Course Outline

MD-101T03 Protecting Modern Desktops and Devices

Course Summary

Description

This 1-day course, every day, more organizations are asking IT to support mobility in the workforce. Modern environments require the Desktop Administrator be able to manage and support phones, tablets, and computers, whether it be owned by the organization or personally owned by the employee. At the same time, IT must still be able to protect the data that these devices access. In this course, the student will be introduced to the key concepts of security in modern management. This course covers authentication, identities, and access, as well as about how to protect these categories. The student will be introduced to Azure Active Directory and learn how to use Microsoft Intune to protect devices and data with compliance policies. Finally, this course will cover key capabilities of Azure Information Protection and Windows Defender Advanced Threat Protection and how to implement these capabilities.

This class is part of the following 5-day comprehensive class: https://www.protechtraining.com/md-101-managing-modern-desktops-pt21956

Objective

After completing this course, learners should be able to:

- Describe the benefits and capabilities of Azure AD.
- Manage users using Azure AD with Active Directory DS.
- Implement Windows Hello for Business.
- Configure conditional access rules based on compliance policies.
- Describe the various tools used to secure devices and data.
- Implement Windows Defender Advanced Threat Protection

Topics

- Managing Authentication in Azure AD
- Managing Devices and Device Policies
- Managing Security
- Course Conclusion

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

Prerequisite

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.

Duration

One Day

Course Outline

MD-101T03 Protecting Modern Desktops and Devices

Course Outline

I. ***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. The module will conclude with securely accessing corporate resources and introduce concepts such as Always On VPN and remote connectivity in Windows 10.

A. Azure AD Overview
B. Managing identities in Azure AD
C. Protecting identities in Azure AD
D. Managing device authentication
E. Enabling corporate access

- Lab : Practice Lab - Managing objects and authentication in Azure AD
- Enabling and configuring Azure AD Premium with Enterprise Mobility + Security (EMS) tenant
- Creating user and group objects with UI and Windows PowerShell
- Configuring Self-service password reset (SSPR) for user accounts in Azure AD
- Joining a device to Azure AD

II. ***Managing Devices and Device Policies***

In this module, students will be introduced to managing device security with Intune. Students will discover how Intune can use device profiles to manage configuration of devices to protect data on a device. 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.

A. Microsoft Intune Overview
B. Managing devices with Intune
C. Implement device compliance policies

- Lab : Practice Lab - Managing devices
- Configuring Microsoft Intune for device management
- Configuring compliance policies and device profiles
- Enrolling Windows 10 devices and managing compliance

III. ***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.

A. Implement device data protection
B. Managing Windows Defender ATP
C. Managing Windows Defender in Windows 10

- Lab : Practice Lab - Managing Security in Windows 10
- Configuring Encrypting File System (EFS)
- Configuring BitLocker
- Configuring a WIP policy in Intune
- Configuring Windows Defender

IV. ***Course Conclusion***

A. Final Exam

- Lab : Graded Lab