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

About this course

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.

Audience profile

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

Prerequisites

- 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.

Skills gained

- 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

COURSE OUTLINE

Module 1: Introduction to Microsoft 365 Security Metrics

In this module, 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, including the Zero Trust approach. You will be introduced to the Microsoft Secure Score, Privileged Identity Management, as well as to Azure Active Directory Identity Protection.

Lessons

- Threat Vectors and Data Breaches
- The Zero Trust Model
- Security Solutions in Microsoft 365
- Introduction to Microsoft Secure Score
- Privileged Identity Management
- Introduction to Azure Active Directory Identity Protection
- Lab : Tenant Setup and PIM
- Initialize your Microsoft 365 Tenant
- PIM Resource Workflows

After completing this module, students will be able to:

- Describe several techniques hackers use to compromise user accounts through email
- Describe techniques hackers use to gain control over resources
- Describe techniques hackers use to compromise data
- Describe the Zero Trust approach to security in Microsoft 365.
- Describe the components of Zero Trust security.
- Describe and five steps to implementing a Zero Trust model in your organization.
- Explain Zero Trust networking
- List the types of threats that can be avoided by using EOP and Office 365 ATP
- Describe how Microsoft 365 Threat Intelligence can be benefit your organization
- Monitor your organization through auditing and alerts
- Describe how ASM enhances visibility and control over your tenant through three core areas
- Describe the benefits of Secure Score and what kind of services can be analyzed
- Describe how to collect data using the Secure Score API
- Know where to identify actions that will increase your security by mitigating risks
- Explain how to determine the threats each action will mitigate and the impact it has on use
- Explain Privileged Identity Management (PIM) in Azure administration
- Configure PIM for use in your organization
- Audit PIM roles
- Explain Microsoft Identity Manager
- Explain Privileged Access Management in Microsoft 365
- Describe Azure Identity Protection and what kind of identities can be protected
- Understand how to enable Azure Identity Protection
- Know how to identify vulnerabilities and risk events
- Plan your investigation in protecting cloud-based identities
- Plan how to protect your Azure Active Directory environment from security breaches

Module 2: Managing Your Microsoft 365 Security Services

This module examines how to manage the Microsoft 365 security services, including Exchange Online Protection, Advanced Threat Protection, Safe Attachments, and Safe Links. You will be introduced to the various reports that monitor your security health.

Lessons

- Introduction to Exchange Online Protection
- Introduction to Advanced Threat Protection
- Managing Safe Attachments
- Managing Safe Links
- Monitoring and Reports
- Lab : Manage Microsoft 365 Security Services
- Implement a Safe Attachments policy
- Implement a Safe Links policy

After completing this module, students will be able to:

- Describe the anti-malware pipeline as email is analyzed by Exchange Online Protection
- List several mechanisms used to filter spam and malware
- Describe additional solutions to protect against phishing and spoofing
- Describe the benefits of the Spoof Intelligence feature
- Describe how Safe Attachments is used to block zero-day malware in email attachments and documents
- Describe how Safe Links protect users from malicious URLs embedded in email and documents

- Create and modify a Safe Attachments policy in the Security & Compliance Center
- Create a Safe Attachments policy by using Windows PowerShell
- Configure a Safe Attachments policy to take certain actions
- Understand how a transport rule can be used to disable the Safe Attachments functionality
- Describe the end-user experience when an email attachment is scanned and found to be malicious
- Create and modify a Safe Links policy in the Security & Compliance Center
- Create a Safe Links policy by using Windows PowerShell
- Understand how a transport rule can be used to disable the Safe Links functionality
- Describe the end-user experience when Safe Links identifies a link to a malicious website or file
- Describe how reports provide visibility into how EOP and ATP is protecting your organization
- Understand where to access reports generated by EOP and ATP
- Understand how to access detailed information from reports generated by EOP and ATP

Module 3: Microsoft 365 Threat Intelligence

In this module, 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.

Lessons

- Overview of Microsoft 365 Threat Intelligence
- Using the Security Dashboard
- Configuring Advanced Threat Analytics
- Implementing Your Cloud Application Security
- Lab : Implement Threat Intelligence
- Conduct a Spear Phishing attack using the Attack Simulator
- Conduct Password attacks using the Attack Simulator
- Prepare for Alert Policies
- Implement a Mailbox Permission Alert
- Implement a SharePoint Permission Alert
- Test the Default eDiscovery Alert

After completing this module, students will be able to:

- Understand how threat intelligence is powered by the Microsoft Intelligent Security Graph
- Describe how the threat dashboard can benefit C-level security officers
- Understand how Threat Explorer can be used to investigate threats and help to protect your tenant
- Describe how the Security Dashboard displays top risks, global trends, and protection quality
- Describe what Advanced Thread Analytics (ATA) is and what requirements are needed to deploy it
- Configure Advanced Threat Analytics
- Manage the ATA services
- Describe Cloud App Security
- Explain how to deploy Cloud App Security
- Control your Cloud Apps with Policies
- Troubleshoot Cloud App Security

Module 4: Introduction to Data Governance in Microsoft 365

This module examines 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).

Lessons

- Introduction to Archiving in Microsoft 365
- Introduction to Retention in Microsoft 365
- Introduction to Information Rights Management
- Introduction to Secure Multipurpose Internet Mail Extension
- Introduction to Office 365 Message Encryption
- Introduction to Data Loss Prevention
- Lab : Implement Message Encryption and IRM
- Configure Microsoft 365 Message Encryption
- Validate Information Rights Management

After completing this module, students will be able to:

- Understand Data Governance in Microsoft 365
- Describe the difference between In-Place Archive and Records Management
- Explain how data is archived in Exchange
- Recognize the benefits of In Place Records Management in SharePoint
- Explain the difference between Message Records Management (MRM) in Exchange and Retention in SCC.
- Understand how MRM works in Exchange
- List the types of retention tags that can be applied to mailboxes

- Know the different Microsoft 365 Encryption Options
- Understand how IRM can be used in Exchange
- Configure IRM protection for Exchange mails
- Explain how IRM can be used in SharePoint
- Apply IRM protection to SharePoint documents
- Tell the differences between IRM protection and AIP classification
- Describe the use of S/MIME
- Explain what digital signatures are
- Apply a digital signature to a message
- Understand how message encryption works
- Perform encryption on a message
- Accomplish decryption of a message
- Understand the co-operation of signing and encryption simultaneously
- Tell what triple-wrapped messages are
- Describe when you can use Office 365 Message Encryption
- Explain how Office 365 Message Encryption works
- Describe Data Loss Prevention (DLP)
- Understand what sensitive information and search patterns are that DLP is using
- Know what a DLP policy is and what it contains
- Recognize how actions and conditions work together for DLP
- Express how actions contain functions to send emails on matches
- Show policy tips to the users if a DLP rule applies
- Use policy templates to implement DLP policies for commonly used information
- Explain document finger
- Understand how to use DLP to protect documents in Windows Server FCI

Module 5: Archiving and Retention in Microsoft 365

This module delves 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.

Lessons

- In-Place Records Management in SharePoint
- Archiving and Retention in Exchange
- Retention Policies in the SCC
- Lab : Implement Archiving and Retention
- Initialize Compliance
- Configure Retention Tags and Policies

After completing this module, students will be able to:

- Understand the process of records management
- Create a file plan for your organization
- Describe two methods for converting active docs to records
- Describe the benefits of In-Place Records Management
- Configure of In-Place Records Management for your organization
- Enable and disable In-Place Archiving
- Create useful retention tags
- Create retention policies to group retention tags
- Assign retention policies to mailboxes
- Allocate permissions and scripts to export and import retention tags
- Export all retention policies and tags from an organization
- Import all retention policies and tags to an organization
- Explain how a retention policy works
- Create a retention policy
- Manage retention policy settings

Module 6: Implementing Data Governance in Microsoft 365 Intelligence

This module examines how to implement the key aspects of data governance, 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.

Lessons

- Evaluating Your Compliance Readiness
- Implementing Compliance Center Solutions
- Building Ethical Walls in Exchange Online
- Creating a Simple DLP Policy from a Built-in Template
- Creating a Custom DLP Policy

- Creating a DLP Policy to Protect Documents
- Working with Policy Tips
- Lab : Implement DLP Policies
- Manage DLP Policies
- Test MRM and DLP Policies

After completing this module, students will be able to:

- Describe the Microsoft 365 Compliance Center and how to access it
- Describe the purpose and function of Compliance score
- Explain the components of of how an organization's Compliance score is determined
- Explain how assessments are used to formulate compliance scores
- Explain how Microsoft 365 helps address Global Data Protection Regulation
- Describe insider risk management functionality in Microsoft 365
- Configure insider risk management policies
- Configure insider risk management policies
- Explain the communication compliance capabilities in Microsoft 365
- Describe what an ethical wall in Exchange is and how it works
- Explain how to create an ethical wall in Exchange
- Identify best practices for building and working with ethical walls in Exchange
- Understand the different built-in templates for a DLP policies
- Determine how to choose the correct locations for a DLP policy
- Configure the correct rules for protecting content
- Enable and review the DLP policy correctly
- Describe how to modify existing rules of DLP policies
- Explain how to add and modify custom conditions and action to a DLP rule
- Describe how to change user notifications and policy tips
- Configure the user override option to a DLP rule
- Explain how incident reports are sent by a DLP rule violation
- Describe how to work with managed properties for DLP policies
- Explain how SharePoint Online creates crawled properties from documents
- Describe how to create a managed property from a crawled property in SharePoint Online
- Explain how to create a DLP policy with rules that apply to managed properties via PowerShell
- Describe the user experience when a user creates an email or site containing sensitive information
- Explain the behavior in Office apps when a user enters sensitive information

Module 7: Managing Data Governance in Microsoft 365

This module focuses 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.

Lessons

- Managing Retention in Email
- Troubleshooting Data Governance
- Implementing Azure Information Protection
- Implementing Advanced Features of AIP
- Implementing Windows Information Protection
- Lab : Implement AIP and WIP
- Implement Azure Information Protection
- Implement Windows Information Protection

After completing this module, students will be able to:

- Determine when and how to use retention tags in mailboxes
- Assign retention policy to an email folder
- Add optional retention policies to email messages and folders
- Remove a retention policy from an email message
- Explain how the retention age of elements is calculated
- Repair retention policies that do not run as expected
- Understand how to systematically troubleshoot when a retention policy appears to fail
- Perform policy tests in test mode with policy tips
- Describe how to monitor DLP policies through message tracking
- Describe the required planning steps to use AIP in your company
- Configure and customize labels
- Create policies to publish labels
- Plan a Deployment of the Azure Information Protection client
- Configure the advance AIP service settings for Rights Management Services (RMS) templates
- Implement automatic and recommended labeling

- Activate the Super User feature for administrative tasks
- Create your tenant key for encryption
- Deploy the AIP scanner for on-premises labeling
- Plan RMS connector deployment to connect on-premises servers
- Describe WIP and what it is used for
- Plan a deployment of WIP policies
- Implement WIP policies with Intune and SCCM
- Implement WIP policies in Windows desktop apps

Module 8: Managing Search and Investigations

This module conclude this section on data governance by examining how to manage search and investigation, including searching for content in the Security and Compliance Center, auditing log investigations, and managing advanced eDiscovery.

Lessons

- Searching for Content in the Security and Compliance Center
- Auditing Log Investigations
- Managing Advanced eDiscovery
- Lab : Manage Search and Investigations
- Implement a Data Subject Request
- Investigate Your Microsoft 365 Data

After completing this module, students will be able to:

- Describe how to use content search
- Design your content search
- Configure search permission filtering
- Explain how to search for third-party data
- Describe when to use scripts for advanced searches
- Describe what the audit log is and the permissions that are necessary to search the Office 365 audit
- Configure Audit Policies
- Enter criteria for searching the audit log
- View, sort, and filter search results
- Export search results to a CSV file
- Search the unified audit log by using Windows PowerShell
- Describe Advanced eDiscovery
- Configure permissions for users in Advanced eDiscovery
- Create Cases in Advanced eDiscovery
- Search and prepare data for Advanced eDiscovery

Module 9: Planning for Device Management

This module provides 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 Microsoft Intune, and you will be introduced to the Microsoft Store for Business and Mobile Application Management.

Lessons

- Introduction to Co-management
- Preparing Your Windows 10 Devices for Co-management
- Transitioning from Configuration Manager to Intune
- Introduction to Microsoft Store for Business
- Planning for Mobile Application Management
- Lab : Implement the Microsoft Store for Business
- Configure the Microsoft Store for Business
- Manage the Microsoft Store for Business

After completing this module, students will be able to:

- Describe the benefits of Co-management
- Plan your organization's Co-management Strategy
- Describe the main features of Configuration Manager
- Describe how Azure Active Directory enables co-management
- Identify the prerequisites for using Co-management
- Configure Configuration Manager for Co-management
- Enroll Windows 10 Devices to Intune
- Modify your co-management settings
- Transfer workloads to Intune
- Monitor your co-management solution
- Check compliance for co-managed devices
- Describe the feature and benefits of the Microsoft Store for Business
- Configure the Microsoft Store for Business

- Manage settings for the Microsoft Store for Business

Module 10: Planning Your Windows 10 Deployment Strategy

This module focuses on planning your Windows 10 deployment strategy, including how to implement Windows Autopilot and Windows Analytics, and planning your Windows 10 subscription activation service.,

Lessons

- Windows 10 Deployment Scenarios
- Implementing and Managing Windows Autopilot
- Planning Your Windows 10 Subscription Activation Strategy
- Resolving Windows 10 Upgrade Errors
- Introduction to Windows Analytics

After completing this module, students will be able to:

- Plan for Windows as a Service
- Plan a Modern Deployment
- Plan a Dynamic Deployment
- Plan a Traditional Deployment
- Describe Windows Autopilot requirements
- Configure Autopilot
- Create and Assign an Autopilot profile
- Deploy and validate Autopilot
- Describe Autopilot Self-deployments, White Glove deployments, and User-drive deployments
- Deploy BitLocker Encryption for Autopiloted Devices
- Understand Windows 10 Enterprise E3 in CSP
- Configure VDA for Subscription Activation
- Deploy Windows 10 Enterprise licenses
- Describe common fixes for Windows 10 upgrade errors
- Use SetupDiag
- Troubleshooting upgrade errors
- Describe Windows error reporting
- Understand the upgrade error codes and resolution procedure
- Describe Windows Analytics
- Describe Device Health
- Describe Update Compliance
- Determine Upgrade Readiness

Module 11: Implementing Mobile Device Management

This module focuses on Mobile Device Management (MDM). You will learn how to deploy it, how to enroll devices to MDM, and how to manage device compliance.

Lessons

- Planning Mobile Device Management
- Deploying Mobile Device Management
- Enrolling Devices to MDM
- Managing Device Compliance
- Lab : Manage Devices with Intune
- Enable Device Management
- Configure Azure AD for Intune
- Create Intune Policies
- Enroll a Windows 10 Device
- Manage and Monitor a Device in Intune

After completing this module, students will be able to:

- Manage devices with MDM
- Compare MDM for Office 365 and Intune
- Understand policy settings for mobile devices
- Control Email and Document Access
- Activate Mobile Device Management Services
- Deploy Mobile Device Management
- Configure Domains for MDM
- Configure an APNs Certificate for iOS devices
- Manage Device Security Policies
- Define a Corporate Device Enrollment Policy
- Enroll devices to MDM
- Understand the Apple Device Enrollment Program
- Understand Enrollment Rules

- Configure a Device Enrollment Manager Role
- Describe Multi-factor Authentication considerations
- Plan for device compliance
- Configure conditional users and groups
- Create Conditional Access policies
- Monitor enrolled devices