Protecting Modern Desktops and Devices

Module 1: Managing Authentication in Azure AD

In this module, students will be introduced to the concept of directory in the cloud with Azure Active Directory (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.

Lessons

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

After completing this module, students will be able to:

- 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.
- Describe methods of enabling access from external networks.

Module 2: 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.

Lessons

- Microsoft Intune Overview

- Managing devices with Intune
- 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

After completing this module, students will be able to:

- Describe mobile device management with Intune.
- Create and assign device profiles to protect data on devices.
- Deploy compliance and conditional access policies.
- Use Intune to monitor device compliance.

Module 3: 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 (Windows Defender ATP) 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 : Practice Lab - Managing Security in Windows 10

- Configuring Encrypting File System (EFS)
- Configuring BitLocker
- Configuring a WIP policy in Intune
- Configuring Windows Defender

After completing this module, students will be able to:

- Describe the methods protecting device data.
- Describe the capabilities and benefits of Windows Defender ATP
- Deploy and manage settings for Windows Defender clients.

Module 4: Course Conclusion

Lessons

- Final Exam

Lab : Graded Lab