

## MD-101T00-AC Managing Modern Desktops

### Overview

**Course Duration:** 5 Days

#### *About This Course*

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 as Azure Active Directory, Azure Information Protection and Windows Defender Advanced Threat Protection, as well as how to leverage them to protect devices and data.

#### *Audience Profile*

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.

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.

#### *At Course Completion*

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*

**Module 1: Modern Management** This module explains the concepts of supporting the desktop through its entire lifecycle. Finally, students will be introduced to the tools and strategies used for desktop deployment. Students will be introduced to the concept of directory in the cloud with Azure AD. Students will learn the similarities and differences between Azure AD and Active Directory DS and how to synchronize between the two. Students will explore identity management in Azure AD and learn about identity protection using Windows Hello for Business, as well as Azure AD Identity Protection and multi-factor authentication. **Lesson**

- The Enterprise Desktop
- Azure AD Overview
- Managing Identities in Azure AD

**Lab: Managing identities in Azure AD**

**Lab: Using Azure AD Connect to connect Active Directories**

After completing this module, students will be able to:

- Describe the enterprise desktop lifecycle.
- Describe the capabilities of Azure AD.
- Manage users using Azure AD with Active Directory DS.
- Implement Windows Hello for Business.
- Join devices to Azure AD.

**Module 2: Device Enrollment** This module will also cover Azure AD join and will be introduced to Microsoft Endpoint Manager, as well as learn how to configure policies for enrolling devices to Endpoint Manager and Intune. **Lesson**

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

**Lab: Configuring and managing Azure AD Join**

**Lab: Manage Device Enrollment into Intune**

**Lab: Enrolling devices into Microsoft Intune**

After completing this module, students will be able to:

- Configure and join devices to Azure AD
- Configure device enrollment in Microsoft Endpoint Manager
- Enroll devices in Endpoint Configuration Manager and Intune

**Module 3: Configuring Profiles** This module dives deeper into Intune device profiles including the types of device profiles and the difference between built-in and custom profiles. The student will learn about assigning profiles to Azure AD groups and monitoring devices and profiles in Intune. You will be introduced to the various user profile types that exist in Windows for on-premises devices. You will learn about the benefits of various profiles and how to switch between types of profiles. You will examine how Folder Redirection works and how to set it up. The lesson will then conclude with an overview of Enterprise State roaming and how to configure it for Azure AD devices. **Lesson**

- Configuring Device Profiles
- Managing User Profiles

**Lab: Creating and Deploying Configuration Profiles**

**Lab: Monitor device and user activity in Intune**

**Lab: Configuring Enterprise State Roaming**

After completing this module, you should be able to:

- Describe the various types of device profiles in Intune
- Create, manage, and monitor profiles
- Manage PowerShell scripts in Intune
- Explain the various user profile types that exist in Windows.
- Explain how to deploy and configure Folder Redirection.
- Configure Enterprise State Roaming for Azure AD devices.

**Module 4: Application Management** In this module, students learn about application management on-premises and cloud-based solutions. This module will cover how to manage Office 365 Pro Plus deployments in Endpoint Manager as well as how to manage apps on non-enrolled devices. The

module will also include managing Win32 apps and deployment using the Microsoft Store for Business. This module will conclude with an overview of Microsoft Edge and Enterprise Mode.

**Lesson**

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

**Lab: Deploying cloud apps using Intune**

**Lab: Configure App Protection Policies for Mobile Device**

**Lab: Deploy Apps using Endpoint Configuration Manager**

**Lab: Deploy Apps using Microsoft Store for Business**

After completing this module, students will be able to:

- Describe the methods for application management.
- Deploy applications using Endpoint Manager and Group Policy.
- Configure Microsoft Store for Business.
- Deploy Office365 Pro Plus using Intune.
- Manage and report application inventory and licenses.

**Module 5: Managing Authentication in Azure AD** This module covers the various solutions for managing authentication. The student will also learn about the different types of VPNs. This module also covers compliance policies and how to create conditional access policies. **Lesson**

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

**Lab: Configuring Multi-factor Authentication**

**Lab: Configuring Self-service password reset for user accounts in Azure AD**

**Lab: Configuring and validating device compliance**

**Lab: Creating device inventory reports**

After completing this module, students will be able to:

- Describe Windows Hello for Business
- Describe Azure AD Identity Protection
- Describe and manage multi-factor authentication
- Describe VPN types and configuration
- Deploy device compliance and conditional access policies
- Generate inventory reports and Compliance reports using Endpoint Manager

**Module 6: Managing Security** In this module, students will learn about data protection. Topics will include Windows & Azure Information Protection, and various encryption technologies supported in Windows 10. This module also covers key capabilities of Windows Defender Advanced Threat Protection and how to implement these capabilities on devices in your organization. The module concludes using Windows Defender and using functionalities such as antivirus, firewall and Credential Guard. **Lesson**

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

**Lab: Configure and Deploy Windows Information Protection Policies by using Intune**

**Lab: Configuring Endpoint security using Intune**

**Lab: Configuring Disk Encryption Using Intune**

After completing this module, students will be able to:

- Describe the methods protecting device data.
- Describe the capabilities and benefits of Windows ATP.
- Deploy and manage settings for Windows Defender clients.

**Module 7: Deployment using Microsoft Endpoint Manager - Part 1** In this two-part module, students will be introduced to deployment using Microsoft Endpoint Manager. Part 1 will cover the tools for assessing the infrastructure and planning a deployment, followed by deployment using the Microsoft Deployment Toolkit and Endpoint Configuration Manager. **Lesson**

- Assessing Deployment Readiness
- On-Premises Deployment Tools and Strategies

**Lab: Deploying Windows 10 using Microsoft Deployment Toolkit**

**Lab: Deploying Windows 10 using Endpoint Configuration Manager**

After completing this module, students will be able to:

- Describe the tools for planning a deployment.
- Deploy Windows 10 using the Microsoft Deployment Toolkit
- Deploy Windows 10 using Endpoint Configuration Manager

**Module 8: Deployment using Microsoft Endpoint Manager - Part 2** This module continues with deployment using Microsoft Endpoint Manager. In part two, the student will learn about using Windows Autopilot and deployment using Microsoft Intune. This module will also include dynamic OS deployment methods, such as Subscription Activation. The module will conclude learning how Co-Management can be used to transitioning to modern management. **Lesson**

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

## Lab: Deploying Windows 10 with Autopilot

## Lab: Configuring Co-Management Using Configuration Manager

After completing this module, students will be able to:

- Deploy Windows 10 using Autopilot
- Configure OS deployment using subscription activation and provisioning packages
- Upgrade, migrate and manage devices using modern management methods

### **Module 9: Managing Updates for Windows 10**

This module covers managing updates to Windows.

This module introduces the servicing options for Windows 10. Students will learn the different methods for deploying updates and how to configure windows update policies. Finally, students will learn how to ensure and monitor updates using Desktop Analytics. **Lesson**

- Updating Windows 10
- Windows Update for Business
- Desktop Analytics

## Lab: Managing Windows 10 security and feature updates

After completing this module, students will be able to:

- 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.

### **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. It is recommended students complete course MD-100, Windows 10, prior to taking this course.