

MD-102T00: Microsoft 365 Endpoint Administrator

Overview

Course Duration: 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 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 Microsoft Entra, Windows Autopilot, Microsoft Intune Suite and Microsoft Defender for Endpoint are explored to protect devices and data.

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 endpoint management

This learning path is designed to provide a comprehensive understanding of enterprise desktops, Windows editions, and Microsoft Entra ID. It includes exploring various Windows editions, including their features and installation methods. It delves into Microsoft Entra ID, highlighting its similarities and differences with AD DS and how to synchronize the two. Furthermore, learners will better understand managing Microsoft Entra identities. Overall, this learning path equips learners with the necessary knowledge and skills to effectively support enterprise desktops and manage Microsoft Entra identities.

Module 2: Execute device enrollment

This learning path will cover Microsoft Entra join and will introduce Microsoft Endpoint Manager. We'll also discuss how to configure policies for enrolling devices to Configuration Manager and Microsoft Intune.

Module 3: Configure profiles for user and devices

This learning path explores Intune device profiles, the benefits of user profiles and how to synchronize profile data across multiple devices.

Module 4: Examine application management

Learners will examine application management methods using on-premises and cloud-based solutions.

Module 5: Manage authentication and compliance

This learning path covers the various solutions for managing authentication. Students will also learn about the different types of VPNs, as well as compliance and conditional access policies.

Module 6: Manage endpoint security

In this learning path, students will learn about data protection and protecting endpoints against threats. This path will also cover the key capabilities of Microsoft Defender solutions.

Module 7: Deploy using on-premises based tools

Students are introduced to deployment using the Microsoft Deployment Toolkit and Configuration Manager.

Module 8: Deploy using cloud based tools

Students will learn about using Windows Autopilot and deployment using Microsoft Intune. Students will also learn how co-management can be used to transition to modern management.

Prerequisites

- Strong technical skills installing, maintaining, and troubleshooting the Windows 10 OS or later.
- Strong understanding of computer networking, client security, and application concepts.
- Experience using Active Directory Domain Services.