

**Qualcomm Car-to-Cloud Platform**

**Cognito Token Generation**

**Version No.1.0**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Prepared By / Last Updated By** | **Reviewed By** | **Approved By** |
| **Name** | Nakhash Alam | Sudheer Kumar | Sudheer Kumar |
| **Role** | PAT | Sr Manager | Sr Manager |
| **Signature** |  |  |  |
| **Date** | 27 May 2021 | 10 June 2021 | 10 June 2021 |

May 26, 2021

Cognizant

Contents

[1. COGNITO TOKEN GENERATION 2](#_Toc74257984)

[1.1. User Confirmation 2](#_Toc74257985)

[1.2. Token Generation 3](#_Toc74257986)

# 1. COGNITO TOKEN GENERATION

Amazon Cognito is a simple user identity and data synchronization service that provides authentication, authorization and user management, helping us securely manage app data across applications for our users. Amazon Cognito allows us to control permissions for different users’ groups in our applications to ensure that they have appropriate access to back-end resources according to the group they belong to.

The project consists of mainly 2 Rest end points:

* Confirm user for the first time login.
* Generating the ID/Bearer token.

## User Confirmation

The Get request */c2c-auth/confirm-password* handles the user confirmation. The user starts to sign in for the first time by submitting the required credentials which include the temporary AWS password. The password is authenticated, and a new password is provided by the user.

**Confirm User**

Request Method: POST

Request URL: <http://localhost:8080/c2c-auth/confirm-password>

**Sample Request Body**

***{***

***“username”: “user1”,***

***“password”: “1234\_AB”,***

***"newPassword": "$Password123$",***

***"userPoolId": "us-east-1\_xxxxxxx",***

***“appClientId”: “1abcdef2ghijkl3m4xxxxyyy78”,***

***"appClientSecret": "1ktf0hgfj1hph6nb9bo7g2ad4tbqv4e8ttvdhxxxxxyyyyy"***

***}***

**Sample Response Status**

Body: User Confirmed

Status: 200 OK

**Sample Exception Response**

Body: AWSCognitoIdentityProviderException or GeneralSecurityException occurred.

Status: 401 Unauthorized

## Token Generation

The Get request /c2c-auth/get-token handles the token generation. After the user has successfully changed his or her password and optionally provided attributed values, the user is signed in and tokens are issued. In the request body the new Password is set as null as it is not needed while generating the token.

**Get Id Token**

Request Method: POST

Request URL: http://localhost:8080/c2c-auth/get-token

Sample Request Body

**{**

**“username”: “user2”,**

**“password”: “$password123$”,**

**"newPassword": null,**

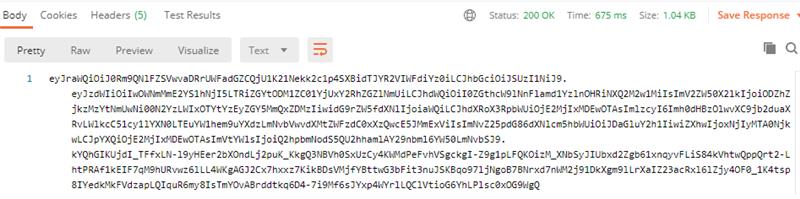
***"userPoolId": "us-east-1\_xxxxxxx",***

***“appClientId”: “1abcdef2ghijkl3m4xxxxyyy78”,***

***"appClientSecret": "1ktf0hgfj1hph6nb9bo7g2ad4tbqv4e8ttvdhxxxxxyyyyy"***

**}**

**Sample Response Status**



**Sample Exception Response**

Status: 400 Bad Request

Body: 401 Unauthorized

***Exceptions***

**CognitoException** is thrown when the following exceptions takes place:

1. NotAuthorizedException - thrown when a user is not authorized.

2. AWSCognitoIdentityProviderException - base exception for all the service exception thrown by Amazon Cognito Identity Provider.

3. GeneralSecurityException- exception class that provides type safety for all the security-related exception classes that extend from it.