Mod 9

## **Module 9: Platform And Application Security**

1. How can I manage the access of resources and features in Anypoint Platform?

By creating and maintaining an organisation/business level hierarchy we can manage and access the resources.

1. What do you mean by an Organization in Anypoint platform?

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.

The organization name is the name you entered in the Company field in the initial Anypoint Platform signup form. You can change the name in the organization settings.

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. For example, one user might have permission to manage API alerts, while another user has permission only to view API alerts.

1. What is the use of a 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.

1. Why do we need more than one Business Groups?

We can create BG under each parent level.

Organisation hierarchy can be achieved.

Application deployment can be done separately

Can allocate different licenses to BG and also different cores to each group

1. How do you create users in Anypoint platform?

To invite new users to your organization:

1. Click **Users** in the left navigation bar.
2. Click **Invite user**.
3. Enter the email addresses of who you want to invite in your organization as a comma-separated list.
4. Optionally, select one or more [roles](https://docs.mulesoft.com/access-management/roles) to which to assign these users.
5. Click **Send Invitation**.

The users who you invite receive email invitations to sign up to your organization. Invited users must use the link they receive in the invitation email to join your organization. When they click through the link they are presented with a sign-up form that already has the **Company** field completed, matching your organization.

Note that the email link expires in one week.

Invited users have access to the same set of resources as you (although they may have different roles that can restrict what they can view or do).

1. How do you create roles in Anypoint platform?
2. Why should operating system access should be restricted to only admin users?

Because if OS access is exposed, there will be access to certificates, secure properties, encryption keys etc.

1. If an Organization has 100’s of users, what Identity provider strategy do you use to enroll them onto Anypoint Platform?

Identity management via identity provider

1. What are the different types of environments used in Anypoint Platform?

* **Production environment**: Provides a production environment where you can deploy applications and APIs publicly.
* **Sandbox environment**: Provides useful environments for development and testing. By default, Anypoint Platform accounts are created with one sandbox environment with one vCore assigned to it.

Sandbox environments enable you to safely test an application without affecting the production environment. For example, you can create a sandbox environment for a QA team where they can test new releases of applications before deploying in production. You can add users to a sandbox environment without permitting them to access the production environment. This helps to secure your production environment and eliminate the risk of a developer accidentally changing an application in production. Once you are sure an application is safe to expose to users, you can easily promote the application from a sandbox environment to a production environment.

* **Design environment**: Enables you to test and run applications at design time. This environment is used by the Design Center application. By default, a new Anypoint Platform account contains one design environment with one vCore assigned to it. Only applications deployed from Design Center can target this environment; you can’t deploy an application to a runtime registered in the Design environment using Runtime Manager.

1. What are the advantages of having different environments in Anypoint Platform?

These environments are independent from each other and enable you to test your applications separate;y w/o affecting others.

1. How do you log user activities in Anypoint Platform?

We can use audit logs to achieve that.

1. What are the features of 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 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.

Audit logs have a retention period of six years. Download your logs periodically if you want to maintain your log files for longer than six years.

1. What strategy do you use to authorize client applications if the customer doesn’t have any external identity provider?

Mule OAuth 2.0 Provider is an OAuth 2.0 provider alternative developed by

MuleSoft that can be used in any MuleSoft API Platform organization

 Mule has provided an Oauth 2.0 provider module in anypoint exchange.

 The OAuth2 Provider Module allows a Mule Application to be configured as an

Authentication Manager (OAuth provider) in Authorisation process.

1. What is the use of an OAuth 2.0 provider? and what are its features?
2. How do you secure configuration properties in a Mule application?

We can secure config properties by using anypoint enterprise security for encryption of data and also by downloading secure properties JAR and doing the encryption of data with the help of that.

1. How do you secure your mule application if the customer doesn’t have API Manager in their Anypoint Platform to apply security policies?

We can use http security filter to secure the data in that case.

1. What ways can you secure sensitive information which is available as part of your payload?

We can encrypt part of the payload/ or entire payload by using different forms of encryption like JCE, PGP encryption etc.

1. How do you encrypt sensitive information in your mule application?

We can use crypto module for encrypting sensitive data in mule application.

This module provides cryptography capabilities to a Mule application. Its main features

include:

 Symmetric encryption and decryption of messages

 Asymmetric encryption and decryption of messages

 Message signing and signature validation of signed messages

This module supports three different strategies to encrypt and sign your messages:

 PGP: Signature/encryption using PGP.

 XML: For signing or encrypting XML documents or elements.

 JCE: For using a wider range of cryptography capabilities as provided by the Java

Cryptography Extension.