Modern Desktop Administrator: Managing Modern Desktops (MD-101)

Modality: Virtual Classroom

Duration: 5 Days

You will obtain a Free Official Exam Voucher (apart from purchases utilizing SATV / Training Vouchers) for the MD-101 Certification if you register in this course without the Master Subscription Plan. If you are enrolled in the Master Subscription, this course doesn't provide an Exam Voucher but you could apply to obtain the Official Exam Voucher individually.

About this course:

When desktops have changed, so approaches to deploy and upgrade them have evolved. Throughout this program, students will discover techniques to prepare and execute a delivery strategy for an OS. Current organizations demand that the Desktop Admin be able to handle and operate computers, phones, and tablets, either owned by the employee or owned by the company. This program will assist you to learn the different techniques available, the situations for which they are suitable and how to implement Windows utilizing current methods. This program will also incorporate implementing and planning an upgrade tactics for Windows.

As need for companies to make it possible for the workforce to be more mobile, the role of a desktop administrator is really not just about desktop management any more. With Bring your own device becoming common and the requirement for workers to obtain line of enterprise applications on personal devices, both mobile and desktop devices should be incorporated in the scope of desktop administration irrespective of ownership. Throughout this program students will learn the main features of co-management strategies and modern management.

Students will examine what it requires for MS Intune to be integrated into your company and how it can be used to handle modern devices and desktops. You will also study about techniques for managing and deploying applications and browser-based apps.

Daily, many companies are requesting for information technology to assist worker mobility. Present environments allow that the Desktop Admin be able to support and handle computers, tablets, and phones, be they owned by the employee personally or by the organization. At same period, IT still wants to be able to secure the data accessed by those apps. The participant will be guided to the core security principles in modern management in this course. This course teaches access, identities, and authentication, and also how these categories can be protected the participant will be guided to the Azure Active Directory and will understand techniques to utilize MS Intune in enforcement policies to secure devices and data. Additionally, this program will discuss main Azure Information Security and Advanced Threat Protection features for Windows Defender, and how to apply these technologies.

The System Administrator can earn an average salary of $65,000 per annum.

Course Objective:

After this training has been finished, students are expected to:

- Understand for which on-premise situations cloud-based solutions can be utilize
- Intune configuration
- Establish an OS implement and update strategy
- Configure and plan Windows update policies
- Handle and implement applications, including Internet and Office 365 ProPlus
- Handle folder redirection and user profiles
- Explain the capabilities and benefits of Azure Active Directory
- Deployment of Windows Hello for Business
- Explain the different tools utilize to protect data and devices
- Grasp the various techniques of deployment
- Migrate and implement desktops to Windows 10
- Grasp the methods and benefits of co-management strategies
- Configure device policies and enroll devices in Intune
- Design a mobile app management tactics
- Explorer settings
- Use Azure Active Directory and AD DS to manage users
- Establish conditional accessibility regulation on the basis of compliance policies
- Advanced Threat Protection by implementing Windows Defender

Audience:

In an enterprise environment the Modern Desktop Manager configure, manage, deploy, monitor, and secure client apps and devices. Obligations involve managing access, updates, apps, identity, and policies. The M365 Enterprise Administrator and the MDA work together to develop and implement a device strategy that satisfies the business requirements of a modern enterprise.

Prerequisite:

The MDA must be experienced with M365 workloads, and seem to have good installation, setup, and maintenance skills for Windows 10 and non-Windows devices. The position of the Modern Desktop Administrator focuses on the management of cloud services rather than on-premises technology.

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, 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-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 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 : 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 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.

Lessons

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

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 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.

Lessons

- 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.