Microsoft 365 Endpoint Administrator

Course: MD 102T00

Length: 5 Days

About this Course

In this 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.

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

Audience profile

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.

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.

After completing this module, you'll be able to:

- 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.

Microsoft 365 Endpoint Administrator
Course: MD 102T00
Length: 5 Days

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.

After completing this module, you'll be able to:
- 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.

Module 3:Understand Microsoft Entra ID
This module explains Microsoft Entra ID. You'll compare Microsoft Entra ID to Active Directory DS, learn about Microsoft Entra ID P1 and P2, and explore Microsoft Entra Domain Services for managing domain-joined devices and apps in the cloud.

After this module, you should be able to:
- Describe Microsoft Entra ID.
- Compare Microsoft Entra ID to Active Directory Domain Services (AD DS).
- Describe how Microsoft Entra ID is used as a directory for cloud apps.
- Describe Microsoft Entra ID P1 and P2.
- Describe Microsoft Entra Domain Services.

Module 4: Manage Microsoft Entra identities
This module teaches how to use Microsoft Entra ID effectively. You'll learn about RBAC, user roles, creating and managing users and groups, using PowerShell cmdlets, and synchronizing objects from AD DS to Microsoft Entra ID.

After this module, you should be able to:
- Describe RBAC and user roles in Microsoft Entra ID.
- Create and manage users in Microsoft Entra ID.
- Create and manage groups in Microsoft Entra ID.
- Use Windows PowerShell cmdlets to manage Microsoft Entra ID.
- Describe how you can synchronize objects from AD DS to Microsoft Entra ID.

Module 5: Manage device authentication
In this module, you learn about device authentication and management in Microsoft Entra ID

After completing this module, you will be able to:
- 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.

Module 6: 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.

After completing this module, you will be able to:
- 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.

Modelu 7: Enroll devices using Microsoft Intune
Students will learn how to configure and setup Intune to more easily manage Windows, Android, and iOS devices.

After completing this module, you will be able to:
- 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.

Microsoft 365 Endpoint Administrator
Course: MD 102T00
Length: 5 Days

Module 8: Execute device profiles
Students learn about the various types of device profiles, and how to create and manage them.

After completing this module, you will be able to:
- Describe the various types of device profiles in Intune.
- Explain the difference between built-in and custom profiles.
- Create and manage profiles.

Module 9: Oversee device profiles
This module introduces students to monitoring profiles to ensure correct assignments and resolving conflicts when multiple profiles are applied.

After completing this module, you will be able to:
- 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.

Module 10: 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.

After completing this module, you will be able to:
- 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.

Module 11: 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.

After this module, you should be able to:
- 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

Module 12: 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.

After this module, you should be able to:
- 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

Module 13: 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.

After this module, you should be able to:
- 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

Microsoft 365 Endpoint Administrator
Course: MD 102T00
Length: 5 Days

Module 14: Protect identities in Microsoft Entra ID
This module introduces students to the various authentication methods used to protect identities.

After this module, you should be able to:
- 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

Module 15: Enable organizational access
This module describes how clients can be configured to access organizational resources using a virtual private network (VPN).

After this module, you should be able to:
- Describe how you can access corporate resources
- Describe VPN types and configuration
- Describe Always On VPN
- Describe how to configure Always On VPN

Module 16: Implement device compliance
This module describes how to use compliance and conditional access policies to help protect access to organizational resources.

After this module, you should be able to:
- Describe device compliance policy
- Deploy a device compliance policy
- Describe conditional access
- Create conditional access policies

Module 17; Generate inventory and compliance reports
This module describes how to use Microsoft Endpoint Manager and Power BI to create compliance and custom reports.

After this module, you should be able to:
- 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

Module 18: 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.

After this module, you should be able to:
- Describe Windows Information Protection
- Plan for Windows Information Protection usage
- Implement and use Windows Information Protection
- Describe the Encrypting File System (EFS)
- Describe BitLocker

Module 19: Manage Microsoft Defender for Endpoint
This module explores using Microsoft Defender for Endpoint to provide additional protection and monitor devices against threats.

After this module, you should be able to:
- 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

Module 20; Manage Microsoft Defender in Windows client
This module explains the built-in security features of Windows clients and how to implement them using policies.

Microsoft 365 Endpoint Administrator
Course: MD 102T00
Length: 5 Days

After this module, you should be able to:
- Describe Windows Security capabilities
- Describe Windows Defender Credential Guard
- Manage Microsoft Defender Antivirus
- Manage Windows Defender Firewall
- Manage Windows Defender Firewall with Advanced Security

Module 21: 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.

After this module, you should be able to:
- Describe Microsoft Defender for Cloud Apps
- Plan for Microsoft Defender for Cloud Apps usage
- Implement and use Microsoft Defender for Cloud Apps

Module 22: 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.

After completing this module, you will be able to:
- 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.

Module 23: 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.

After completing this module, you will be able to:
- 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.

Module 24: Deploy using Microsoft Configuration Manager
This module explains the common day to day tasks that Administrators would use Configuration Manager to perform.

After completing this module, you'll be able to:
- Describe the capabilities of Configuration Manager.
- Describe the key components of Configuration Manager.
- Describe how to troubleshoot Configuration Manager deployments.

Module 25; 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.

After completing this module, you will be able to:
- 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.

Microsoft 365 Endpoint Administrator
Course: MD 102T00
Length: 5 Days

- Describe how to troubleshoot common Autopilot issues.
- Describe the process of deployment using traditional methods.

Module 26: Implement dynamic deployment methods

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

After completing this module, you will be able to:
- 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 Microsoft Entra join.

Module 27: 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.

After completing this module, you should be able to:
- Identify usage scenarios for Microsoft Entra 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.

Module 28: 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.

After completing this module, you should be able to:
- 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

Module 29; 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.

After completing this module, you should be able to:
- 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