# Access Management

Anypoint Access Management enables you to create Anypoint Platform account or configure External Identity.

It configures access and permissions within your organization and, depending on the access level, manages the users and their roles.

It provides administrative and organizational abilities that apply to the various entitlements in Anypoint Platform

Exercises:

* + - * 1. Create a mule application and implement OAuth2 using Mule Auth provider
        2. Create a mule application and implement secure property placeholder to encrypt sensitive information like passwords and use hidden properties
        3. Access Audit Logs using Platform API
        4. Business Groups
        5. Use crypto module in dataweave to encrypt a part of payload
        6. Create a mule application and implement OAuth2 using Mule Auth provider
        7. Create a mule application and implement secure property placeholder to encrypt sensitive information like passwords and use hidden properties

https://www.youtube.com/watch?v=xZk716qHNA0

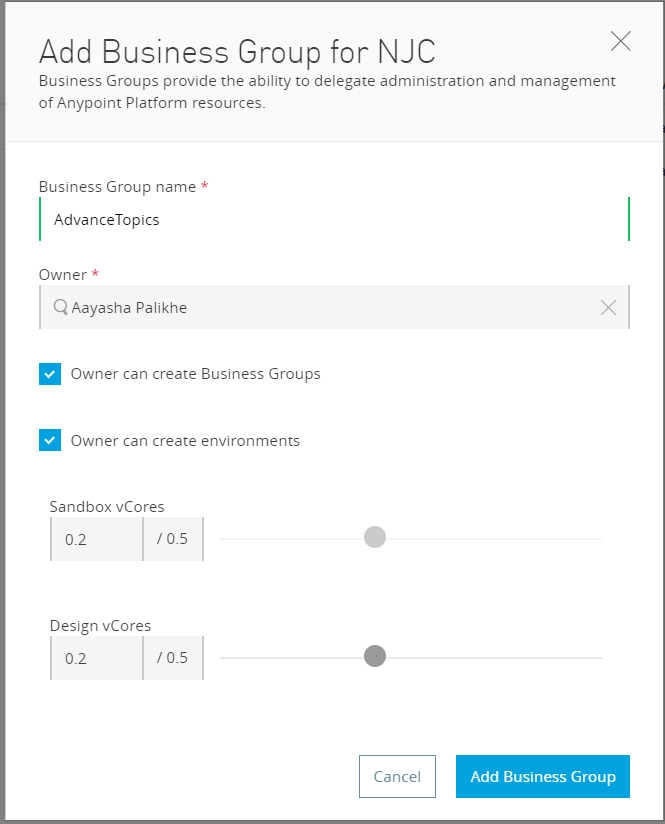
* + - * 1. Access Audit Logs using Platform API
        2. Business Groups

Create a Business Group

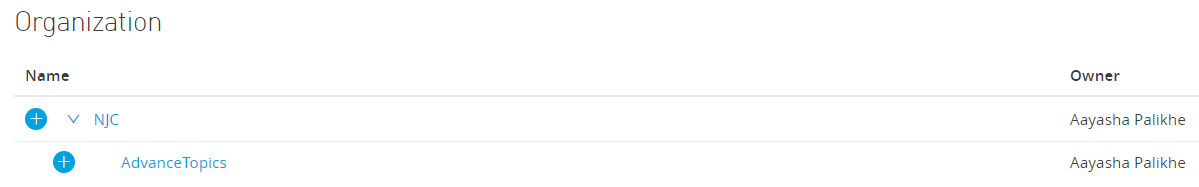
Log in to anypoint platform

In Access Management> Organzation Press + sign to add new Group

Complete the “Add Business Group For NJC “



After creating it you will see as



dd

* + - * 1. **Use crypto module in dataweave to encrypt a part of payload**

Ref: https://dzone.com/articles/implementing-dataweave-crypto-with-mulesoft

* Uses various algorithms like MD5, SHA1
* To use Crypto in the Datawave, one must import Crypto by using **import dw::Crypto**
* We can perform various functions in dataweave to encrypt the part of our payload.

1. **HMACBinary:**

HMACBinary function will compute the HMAC hash with a Cryptographic Secret key on input data

Hashing Algorithm. By default, HmacSHA1 is used

1. **HMACWith**

HMACWith function will compute the HMAC hash with a Cryptographic Secret key on input data and transform the message into lowercase and hexadecimal string.

Hashing Algorithm. By default, HmacSHA1 is used

1. **MD5**

MD5 function will compute the MD5 hash and transform the binary message into lowercase and hexadecimal string.

1. **SHA1**

SHA1 function will compute the SHA1 hash and transform the message into lowercase and hexadecimal string.

1. HashWith

HashWith function will compute hash depending on the algorithm provided.

Supported algorithms are SHA1, SHA256, SHA384, SHA512, MD2, MD5 etc