Course Outline

MS-101T00-A: Microsoft 365 Mobility and Security

Course Summary

Description

This course covers three central elements of Microsoft 365 enterprise administration – Microsoft 365 security management, Microsoft 365 compliance management, and Microsoft 365 device management. In Microsoft 365 security management, you will examine all the common types of threat vectors and data breaches facing organizations today, and you will learn how Microsoft 365's security solutions address these security threats. You will be introduced to the Microsoft Secure Score, as well as to Azure Active Directory Identity Protection. You will then learn how to manage the Microsoft 365 security services, including Exchange Online Protection, Advanced Threat Protection, Safe Attachments, and Safe Links. Finally, you will be introduced to the various reports that monitor your security health. You will then transition from security services to threat intelligence; specifically, using the Security Dashboard and Advanced Threat Analytics to stay ahead of potential security breaches. With your Microsoft 365 security components now firmly in place, you will examine the key components of Microsoft 365 compliance management. This begins with an overview of all key aspects of data governance, including data archiving and retention, Information Rights Management, Secure Multipurpose Internet Mail Extension (S/MIME), Office 365 message encryption, and data loss prevention (DLP). You will then delve deeper into archiving and retention, paying particular attention to in-place records management in SharePoint, archiving and retention in Exchange, and Retention policies in the Security and Compliance Center. Now that you understand the key aspects of data governance, you will examine how to implement them, including the building of ethical walls in Exchange Online, creating DLP policies from built-in templates, creating custom DLP policies, creating DLP policies to protect documents, and creating policy tips. You will then focus on managing data governance in Microsoft 365, including managing retention in email, troubleshooting retention policies and policy tips that fail, as well as troubleshooting sensitive data. You will then learn how to implement Azure Information Protection and Windows Information Protection. You will conclude this section by learning how to manage search and investigation, including searching for content in the Security and Compliance Center, auditing log investigations, and managing advanced eDiscovery. The course concludes with an in-depth examination of Microsoft 365 device management. You will begin by planning for various aspects of device management, including preparing your Windows 10 devices for co-management. You will learn how to transition from Configuration Manager to Intune, and you will be introduced to the Microsoft Store for Business and Mobile Application Management. At this point, you will transition from planning to implementing device management; specifically, your Windows 10 deployment strategy. This includes learning how to implement Windows Autopilot, Windows Analytics, and Mobile Device Management (MDM). When examining MDM, you will learn how to deploy it, how to enroll devices to MDM, and how to manage device compliance.

Topics

- Microsoft 365 Security Metrics
- Microsoft 365 Security Services
- Microsoft 365 Threat Intelligence
- Data Governance in Microsoft 365
- Archiving and Retention in Office 365
- Data Governance in Microsoft 365 Intelligence
- Search and Investigations
- Device Management
- Windows 10 Deployment Strategies
- Mobile Device Management

Audience

This course is designed for persons who are aspiring to the Microsoft 365 Enterprise Admin role and have completed one of the Microsoft 365 role-based administrator certification paths.

Prerequisite

- Completed a role-based administrator course such as Messaging, Teamwork, Security and Compliance, or Collaboration.
- A proficient understanding of DNS and basic functional experience with Microsoft 365 services.
- A proficient understanding of general IT practices.

Duration

Five Days

Course Outline

MS-101T00-A: Microsoft 365 Mobility and Security

Course Outline

I. ***Introduction to Microsoft 365 Security Metrics***
   A. Threat Vectors and Data Breaches
   B. Security Solutions in Microsoft 365
   C. Introduction to the Secure Score
   D. Introduction to Azure Active Directory Identity Protection

II. ***Managing Your Microsoft 365 Security Services***
   A. Introduction to Exchange Online Protection
   B. Introduction to Advanced Threat Protection
   C. Managing Safe Attachments
   D. Managing Safe Links
   E. Monitoring and Reports

III. ***Lab 1 - Manage Microsoft 365 Security Services***
   A. Lab: Manage Microsoft 365 Security Services
      1. Exercise 1 - Set up a Microsoft 365 Trial Tenant
      2. Exercise 2 - Implement an ATP Safe Links policy and Safe Attachment policy

IV. ***Microsoft 365 Threat Intelligence***
   A. Overview of Microsoft 365 Threat Intelligence
   B. Using the Security Dashboard
   C. Configuring Advanced Threat Analytics
   D. Implementing Your Cloud Application Security

V. ***Lab 2 - Implement Alert Notifications Using the Security Dashboard***
   A. Lab : Implement Alert Notifications Using the Security Dashboard
      1. Exercise 1 - Prepare for implementing Alert Policies
      2. Exercise 2 - Implement Security Alert Notifications
      3. Exercise 3 - Implement Group Alerts
      4. Exercise 4 - Implement eDiscovery Alerts

VI. ***Introduction to Data Governance in Microsoft 365***
   A. Introduction to Archiving in Microsoft 365
   B. Introduction to Retention in Microsoft 365
   C. Introduction to Information Rights Management
   D. Introduction to Secure Multipurpose Internet Mail Extension
   E. Introduction to Office 365 Message Encryption
   F. Introduction to Data Loss Prevention

VII. ***Archiving and Retention in Office 365***
   A. In-Place Records Management in SharePoint
   B. Archiving and Retention in Exchange
   C. Retention Policies in the SCC

VIII. ***Lab 3 - Implement Archiving and Retention***
   A. Lab : Implement Archiving and Retention
      1. Exercise 1 - Initialize Compliance in Your Organization
      2. Exercise 2 - Configure Retention Tags and Policies
      3. Exercise 3 - Implement Retention Policies

IX. ***Implementing Data Governance in Microsoft 365 Intelligence***
   A. Planning Your Security and Compliance Needs
   B. Building Ethical Walls in Exchange Online
   C. Creating a Simple DLP Policy from a Built-in Template
   D. Creating a Custom DLP Policy
   E. Creating a DLP Policy to Protect Documents
   F. Working with Policy Tips

Course Outline

MS-101T00-A: Microsoft 365 Mobility and Security

Course Outline (cont.)

X. *Lab 4 - Implement DLP Policies*
- A. Lab : Implement DLP Policies
  1. Exercise 1 - Manage DLP Policies
  2. Exercise 2 - Test MRM and DLP Policies

XI. *Managing Data Governance in Microsoft* 365
- A. Managing Retention in Email
- B. Troubleshooting Data Governance
- C. Implementing Azure Information Protection
- D. Implementing Advanced Features of AIP
- E. Implementing Windows Information Protection

XII. *Lab 5 - Implement AIP and WIP*
- A. Lab : Implement AIP and WIP
  1. Exercise 1 - Implement Azure Information Protection
  2. Exercise 2 - Implement Windows Information Protection

XIII. *Managing Search and Investigations*
- A. Searching for Content in the Security and Compliance Center
- B. Auditing Log Investigations
- C. Managing Advanced eDiscovery

XIV. *Lab 6 - Manage Search and Investigations*
- A. Lab : Manage Search and Investigations
  1. Exercise 1 - Investigate Your Microsoft 365 Data
  2. Exercise 2 - Configure and Deploy a Data Subject Request

XV. *Planning for Device Management*
- A. Introduction to Co-management
- B. Preparing Your Windows 10 Devices for Co-management
- C. Transitioning from Configuration Manager to Intune
- D. Introduction to Microsoft Store for Business
- E. Planning for Mobile Application Management

XVI. *Lab 7 - Implement the Microsoft Store for Business*
- A. Lab : Implement the Microsoft Store for Business
  1. Exercise 1 - Configure the Microsoft Store for Business
  2. Exercise 2 - Manage the Microsoft Store for Business

XVII. *Planning Your Windows 10 Deployment Strategy*
- A. Windows 10 Deployment Scenarios
- B. Implementing Windows Autopilot
- C. Planning Your Windows 10 Subscription Activation Strategy
- D. Resolving Windows 10 Upgrade Errors
- E. Introduction to Windows Analytics

XVIII. *Implementing Mobile Device Management*
- A. Planning Mobile Device Management
- B. Deploying Mobile Device Management
- C. Enrolling Devices to MDM
- D. Managing Device Compliance

XIX. *Lab 8 - Manage Devices with Intune*
- A. Lab : Manage Devices with Intune
  1. Exercise 1 - Enable Device Management
  2. Exercise 2 - Configure Azure AD for Intune
  3. Exercise 3 - Create Intune Policies
  4. Exercise 4 - Enroll a Windows 10 Device
  5. Exercise 5 - Manage and Monitor a Device in Intune