STEPS TO CONFIGURE AWS IoT

Log into to Amazon AWS Console at console.aws.amazon.com. Make sure your region is set to Singapore.

1. Create a User Pool
   • Go to http://ap-southeast-1.console.aws.amazon.com
   • Choose "Services > Security, Identity & Compliance > Cognito"
   • Click "Manage User Pools"
   • Type a name for the user pool and click "Review Defaults"
   • Click "Create Pool" and a user pool will be created.

2. Create project in AWS Console
   • Go to http://ap-southeast-1.console.aws.amazon.com
   • Choose "Services > Mobile Services > Mobile Hub", create a new project by clicking on "Create"
   • Give the project a name. Click "Next"
   • Choose "Android" platform. Click "Next"
   • Choose "Next" because we will download the cloud config file later after making some modifications.
   • Click "Done". A screen will be shown where you can enable backend features for your newly created project.
   • From "Add More Backend Features" section, choose "User Sign-in"
   • Click "Import an existing user pool"
   • Your recently created cognito user pool should appear in a list below. Select it and choose "import user pool" button at the bottom.
   • You will see a notification at the top. Click "Choose this banner to return to the project details page..." to return to project details.
   • Click the blinking "Integrate" button. It will prepare a new cloud config file with new settings. So click "Download config file" and save it.
   • Click "Next" and then "Done"

3. Create Cognito Identity Pool
   • Go to http://ap-southeast-1.console.aws.amazon.com
   • Choose "Services > Security, Identity & Compliance > Cognito"
   • Click "Manage Identity Pools"
   • Click "Create new identity pool"
   • Type a name
   • Expand "Authentication providers" section
   • Enter "User Pool ID" from previously created user pool page (On user pool page, click "General Settings" in left panel to see User Pool ID)"
   • Enter "App Client ID" from previously created user pool page (On

user pool page, click "App Clients" under "General Settings" in left panel to see App Client ID)"
- Now click "Create Pool" to create the identity pool
- On next page, it will create two roles, one for authenticated users and another for unauthenticated users. Click "Allow"
- On next page, it will show Getting started with Amazon Cognito. Note down the identity pool id highlighted in red.

4. Assign action policy to roles created with Cognito Identity Pool
- Go to http://ap-southeast-1.console.aws.amazon.com
- Choose "Services > Security, Identity & Compliance > IAM"
- Click "Roles" in left panel
- You will see the roles created above with Cognito Identity Pool. Click the Auth role.
- Now click "Attach Policies"
- In search box, type "AWSIoTFullAccess" and select AWSIoTFullAccess below. Now click "Attach policy"

Note: We can assign partial access for IoT resources here e.g. only subscribing to a topic or publishing to a single topic etc.

5. Create Policy for Cognito Identities:
- Go to http://ap-southeast-1.console.aws.amazon.com
- Choose "Services > Internet of Things > IoT"
- From left panel, choose "Secure > Policies"
- Click "Create a policy"
- Type name for the policy
- Choose "Advanced mode" and replace the text with following:
```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "iot:Connect",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iot:Publish",
        "iot:Subscribe",
        "iot:Receive"
      ],
      "Resource": "*"
    }
  ]
}
```

- Now click "Create" button

I will need the following to integrate into Android development.
    - IoT Endpoint
    - Cloud config document downloaded - Step 2
    - identity pool id - Step 3
    - Name of policy created - Step 5