Firstly, in Cognito UserPool create a user using the below steps:

1. Navigate to the Users and groups under General settings tab.
2. The Users tab in the Users and groups tab has a Create user button, click it.
3. When you choose Create user, a Create user form appears, which you can use to enter information about the new user.
4. Enter a user name.
5. Select Email to send an invitation to this new user option.
6. Untick "Mark phone number as verified?" option.
7. Provide an Email address in the Email text field and select the option Mark email as verified.

Next, configure the App Client using the below steps:

1. On the App integration tab, click on App client settings.
2. For Enabled Identity Providers, tick mark Cognito User Pool.
3. Enter the Callback URLs you want, separated by commas. For eg: [https://example.com](https://example.com/)
4. (Optional) Enter the Sign out URLs you want, separated by commas. For eg: [https://example.com](https://example.com/)
5. Under OAuth 2.0, select Implicit grant (required) and Authorization code grant (optional).
6. For Allowed OAuth Scopes, select all the scopes.
7. Save changes

Now, to get the tokens you can either use the Hoster UI or the CLI command.

**[Option-1] Obtaining tokens using Hosted UI**

To get the Hosted UI, follow the below steps:

1. Select Choose domain name.
2. On the Domain name page, type a domain prefix and save changes. Make a note of the complete domain address. [Check availability option may not work at the moment, please save the changes directly. You need to make sure that the domain is unique. If you get an error, try putting a unique domain name.]
3. Choose Save changes.
4. You can view the hosted UI sign-in webpage with the following URL where response\_type=token. After a successful sign-in, Amazon Cognito returns user pool tokens to your web browser's address bar.

https://"<\your-domain>"/login?response\_type=token&client\_id="<\your-app-client-id>"&redirect\_uri="<\your-callback-url>"

Note: Replace value with actual Cognito UserPool configuration.

**Find the following values at:**

1. Domain Name: You will find the domain name Domain name section under App integration. It has the following format: <\your-domain>.auth.ap-south-1.amazoncognito.com
2. Client Id: You will find the Client Id in App Client section under General settings.
3. Callback/Redirect Url: You will find the Callback/Redirect Url in the App Integration section under App client settings. It is present in Callback URL(s).

Once you see the Hosted UI page, enter the username and the password (received via Email). Upon successful login, you will be redirected to the configured callback Url and you will find the JSON web token (JWT) identity token in the browser Url after the #idtoken= parameter in the response.

**[Option-2] Obtaining tokens using CLI**

First run AdminInitiateAuth command. AWS CLI Syntax for AdminInitiateAuth:

aws cognito-idp admin-initiate-auth --user-pool-id "<\user-pool-id>" --client-id "<\client-id>" --auth-flow ADMIN\_NO\_SRP\_AUTH --auth-parameters USERNAME="<\username>",PASSWORD="<\password>" --region "<\value>" --region "<\region>"

You will then get a NEW\_PASSWORD\_REQUIRED challenge which you need to answer using AdminRespondToAuthChallenge command:

aws cognito-idp admin-respond-to-auth-challenge --user-pool-id "<\user-pool-id>" --client-id "<\client-id>" --challenge-name NEW\_PASSWORD\_REQUIRED --challenge-responses NEW\_PASSWORD="<\password>",USERNAME="<\username>" --session "<\value>" --region "<\region>"

Note: Replace value with actual Cognito UserPool configuration.

**Find the following values at:**

1. Client Id: You will find the Client Id in App Client section under General settings.
2. UserPool Id: Click on the general settings tab and you will find the UserPool Id.

Now, check if the user is in CONFIRMED state by Navigating to the Users and groups under General settings tab.

As the JAM challenge answer, submit the username and password of the user you have create in the following format: **username:password**