**Module 9: Platform And Application Security**

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

With Anypoint Access Management we can configure access and permissions within Organization based on access level, manage users and roles

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

1. What is the use of a Business Group?

* 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.
* 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?

* Business groups are self-contained resource groups that contain Anypoint Platform resource such as APIs and applications.
* Organisation hierarchy can be achieved with Business group
* Able to allocate different user, roles and resource to each business group

1. How do you create users in Anypoint platform?

To add users to an organization, as an organization administrator, or of one of its business groups, you can invite new users and manage existing users for your organization on the Access Management Administration page, which you can reach by selecting the Users option in your Access Management section.

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 to which to assign these users.
5. Click Send Invitation.

The users who you invite receive email invitations to sign up to your organization. The email link expires in one week. 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.

1. How do you create roles in Anypoint platform?

To Create a Custom Role,:

1. Click the Roles tab in the left navigation of the Access Management page for your organization.
2. Click Add role.
3. Enter a Name and Description for your custom role.
4. Your custom role now appears in your list of roles.
5. Click the name of your new role to assign permissions to it.
6. Why should operating system access should be restricted to only admin users?
7. If an Organization has 100’s of users, what Identity provider strategy do you use to enrol them onto Anypoint Platform?

Store all user details in an external identity provider like Okta, pingfederate, ldap and configure Identity provider in Anypoint Access management

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

* Production: Provides a production environment where you can deploy applications and APIs publicly.
* Sandbox: Provides useful environments for development and testing

Sandbox environments enable you to safely test an application without affecting the production environment.

* Design: Enables you to test and run applications at design time. This environment is used by the Design Center application

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

Anypoint Platform enables you to create and manage separate deployment environments for APIs and applications. These environments are independent from each other and enable you to test your applications under the same conditions as your production environment.

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

Changes made by users within Anypoint platform organizations are logged through an audit logging services.

It can be access through the audit logging query API or through the audit logging UI

12. What are the features of Audit Logs?

Each log entry has set of properties that provide information about the activity

o   **Time**: The timestamp when the activity occurred.

o   **Product**: The product where the object resides, for example, Access Management

o **Type**: The type of the object on which the action is performed, for example, Organization

o   **Action**: The action associated with the object, for example, Create

o   **Object**: The name of the Object, for example, foo

o   **User**: The User who performed the action, for example, johndoe

o   **Environment**: Environment names for events from API Manager, Runtime Manager, CloudHub, Partner Manager, and MQ.

o  **Parent**: (Optional) The parent of the object (if any) on which the action is performed. Mainly relevant to APIs.

o   **Payload**: (Optional) More information about the log properties. For example, if an Organization was created, then the payload would contain information about the organization and the owner, such as IDs.

13. 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.

14. What is the use of an OAuth 2.0 provider? and what are its features?

OAuth provider: It is a software which provides the secure token to the client and validates the token. There are many third party OAuth providers like Okta, Github, OpenAM etc

15. How do you secure configuration properties in a Mule application?

* We need to encrypt sensitive data in configuration file.
* Use secure property module provided by Mulesoft
* We can encrypt the whole configuration file or encrypt individual property inside file
* For securing file we have two option
  + Use premium security connector in Anypoint Studio
  + Encrypt properties using the secure properties tool

16. 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 Baic Security Filter Module of Http connector
* Used for protecting API by allowing accessing to only certain groups

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

We can encrypt payload to secure sensitive information

18. 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](https://docs.mulesoft.com/mule-runtime/4.3/cryptography-pgp): Signature/encryption using PGP.
* [XML](https://docs.mulesoft.com/mule-runtime/4.3/cryptography-xml): For signing or encrypting XML documents or elements.
* [JCE](https://docs.mulesoft.com/mule-runtime/4.3/cryptography-jce): For using a wider range of cryptography capabilities as provided by the Java Cryptography Extension.