Microsoft 365 Identity and Device management

Duration: 40 Hours

Module 1: Microsoft 365 Identity Management

This Module provides instruction on

- how to manage your Microsoft 365 tenant, including Function as the integrating hub for all Microsoft 365 workloads.
- Coordinate across multiple Microsoft 365 workloads.
- Work with architects and other administrators responsible for workloads, infrastructure, identity, security, compliance, endpoints, and applications

Lesson 1: Configure your Microsoft 365 experience

- **Manage users, licenses, guests, and contacts in Microsoft 365**
  - Identify which user identity model best suited for your organization.
  - Create user accounts from both the Microsoft 365 admin center and Windows PowerShell.
  - Manage user accounts and licenses in Microsoft 365.
  - Recover deleted user accounts in Microsoft 365.
  - Perform bulk user maintenance in Microsoft Entra ID.
  - Create and manage guests and collaborate with them in SharePoint sites.
  - Create and manage contacts.

- **Manage groups in Microsoft 365**
  - Describe the various types of groups available in Microsoft 365.
  - Create and manage groups using the Microsoft 365 admin center and Windows PowerShell.
  - Create a Microsoft 365 group naming policy.
  - Create and manage groups in Exchange Online and SharePoint Online.

- **Add a custom domain in Microsoft 365**
  - Identify the factors that must be considered when adding a custom domain to Microsoft 365.
  - Plan the DNS zones used in a custom domain.
  - Plan the DNS record requirements for a custom domain.
  - Add a custom domain to your Microsoft 365 deployment.

Lesson 2: Manage your Microsoft 365 tenant

- **Configure administrative roles in Microsoft 365**
  - Describe the Azure RBAC permission model used in Microsoft 365.
  - Describe the most common Microsoft 365 admin roles.
  - Identify the key tasks assigned to the common Microsoft 365 admin roles.
  - Delegate admin roles to partners.
  - Manage permissions using administrative units in Microsoft Entra ID.

- **Manage tenant health and services in Microsoft 365**
  - Monitor your organization's Microsoft 365 service health in the Microsoft 365 admin center.
  - Implement Microsoft 365 network connectivity for assessments and insights.

Lesson 3: Implement identity synchronization

- **Explore identity synchronization**
  - Describe the Microsoft 365 authentication and provisioning options
  - Explain the two identity models in Microsoft 365 - cloud-only identity and hybrid identity
  - Explain the three authentication methods in the hybrid identity model - Password hash synchronization, Pass-through authentication, and federated authentication

- **Prepare for identity synchronization to Microsoft 365**
  - Identify the tasks necessary to configure your Azure Active Directory environment.
  - Plan directory synchronization to synchronize your on-premises Active Directory objects to Azure AD.
  - Identify the features of Microsoft Entra Connect Sync and Microsoft Entra Cloud Sync.

- **Implement directory synchronization tools**
  - Configure Microsoft Entra Connect Sync and Microsoft Entra Cloud Sync prerequisites.
  - Set up Microsoft Entra Connect Sync and Microsoft Entra Cloud Sync.

Lesson 4: Manage identity and access in Microsoft 365

- **Examine threat vectors and data breaches**
  - Describe techniques hackers use to gain control over resources.
  - Describe techniques hackers use to compromise data.
  - Mitigate an account breach.

- **Explore the Zero Trust security model**
  - Describe the Zero Trust approach to security in Microsoft 365.
  - Describe the principles and components of the Zero Trust security model.

- **Manage secure user access in Microsoft 365**
  - Manage user passwords.
  - Create Conditional Access policies.
  - Enable security defaults.
  - Describe pass-through authentication.
  - Enable multifactor authentication.
  - Describe self-service password management.
  - Implement Microsoft Entra Smart Lockout.

- **Explore security solutions in Microsoft Defender XDR**
  - Identify the features of Microsoft Defender for Office 365 that enhance email security in a Microsoft 365 deployment
  - Explain how Microsoft Defender for Identity identifies, detects, and investigates advanced threats, compromised identities, and malicious insider actions directed at your organization
  - Describe how Microsoft 365 Threat Intelligence can be beneficial to your organization's security officers and administrators

- **Examine Microsoft Secure Score**
  - Describe the benefits of Secure Score and what kind of services can be analyzed

- **Examine Privileged Identity Management in Microsoft Entra ID**
  - Describe how PIM enables you to manage, control, and monitor access to important resources in your organization.
  - Configure the PIM role assignment process for use in your organization.

Module 2: Microsoft 365 Endpoint Administrator

The course introduces essential elements of modern management, co-management approaches, and Microsoft Intune integration. It covers app deployment, management of browser-based applications, and key security concepts such as authentication, identities, access, and compliance policies. Technologies like Azure Active Directory, Azure Information Protection, and Microsoft Defender for Endpoint are explored to protect devices and data.

Lesson 1: Explore endpoint management

- **Explore the Enterprise Desktop**
    - Describe the benefits of Modern Management.
    - Explain the enterprise desktop life-cycle model.
    - Describe considerations for planning hardware strategies.
    - Describe considerations for post-deployment and retirement.

- **Explore Windows Editions**
    - Explain the differences between the different editions of Windows.
    - Select the most suitable Windows device for your needs.
    - Describe the minimum recommended hardware requirements for installing Windows 11.

Lesson 2: Execute device enrolment

- **Manage device authentication**
    - Describe Microsoft Entra join.
    - Describe Microsoft Entra join prerequisites, limitations, and benefits.
    - Join device to Microsoft Entra ID.
    - Manage devices joined to Microsoft Entra ID.

- **Enroll devices using Microsoft Intune**
    - Prepare Microsoft Intune for device enrollment.
    - Configure Microsoft Intune for automatic enrollment.
    - Explain how to enroll Windows, Android, and iOS devices in Intune.
    - Explain when and how to use Intune Enrollment Manager.
    - Understand how to monitor and perform remote actions on enrolled devices.

Lesson 3: Configure profiles for user and devices

- **Execute device profiles**
    - Describe the various types of device profiles in Intune.
    - Explain the difference between built-in and custom profiles.
    - Create and manage profiles.
- **Oversee device profiles**
    - Monitor the assignments of profiles.
    - Understand how profiles are synchronized and how to manually force synchronization.
- **Maintain user profiles**
    - Explain the various user profile types that exist in Windows.
    - Describe how a user profile works.
    - Configure user profiles to conserve space.
    - Explain how to deploy and configure Folder Redirection.

Lesson 4: Examine application management

- **Execute mobile application management**
    - Explain Mobile Application Management.
    - Understand application considerations in MAM.

- Use Intune for MAM.
- Implement and manage MAM policies.

- **Deploy and update applications**
  - Explain how to deploy applications using Intune
  - Understand Microsoft Store Apps.
  - Learn how to deploy apps using Microsoft Store Apps.

- **Administer endpoint applications**
  - Explain how to manage apps in Intune.
  - Understand how to manage apps on nonenrolled devices.
  - Understand how to deploy Microsoft 365 Apps using Intune.

Lesson 5: Manage authentication and compliance

- **Protect identities in Microsoft Entra ID**
  - Describe Windows Hello for Business
  - Describe Windows Hello deployment and management
  - Describe Microsoft Entra ID Protection
  - Describe and manage self-service password reset in Microsoft Entra ID
  - Describe and manage multi-factor authentication

- **Implement device compliance**
  - Describe device compliance policy
  - Deploy a device compliance policy
  - Describe conditional access
  - Create conditional access policies

- **Generate inventory and compliance reports**
  - Generate inventory reports and Compliance reports using Microsoft Intune
  - Report and monitor device compliance

Lesson 6: Manage endpoint security

- **Deploy device data protection**
  - Describe Windows Information Protection
  - Plan for Windows Information Protection usage
  - Implement and use Windows Information Protection
  - Describe the Encrypting File System (EFS)
  - Describe BitLocker

- **Manage Microsoft Defender for Endpoint**
  - Describe Microsoft Defender for Endpoint.
  - Describe key capabilities of Microsoft Defender for Endpoint.
  - Describe Microsoft Defender Application Guard.
  - Describe Microsoft Defender Exploit Guard.
  - Describe Windows Defender System Guard.

- **Manage Microsoft Defender in Windows client**
    - Manage Microsoft Defender Antivirus
    - Manage Windows Defender Firewall

Lesson 7: Deploy using cloud based tools

- **Deploy Devices using Windows Autopilot**
    - Describe the process of preparing for an Autopilot deployment.
    - Describe the process of registering devices in Autopilot.
    - Describe the different methods and scenarios of Autopilot deployments.
    - Describe how to troubleshoot common Autopilot issues.

- **Implement dynamic deployment methods**
    - Describe the benefits of Provisioning Packages.
    - Explain how Windows Configuration Designer creates Provisioning Packages.
    - Describe the benefits of using MDM enrollment with Microsoft Entra join.

- **Plan a transition to modern endpoint management**
    - Identify usage scenarios for Microsoft Entra join.
    - Identify workloads that you can transition to Intune.
    - Identify prerequisites for co-management.
    - Plan a transition to modern management using Microsoft Intune.