

Days: 5

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.

Audience: Desktop Administrators that deploy, configure, secure, manage, and monitor devices and client applications in an enterprise environment.

Description: This five-day course is for Desktop Administrators that deploy, configure, secure, manage, and monitor devices and client applications in an enterprise environment. As desktops has evolved, so have methods for deploying and updating them. In this course, you'll learn how to plan and implement an operating system deployment strategy. This course will help you understand the various methods available, the scenarios they're suited for, as well as how to deploy Windows using modern methods. This course will also cover planning and implementing an update strategy for Windows.

With BYOD becoming commonplace and the need for employees to access line of business apps on personal devices, the scope of desktop administration must include both desktop and mobile devices, regardless of ownership. During this course, you'll be introduced to key components of modern management and co-management strategies. You'll examine what it takes to incorporate Microsoft Intune into your organization and how to use it to manage modern desktops and devices. You'll also learn about methods for deployment and management of apps and browser-based applications.

OUTLINE:

MODULE 1: PLANNING AN OPERATING SYSTEM DEPLOYMENT STRATEGY

This module explains how to plan and implement a deployment strategy. It covers various methods and scenarios for deploying Windows. It discusses on-premise and cloud technologies as well as considerations for new deployments, upgrading, and migrations.

LESSONS

- Overview of Windows as a service
- Windows 10 Deployment options
- Considerations for Windows 10 deployment

LAB: PRACTICE LAB - PLANNING WINDOWS 10 DEPLOYMENT

AFTER COMPLETING THIS MODULE, STUDENTS WILL BE ABLE TO:

- Describe Windows as a Service.
- Describe the different methods for deployment.
- Understand the differences between on-premise and cloud-based solutions.
- Describe methods of dynamic provisioning.
- Describe the different tools available in the Windows Assessment and Deployment Kit.
- Describe the scenarios and limitations for in-place upgrades and migrations.

MD-101: Managing Modern Desktops

MODULE 2: IMPLEMENTING WINDOWS 10

This module covers new modern methods for deploying Windows 10 such as Windows Autopilot and provisioning packages. This module also covers tool used in upgrade planning, application compatibility and migration methods.

LESSONS

- Implementing Windows 10 by using dynamic deployment
- Implementing Windows 10 by using Windows Autopilot
- Upgrading devices to Windows 10
- Lab: Practice Lab - Implementing Windows 10
- Creating and deploying provisioning package
- Migrating user settings
- Deploying Windows 10 with AutoPilot

AFTER COMPLETING THIS COURSE, LEARNERS SHOULD BE ABLE TO:

- Develop an Operating System deployment and upgrade strategy
- Understand the different methods of deployment.
- Understand which scenarios on-premise and cloud-based solutions can be used for.
- Deploy and migrate desktops to Windows 10.
- Plan and configure Windows Update policies.

MODULE 3: 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.

LESSONS

- Implementing Windows 10 by using dynamic deployment
- Implementing Windows 10 by using Windows Autopilot
- Upgrading devices to Windows 10

LAB: PRACTICE LAB - MANAGING UPDATES FOR WINDOWS 10

- Manually configuring Windows Update settings
- Configuring Windows Update by using GPOs

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 Windows Analytics to assess upgrade readiness and update compliance.

MODULE 4: DEVICE ENROLLMENT

In this module, students will examine the benefits and prerequisites for co-management and learn how to plan for it. This module will also cover Azure AD join and will be introduced to Microsoft Intune, as well as learn how to configure policies for enrolling devices. The module will conclude with an overview of device inventory in Intune and reporting using the Intune console, Power BI and Microsoft Graph.

LESSONS

- Device management options
- Manage Intune device enrollment and inventory

LAB: PRACTICE LAB - DEVICE ENROLLMENT AND MANAGEMENT

- Installing the MDM Migration Analysis Tool (MMAT)
- Obtain Intune and Azure AD Premium licenses and enable device management
- Enrolling devices in Intune
- Managing devices in Intune
- Creating device inventory reports

MD-101: Managing Modern Desktops

AFTER COMPLETING THIS MODULE, STUDENTS WILL BE ABLE TO:

- Describe benefits and methods for migrating to co-management.
- Deploy an MDM with Microsoft Intune.
- Configure device enrollment.
- Enroll desktop and mobile devices in Windows Intune.
- Configure and download inventory reports.

MODULE 5: 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. The module will conclude with an overview of using Windows Analytics for health and compliance reporting.

LESSONS

- Configuring device profiles
- Managing user profiles
- Monitoring devices

LAB: PRACTICE LAB - MANAGING PROFILES

- Configuring roaming user profiles and Folder Redirection
- Create and deploy device profile based on the scenario
- Change deployed policy and monitor user and device activity
- Configuring Enterprise State Roaming

AFTER COMPLETING THIS MODULE, STUDENTS WILL BE ABLE TO:

- Describe the types of device profiles.
- Create and assign device profiles.
- Configure user profile and folder redirection.
- Monitor and report on devices using Intune and Windows Analytics.

MODULE 6: APPLICATION MANAGEMENT

In this module, students learn about application management on-premise and cloud-based solutions. This module will cover how to manage Office 365 ProPlus deployments in Intune as well as how to manage apps on non-enrolled devices. The module will conclude with an overview of Enterprise Mode with Internet Explorer and Microsoft Edge and tracking your installed applications, licenses, and assigned apps using Intune.

LESSONS

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

LAB: PRACTICE LAB - MANAGING APPLICATIONS

- Deploying apps by using Intune
- Configure and deploy Office 365 ProPlus from Intune
- Configure mobile application management (MAM) policies in Intune

AFTER COMPLETING THIS MODULE, STUDENTS WILL BE ABLE TO:

- Describe the methods for application management.
- Deploy applications using Intune and Group Policy.
- Configure Microsoft Store for Business.
- Deploy Office365 ProPlus using Intune.
- Manage and report application inventory and licenses.
- Configure Internet Explorer Enterprise Mode.

MD-101: Managing Modern Desktops

MODULE 7: MANAGING AUTHENTICATION IN AZURE AD

In this module, 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. The module will conclude with securely accessing corporate resources and introduce concepts such as Always On VPN and remote connectivity in Windows 10.

LESSONS

- Azure AD Overview
- Managing identities in Azure AD
- Protecting identities in Azure AD
- Managing device authentication
- Enabling corporate access

LAB: PRACTICE LAB - MANAGING OBJECTS AND AUTHENTICATION IN AZURE AD

- Enabling and configuring Azure AD Premium with Enterprise Mobility + Security (EMS) tenant
- Creating user and group objects with UI and Windows PowerShell
- Configuring Self-service password reset (SSPR) for user accounts in Azure AD
- Joining a device to Azure AD

AFTER COMPLETING THIS MODULE, STUDENTS WILL BE ABLE TO:

- 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.
- Describe methods of enabling access from external networks.

MODULE 8: MANAGING DEVICES AND DEVICE POLICIES

In this module, students will be introduced to managing device security with Intune. Students will discover how Intune can use device profiles to manage configuration of devices to protect data on a device. Students will learn how to create and deploy compliance policies and use compliance policies for conditional access. The module concludes with monitoring devices enrolled in Intune.

LESSONS

- Microsoft Intune Overview
- Managing devices with Intune
- Implement device compliance policies

LAB: PRACTICE LAB - MANAGING DEVICES

- Configuring Microsoft Intune for device management
- Configuring compliance policies and device profiles
- Enrolling Windows 10 devices and managing compliance

AFTER COMPLETING THIS MODULE, STUDENTS WILL BE ABLE TO:

- Describe mobile device management with Intune.
- Create and assign device profiles to protect data on devices.
- Deploy compliance and conditional access policies.
- Use Intune to monitor device compliance.

MD-101: Managing Modern Desktops

MODULE 9: 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.

LESSONS

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

LAB: PRACTICE LAB - MANAGING SECURITY IN WINDOWS 10

- Configuring Encrypting File System (EFS)
- Configuring BitLocker
- Configuring a WIP policy in Intune
- Configuring Windows Defender

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.