Managing Modern Desktops

Course MD-101T00-A: 4 days; Instructor-Led

Introduction

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 Microsoft Defender for Endpoint as well as how to leverage them to protect devices and data.

At Course Completion

After completing this course, students will 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.

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. 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 later and non-Windows devices. The MDA role focuses on cloud services rather than on-premises management technologies.

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 later, 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 Client, prior to taking this course.

Course Outline

Module 1: Modern Management

This module explains the concepts of supporting the desktop through it's entire lifecycle. Finally, students will be introduced to the tools and strategies used for desktop deployment. Students well 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.

Lessons

- 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.

Lessons

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

Lab : Manage Device Enrollment into Intune
Lab : Configuring and managing Azure AD Join
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.

Lessons

- Configuring Device Profiles
- Managing User Profiles

Lab : Configuring Enterprise State Roaming
Lab : Creating and Deploying Configuration Profiles
Lab : Monitor device and user activity in Intune

After completing this module, students will 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-premise and cloud-based solutions. This module will cover how to manage Office 365 ProPlus 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.

Lessons

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

Lab : Configure App Protection Policies for Mobile Device
Lab : Deploying cloud apps using Intune

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 ProPlus 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.
Lessons

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

Lab : Creating device inventory reports
Lab : Configuring and validating device compliance
Lab : Configuring Multi-factor Authentication
Lab : Configuring Self-service password reset for user accounts in Azure AD
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. This module also covers key capabilities of Microsoft Defender for Endpoint and how to implement these capabilities on devices in your organization. The module concludes using Microsoft Defender and using functionalities such as antivirus, firewall and Credential Guard.
Lessons

- Implement device data protection
- Managing Microsoft Defender for Endpoint
- Managing Microsoft Defender in Windows Client

Lab : Configuring Endpoint security using Intune
Lab : Configure and Deploy Windows Information Protection Policies by 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 well 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.
Lessons

- Assessing Deployment Readiness
- On-Premise 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 clients using the Microsoft Deployment Toolkit
- Deploy Windows clients 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. Finally, students will be introduced to Azure Virtual Desktops and how to configure and manage cloud PC using Windows 365.

Lessons

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

Lab : Configuring Co-Management Using Configuration Manager

Lab : Deploying Windows 10 with Autopilot

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 and Using Analytics

This module covers managing updates to Windows. This module introduces the servicing options for Windows clients. 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.

Lessons

- Updating Windows Clients
- Windows Update for Business
- Desktop Analytics
- Endpoint Analytics

Lab : Managing Windows 10 security and feature updates

After completing this module, students will be able to:

- Describe the Windows client 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.
- Use Endpoint Analytics to monitor user experience and assess Windows 11 readiness

