MD-101T00: Managing Modern Desktops

Course Duration: 5 Days

Class times: 9am-4pm

Course Level: intermediate

Language: English

Mode of Training: Virtually Instructor-Led

Prerequisites

Job Role: Administrator

Related Exam: MD-101

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

Course Outline

Module 1: Examine the enterprise desktop.

This module introduces the student to the concepts of modern management and the enterprise desktop lifecycle.

Learning objectives

After completing this module, you will be able to:

- 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

This module introduces students to the concepts of Azure Active Directory.

Learning objectives

After this module, you should be able to:

- 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

This module introduces students to identity concepts including role-based access control and managing groups.

Learning objectives

After this module, you should be able to:

- 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.

In this module, you will learn about device authentication and management in Azure Active Directory.

Learning objectives

After completing this module, you will be able to:

- 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

This module introduces students to client deployment options and some of the high-level management and monitoring options that are available using Configuration Manager.

Learning objectives

After completing this module, you will be able to:

- 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

Students will learn how to configure and setup Intune to manage Windows, Android, and iOS devices more easily.

Learning objectives

After completing this module, you will be able to:

- 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

Students will learn about the various types of device profiles, and how to create and manage them.

Learning objectives

After completing this module, you will be able to:

- 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

This module introduces students to monitoring profiles to ensure correct assignments and resolving conflicts when multiple profiles are applied.

Learning objectives

After completing this module, you will be able to:

- 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.

Students will learn about the benefits of various Windows user profiles, how to manage them, and how to facilitate profile data synchronization across multiple devices.

Learning objectives

After completing this module, you will be able to:

- 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.

This module introduces Mobile Application Management (MAM). Students will learn about considerations for implementing MAM and will be introduced to the management of MAM using Microsoft Endpoint Manager.

Learning objectives

After this module, you should be able to:

- 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.

In this module, you will be introduced to application deployment in Intune and Microsoft Store for Business.

Learning objectives

After this module, you should be able to:

- 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.

In this module, you will be introduced to managing apps on Intune managed devices. The module will then conclude with an overview of how to use IE Mode with Microsoft Edge.

Learning objectives

After this module, you should be able to:

- 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.

This module describes how you can use Intune to create and manage WIP policies that manage this protection. The module also covers implementing BitLocker and Encrypting File System.

Learning objectives

After this module, you should be able to:

- 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

This module explores using Microsoft Defender for Endpoint to provide additional protection and monitor devices against threats.

Learning objectives

After this module, you should be able to:

- 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.

This module explains the built-in security features of Windows clients and how to implement them using policies.

Learning objectives

After this module, you should be able to:

- 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

This module introduces students to the various authentication methods used to protect identities.

Learning objectives

After this module, you should be able to:

- 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.

Module 17: Enable organizational access.

This module describes how clients can be configured to access organizational resources using a virtual private network (VPN).

Learning objectives

- 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.

This module describes how to use compliance and conditional access policies to help protect access to organizational resources.

Learning objectives

After this module, you should be able to:

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

Module 19: Generate inventory and compliance reports.

This module describes how to use Microsoft Endpoint Manager and Power BI to create compliance and custom reports.

Learning objectives

After this module, you should be able to:

- 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.

Discusses some of the tools that you can use to perform detailed assessments of existing deployments and describes some of the challenges that you may face.

Learning objectives

After completing this module, you will be able to:

- 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

Discusses the shifts from traditional to modern management and where on-premises solutions best fit in today's enterprise.

Learning objectives

After completing this module, you will be able to:

- 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

This module explains the common day to day tasks that Administrators would use Configuration Manager to perform.

Learning objectives

After completing this module, you'll be able to:

- 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.

Use Autopilot to deploy new hardware or refreshing an existing hardware with the organization's desired configuration, without using the traditional imaging process.

Learning objectives

After completing this module, you will be able to:

- 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.

Use dynamic provisioning methods such as Subscription Activation, Provisioning packages, and Azure AD join to reconfigure an existing operating system.

Learning objectives

After completing this module, you will be able to:

- 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.

Explore considerations and review the planning of transitioning to modern management, focusing on migration and newly provisioned devices.

Learning objectives

After completing this module, you should be able to:

- 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

Use Endpoint Manager to manage Azure Virtual Desktops and Windows 365 cloud PCs.

Learning objectives

After completing this module, you should be able to:

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

Module 27: Update Windows client

Explore the Windows servicing channels and use tools such as Windows Server Update Service (WSUS) to manage Windows update deployments.

Learning objectives

After completing this module, you will be able to:

- 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

Leverage Windows Update for Business to control the distribution and methods for Windows update delivery.

Learning objectives

After completing this module, you'll be able to:

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

Module 29: Explore Desktop Analytics

Use Desktop Analytics to evaluate client's health information to plan an update deployment.

Learning objectives

After completing this module, you will be able to:

- 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

Use Endpoint analytics to help identify policies or hardware issues that ultimately create a poor user experience and help remediate those issues.

Learning objectives

After completing this module, you will be able to:

- 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.

Microsoft Solutions Partner
Modern Work

Microsoft Solutions Partner
Infrastructure
Azure

FORTINET AUTHORIZED PARTNER

mile2 AUTHORIZED TRAINING CENTER

eset Gold Partner

DARKTRACE

IIBA Endorsed Education Provider™

www.cttl.net
transform@cttl.net
1-868-678-2885