# 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 anypoint 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.

Resources like vCores are assigned to business groups, and vCores assigned to a business group are available only to that particular group and unavailable even to the parent organization

* These are self contained resource group
* Max group can be of 100 it include all the sub groups
* 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
  + The users whom you send an invite will receive a link to signup to your anypoint account
* 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
  + To allow users to perform task like deploy an application you must send an invite

Identity Management

* configure identity management in Anypoint Platform to set up users for single sign-on
* Externam Identity Management can be done by two ways:
  + OpenID Connect
    - End user is verified by authorized server
    - DISADV: do not support single logout
      * Do not support role mapping: role are not added automatically
    - Example of SAML provider are: Okta, PingFederate, Salesforce
  + SAML
    - It is a web based authorization include cross domain SSO
    - Every step has separate URL
    - Everything works on the URL basis
    - Example of SAML provider are: Okta, PingFederate, Salesforce
* **Limitations**
  + OpenID Connect does not support single logout.
  + OpenID Connect does not support role mapping.
  + If a SAML user belongs to certain groups, Anypoint Platform does not automatically grant equivalent roles in the organization.
  + Anypoint Platform does not generate the SAML assertion for single sign on. Your IdP generates the sign-on URL that you configure.
  + External identity configuration is available only at the organization level. You cannot configure an external identity provider for a business group

# 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.
* A role is a set of pre-defined permissions for each product, or feature, within Anypoint Platform. Depending on the product, you can use pre-defined roles with standard permissions, or you can specify your own permissions for each role
* Roles are business group specific, so ensure that you are in the correct business group
* 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 2.0

* It is an authorization server
* In this client sends a request to the Okta. The okta responds with a bearer token. The bearer token is then validated by the API gateway with the Okta server
* If it validates true then it gives access to the resources

# Audit Logs

* The audit logging service provides a queryable history of actions performed within the Anypoint Platform.
* It keeps track of all users who have interacted with objects in the system, and timestamps of those actions.
* It also provides mechanisms for querying the set of users who have performed actions, the set of objects that had actions performed on them, and other endpoints that enable the querying of log entries.
* accessed from **UI of anypoint platform** or from **Audit logging Query API** provided by Mulesoft.

# Secure Configuration Properties

* it is a mechanism to encrypt the properties file to protect the resources **in .yaml or .properties** file
* we store information like Client ID, Secret, UserId, UserPassword, Splunk Tokens, Oauth Token, AWS Keys
* adv: encrypt the data inside any property files to **restrict unauthorized access** and **to protect the data**.
* Supported Configuration file types are: **.yam and .properties** file
* Supported Algorithms: AES(default), DES, Blowfish, RS2, RCA etc
* Supported Modes: CBC, CFB, ECB, OFB
* Steps:
  + Create a config file in the src/main/resources
  + Encrypt the sensitive information
  + Set up config setting
* Two ways to perform encryption
  + Encrypt security: <https://nl.devoteam.com/en/blog-post/how-to-secure-properties-and-hide-encryption-key-in-cloudhub-mule-4/>
    - This method does not support the yaml structure
  + Secure property in .jar file
    - Adv: encrypt all the file at a time
    - Disadv: require to copy the encrypted to config file manually

# Oauth 2.0

* Protocol for standardization
* If API is Oauth secured , the client is verified
* Providers: Okta, PingFederate, OpenAM
* TO use it we need to build an application
* Oauth Dance: authentication module operation
  + Create client: create client in object store
  + Delete client
  + Validate token
  + Revoke token
* Scope- limiting access in a resource to read / write
* This is applied at the organization level
* The oauth tokenization policy: it will check if the policy created matched the policy applied are same
* When to use Oauth provide?
  + If customer don’t have any identity provider
  + If customer don’t want to have a contract with third party
* Every time an application is created a token is generated specific to it
* What resources are limiting when we use scope?
* Client type
  + Confidential
  + Public
* Grant Type: determines how token is generated
  + Authorization code
    - Most secure
    - Frequently used
    - When clien send a request first an intermediary token is generated before the actual token
  + Implicit
    - Used by the java script and mobile apps
    - No intermediary code
  + Resource
    - USER CREDENTAIL DATA IS STORED
  + Client\_Credential
    - Least secure of all
    - Only validates client id and client secret
    - Uses simple oauth runtime
    - Process
      * First you pass client id and client secret to request for a token
      * Response: get the token
      * This token is used in authorization header to request for resources or access to an api

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

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

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

* + - * 1. 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. Using anypoint securitu suite

https://docs.mulesoft.com/mule-runtime/3.9/installing-anypoint-enterprise-security

1. Using Jar file

https://nl.devoteam.com/en/blog-post/how-to-secure-properties-and-hide-encryption-key-in-cloudhub-mule-4/

* + - * 1. Access Audit Logs using Platform API

Step 1: Get the bearer token

Use the command in cmd prompt

C:\Users\aayas>curl -s https://anypoint.mulesoft.com/accounts/login -d "username=adv2020&password=Addvance2020"

Result:

{

"access\_token": "1a489a27-dfe8-4de1-be99-fa5db90771fd",

"token\_type": "bearer",

"redirectUrl": "/home/"

}

Step2:

C:\Users\aayas>curl -X POST https://anypoint.mulesoft.com/audit/v2/organization/1a489a27-dfe8-4de1-be99-fa5db90771fd/query?include\_inteenal=false -H 'Content-Type:application/json' -H 'Authorization: Bearer tokenValue' -d '{"startDate":"2020:10:11T21:28Z","endDate":"2020:10:11T23:00Z"}'

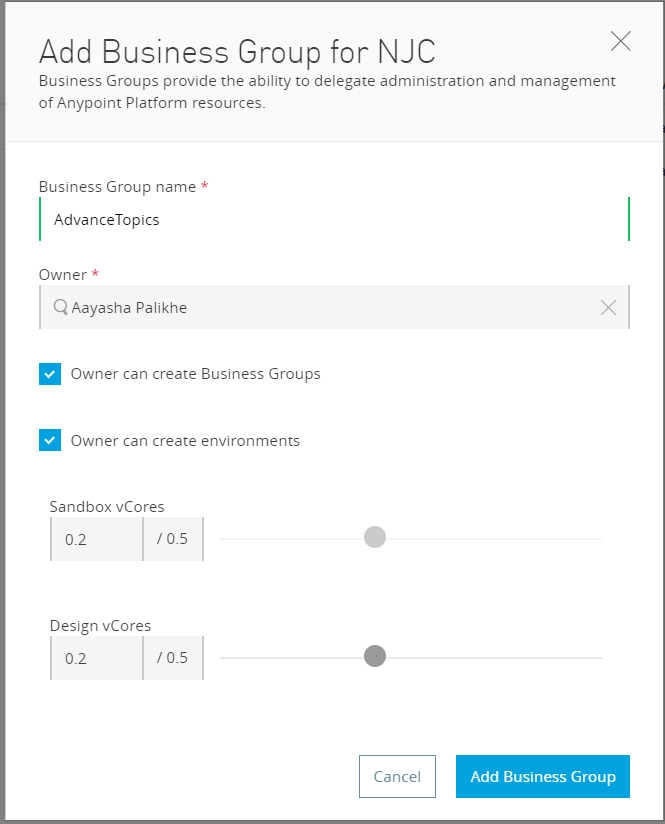
* + - * 1. Business Groups

Create a Business Group

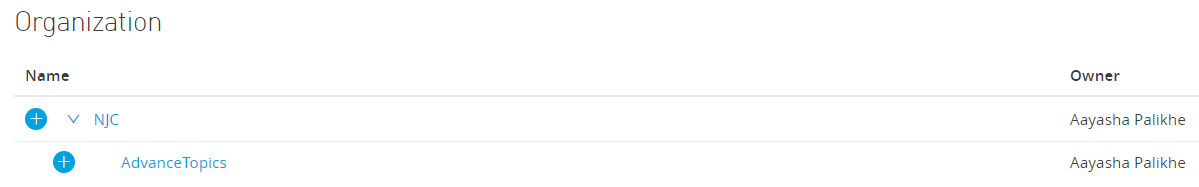
Log in to anypoint platform

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