Providing Authentication for API Endpoint using API Key

1. Creating an API Key
   1. In Left Panel of API, Select API Keys
   2. Create a New API Key
2. Create a Usage Plan
   1. In Left Panel of API, Select Usage Plans
   2. Provide with a Name for the Usage Plan
   3. Rate temporarily is assigned as 100 Requests per Second
   4. Burst rate is assigned temporarily as 200 Requests per Second
   5. For Associated API Stages:
      1. Select the API which needs to be assigned with the API Key Created in First Step
      2. Select the Stage in which assignment of the API Key needs to be deployed
      3. Create this Usage Plan
3. Select the API we wish to authenticate using Access Key
   1. In Left Panel, under the API, Choose ‘Resources’
   2. Select the specific resource we want to authenticate (e.g. GET, POST, DELETE)
   3. Click on ‘Method Request’ box
   4. Change ‘API Key Required’ option to true
   5. Add a new HTTP Request Header named ‘x-api-key’
   6. Mark this header as ‘Required’
4. Deploy the API under the same ‘stage’ name which we have chosen in second step.
5. Visit the Lambda Function which is attached to this specific API
   1. Click on ‘Triggers’ option
   2. Verify if the API Link and method name, which is associated with this Lambda function, is same as the method name which is associated with the API.
6. Test the process now using Postman
   1. Use body as raw using:

{

"operation": "create",

"tableName": "Device1-Table",

"payload": {

"Item": {

"DeviceId": "Device1",

"DateTime": "2017-09-27 13:55",

"Milk Temperature": "4.4",

"TSS Temperature": "-5.1",

"AC Voltage": "240",

"Battery Voltage": "22"

}

}

}

* 1. Use Header with ‘key’ : ‘x-api-key’ and ‘Value’ : ‘API\_KEY\_VALUE’
  2. Use POST method (we have deployed this method in the API)
  3. Use URL of the API for that specific POST Method
  4. Click ‘Send’