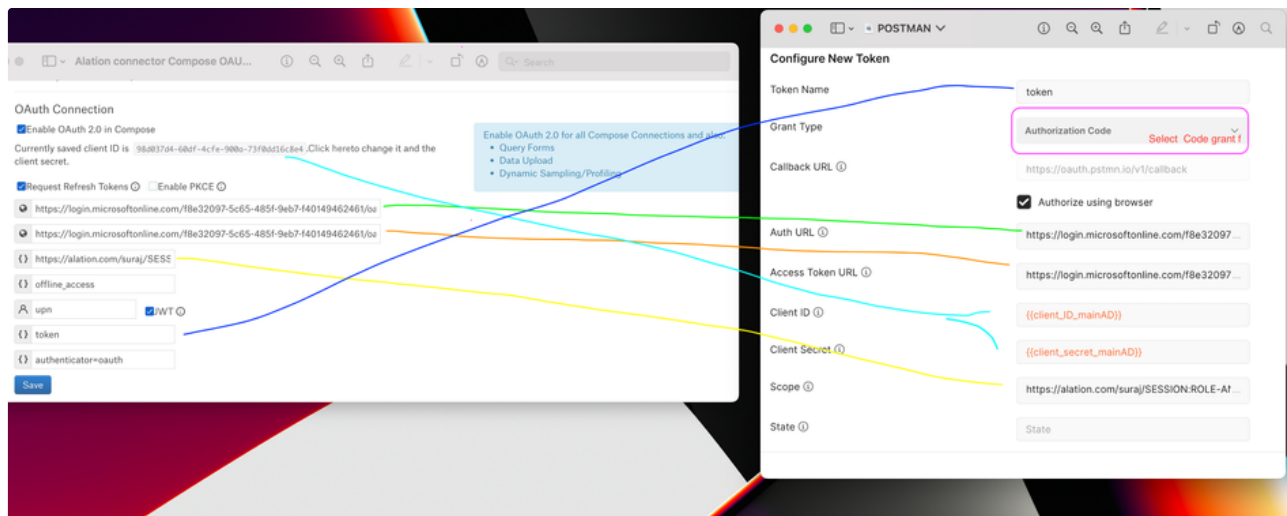
Select OAuth 2.0



Start filling the middle panel with configuration details

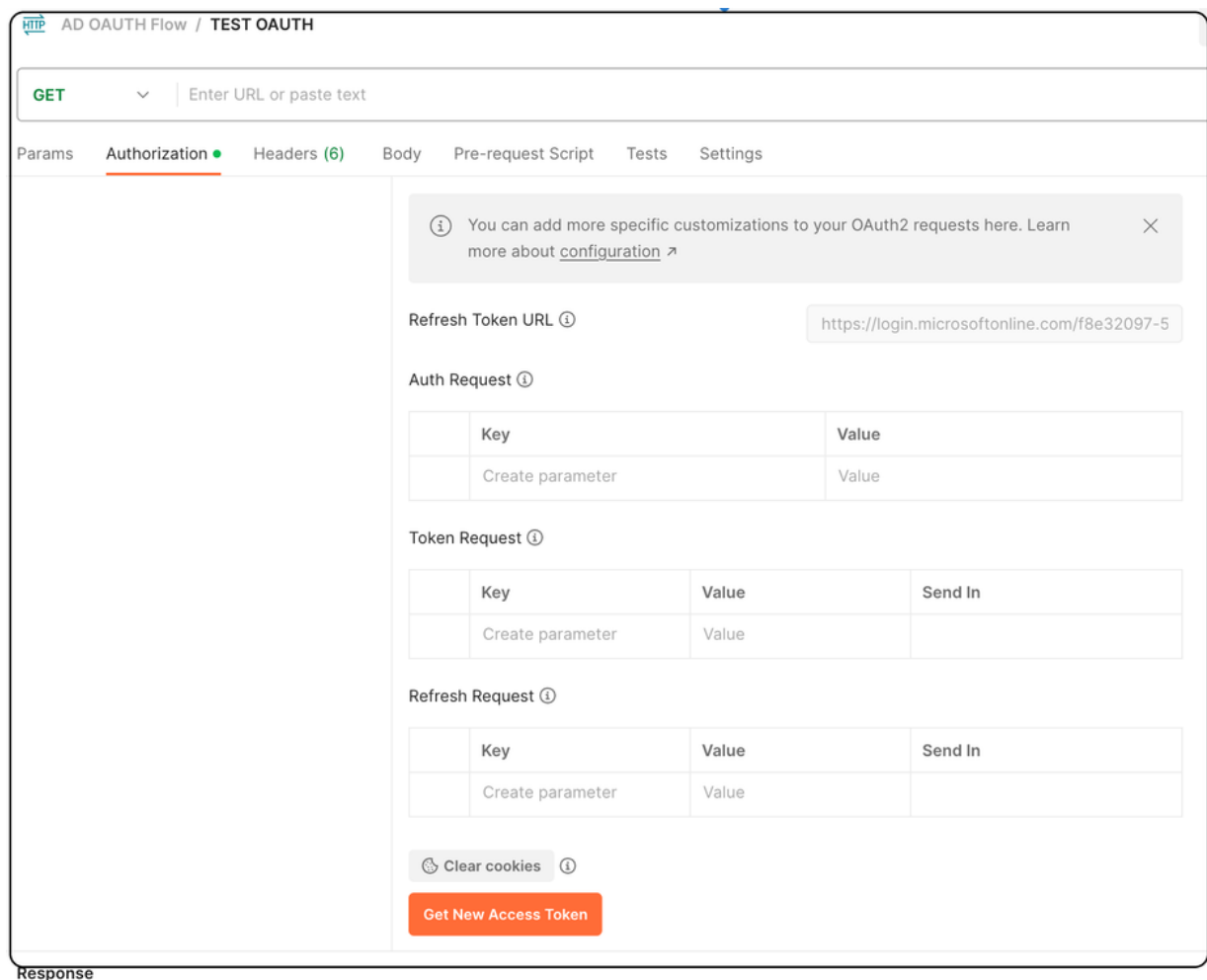


Map with same values use in Alation choose the Grant type as Code in PostMan



Step3: Testing

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

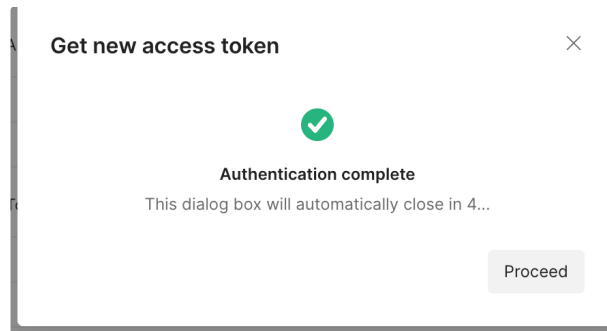


Note1: On click Get New Access Token

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

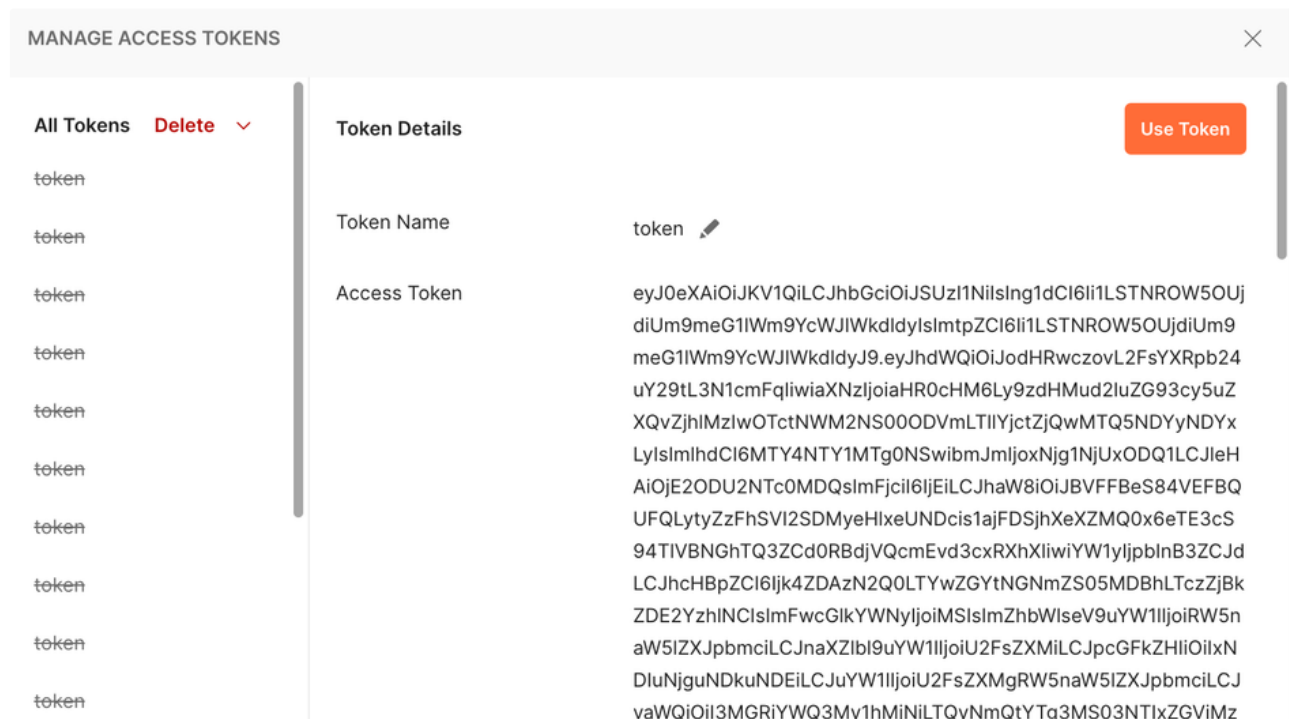
some time your browser will block url, see if any any warning if so allow that.

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

AD OAUTH Flow / TEST OAUTH

GET
Enter URL or paste text

Params
Authorization
Headers (6)
Body
Pre-request Script
Tests
Settings

Type
OAuth 2.0

The authorization data will be automatically generated when you send the request. Learn more about [authorization](#)

Add authorization data to
Request URL

Current Token
This token is only available to you. Sync the token to let collaborators on this request use it.

Token
token
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIng1c...

Expires at 7:04 pm today. Refresh

Header Prefix
Bearer

Auto-refresh token
Your expired token will be auto-refreshed before sending a request.

Share token
This will allow anyone with access to this request to view and use it.

Configure New Token

Token Name
token

Grant Type
Authorization Code

Now copy the Token

Environments
History

Params
Authorization
Headers (6)
Body
Pre-request Script
Tests
Settings

Type
OAuth 2.0

The authorization data will be automatically generated when you send the request. Learn more about [authorization](#)

Add authorization data to
Request URL

Current Token
This token is only available to you. Sync the token to let collaborators on this request use it.

Token
token
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIng1c...

Expires at 7:04 pm today. Refresh

Header Prefix
Bearer

Auto-refresh token
Your expired token will be auto-refreshed before sending a request.

Share token
This will allow anyone with access to this request to view and use it.

Configure New Token

Token Name
token

Grant Type
Authorization Code

Set: AzureAD ENV
Undo
Redo
Cut
Copy
Paste
Select All
Find: eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIng1dCI6Ii1LSTNROW5OUjdiUm9meG1lWm9...32ngQFv2tuxjT0eRP5tegXbt-L5z08nopRaHBGwglwmpy0\_ZYofx6yUz4GvGac8IL4UcUQ
EncodeURIComponent
DecodeURIComponent

Response

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

[illegible]

```
Decoded Token    Claims

{
  "typ": "JWT",
  "alg": "RS256",
  "x5t": "-KI3Q9nNR7bRofxmeZoXqbHEGw",
  "kid": "-KI3Q9nNR7bRofxmeZoXqbHEGw"
}

{
  "aud": "https://alation.com/sura",
  "iss": "https://sts.windows.net/f8e32097-5c65-485f-9eb7-f40149462461/",
  "iat": 1685652024,
  "nbf": 1685652024,
  "exp": 1685657083,
  "acr": "1",
  "aio": "ATQky/8TAAAAO7mtQU8kvcgsZ+SwoTOGLiN1BUG0X8HtZway9mJHrGhfmSGfQQ4rob9i57dRdb",
  "amr": {
    "pwd"
  },
  "appid": "98d037d4-60df-4cfe-900a-73f0dd16c8e4",
  "appidacr": "1",
  "family_name": "Engineering",
  "given_name": "Sales",
  "ipaddr": "142.68.49.41",
  "name": "Sales Engineering",
  "oid": "3f0dad73-a23b-426d-a871-7521deb35b11",
  "rh": "9.AXVAlpJj-GYCKDie_QBSUYkYVExqvqRGRIxgHrwefoUKAGM.",
  "scp": "SESSION:ROLE-ANY",
  "sub": "u0A0_J2YnvItbQyPXJ3GSakeG7EtrcoNX-bCqltLcLI",
  "tid": "f8e32097-5c65-485f-9eb7-f40149462461",
  "unique_name": "sales.engineering@alation.onmicrosoft.com",
  "upn": "sales.engineering@alation.onmicrosoft.com",
  "uti": "CP2a0wz0ESVHFITzflrAA",
  "ver": "1.0"
}.[Signature]
```

Test at Snowflake side:

Same token you can test : replace your token value

```
1 SELECT SYSTEM$VERIFY_EXTERNAL_OAUTH_TOKEN('eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIng1dCI6Ii1LSTNR0W5OUjdiUm9meG1lWm
```

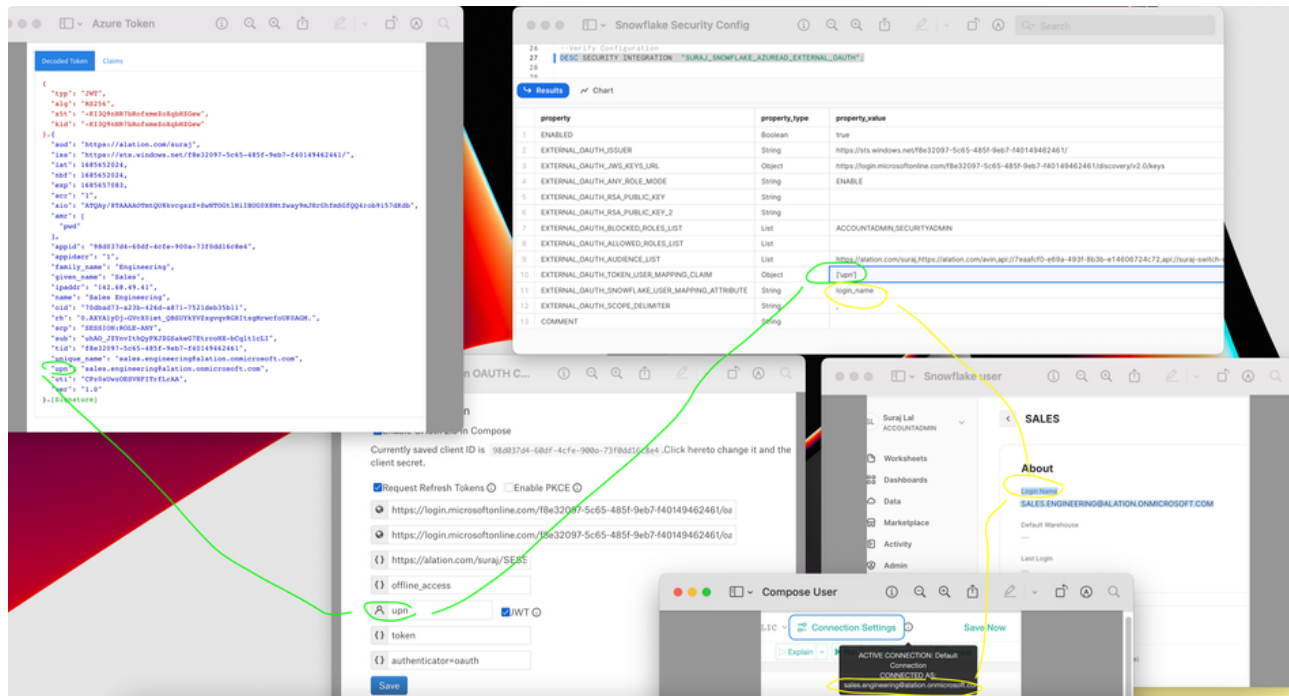
[illegible]

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

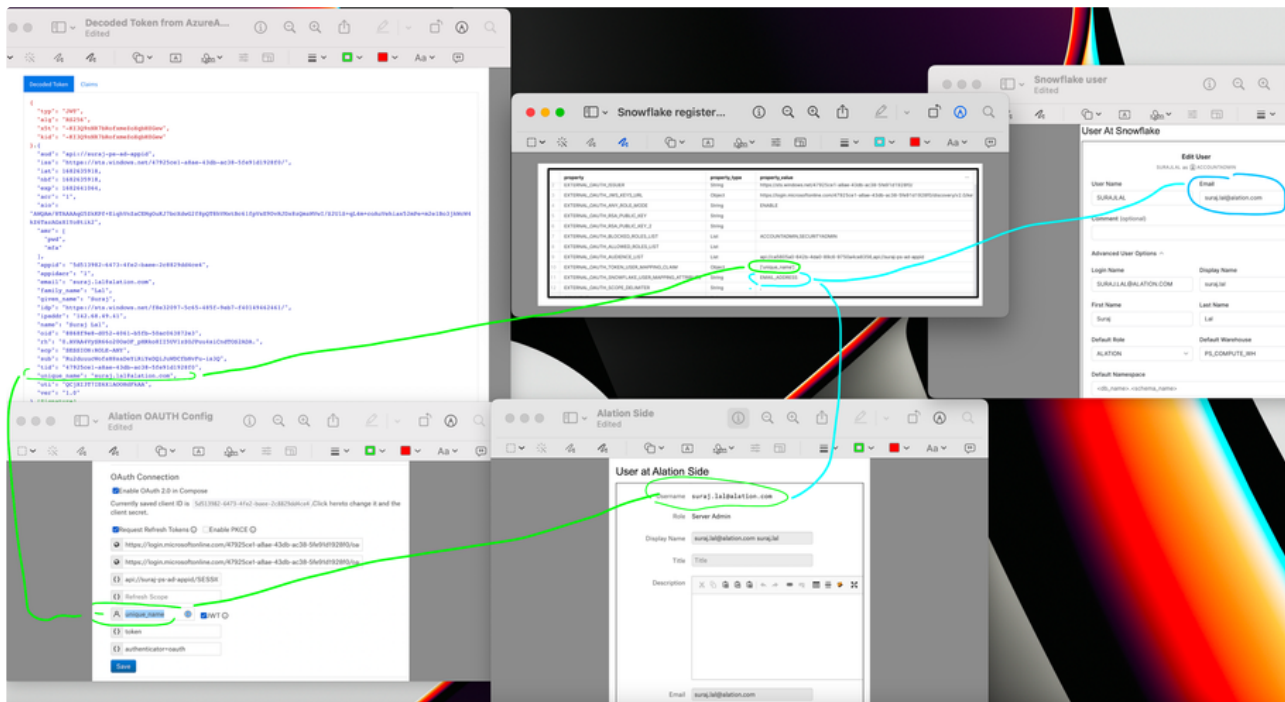
upn in Azure token

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

OAUTH Flow / OKTA test

Save

Enter URL or paste text

Send

Authorization

Headers (6)

Body

Pre-request Script

Tests

Settings

Cookies

Grant Type

Authorization Code

Callback URL ⓘ

https://oauth.pstmn.io/v1/callback

☒ Authorize using browser

Auth URL ⓘ

https://dev-66731772.okta.com/oauth2/a...

Access Token URL ⓘ

https://dev-66731772.okta.com/oauth2/a...

Client ID ⓘ

00a8jq9eoczePGg1g5d7

Client Secret ⓘ

Ee9T-LftzgpbcCVyED52h8P6cgCsWiF..

Scope ⓘ

SESSION:ROLE-ANY

State ⓘ

alation

Client Authentication ⓘ

Send as Basic Auth header

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

Applications

Applications

Self Service

API Service Integrations

Security

Workflow

Reports

Settings

Terms of Service URI ⓘ

Policy URI ⓘ

Logo URI ⓘ

https://ok12static.oktacdn.com/fs/bcg/4/gfs8jqbybsp7dkV015d7

LOGIN

Sign-in redirect URIs ⓘ

☐ Allow wildcard \* in login URI redirect.

https://suraj-ha-sandbox-r53.alationproserv.com/api/datasource\_auth/oauth/callback/

https://oauth.pstmn.io/v1/callback

Sign-out redirect URIs ⓘ

# Error Recording at Snowflake Side

```
1 select * from SNOWFLAKE.ACCOUNT_USAGE.login_history order by event_timestamp;
2
3
4 select *
5 from table(SNOWFLAKE.information_schema.login_history_by_user())
6 order by event_timestamp;
7
8 --For Last One Hour
9 select *
10 from table(SNOWFLAKE.information_schema.login_history(TIME_RANGE_START => dateadd('hours', -1, current_timestamp())
11 order by event_timestamp;
12
13
14 --For Last Four Hour
15 select *
16 from table(SNOWFLAKE.information_schema.login_history(TIME_RANGE_START => dateadd('hours', -4, current_timestamp())
17 order by event_timestamp;
```

Check the Error message

1  
2  
3

Results Chart

	EVENT_TYPE	USER_NAME	CLIENT_IP	REPORTED_CLIENT_TYPE	REPORTED_CLIENT_VERSION	FIRST_AUTHENTICATION_FACTOR	SECOND_AUTHENTICATION_FACTOR	IS_SUCCESS	ERROR_CODE	ERROR_MESSAGE
1	LOGIN	SURAJALAL	3.208.71.154	JOBC_DRIVER	3.13.21	GAUTH_ACCESS_TOKEN	NULL	YES	NULL	NULL
1	LOGIN	SURAJALAL	3.208.71.154	JOBC_DRIVER	3.13.21	GAUTH_ACCESS_TOKEN	NULL	YES	NULL	NULL
1	LOGIN	SURAJALAL	3.208.71.154	JOBC_DRIVER	3.13.21	GAUTH_ACCESS_TOKEN	NULL	YES	NULL	NULL
1	LOGIN	SURAJALAL	3.208.71.154	JOBC_DRIVER	3.13.21	GAUTH_ACCESS_TOKEN	NULL	YES	NULL	NULL
1	LOGIN	SURAJALAL	3.208.71.154	JOBC_DRIVER	3.13.21	GAUTH_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

```
[In [1]: OAuthTokens.objects.order_by('-id')[0].access_token
Out[1]: 'eyJraWQiOiJ3S3JQWXBZRMJhUElOVG95R1lpY0U5bE4xZHVfRUJYV1H1UWNxTS1XZGxJJi
iYWxnIjoiUlMyNTYifQ.eyJ2ZXIiOiJEsImp0aSI6IkFULj1SSX1oM2F4V1lnYUpEcjVme
UWR1LW1JbWVkyWNoNHVMOHMub2FyMTRhYThxbGNFWUpaYzY1ZDciLCJpc3MiOiJodHRwc
NjczMTc3Mi5va3RhLmNvbS9vYXV0aDIvYXVzOGpxampyd1VWU0tmVjg1ZDciLCJhdWQiO
IiwiaWF0IjoxNjg2Njc3MTMzLCJleHAiOiJlE2ODY2ODAzMzMzMmImNpZCI6IjBvYThqcT11k
NWQ3IiwidWlkIjoiMDB1OXh1ZjkwODg2QWxUV1A1ZDciLCJzY3AiOi01sib2ZmbGluZV9hY
RVNTSU9001JPTeUtQU5ZIl0sImF1dGhfdGltZSI6MTY4NjY3NjY0Nywic3ViIjoiU1VSQ
U1RAQUxBVElPTlBTLk90TU1DUK9TT0ZULkNPTSJ9.xli_X-Bs01-0LaZPPxaED8uW0icg
Vl5i7vH6-0PRqyS687cNH18ACimsVJDyxYBOMJYVHC-pxXMDLmcGTOfwf-ccVhSAtzYGg
vD6b_EKkS4PKMKpHi7sfe47pn0Q3GYn33hkamnE4rTu5otYYI1HmtaPfFLJRY99mz1qvl
88L_GsGWD1aLIUorPP0lagUCuvC03SxfUcXH8G32tgu4QRhdcc9Un8yL431Yueott7zs1
XB_QForhf8RhWC9fFg4IpdGsxtQuQcSvXHJU1CN5IVaWdPvss-fcYjcIwtFXMA'
```

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

```
1 SELECT SYSTEM$VERIFY_EXTERNAL_OAUTH_TOKEN('eyJraWQiOiJ3S3JQWXBZRMJhUElOVG95R1lpY0U5bE4xZHVfRUJYV1H1UWNxTS1XZGxJJi
```

## 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.



1--OAUTH Errors

2SELECT JSON\_EXTRACT\_PATH\_TEXT(SYSTEM\$GET\_LOGIN\_FAILURE\_DETAILS('44d9d1bd-0bd5-4c73-a95f-dcb41f0c4f36'),'errorCode');

3

4SELECT SYSTEM\$GET\_LOGIN\_FAILURE\_DETAILS('44d9d1bd-0bd5-4c73-a95f-dcb41f0c4f36');

ResultsChart

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

44SELECT SYSTEM\$GET\_LOGIN\_FAILURE\_DETAILS('44d9d1bd-0bd5-4c73-a95f-dcb41f0c4f36');

45SSO Authentication Failure

ResultsChart

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}	