# MD-102

## Microsoft 365 Endpoint Administrator

### Description:

In this five-day course, students will learn to plan and execute an endpoint deployment strategy using contemporary deployment techniques and implementing update strategies. 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.

### Students will be able to:

Students will have expertise in deploying, configuring, protecting, managing, and monitoring devices and client applications in Microsoft 365 environment. They will be able to manage identity, security, access, policies, updates, and endpoint applications. Furthermore, implementation of solutions for the effective deployment and management of endpoints on various operating systems, platforms and device types, will be addressed, as well as management of endpoints at scale using Microsoft Intune, Windows 365, Windows Autopilot, Microsoft Defender for Endpoint and Azure Active Directory (Azure AD), which are part of Microsoft Entra.

### Course requirements:

The Modern Desktop Administrator must be familiar with M365 workloads and must have strong skills and experience of deploying, configuring, and maintaining Windows 11 and later, and non-Windows devices.

### This course is intended for:

A Microsoft 365 Endpoint Administrator who is responsible for deploying, configuring, securing, managing, and monitoring devices and client applications in a corporate setting.

### Literature:

Students will receive the original certified Microsoft study materials and access to labs.

### Hardware:

All classrooms are equipped with high-standard computers connected to the Internet, the classrooms are spacious, air-conditioned, barrier-free and with Wi-Fi connection. If interested, you can join the course online-live.

### Syllabus:

### Module 1: Windows client deployment

- Preparing to deploy the Windows client
    - Selection of tool for deployment based on requirements

    - Choice between migration and modifications
    - Choosing a display and/or delivery strategy
    - Selection of Windows edition based on requirements
    - Implementation of subscription-based activations
- Plan and implement a Windows client deployment using Windows Autopilot
    - Configure device registration for Autopilot
    - Creation, validation and assignment of deployment profiles
    - Enrollment Status Page (ESP) Setup
    - Deploy Windows devices using Autopilot
    - Troubleshooting Autopilot deployment
- Plan and implement a Windows client deployment using the Microsoft Deployment Toolkit (MDT)
    - Planning and implementation of MDT deployment infrastructure
    - Creating, managing and deploying images
    - Monitoring and troubleshooting deployment issues
    - Plan and configure user state migration
- Configure remote management
    - Configure remote help in Intune
    - Remote desktop configuration on a Windows client
    - Configure the Windows Administrative Center
    - Configure PowerShell Remote Control and Windows Remote Management (WinRM)

## Module 2: Identity and compliance management

- Identity management
    - Implementation of user authentication on Windows devices, including Windows Hello for Business, without passwords and tokens
      Manage role-based access control (RBAC) for Intune
      Device registration and device connection to Azure AD
      Implementation of Intune Connector for Active Directory
      Manage local group membership on Windows devices
      Implementation and management of Local Password Management Solution (LAPS) for Azure AD
- Implement compliance policies for all supported device platforms using Intune
    - Defining compliance policies to meet requirements
    - Implementation of compliance policies
    - Implementation of Conditional Access policies that require compliance status
    - Manage compliance policy notices
    - Device compliance monitoring
    - Troubleshooting compliance policies

## Module 3: Management, maintenance and protection of equipment

- Device lifecycle management in Intune
    - Configure registration settings
    - Configuration of automatic and mass registration, including Windows, Apple and Android
    - Configure policy sets
    - Restart, remove or erase the device
    - Manage device configuration for all supported device platforms using Intune
    - Creation of configuration profiles to meet requirements
    - Implementation of configuration profiles
    - Monitoring and troubleshooting configuration profiles
    - Configure and implement Windows public terminal mode

    - Configuration and implementation of profiles on Android devices, including fully managed, dedicated, company and work profiles
    - Planning and implementation of Microsoft Tunnel for Intune
- Device monitoring
    - Device monitoring using Intune
    - Device monitoring using Azure Monitor
    - Analyzing and responding to issues identified in endpoint analysis and acceptance scores
- Device update management for all supported device platforms using Intune
    - Scheduling device updates
    - Create and manage update policies using Intune
    - Android update management using configuration profiles
    - Update tracking
    - Troubleshooting updates in Intune
    - Configuring optimal delivery of Windows clients using Intune
    - Create and manage update circuits using Intune
- Implementation of endpoint protection for all supported device platforms
    - Implementation and management of the security line in Intune
    - Create and manage configuration policies for endpoint security including antivirus, encryption, firewall, endpoint detection and response (EDR), and attack mitigation (ASR).
    - Device integration into Defender for Endpoint
    - Implementation of auto-response features in Defender for Endpoint
    - Troubleshoot and respond to device issues identified on the Microsoft Defender Vulnerability Management dashboard

## Module 4: Application management

- Deploy and update applications for all supported device platforms
    - Application deployment using Intune
    - Configure Microsoft 365 Apps deployment using the Microsoft Office Deployment Tool or the Office
    - Customization Tool (OCT)
    - Manage Microsoft 365 Apps using the Microsoft 365 Apps admin center
    - Deployment of Microsoft 365 Apps using Intune
    - Configure policies for Office applications using Group Policy or Intune
    - Deploy apps to platform-specific app stores using Intune
- Planning and implementing application configuration and protection policies
    - Planning and implementing application security policies for iOS and Android
    - Manage application protection policies
    - Implementation of conditional access policies for application protection policies
    - Planning and implementing application configuration policies for managed applications and managed devices
    - Manage application configuration policies