MD-102T00: Microsoft 365 Endpoint Administrator

Duration: 40 Hours (5 Days)

Course Overview

The MD-102: Endpoint Administrator course is designed to equip learners with the skills and knowledge necessary to manage and secure modern endpoints within an enterprise environment. Throughout the course, participants will delve into various aspects of endpoint management, starting with exploring enterprise desktops, understanding different Windows editions, and managing identities in Azure Active Directory. Learners will also gain hands-on experience with device enrollment, both through Microsoft Configuration Manager and Microsoft Intune. They will configure user and device profiles, manage applications, and ensure authentication and compliance to protect organizational data. A significant part of the course is dedicated to endpoint security, where students learn to deploy Microsoft Defender in various capacities and manage data protection. Additionally, the course covers deployment strategies using both on-premises and cloud-based tools, including Windows Autopilot, Microsoft Deployment Toolkit, and modern management of Windows 365 and Azure Virtual Desktop. By the end of the MD-102 course, learners will have a comprehensive understanding of endpoint management, enabling them to effectively manage and secure devices within a modern enterprise infrastructure.

Audience profile

The MD-102: Endpoint Administrator course focuses on managing enterprise environments, making it ideal for IT professionals in device management roles.

- IT Administrators
- Systems Administrators
- Desktop Support Technicians
- Endpoint Security Specialists
- Microsoft 365 Managed Service Providers
- IT Support Engineers
- Network Administrators
- Infrastructure Engineers
- IT Professionals seeking to understand Azure Active Directory and Microsoft Intune
- Professionals responsible for Windows 10/11 deployments
- Cloud Solution Architects focusing on Microsoft 365
- Help Desk Technicians aiming for career advancement in IT management
- Cybersecurity Analysts with a focus on endpoint protection
- Compliance Officers dealing with device compliance and authentication
- Technical Consultants specializing in modern workplace solutions
- IT Managers looking to improve device management strategies
- Enterprise Architects involved in endpoint strategy and planning
- Virtual Desktop Infrastructure (VDI) Specialists

Course Syllabus

Deploy Windows Client (20–25%)

Prepare for a Windows Client Deployment

- Select a deployment tool based on requirements
- Choose between migrate and rebuild
- Choose an imaging and/or provisioning strategy
- Select a Windows edition based on requirements
- Implement subscription-based activation
- Deploy Windows 365

Plan and Implement a Windows Client Deployment by Using Windows Autopilot

- Configure device registration for Autopilot
- Create, validate, and assign deployment profiles
- Set up the Enrollment Status Page (ESP)
- Deploy Windows devices by using Autopilot
- Troubleshoot an Autopilot deployment

Configure remote management

- Configure Remote Help in Intune
- Configure Remote Desktop on a Windows client
- Configure the Windows Admin Center
- Configure PowerShell remoting and Windows Remote Management (WinRM)

Manage Identity and Compliance (15–20%)

Manage Identity

- Implement user authentication on Windows devices, including Windows Hello for Business, passwordless, and tokens
- Manage role-based access control (RBAC) for Intune
- Register devices in and join devices to Microsoft Entra
- Implement the Intune Connector for Active Directory
- Manage the membership of local groups on Windows devices
- Implement and manage Local Administrative Passwords Solution (LAPS) for Microsoft Entra

Implement compliance policies for all supported device platforms by using Intune

- Specify compliance policies to meet requirements
- Implement compliance policies
- Implement Conditional Access policies that require a compliance status
- Manage notifications for compliance policies
- Monitor device compliance
- Troubleshoot compliance policies

Manage, maintain, and protect devices (40–45%)

Manage the device lifecycle in Intune

- Configure enrollment settings
- Configure automatic and bulk enrollment, including Windows, iOS, and Android
- Configure policy sets
- Restart, retire, or wipe devices

Manage device configuration for all supported device platforms by using Intune

- Specify configuration profiles to meet requirements
- Implement configuration profiles
- Monitor and troubleshoot configuration profiles
- Configure and implement Windows kiosk mode
- Configure and implement profiles on Android devices, including fully managed, dedicated, corporate owned, and work profile
- Plan and implement Microsoft Tunnel for Intune

Monitor devices

- Monitor devices by using Intune
- Monitor devices by using Azure Monitor
- Analyze and respond to issues identified in Endpoint analytics and Adoption Score

Manage device updates for all supported device platforms by using Intune

- Plan for device updates
- Create and manage update policies by using Intune
- Manage Android updates by using configuration profiles
- Monitor updates
- Troubleshoot updates in Intune
- Configure Windows client delivery optimization by using Intune
- Create and manage update rings by using Intune

Implement endpoint protection for all supported device platforms

- Implement and manage security baselines in Intune
- Create and manage configuration policies for Endpoint security including antivirus, encryption, firewall, endpoint detection and response (EDR), and attack surface reduction (ASR)
- Onboard devices to Microsoft Defender for Endpoint
- Implement automated response capabilities in Microsoft Defender for Endpoint
- Review and respond to device issues identified in the Microsoft Defender Vulnerability Management dashboard

Manage applications (15–20%)

Deploy and update apps for all supported device platforms

- Deploy apps by using Intune
- Configure Microsoft 365 Apps deployment by using the Microsoft Office Deployment Tool or Office Customization Tool (OCT)
- Manage Microsoft 365 Apps by using the Microsoft 365 Apps admin center
- Deploy Microsoft 365 Apps by using Intune
- Configure policies for Office apps by using Group Policy or Intune
- Deploy apps from platform-specific app stores by using Intune

Plan and implement app protection and app configuration policies

- Plan and implement app protection policies for iOS and Android
- Manage app protection policies
- Implement Conditional Access policies for app protection policies
- Plan and implement app configuration policies for managed apps and managed devices
- Manage app configuration policies