New Horizons®

MD-101T00 Managing Modern Desktops

Summary

Length: 40 hours Level: Experienced

In this course, students will learn how to plan and implement an operating system deployment strategy using modern deployment methods, as well as how to implement an update strategy. Students will be introduced to key components of modern management and co-management strategies. This course also covers what it takes to incorporate Microsoft Intune into your organization. Students will also learn about methods for deployment and management of apps and browser-based applications. Students will be introduced to the key concepts of security in modern management including authentication, identities, access, and compliance policies. Students will be introduced to technologies such Azure Active Directory, Azure Information Protection and Windows Defender Advanced Threat Protection, as well as how

Learning Objectives

After completing this course, learners should be able to:
Plan, develop, and implement an Operating System deployment, upgrade, and update strategy.
Understand the benefits and methods of co-management strategies.
Plan and implement device enrollment and configuration.
Manage and deploy applications and plan a mobile application management strategy.
Manage users and authentication using Azure AD and Active Directory DS.
Describe and implement methods used to protect devices and data.

Course Outline

1. **Modern Management**

   The Enterprise Desktop
   Azure AD Overview
   Managing Identities in Azure AD

2. **Device Enrollment**

   Manage Device Authentication
   Device Enrollment using Microsoft Endpoint Configuration Manager
   Device Enrollment using Microsoft Intune

3. **Configuring Profiles**

   Configuring Device Profiles
   Managing User Profiles

4. **Application Management**

   Implement Mobile Application Management (MAM)
   Deploying and updating applications
   Administering applications

5. **Managing Authentication in Azure AD**

   Protecting Identities in Azure AD
   Enabling Organization Access
   Implement Device Compliance Policies
   Using Reporting

6. Managing Security

Implement device data protection
Managing Windows Defender ATP
Managing Windows Defender in Windows 10

7. Deployment using Microsoft Endpoint Manager - Part 1

Assessing Deployment Readiness
On-Premise Deployment Tools and Strategies

8. Deployment using Microsoft Endpoint Manager - Part 2

Deploying New Devices
Dynamic Deployment Methods
Planning a Transition to Modern Management

9. Managing Updates for Windows 10

Updating Windows 10
Windows Update for Business
Desktop Analytics

10. Managing Windows 10 security and feature updates

Describe the Windows 10 servicing channels
Configure a Windows update policy using Group Policy settings
Configure Windows Update for Business to deploy OS updates
Use Desktop Analytics to assess upgrade readiness

Audience

The Modern Desktop Administrator deploys, configures, secures, manages, and monitors devices and client applications in an enterprise environment. Responsibilities include managing identity, access, policies, updates, and apps. The MDA collaborates with the M365 Enterprise Administrator to design and implement a device strategy that meets the business needs of a modern organization.

Prerequisites

The Modern Desktop Administrator must be familiar with M365 workloads and must have strong skills and experience of deploying, configuring, and maintaining Windows 10 and non-Windows devices. The MDA role focuses on cloud services rather than on-premises management technologies.