**CHAP (Challenge Handshake Authentication Protocol)**

1. As a prerequisite client gets registered and further authenticated with Client ID, Username and Password.

Example:

Client ID: 623a20f6-9ee6-11e8-8ea6-87ff64ab94b0

Username: admin

Password: Mule123!

1. Client will request to generate a challenge key.

Challenge Key: curl -k -I -X GET https://{{ip}}:{{port}}/api/accessmgmt/auth -H

With their ‘ClientID: 623a20f6-9ee6-11e8-8ea6-87ff64ab94b0’

1. In response to the request, a challenge key gets generated and notified the same to the client i.e.

Response: 200 OK

Body: a7451b74-a1fc-11e8-bc5e-43c2515321d0

1. Client to perform the following events.

* Cipher Text is generated for “username: password” with a sequenced base, i.e. AES128HASH.
* i.e., encrypt (“Body: a7451b74-a1fc-11e8-bc5e-43c2515321d0", “admin: Mule123! “ )
* Cipher Text is further secured using Base64 encoding, this secured Cipher Text is called secure hash.

1. Client requests, server to generate CHAP authentication token by sending the secure hash.

CODE:

**{**

**"intentName": "VM",**

**"intentDescription": "virtual machine provisioning intent",**

**"notes": "null",**

**"isScheduled": false,**

**"intentParameters": {**

**"ORIGIN": "Phone",**

**"STATUS": "New",**

**"SUBTYPE": "VM with no VLAN",**

**"DESCRIPTION": null,**

**"PRIORITY": "Medium",**

**"REGION": "US-WEST-Phoenix",**

**"TYPE": "Service Catalog",**

**"STORAGE": "120GB",**

**"CREATEDDATE": "2018-07-24T09:01:59.000Z",**

**"CASENUMBER": "00001105",**

**"ID": "5007F00000NopbdQAB",**

**"CLOSEDDATE": null,**

**"GUESTOS": "Linux"**

**}**

**}**

1. This CHAP authentication token is used by client for all other API calls.