Course Outline

Managing Modern Desktops

Course MD-101T00: 5 days Instructor Led

Overview

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.

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.

Course Objectives

- Examine the enterprise desktop
- Explore Azure Active Directory
- Manage identities in Azure Active Directory
- Manage device authentication
- Enroll devices using Microsoft Endpoint Configuration Manager
- Enroll devices using Microsoft Intune
- Implement device profiles
- Monitor device profiles
- Manage user profiles
- Implement mobile application management
- Deploy and update applications
- Administer applications
- Implement device data protection
- Manage Microsoft Defender for Endpoint
- Manage Microsoft Defender in Windows client
- Protect identities in Azure AD
- Enable organizational access
- Implement device compliance policies
- Generate inventory and compliance reports
- Assess deployment readiness
- Deploy using the Microsoft Deployment Toolkit
- Deploy using Endpoint Configuration Manager
- Deploy new devices

- Implement dynamic deployment methods
- Plan a transition to modern management
- Manage Cloud PCs and Virtual Desktops
- Update Windows client
- Update clients using Windows Update for Business
- Explore Desktop Analytics
- Explore Endpoint Analytics

Course Outline

Module 1: Examine the enterprise desktop

- Describe the benefits of Modern Management.
- Explain the enterprise desktop life-cycle model.
- Describe considerations for planning hardware strategies.
- Describe the steps in planning OS and app deployment.
- Describe considerations for post-deployment and retirement.

Module 2: Explore Azure Active Directory

- Describe Azure AD.
- Compare Azure AD to Active Directory Domain Services (AD DS).
- Describe how Azure AD is used as a directory for cloud apps.
- Describe Azure AD Premium P1 and P2.
- Describe Azure AD Domain Services.

Module 3: Manage identities in Azure Active Directory

- Describe RBAC and user roles in Azure AD.
- Create and manage users in Azure AD.
- Create and manage groups in Azure AD.
- Use Windows PowerShell cmdlets to manage Azure AD.
- Describe how you can synchronize objects from AD DS to Azure AD.

Module 4: Manage device authentication

- Describe Azure AD join.
- Describe Azure AD join prerequisites, limitations and benefits.
- Join device to Azure AD.
- Manage devices joined to Azure AD.

Module 5: Enroll devices using Microsoft Endpoint Configuration Manager

- Describe Microsoft Endpoint Manager.
- Understand the advantages of managing a client with Configuration Manager.

- Deploy the Configuration Manager client.
- Monitor the Configuration Manager client.
- Manage Configuration Manager devices.

Module 6: Enroll devices using Microsoft Intune

- Prepare Microsoft Intune for device enrollment.
- Configure Microsoft Intune for automatic enrollment.
- Explain how to enroll Windows, Android and iOS devices in Intune.
- Explain when and how to use Intune Enrollment Manager.
- Understand how to monitor and perform remote actions on enrolled devices.

Module 7: Implement device profiles

- Describe the various types of device profiles in Intune.
- Explain the difference between built-in and custom profiles.
- Create and manage profiles.

Module 8: Monitor device profiles

- Monitor the assignments of profiles.
- Understand how profiles are synchronized and how to manually force synchronization.
- Use PowerShell to execute and monitor scripts on devices.

Module 9: Manage user profiles

- Explain the various user profile types that exist in Windows.
- Describe how a user profile works.
- Configure user profiles to conserve space.
- Explain how to deploy and configure Folder Redirection.
- Explain Enterprise State Roaming.
- Configure Enterprise State Roaming for Azure AD devices.

Module 10: Implement mobile application management

- Explain Mobile Application Management
- Understand application considerations in MAM
- Explain how to use Configuration Manager for MAM
- Use Intune for MAM
- Implement and manage MAM policies

Module 11: Deploy and update applications

- Explain how to deploy applications using Intune
- Learn how to deploy applications using Group Policy

- Understand Microsoft Store for Business
- Learn how to configure Microsoft Store for Business
- Explain how to use Microsoft Store for Business

Module 12: Administer applications

- Explain how to manage apps in Intune
- Understand how to manage apps on non-enrolled devices
- Understand how to deploy Microsoft 365 Apps using Intune
- Learn how to configure and manage IE mode in Microsoft Edge
- Learn about app inventory options in Intune

Module 13: Implement device data protection

- Describe Windows Information Protection
- Plan for Windows Information Protection usage
- Implement and use Windows Information Protection
- Describe the Encrypting File System (EFS)
- Describe BitLocker

Module 14: Manage Microsoft Defender for Endpoint

- Describe Microsoft Defender for Endpoint
- Describe key capabilities of Microsoft Defender for Endpoint
- Describe Microsoft Defender Application Guard
- Describe Microsoft Defender Exploit Guard
- Describe Windows Defender System Guard

Module 15: Manage Microsoft Defender in Windows client

- Describe Windows Security capabilities
- Describe Windows Defender Credential Guard
- Manage Microsoft Defender Antivirus
- Manage Windows Defender Firewall
- Manage Windows Defender Firewall with Advanced Security

Module 16: Protect identities in Azure AD

- Describe Windows Hello for Business
- Describe Windows Hello deployment and management
- Describe Azure AD Identity Protection
- Describe and manage self-service password reset in Azure AD
- Describe and manage multi-factor authentication

Course Outline

Module 17: Enable organizational access

- Describe how you can access corporate resources
- Describe VPN types and configuration
- Describe Always On VPN
- Describe how to configure Always On VPN

Module 18: Implement device compliance policies

- Describe device compliance policy
- Deploy a device compliance policy
- Describe conditional access
- Create conditional access policies

Module 19: Generate inventory and compliance reports

- Generate inventory reports and Compliance reports using Microsoft Intune
- Report and monitor device compliance
- Create custom reports using the Intune Data Warehouse
- Use the Microsoft Graph API for building custom reports

Module 20: Assess deployment readiness

- Describe the guidelines for an effective enterprise desktop deployment.
- Explain how to assess the current environment.
- Describe the tools that you can use to assess your current environment.
- Describe the methods of identifying and mitigating application compatibility issues.
- Explain considerations for planning a phased rollout.

Module 21: Deploy using the Microsoft Deployment Toolkit

- Describe the fundamentals of using images in traditional deployment methods.
- Describe the key benefits, limitations, and decisions when planning a deployment of - Windows using Microsoft Deployment Toolkit (MDT).
- Describe how Configuration Manager builds upon MDT and how both can work in harmony.
- Explain the different options and considerations when choosing the user interaction experience during deployment, and which methods and tools support these experiences.

Module 22: Deploy using Endpoint Configuration Manager

- Describe the capabilities of Configuration Manager.
- Describe the key components of Configuration Manager.
- Describe how to troubleshoot Configuration Manager deployments.

Module 23: Deploy new devices

- Explain the benefits of modern deployment for new devices.
- Describe the process of preparing for an Autopilot deployment.
- Describe the process of registering devices in Autopilot.
- Describe the different methods and scenarios of Autopilot deployments.
- Describe how to troubleshoot common Autopilot issues.
- Describe the process of deployment using traditional methods.

Module 24: Implement dynamic deployment methods

- Describe how Subscription Activation works.
- Describe the benefits of Provisioning Packages.
- Explain how Windows Configuration Designer creates Provisioning Packages.
- Describe the benefits of using MDM enrollment with Azure AD join.

Module 25: Plan a transition to modern management

- Identify usage scenarios for Azure AD join.
- Identify workloads that you can transition to Intune.
- Identify prerequisites for co-management.
- Identify considerations for transitioning to modern management.
- Plan a transition to modern management using existing technologies.
- Plan a transition to modern management using Microsoft Intune.

Module 26: Manage Cloud PCs and Virtual Desktops

- Describe the differences between Azure Virtual Desktop and Windows 365.
- Configure Windows 365 using Endpoint Manager admin center.
- Create a provisioning policy to deploy a Windows 365 desktop.
- Reprovision and resize Windows 365 desktops.

Module 27: Update Windows client

- Describe Windows servicing options and channels.
- Explain available methods for applying updates to Windows.
- Configure Windows Update settings in Windows.
- Describe available Group Policy settings for configure Windows Update.
- Explain how Windows Insider for Business works.

Module 28: Update clients using Windows Update for Business

- Describe Windows Update for Business.
- Configure Windows Update for Business.
- Identify scenarios for using Windows Update for Business.

Course Outline

Module 29: Explore Desktop Analytics

- Describe the benefits of Desktop Analytics.
- Describe how Desktop Analytics is configured.
- Explain how Desktop Analytics can assess compatibility and monitor health.
- Describe how Desktop Analytics can be used to create a deployment plan.

Module 30: Explore Endpoint Analytics

- Describe the benefits of Endpoint Analytics.
- Describe how Endpoint Analytics can monitor performance and the user experience.
- Describe how Endpoint Analytics can identify application issues.
- Describe how Endpoint Analytics can be used to help transition to modern management and Windows 11.