WF-06: B2B (Business-to-Business) users - Onboarding

Overview

The page represents sequence and flow diagrams for 'Okta integration with AWS Cognito' for Business to Business (B2B) users on Production.

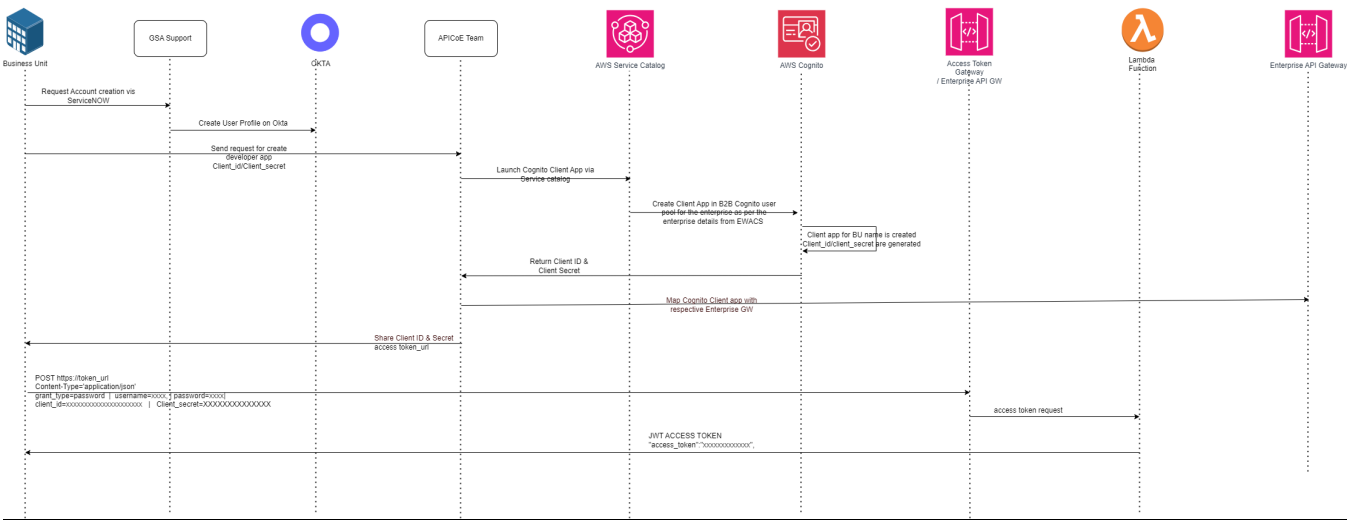
Pre-Requisites

Get Business user information from EWACS

EWACS & OKTA Details	
Section	**Select/Include**
Region	<<Region Name>>
Description	Request EWACS account created in EWACS Production
Details	First Name: Last Name: Email: DL or team name Telephone User ID User Role: End User EWACS Product Name (to be assigned to the account) List of IPs (as per IP restriction requirement)
Assignment Group	Select "EITS IAM SSO Requests" for US account Select "EITS IAM EWACS Requests" for UK account

Sequence Diagram

A) Create B2B account

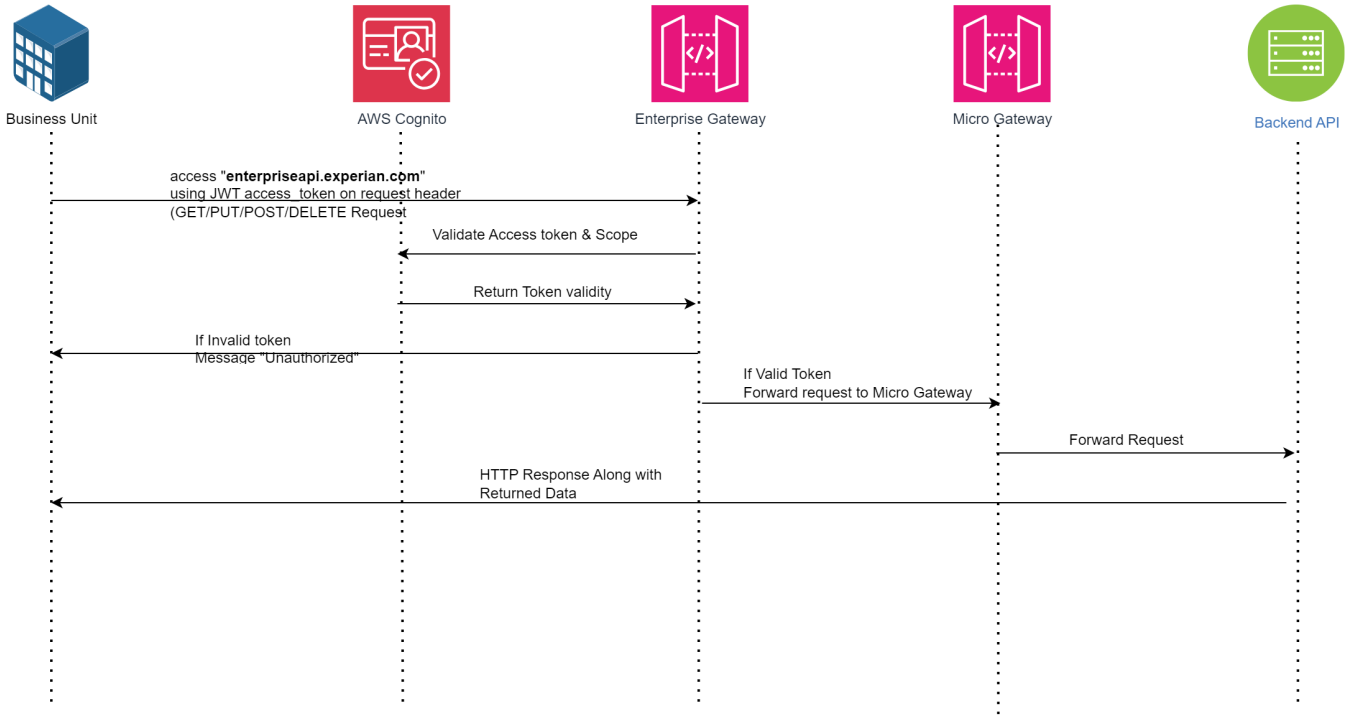


Sequence Flow/Steps

Onboarding B2B user

1. Business Unit will raise a **ServiceNow** request to onboard a new B2B user
2. The GSA Support team will then go ahead and create an user profile on OKTA
3. Business Unit will request client_id/client_secret, token_url for the client application from APICoE team via **ServiceNow**
4. APICoE team will Launch Cognito Client App via Service catalog
5. Create Client App in B2B AWS Cognito user pool for the B2B user as per the user profile details recevied from EWACS system. Client_id /client_secret is generated for the Cognito Client app
6. APICoE team maps Cognito Client application with respective API GW
7. AWS Cognito returns 'Client_id/client_secret' to APICoE team
8. APICoE team shares client_id/client_secret, token_url with Business Unit
9. Business user uses token_url to invoke Access Token Gateway (Enterprise API Gateway) using 'grant_type=password', Okta user/password
10. Access Token Gateway sends the 'access token request' to Enterprise Gateway
11. Enterprise Gateway returns the 'JWT access token' back to the Business user

B) B2B user access to invoke APIs



Sequence Flow/Steps

B2B user access once onboarding is done

1. Business user accesses the 'enterpriseapi.experian.com' using JWT access_token on request header. The request reaches the Enterprise Gateway first.
2. Enterprise Gateway will validate the access token and the scope with AWS Cognito.
3. AWS Cognito returns token validity back to Enterprise Gateway.
4. If the token is invalid then 'Unauthorized message is sent to the user from Enterprise Gateway. If the token is valid, then the request is forwarded to MicroGateway from Enterprise Gateway.
5. Microgateway will forward the request to the respective backend API.
6. Backend API will return the data with HTTP response.