Managing Modern Desktops

Length: 5 days
Format: Bootcamp
Time: Day

About This Course

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 Windows Defender Advanced Threat Protection, as well as how to leverage them to protect devices and data.

Required Exams

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

Course Objectives

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.

Outline

Module 1: Planning an Operating System Deployment Strategy

This module explains how to plan and implement a deployment strategy. Students will learn about the concepts of supporting the desktop through it's entire lifecycle. This module also covers assessing an existing environment and the tools used to prepare a deployment strategy. Finally, students will be introduced to the tools and strategies used for desktop deployment.

Lessons

* The Enterprise Desktop
* Assessing Deployment Readiness
* Deployment Tools & Strategies

Module 2: Implementing Windows 10

This module covers the modern methods of Windows deployment used in common scenarios such as upgrading and migrating to Windows 10, as well as deploying new devices and refreshing existing devices. Students will also learn about alternate methods of OS deployment as well as considerations when choosing methods of deployment.

Lessons

* Upgrading Devices to Windows 10
* Deploying New Devices and Refreshing
* Migrating Devices to Windows 10
* Alternate Deployment Methods
* Imaging Considerations

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. Finally, students will learn how to ensure and monitor update compliance using Windows Analytics.

Lessons

* Updating Windows 10
* Windows Update for Business
* Introduction to Windows Analytics

Module 4: Device Enrollment

TIn 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
* Microsoft Intune Overview
* Manage Intune device enrollment and inventory
* Managing devices with Intune

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

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

Module 7: Managing Authentication in Azure AD

In this module, 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

* Azure AD Overview
* Managing identities in Azure AD
* Protecting identities in Azure AD
* Managing device authentication

Module 8: Managing Device Access and Compliance

In this module, students will be introduced to managing device security. The module will cover securely accessing corporate resources and introduce concepts such as Always On VPN and remote connectivity in Windows 10. 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
* Implement device compliance policies

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