Document Generated: 12/18/2025

Learning Style: Virtual Classroom

Technology: Microsoft

Difficulty: Intermediate

Course Duration: 5 Days

Next Course Date: January 26, 2026

Microsoft 365 Endpoint Administrator (MD-102)

About this Course:

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.

Course Objectives:

- 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.
- 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
- Describe RBAC and user roles in Azure AD.
- Create and manage users in Azure AD.
- Create and manage groups in Azure AD.
- Use Windows PowerShell cmdlets to manage Azure AD.
- Describe how you can synchronize objects from AD DS to Azure AD.
- Describe Microsoft Endpoint Manager.
- Understand the advantages of managing a client with Configuration Manager.
- Deploy the Configuration Manager client.
- Monitor the Configuration Manager client.
- Manage Configuration Manager devices.
- Describe Microsoft Endpoint Manager.
- Understand the advantages of managing a client with Configuration Manager.
- Deploy the Configuration Manager client.
- Monitor the Configuration Manager client.
- Manage Configuration Manager devices.
- 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.
- Describe the various types of device profiles in Intune.
- Explain the difference between built-in and custom profiles.
- Create and manage profiles.
- Monitor the assignments of profiles.
- Understand how profiles are synchronized and how to manually force synchronization.
- Use PowerShell to execute and monitor scripts on devices.
- 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.
- Explain Enterprise State Roaming.
- Configure Enterprise State Roaming for Azure AD devices.
- Explain Mobile Application Management
- Understand application considerations in MAM
- Explain how to use Configuration Manager for MAM
- Use Intune for MAM
- Implement and manage MAM policies

- Explain how to deploy applications using Intune and Configuration Manager
- Learn how to deploy applications using Group Policy
- Understand Microsoft Store Apps
- Learn how to deploy apps using Microsoft Store Apps
- Learn how to configure Microsoft Store Apps
- Explain how to manage apps in Intune
- Understand how to manage apps on non-enrolled devices
- Understand how to deploy Microsoft 365 Apps using Intune
- Learn how to configure and manage IE mode in Microsoft Edge
- Learn about app inventory options in Intune
- Describe Windows Hello for Business
- Describe Windows Hello deployment and management
- Describe Azure AD Identity Protection
- Describe and manage self-service password reset in Azure AD
- Describe and manage multi-factor authentication
- Describe how you can access corporate resources
- Describe VPN types and configuration
- Describe Always On VPN
- Describe how to configure Always On VPN
- Describe device compliance policy
- Deploy a device compliance policy
- Describe conditional access
- Create conditional access policies
- Generate inventory reports and Compliance reports using Microsoft Intune
- Report and monitor device compliance
- Create custom reports using the Intune Data Warehouse
- Use the Microsoft Graph API for building custom reports
- Describe Windows Information Protection
- Plan for Windows Information Protection usage
- Implement and use Windows Information Protection
- Describe the Encrypting File System (EFS)
- Describe BitLocker
- 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
- Describe Windows Security capabilities
- Describe Windows Defender Credential Guard
- Manage Microsoft Defender Antivirus
- Manage Windows Defender Firewall
- Manage Windows Defender Firewall with Advanced Security
- Describe Microsoft Defender for Cloud Apps
- Plan for Microsoft Defender for Cloud Apps usage
- Implement and use Microsoft Defender for Cloud Apps
- Describe the guidelines for an effective enterprise desktop deployment.
- Explain how to assess the current environment.
- Describe the tools that you can use to assess your current environment.
- Describe the methods of identifying and mitigating application compatibility issues.
- Explain considerations for planning a phased rollout.

- Describe the fundamentals of using images in traditional deployment methods.
- Describe the key benefits, limitations, and decisions when planning a deployment of - Windows using Microsoft Deployment Toolkit (MDT).
- Describe how Configuration Manager builds upon MDT and how both can work in harmony.
- Explain the different options and considerations when choosing the user interaction experience during deployment, and which methods and tools support these experiences.
- Describe the capabilities of Configuration Manager.
- Describe the key components of Configuration Manager.
- Describe how to troubleshoot Configuration Manager deployments.
- Explain the benefits of modern deployment for new devices.
- 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.
- Describe the process of deployment using traditional methods.
- Describe how Subscription Activation works.
- Describe the benefits of Provisioning Packages.
- Explain how Windows Configuration Designer creates Provisioning Packages.
- Describe the benefits of using MDM enrollment with Azure AD join.
- Identify usage scenarios for Azure AD join.
- Identify workloads that you can transition to Intune.
- Identify prerequisites for co-management.
- Identify considerations for transitioning to modern management.
- Plan a transition to modern management using existing technologies.
- Plan a transition to modern management using Microsoft Intune.
- Describe the key features of Windows 365
- Describe the Windows 365 management experience
- Describe the Windows 365 security model
- Describe the Windows 365 deployment options
- Describe the Windows 365 licensing model
- Describe the key features of Azure Virtual Desktop
- Describe the Azure Virtual Desktop management experience
- Describe the Azure Virtual Desktop security model
- Describe the Azure Virtual Desktop deployment options

Audience:

The Microsoft 365 Endpoint Administrator is responsible for deploying, configuring, securing, managing, and monitoring devices and client applications in a corporate setting. Their duties include managing identity, access, policies, updates, and apps. They work alongside the M365 Enterprise Administrator to develop and execute a device strategy that aligns with the requirements of a modern organization. Microsoft 365 Endpoint Administrators should be well-versed in M365 workloads and possess extensive skills and experience in deploying, configuring, and maintaining Windows 11 and later, as well as non-Windows devices. Their role emphasizes cloud services over on-premises management technologies.

Prerequisites:

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.

Course Outline:

Module 1: Explore the Enterprise Desktop

This module covers modern endpoint management and enterprise desktop lifecycle concepts. It teaches the stages of the lifecycle (planning, deployment, maintenance) and provides a foundation for future learning.

Learning Objectives:

- 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.

Lessons:

- Examine benefits of modern management
- Examine the enterprise desktop life-cycle model
- Examine planning and purchasing
- Examine desktop deployment
- Plan an application deployment
- Plan for upgrades and retirement

Module 2 : Explore Windows Editions

This module covers Windows OS editions, features, and installation methods. Learners gain a deeper understanding of the available editions and corresponding installation processes.

Learning Objectives:

- 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

Lessons:

- Examine Windows client editions and capabilities
- Select client edition
- Examine hardware requirements

Module 3: Manage Azure Active Directory identities.

This module teaches how to use Azure AD effectively. You'll learn about RBAC,

user roles, creating and managing users and groups, using PowerShell cmdlets, and synchronizing objects from AD DS to Azure AD

Learning Objectives:

- Describe RBAC and user roles in Azure AD.
- Create and manage users in Azure AD.
- Create and manage groups in Azure AD.
- Use Windows PowerShell cmdlets to manage Azure AD.
- Describe how you can synchronize objects from AD DS to Azure AD.

Lessons:

- Examine RBAC and user roles in Azure AD
- Create and manage users in Azure AD
- Create and manage groups in Azure AD
- Manage Azure AD objects with PowerShell
- Synchronize objects from AD DS to Azure AD

Module 4: Manage device authentication.

In this module, you learn about device authentication and management in Azure Active Directory

Learning Objectives:

- Describe Microsoft Endpoint Manager.
- Understand the advantages of managing a client with Configuration Manager.
- Deploy the Configuration Manager client.
- Monitor the Configuration Manager client.
- Manage Configuration Manager devices.

Lessons:

- Describe Azure AD join
- Examine Azure AD join prerequisites limitations and benefits
- Join devices to Azure AD
- Manage devices joined to Azure AD

Module 5 : Enroll devices using Microsoft Configuration Manager

This module introduces students to client deployment options and some of the high-level management and monitoring options that are available using Configuration Manager.

Learning Objectives:

- Describe Microsoft Endpoint Manager.
- Understand the advantages of managing a client with Configuration

Manager.
- Deploy the Configuration Manager client.
- Monitor the Configuration Manager client.
- Manage Configuration Manager devices.

Lessons:

- Deploy the Microsoft Configuration Manager client
- Monitor the Microsoft Configuration Manager client
- Manage the Microsoft Configuration Manager client

Module 6: Enroll devices using Microsoft Intune

Students will learn how to configure and setup Intune to more easily manage Windows, Android, and iOS devices.

Learning Objectives:

- 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:

- Manage mobile devices with Intune
- Enable mobile device management
- Explain considerations for device enrollment
- Manage corporate enrollment policy
- Enroll Windows devices in Intune
- Enroll Android devices in Intune
- Enroll iOS devices in Intune
- Explore device enrollment manager
- Monitor device enrollment
- Manage devices remotely

Module 7: Execute device profiles

Students learn about the various types of device profiles, and how to create and manage them.

Learning Objectives:

- Describe the various types of device profiles in Intune.
- Explain the difference between built-in and custom profiles.
- Create and manage profiles.

Lessons:

- Explore Intune device profiles
- Create device profiles
- Create a custom device profile

Module 8 : Oversee device profiles

This module introduces students to monitoring profiles to ensure correct assignments and resolving conflicts when multiple profiles are applied.

Learning Objectives:

- Monitor the assignments of profiles.
- Understand how profiles are synchronized and how to manually force synchronization.
- Use PowerShell to execute and monitor scripts on devices.

Lessons:

- Monitor device profiles in Intune
- Manage device sync in Intune
- Manage devices in Intune using scripts

Module 9: Maintain user profiles

Students learn about the benefits of various Windows user profiles, how to manage them, and how to facilitate profile data synchronization across multiple devices.

Learning Objectives:

- 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.
- Explain Enterprise State Roaming.
- Configure Enterprise State Roaming for Azure AD devices.

Lessons:

- Examine user profile
- Explore user profile types
- Examine options for minimizing user profile size
- Deploy and configure folder redirection
- Sync user state with Enterprise State Roaming
- Configure Enterprise State Roaming in Azure

Module 10: Execute mobile application management

This module introduces Mobile Application Management (MAM). Students will learn about considerations for implementing MAM and will be introduced to the management of MAM using Intune and Configuration Manager.

Learning Objectives:

- Explain Mobile Application Management
- Understand application considerations in MAM
- Explain how to use Configuration Manager for MAM
- Use Intune for MAM
- Implement and manage MAM policies

Lessons:

- Examine mobile application management
- Examine considerations for mobile application management
- Prepare line-of-business apps for app protection policies
- Implement mobile application management policies in Intune
- Manage mobile application management policies in Intune

Module 11: Deploy and update applications

In this module, you'll master deploying applications using Intune, Configuration Manager, Group Policy, and Microsoft Store Apps. These powerful tools and techniques will equip you to manage and maintain diverse applications across your organization effectively.

Learning Objectives:

- Explain how to deploy applications using Intune and Configuration Manager
- Learn how to deploy applications using Group Policy
- Understand Microsoft Store Apps
- Learn how to deploy apps using Microsoft Store Apps
- Learn how to configure Microsoft Store Apps

Lessons:

- Deploy applications with Intune
- Add apps to Intune
- Manage Win32 apps with Intune
- Deploy applications with Configuration Manager
- Deploying applications with Group Policy
- Assign and publish software
- Explore Microsoft Store for Business
- Implement Microsoft Store Apps
- Update Microsoft Store Apps with Intune
- Assign apps to company employees

Moudle 12: Administer endpoint applications

In this module, you're introduced to managing apps on Intune managed devices. The module will then conclude with an overview of how to use IE Mode with Microsoft Edge.

Learning Objectives:

- Explain how to manage apps in Intune
- Understand how to manage apps on non-enrolled devices
- Understand how to deploy Microsoft 365 Apps using Intune
- Learn how to configure and manage IE mode in Microsoft Edge
- Learn about app inventory options in Intune

Lessons:

- Manage apps with Intune
- Manage Apps on non-enrolled devices
- Deploy Microsoft 365 Apps with Intune
- Additional Microsoft 365 Apps Deployment Tools
- Configure Microsoft Edge Internet Explorer mode
- App Inventory Review

Module 13: Protect identities in Azure Active Directory

This module introduces students to the various authentication methods used to protect identities.

Learning Objectives:

- Describe Windows Hello for Business
- Describe Windows Hello deployment and management
- Describe Azure AD Identity Protection
- Describe and manage self-service password reset in Azure AD
- Describe and manage multi-factor authentication

Lessons

- Explore Windows Hello for Business
- Deploy Windows Hello
- Manage Windows Hello for Business
- Explore Azure AD identity protection
- Manage self-service password reset in Azure AD
- Implement multi-factor authentication

Module 14: Enable organizational access

This module describes how clients can be configured to access organizational resources using a virtual private network (VPN).

Learning Objectives:

- Describe how you can access corporate resources
- Describe VPN types and configuration
- Describe Always On VPN
- Describe how to configure Always On VPN

Lessons:

- Enable access to organization resources
- Explore VPN types and configuration
- Explore Always On VPN
- Deploy Always On VPN

Module 15: Implement device compliance

This module describes how to use compliance and conditional access policies to help protect access to organizational resources.

Learning Objectives:

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

Lesson:

- Protect access to resources using Intune
- Explore device compliance policy
- Deploy a device compliance policy
- Explore conditional access
- Create conditional access policies

Module 16: Generate inventory and compliance reports

This module describes how to use Microsoft Endpoint Manager and Power BI to create compliance and custom reports.

Learning Objectives:

- Generate inventory reports and Compliance reports using Microsoft Intune
- Report and monitor device compliance
- Create custom reports using the Intune Data Warehouse
- Use the Microsoft Graph API for building custom reports

Lessons:

- Report enrolled devices inventory in Intune
- Monitor and report device compliance
- Build custom Intune inventory reports
- Access Intune using Microsoft Graph API

Module 17: Deploy device data protection

This module describes how you can use Intune to create and manage WIP policies that manage this protection. The module also covers implementing BitLocker and

Encrypting File System.

Learning Objectives:

- Describe Windows Information Protection
- Plan for Windows Information Protection usage
- Implement and use Windows Information Protection
- Describe the Encrypting File System (EFS)
- Describe BitLocker

Lessons:

- Explore Windows Information Protection
- Plan Windows Information Protection
- Implement and use Windows Information Protection
- Explore Encrypting File System in Windows client
- Explore BitLocker

Module 18: Manage Microsoft Defender for Endpoint

This module explores using Microsoft Defender for Endpoint to provide additional protection and monitor devices against threats.

Learning Objectives:

- 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

Lessons:

- Explore Microsoft Defender for Endpoint
- Examine key capabilities of Microsoft Defender for Endpoint
- Explore Windows Defender Application Control and Device Guard
- Explore Microsoft Defender Application Guard
- Examine Windows Defender Exploit Guard
- Explore Windows Defender System Guard

Module 19: Manage Microsoft Defender in Windows client

This module explains the built-in security features of Windows clients and how to implement them using policies.

Learning Objectives:

- Describe Windows Security capabilities
- Describe Windows Defender Credential Guard
- Manage Microsoft Defender Antivirus

- Manage Windows Defender Firewall
- Manage Windows Defender Firewall with Advanced Security

Lessons:

- Explore Windows Security Center
- Explore Windows Defender Credential Guard
- Manage Microsoft Defender Antivirus
- Manage Windows Defender Firewall
- Explore Windows Defender Firewall with Advanced Security

Module 20: Manage Microsoft Defender for Cloud Apps

This module covers Microsoft Defender for Cloud Apps, focusing on securing sensitive data, its relevance in dynamic work settings, and effective utilization for improved security posture.

Learning Objectives:

- Describe Microsoft Defender for Cloud Apps
- Plan for Microsoft Defender for Cloud Apps usage
- Implement and use Microsoft Defender for Cloud Apps

Lessons:

- Explore Microsoft Defender for Cloud Apps
- Planning Microsoft Defender for Cloud Apps
- Implement Microsoft Defender for Cloud Apps

Module 21: Assess deployment readiness

Discusses some of the tools that you can use to perform detailed assessments of existing deployments, and describes some of the challenges that you may face.

Learning Objectives

- Describe the guidelines for an effective enterprise desktop deployment.
- Explain how to assess the current environment.
- Describe the tools that you can use to assess your current environment.
- Describe the methods of identifying and mitigating application compatibility issues.
- Explain considerations for planning a phased rollout.

Lessons:

- Examine deployment guidelines
- Explore readiness tools
- Assess application compatibility
- Explore tools for application compatibility mitigation
- Prepare network and directory for deployment

- Plan a pilot

Module 22: Deploy using the Microsoft Deployment Toolkit

Discusses the shifts from traditional to modern management and where on-premises solutions best fit in today?s enterprise.

Learning Objectives:

- Describe the fundamentals of using images in traditional deployment methods.
- Describe the key benefits, limitations, and decisions when planning a deployment of - Windows using Microsoft Deployment Toolkit (MDT).
- Describe how Configuration Manager builds upon MDT and how both can work in harmony.
- Explain the different options and considerations when choosing the user interaction experience during deployment, and which methods and tools support these experiences.

Lessons:

- Evaluate traditional deployment methods
- Set up the Microsoft Deployment Toolkit for client deployment
- Manage and deploy images using the Microsoft Deployment Toolkit

Module 23: Deploy using Microsoft Configuration Manager

This module explains the common day to day tasks that Administrators would use Configuration Manager to perform.

Learning Objectives:

- Describe the capabilities of Configuration Manager.
- Describe the key components of Configuration Manager.
- Describe how to troubleshoot Configuration Manager deployments.

Lesson:

- Explore client deployment using Configuration Manager
- Examine deployment components of Configuration Manager
- Manage client deployment using Configuration Manager
- Plan in-place upgrades using Configuration Manager

Module 24: Deploy Devices using Windows Autopilot

Use Autopilot to deploy new hardware or refreshing an existing hardware with the organization?s desired configuration, without using the traditional imaging process.

Learning Objectives:

- Explain the benefits of modern deployment for new devices.
- 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.
- Describe the process of deployment using traditional methods.

Lessons:

- Use Autopilot for modern deployment
- Examine requirements for Windows Autopilot
- Prepare device IDs for Autopilot
- Implement device registration and out-of-the-box customization
- Examine Autopilot scenarios
- Troubleshoot Windows Autopilot

Module 25: Implement dynamic deployment methods

Use dynamic provisioning methods such as Subscription Activation, Provisioning packages, and Azure AD join to reconfigure an existing operating system.

Learning Objectives:

- Describe how Subscription Activation works.
- Describe the benefits of Provisioning Packages.
- Explain how Windows Configuration Designer creates Provisioning Packages.
- Describe the benefits of using MDM enrollment with Azure AD join.

Lessons:

- Examine subscription activation
- Deploy using provisioning packages
- Use Windows Configuration Designer
- Use Azure AD join with automatic MDM enrollment

Module 26: Plan a transition to modern endpoint management

Explore considerations and review the planning of transitioning to modern management, focusing on migration and newly provisioned devices.

Learning Objectives:

- Identify usage scenarios for Azure AD join.
- Identify workloads that you can transition to Intune.
- Identify prerequisites for co-management.
- Identify considerations for transitioning to modern management.
- Plan a transition to modern management using existing technologies.
- Plan a transition to modern management using Microsoft Intune.

Lessons:

- Explore using co-management to transition to modern endpoint management
- Examine prerequisites for co-management
- Evaluate modern management considerations
- Evaluate upgrades and migrations in modern transitioning
- Migrate data when modern transitioning
- Migrate workloads when modern transitioning

Module 27: Manage Windows 365

This module teaches managing Microsoft's cloud-based PC management solution, Windows 365, offering personalized, secure Windows 11 experience from any device. Learn features, setup, management, security, deployment options, and licensing to optimize your environment.

Learning Objectives:

- Describe the key features of Windows 365
- Describe the Windows 365 management experience
- Describe the Windows 365 security model
- Describe the Windows 365 deployment options
- Describe the Windows 365 licensing model

Lessons:

- Explore Windows 365
- Configure Windows 365
- Administer Windows 365

Module 28: Manage Azure Virtual Desktop

Learn to manage Azure Virtual Desktop, a cloud-based VDI solution providing personalized, secure Windows 11 experiences. Understand key features, management, security, and deployment options for optimizing your environment.

Learning Objectives:

- Describe the key features of Azure Virtual Desktop
- Describe the Azure Virtual Desktop management experience
- Describe the Azure Virtual Desktop security model
- Describe the Azure Virtual Desktop deployment options

Lessons:

- Examine Azure Virtual Desktop
- Explore Azure Virtual Desktop
- Configure Azure Virtual Desktop
- Administer Azure Virtual Desktop