# <https://dzone.com/articles/mule-oauth-20-provider-in-mule-4>

https://www.youtube.com/watch?v=IYKaps1ndxI

# 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

**Features of Access Management:**

* Managing organizations, business groups,  users, roles, permissions, and environments
* Monitoring subscriptions and audit log
* Connect to existing (Idp) IDentity Management Solutions

# Organization

An Organization is an administrative collection of resources and users. When you create an Anypoint Platform account, a master (or root) organization is created, and you are assigned as the owner of the organization. Organization owners automatically inherit the Organization Administrators role.

An organization is an account where multiple users can share resources, including applications and environments. The level of access users have to various resources depends on their assigned roles and permissions.

* Organization owner : who creates an any point account
* Every organization have client ID and client secret
* It is used to authenticate the user and APIS
* The default time to expire is 60 mins
* The max time to is 180 mins

# Business Group

- Business groups are self-contained resource groups that contain Anypoint Platform resources such as APIs and applications. Business groups provide a way to separate and control access to Anypoint Platform resources, as users have access only to the business groups in which they have a role

Business groups provide more fine grained control over access to resources. It lets you delegate management of your Anypoint Platform resources including APIs, Runtime Manager applications, other business groups, users and roles. Each Business Group has its own set of permissions and roles. It provides complete isolation of resources and leads to multi-tenant use cases within an Anypoint Platform account.

* These are self contained resource group
* Max group can be of 100
* Deleting a business group will delete all its nested child. Once deleted it cannot be recovered so its not recommended to delete the root business group

User roles-

* Organization Administrators role to manage users
* Disadv: when we assign a user role we have to assign it in each business group that user will be added into
* This can be overcome: creating a team and adding the user permission on the team
* Roles and permissions are grouped under organizations (and also, optionally, under business groups). This means that you can only assign roles and permissions that are related to resources that exist in the organization and/or business group that you are selecting.
* User --- Permission -- API: which API user can see
  + - * -- Runtime: create/ delete, manage VPC
      * -- Role: assign roles, organize admin role, organize center role
* Internal user
  + To add users to an organization, or in a business groups, you can invite new users and manage existing users for your organization on the Access Management Administration page
* External user
  + When you make an API portal public, users from any other Anypoint Platform organization can register client applications to call your API
  + Admin can disable external user at any time
  + Block them from accessing the portal

Identity Management

* configure identity management in Anypoint Platform to set up users for single sign-on
* Can be done by two ways:
  + OpenID Connect
    - DISADV: do not support single logout
      * Do not support role mapping: role are not added automatically
  + SAML
    - Every step has separate URL
    - Everything works on the URL basis

# Roles

* To manage roles and permissions within Anypoint Platform, you must have the Organization Administrators role.
* To manage user permissions for an API version, you must have the API Versions Owner role.
* Anypoint Platform provides two types of roles
  + Default role:  Roles that are created automatically when an organization or business group is created
  + Custom role: You can create and delete custom roles. You can assign users and add permissions to a custom role, as well as associate a custom role with specific Anypoint Platform products

# Client Management

* acts as a client provider by default, but you can also configure external client providers to authorize client applications.
* Owner can apply an OAuth 2.0 policy to authorize client applications

Oauth

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

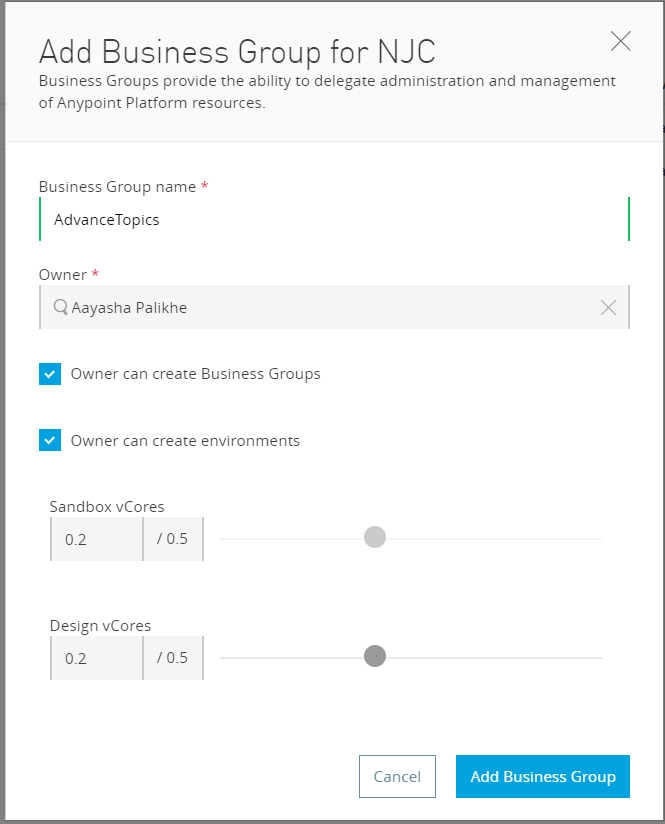
* + - * 1. Access Audit Logs using Platform API
        2. Business Groups

Create a Business Group

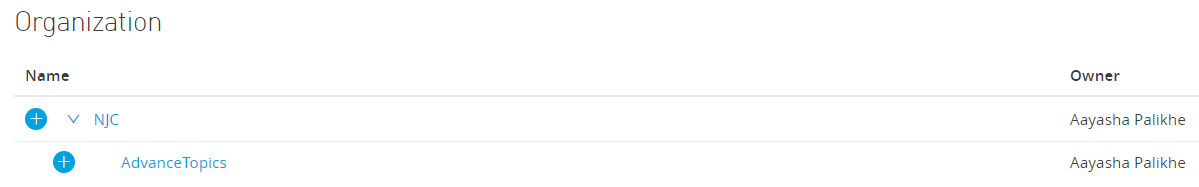
Log in to anypoint platform

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