MS-MS102T00: MICROSOFT 365 ADMINISTRATOR

DURATION	LEVEL	TECHNOLOGY	DELIVERY METHOD	TRAINING CREDITS
5 Days	Intermediate	Microsoft 365	Instructor-led	NA

INTRODUCTION

This course covers the following key elements of Microsoft 365 administration: Microsoft 365 tenant management, Microsoft 365 identity synchronization, and Microsoft 365 security and compliance. In Microsoft 365 tenant management, you learn how to configure your Microsoft 365 tenant, including your organizational profile, tenant subscription options, component services, user accounts and licenses, security groups, and administrative roles. You then transition to configuring Microsoft 365, with a primary focus on configuring Office client connectivity. Finally, you explore how to manage user-driven client installations of Microsoft 365 Apps for enterprise deployments. The course then transitions to an in-depth examination of Microsoft 365 identity synchronization, with a focus on Azure Active Directory Connect and Connect Cloud Sync. You learn how to plan for and implement each of these directory synchronization options, how to manage synchronized identities, and how to implement password management in Microsoft 365 using multifactor authentication and self-service password management. In Microsoft 365 security management, you begin examining the common types of threat vectors and data breaches facing organizations today. You then learn how Microsoft 365's security solutions address each of these threats. You are introduced to the Microsoft Secure Score, as well as to Azure Active Directory Identity Protection. You then learn how to manage the Microsoft 365 security services, including Exchange Online Protection, Safe Attachments, and Safe Links. Finally, you are introduced to the various reports that monitor an organization's security health. You then transition from security services to threat intelligence; specifically, using Microsoft 365 Defender, Microsoft Defender for Cloud Apps, and Microsoft Defender for Endpoint. Once you have this understanding of Microsoft 365's security suite, you then 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, Microsoft Purview message encryption, and data loss prevention (DLP). You then delve deeper into archiving and retention, paying particular attention to Microsoft Purview insider risk management, information barriers, and DLP policies. You then examine how to implement these compliance features by using data classification and sensitivity labels.

AUDIENCE PROFILE

This course is designed for persons aspiring to the Microsoft 365 Administrator role and have completed at least one of the Microsoft 365 role-based administrator certification paths.

PREREQUISITES

Before attending this course, delegates must have:

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

COURSE OBJECTIVES

After completing this course, students will be able to:

- Design, configure, and manage your Microsoft 365 tenant.
- Configure your company's organization profile, which is essential for setting up for your company's tenant.
- Maintain minimum subscription requirements for your company.
- Manage your services and add-ins by assigning more licenses, purchasing more storage, and so on.
- Create a checklist that enables you to confirm your Microsoft 365 tenant meets your business needs.
- Identify which user identity model is best suited for your organization.
- Create user accounts from both the Microsoft 365 admin center and Windows PowerShell.
- Manage user accounts and licenses in Microsoft 365.
- Recover deleted user accounts in Microsoft 365.
- Perform bulk user maintenance in Azure Active Directory.
- Describe the various types of groups available in Microsoft 365.
- Create and manage groups using the Microsoft 365 admin center and Windows PowerShell.
- Create and manage groups in Exchange Online and SharePoint Online.
- Identify the factors that must be considered when adding a custom domain to Microsoft 365.

- Plan the DNS zones used in a custom domain.
- Plan the DNS record requirements for a custom domain.
- Add a custom domain to your Microsoft 365 deployment.
- Describe how Outlook uses Autodiscover to connect an Outlook client to Exchange Online.
- Identify the DNS records needed for Outlook and other Office-related clients to automatically locate the services in Microsoft 365 using the Autodiscover process.
- Describe the connectivity protocols that enable Outlook to connect to Microsoft 365.
- Identify the tools that can help you troubleshoot connectivity issues in Microsoft 365 deployments.

COURSE CONTENT

Module 1: Configure your Microsoft 365 experience

This module examines each of the tasks that an organization must complete to successfully configure its Microsoft 365 experience.

Lessons

- Introduction
- Explore your Microsoft 365 cloud environment
- Configure your Microsoft 365 organizational profile
- Manage your tenant subscriptions in Microsoft 365
- Integrate Microsoft 365 with customer engagement apps
- Configure tenant-level sharing settings for SharePoint and OneDrive
- Configure tenant-level settings for Microsoft Teams
- Enable Unified Audit Logging in Microsoft 365
- Complete your tenant configuration in Microsoft 365
- Knowledge check
- Summary

After completing the course, delegates will be able to

- Configure your company's organization profile, which is essential for setting up for your company's tenant.
- Maintain minimum subscription requirements for your company.
- Manage your services and add-ins by assigning more licenses, purchasing more storage, and so on.
- Create a checklist that enables you to confirm your Microsoft Entra tenant meets your business needs.

Module 2: Manage users, licenses, guests, and contacts in Microsoft 365

This module provides instruction on how to create and manage user accounts, assign Microsoft 365 licenses to users, recover deleted user accounts, and create and manage guests and contacts.

Lessons

- Introduction
- Determine the user identity model for your organization
- Create user accounts in Microsoft 365
- Manage user account settings in Microsoft 365
- Manage user licenses in Microsoft 365
- Recover deleted user accounts in Microsoft 365
- Perform bulk user maintenance in Microsoft Entra ID
- Create and manage guest users using B2B collaboration
- Collaborate with guests in a SharePoint site
- Create and manage contacts
- Knowledge check
- Summary

After completing the course, delegates will be able to:

- Identify which user identity model is best suited for your organization.
- Create user accounts from both the Microsoft 365 admin centre and Windows PowerShell.
- Manage user accounts and licenses in Microsoft 365.
- Recover deleted user accounts in Microsoft 365.
- Perform bulk user maintenance in Microsoft Entra ID.
- Create and manage guests and collaborate with them on SharePoint sites.
- Create and manage contacts.

Module 3: Manage groups in Microsoft 365

This module provides instructions on how to create groups for distributing email to multiple users within Exchange Online. It also explains how to create groups to support collaboration in SharePoint Online.

Lessons

- Introduction
- Examine groups in Microsoft 365
- Create and manage groups in Microsoft 365
- Create dynamic groups using Microsoft Entra rule builder
- Create a Microsoft 365 group naming policy
- Create groups in Exchange Online and SharePoint Online
- Knowledge check
- Summary

After completing the course, delegates will be able to:

- Describe the various types of groups available in Microsoft 365.
- Create and manage groups using the Microsoft 365 admin center and Windows PowerShell.
- Create and manage groups in Exchange Online and SharePoint Online.

Module 4: Add a custom domain in Microsoft 365

This module provides instructions on how to add a custom domain to your Microsoft 365 deployment. It also examines the DNS requirements that are necessary to support a new domain.

Lessons

- Introduction
- Plan a custom domain for your Microsoft 365 deployment.
- Plan the DNS zones for a custom domain.
- Plan the DNS record requirements for a custom domain.
- Create a custom domain in Microsoft 365.
- Knowledge check.
- Summary

After completing the course, delegates will be able to

- Identify the factors that must be considered when adding a custom domain to Microsoft 365.
- Plan the DNS zones used in a custom domain.
- Plan the DNS record requirements for a custom domain.
- Add a custom domain to your Microsoft 365 deployment.

Module 5: Configure client connectivity to Microsoft 365

This module examines how clients connect to Microsoft 365. It also provides instruction on how to configure name resolution and Outlook clients, and how to troubleshoot client connectivity.

Lessons

- Introduction
- Examine how automatic client configuration works.
- Explore the DNS records required for client configuration.
- Configure Outlook clients.

- Troubleshoot client connectivity.
- Knowledge check.

After completing the course, delegates will be able to

- Describe how Outlook uses Autodiscover to connect an Outlook client to Exchange Online.
- Identify the DNS records needed for Outlook and other Office-related clients to automatically locate the services in Microsoft 365 using the Autodiscover process.
- Describe the connectivity protocols that enable Outlook to connect to Microsoft 365.
- Identify the tools that can help you troubleshoot connectivity issues in Microsoft 365 deployments.

Module 6: Manage permissions, roles, and role groups in Microsoft 365

This module examines the use of roles and role groups in the Microsoft 365 permission model, including role management, best practices when configuring admin roles, delegating roles, and elevating privileges.

Lessons

- Introduction
- Examine the use of roles in the Microsoft 365 permission model
- Manage roles across the Microsoft 365 ecosystem
- Explore administrator roles in Microsoft 365
- Examine best practices when configuring administrative roles
- Assign admin roles to users in Microsoft 365
- Delegate admin roles to partners
- Implement role groups in Microsoft 365
- Manage permissions using administrative units in Microsoft Entra ID
- Manage SharePoint permissions to prevent oversharing of data
- Elevate privileges using Microsoft Entra Privileged Identity Management
- Knowledge check
- Summary

After completing the course, delegates will be able to:

- Understand how roles are used in the Microsoft 365 ecosystem.
- Describe the Azure role-based access control permission model used in Microsoft 365.
- Identify the key tasks assigned to the common Microsoft 365 admin roles.
- Identify best practices when configuring admin roles.
- Delegate admin roles to partners.
- Implement role groups in Microsoft 365.
- Manage permissions using administrative units in Microsoft Entra ID.
- Manage permissions in SharePoint to prevent oversharing of data.
- Elevate privileges to access admin centres by using Microsoft Entra ID Privileged Identity Management.

Module 7: Manage tenant health and services in Microsoft 365

This module examines how to monitor your organization's transition to Microsoft 365 using Microsoft 365 tools. It also examines how to develop an incident response plan and request assistance from Microsoft.

Lessons

- Introduction
- Monitor the health of your Microsoft 365 services
- Monitor tenant health using Microsoft 365 Adoption Score
- Monitor tenant health using Microsoft 365 usage analytics
- Implement Microsoft 365 Network Connectivity Assessments and Insights
- Implement Microsoft 365 Backup (Preview)
- Develop an incident response plan
- Request assistance from Microsoft
- Knowledge check.
- Summary

After completing the course, delegates will be able to:

- Monitor your organization's Microsoft 365 service health in the Microsoft 365 admin centre.
- Implement Microsoft 365 network connectivity for assessments and insights.
- Implement Microsoft 365 Backup (Preview) for fast content backup and restoration.
- Develop an incident response plan to deal with incidents that can occur with your Microsoft 365 service.
- Request assistance from Microsoft to address technical, presales, billing, and subscription support issues.

Module 8: Deploy Microsoft 365 Apps for enterprise

This module examines how to implement the Microsoft 365 Apps for enterprise productivity suite in both user-driven and centralized deployments.

Lessons

- Introduction
- Explore Microsoft 365 Apps for enterprise functionality
- Complete a self-service installation of Microsoft 365 Apps for enterprise
- Deploy Microsoft 365 Apps for enterprise with Microsoft Configuration Manager
- Deploy Microsoft 365 Apps for enterprise from the cloud
- Deploy Microsoft 365 Apps for enterprise from a local source
- Manage updates to Microsoft 365 Apps for enterprise
- Explore the update channels for Microsoft 365 Apps for enterprise
- Manage your cloud apps using the Microsoft 365 Apps admin centre
- Knowledge check
- Summary

After completing the course, delegates will be able to:

- Describe the Microsoft 365 Apps for enterprise functionality.
- Plan a deployment strategy for Microsoft 365 Apps for enterprise.
- Complete a user-driven installation of Microsoft 365 Apps for enterprise.
- Deploy Microsoft 365 Apps for enterprise with Microsoft Endpoint Configuration Manager.
- Identify the mechanisms for managing centralized deployments of Microsoft 365 Apps for enterprise.
- Deploy Microsoft 365 Apps for enterprise with the Office Deployment Toolkit.
- Describe how to manage Microsoft 365 Apps for enterprise updates.
- Determine which update channel and application method applies for your organization.
- Add Microsoft 365 Apps for enterprise to Microsoft Intune.
- Deploy Microsoft 365 Apps for enterprise security baseline.

Module 9: Analyse your Microsoft 365 workplace data using Microsoft Viva Insights

This module examines the workplace analytical features of Microsoft Viva Insights, including how it works, and how it generates insights and improves collaboration within an organization.

Lessons

- Introduction
- Examine the analytical features of Microsoft Viva Insights
- Explore Personal insights
- Explore Team insights
- Explore Organizational insights
- Explore Advanced insights
- Knowledge check.
- Summary

After completing the course, delegates will be able to:

- Identify how Microsoft Viva Insights can help improve collaboration behaviours in your organization.
- Describe how the personal insights app analyses how you work.
- Describe how the Team insights app provides visibility into teamwork habits that might lead to stress and burnout.
- Describe how the Organization insights app enables managers to see how their work culture affects employee wellbeing.
- Describe how the Advanced insights app addresses critical questions about resiliency and work culture.

Module 10: Explore identity synchronization

This module examines identity synchronization and explores the authentication and provisioning options that can be used, and the inner workings of directory synchronization.

Lessons

- Introduction
- Examine identity models for Microsoft 365
- Examine authentication options for the hybrid identity model
- Explore directory synchronization
- Knowledge check
- Summary

After completing the course, delegates will be able to:

- Describe the Microsoft 365 authentication and provisioning options
- Explain the two identity models in Microsoft 365 - cloud-only identity and hybrid identity
- Explain the three authentication methods in the hybrid identity model - Password hash synchronization, Pass-through authentication, and federated authentication
- Describe how Microsoft 365 commonly uses directory synchronization

Module 11: Prepare for identity synchronization to Microsoft 365

This module examines all the planning aspects that must be considered when implementing directory synchronization between on-premises Active Directory and Microsoft Entra ID.

Lessons

- Introduction
- Plan your Microsoft Entra ID deployment
- Prepare for directory synchronization
- Choose your directory synchronization tool
- Plan for directory synchronization using Microsoft Entra Connect Sync
- Plan for directory synchronization using Microsoft Entra Cloud Sync
- Knowledge check
- Summary

After completing the course, delegates will be able to

- Identify the tasks necessary to configure your Azure Active Directory environment.
- Plan directory synchronization to synchronize your on-premises Active Directory objects to Azure AD.
- Identify the features of Microsoft Entra Connect Sync and Microsoft Entra Cloud Sync.
- Choose which directory synchronization best fits your environment and business needs.

Module 12: Implement directory synchronization tools

This module examines the Microsoft Entra Connect Sync and Microsoft Entra Cloud Sync installation requirements, the options for installing and configuring the tools, and how to monitor synchronization services using Microsoft Entra Connect Health.

Lessons

- Introduction
- Configure Microsoft Entra Connect Sync prerequisites
- Configure Microsoft Entra Connect Sync
- Monitor synchronization services using Microsoft Entra Connect Health
- Configure Microsoft Entra Cloud Sync prerequisites
- Configure Microsoft Entra Cloud Sync
- Knowledge check
- Summary

After completing the course, delegates will be able to:

- Configure Microsoft Entra Connect Sync and Microsoft Entra Cloud Sync prerequisites.
- Set up Microsoft Entra Connect Sync and Microsoft Entra Cloud Sync.
- Monitor synchronization services using Microsoft Entra Connect Health.

Module 13: Manage synchronized identities

This module examines how to manage user identities when you configure Microsoft Entra Connect Sync, how to manage users and groups in Microsoft 365 with Microsoft Entra Connect Sync, and how to maintain directory synchronization.

Lessons

- Introduction
- Manage users with directory synchronization
- Manage groups with directory synchronization
- Maintain directory synchronization using Microsoft Entra Connect Sync security groups
- Configure object filters for directory synchronization
- Explore Microsoft Identity Manager
- Troubleshoot directory synchronization
- Knowledge check
- Summary

After completing the course, delegates will be able to:

- Ensure users synchronize efficiently.
- Manage groups with directory synchronization.
- Use Microsoft Entra Connect Sync Security Groups to help maintain directory synchronization.
- Configure object filters for directory synchronization.
- Explain how Microsoft Identity Manager helps organizations manage and synchronize user identities across their organizations and hybrid environments.
- Troubleshoot directory synchronization using various troubleshooting tasks and tools.

Module 14: Examine threat vectors and data breaches

This module examines the types of threat vectors and their potential outcomes that organizations must deal with on a daily basis and how users can enable hackers to access targets by unwittingly executing malicious content.

Lessons

- Introduction
- Explore today's work and threat landscape

- Examine how phishing retrieves sensitive information
- Examine how spoofing deceives users and compromises data security
- Compare spam and malware
- Examine account breaches
- Examine elevation of privilege attacks
- Examine how data exfiltration moves data out of your tenant
- Examine how attackers delete data from your tenant
- Examine how data spillage exposes data outside your tenant
- Examine other types of attacks
- Knowledge check
- Summary

After completing the course, delegates will be able to

- Describe 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.
- Mitigate an account breach.
- Prevent an elevation of privilege attack.
- Prevent data exfiltration, data deletion, and data spillage.

Module 15: Explore the Zero Trust security model

This module examines the concepts and principles of the Zero Trust security model, as well as how Microsoft 365 supports it, and how your organization can implement it.

Lessons

- Introduction
- Examine the principles and components of the Zero Trust model
- Plan for a Zero Trust security model in your organization
- Examine Microsoft's strategy for Zero Trust networking
- Adopt a Zero Trust approach
- Knowledge check
- Summary

After completing the course, delegates will be able to:

- Describe the Zero Trust approach to security in Microsoft 365.
- Describe the principles and components of the Zero Trust security model.
- Describe the five steps to implementing a Zero Trust security model in your organization.
- Explain Microsoft's story and strategy around Zero Trust networking.

Module 16: Manage secure user access in Microsoft 365

This module examines the various features provided in the Microsoft 365 ecosystem for securing user access, such as Conditional Access policies, multifactor authentication, self-service password management, Smart Lockout policies, and security defaults.

Lessons

- Introduction
- Examine the identity and access tools used in Microsoft 365
- Manage user passwords
- Implement Conditional Access policies
- Enable pass-through authentication
- Implement multifactor authentication
- Enable passwordless sign-in with Microsoft Authenticator
- Explore self-service password management
- Explore Windows Hello for Business
- Implement Microsoft Entra Smart Lockout
- Explore Security Defaults in Microsoft Entra ID
- Investigate authentication issues using sign-in logs
- Knowledge check
- Summary

After completing the course, delegates will be able to:

- Manage user passwords.
- Create Conditional Access policies.
- Enable security defaults.
- Describe pass-through authentication.
- Enable multifactor authentication.
- Describe self-service password management.
- Implement Microsoft Entra Smart Lockout.

Module 17: Explore security solutions in Microsoft Defender XDR

This module introduces you to several features in Microsoft 365 that can help protect your organization against cyberthreats, detect when a user or computer is compromised, and monitor your organization for suspicious activities.

Lessons

- Introduction
- Enhance Exchange Online Protection with Microsoft Defender for Office 365
- Protect your organization's identities using Microsoft Defender for Identity
- Protect your enterprise network against advanced threats using Microsoft Defender for Endpoint
- Protect against cyber-attacks using Microsoft 365 Threat Intelligence
- Provide insight into suspicious activity using Microsoft Defender for Cloud App Security
- Review the security reports in Microsoft Defender XDR
- Knowledge check
- Summary

After completing the course, delegates will be able to:

- Identify the features of Microsoft Defender for Office 365 that enhance email security in a Microsoft 365 deployment
- Explain how Microsoft Defender for Identity identifies, detects, and investigates advanced threats, compromised identities, and malicious insider actions directed at your organization
- Explain how Microsoft Defender for Endpoint helps enterprise networks prevent, detect, investigate, and respond to advanced threats
- Describe how Microsoft 365 Threat Intelligence can be beneficial to your organization's security officers and administrators
- Describe how Microsoft Cloud App Security enhances visibility and control over your Microsoft 365 tenant through three core areas

Module 18: Examine Microsoft Secure Score

This module examines how Microsoft Secure Score helps organizations understand what they've done to reduce the risk to their data and shows them what they can do to further reduce that risk.

Lessons

- Introduction
- Explore Microsoft Secure Score
- Assess your security posture with Microsoft Secure Score
- Improve your secure score
- Track your Microsoft Secure Score history and meet your goals
- Knowledge check
- Summary

After completing the course, delegates will be able to:

- Describe the benefits of Secure Score and what kind of services can be analysed
- Describe how to collect data using the Secure Score API
- Describe how to use the tool to identify gaps between your

current state and where you would like to be regarding security
- Identify actions that increase your security by mitigating risks
- Explain where to look to determine the threats each action mitigates and the impact it has on users

Module 19: Examine Privileged Identity Management in Microsoft Entra ID

This module examines how Privileged Identity Management ensures users in your organization have just the right privileges to perform the tasks they need to accomplish.

Lessons
- Introduction
- Explore Privileged Identity Management in Microsoft Entra ID
- Configure Privileged Identity Management
- Audit Privileged Identity Management
- Knowledge check
- Summary

After completing the course, delegates will be able to:
- Describe how Privileged Identity Management enables you to manage, control, and monitor access to important resources in your organization
- Configure Privileged Identity Management for use in your organization
- Understand how PIM audit history enables you to see all the user assignments and activations within a given time period for all privileged roles.

Module 20: Examine Microsoft Entra ID Protection

This module examines how Azure Identity Protection provides organizations with the same protection systems used by Microsoft to secure identities.

Lessons
- Introduction
- Explore Microsoft Entra ID Protection
- Enable the default protection policies in Microsoft Entra ID Protection
- Explore the vulnerabilities and risk events detected by Microsoft Entra ID Protection
- Plan your identity investigation
- Knowledge check
- Summary

After completing the course, delegates will be able to:
- Describe Azure Identity Protection (AIP) and what kind of identities can be protected
- Enable the three default protection policies in AIP
- Identify the vulnerabilities and risk events detected by AIP
- Plan your investigation in protecting cloud-based identities
- Plan how to protect your Azure Active Directory environment from security breaches

Module 21: Examine email protection in Microsoft 365

This module examines how Exchange Online Protection (EOP) protects organizations from phishing and spoofing. It also explores how EOP blocks spam, bulk email, and malware before they arrive in users' mailboxes.

Lessons
- Introduction
- Examine the anti-malware pipeline
- Detect messages with spam or malware using Zero-hour auto-purge
- Explore anti-spoofing protection provided by Exchange Online Protection
- Explore other anti-spoofing protection
- Examine outbound spam filtering
- Knowledge check
- Summary

After completing the course, delegates will be able to:
- Describe how Exchange Online Protection analyses email to provide anti-malware pipeline protection.
- List several mechanisms used by Exchange Online Protection to filter spam and malware.
- Describe other solutions administrators might implement to provide extra protection against phishing and spoofing.
- Understand how EOP protects against outbound spam.

Module 22: Enhance your email protection using Microsoft Defender for Office 365

This module examines how Microsoft Defender for Office 365 extends EOP protection through various tools, including Safe Attachments, Safe Links, spoofed intelligence, spam filtering policies, and the Tenant Allow/Block List.

Lessons
- Introduction
- Climb the security ladder from EOP to Microsoft Defender for Office 365
- Expand EOP protections by using Safe Attachments and Safe Links
- Manage spoofed intelligence
- Configure outbound spam filtering policies
- Mange email access in Microsoft 365
- Submit messages, URLs, files, and attachments to Microsoft for analysis
- Knowledge check
- Summary

After completing the course, delegates will be able to:
- Describe how the Safe Attachments feature in Microsoft Defender for Office 365 blocks zero-day malware in email attachments and documents.
- Describe how the Safe Links feature in Microsoft Defender for Office 365 protects users from malicious URLs embedded in email and documents that point to malicious websites.
- Create outbound spam filtering policies.
- Block and unblock users from sending emails through Microsoft Defender for Office 365.
- Submit messages, URLs, files, and attachments to Microsoft for analysis.

Module 23: Manage Safe Attachments

This module examines how to manage Safe Attachments in your Microsoft 365 tenant by creating and configuring policies and using transport rules to disable a policy from taking effect in certain scenarios.

Lessons
- Introduction
- Protect users from malicious attachments by using Safe Attachments
- Create Safe Attachment policies using Microsoft Defender for Office 365
- Create Safe Attachments policies using PowerShell
- Modify an existing Safe Attachments policy
- Create a transport rule to bypass a Safe Attachments policy
- Examine the end-user experience with Safe Attachments
- Knowledge check
- Summary

After completing the course, delegates will be able to:
- Create and modify a Safe Attachments policy using Microsoft Defender XDR
- Create a Safe Attachments policy by using PowerShell
- Configure a Safe Attachments policy

- Describe how a transport rule can disable a Safe Attachments policy
- Describe the end-user experience when an email attachment is scanned and found to be malicious

Module 24: Manage Safe Links

This module examines how to manage Safe Links in your tenant by creating and configuring policies and using transport rules to disable a policy from taking effect in certain scenarios.

Lessons

- Introduction
- Protect users from malicious URLs by using Safe Links
- Create Safe Links policies using Microsoft Defender XDR
- Create Safe Links policies using PowerShell
- Modify an existing Safe Links policy
- Create a transport rule to bypass a Safe Links policy
- Examine the end-user experience with Safe Links
- Knowledge check
- Summary

After completing the course, delegates will be able to:

- Create and modify a Safe Links policy using Microsoft Defender XDR
- Create a Safe Links policy using PowerShell
- Configure a Safe Links policy
- Describe how a transport rule can disable a Safe Links policy
- Describe the end-user experience when Safe Links identifies a link to a malicious website embedded in email and a link to a malicious file hosted on a website

Module 25: Explore threat intelligence in Microsoft Defender XDR

This module examines how Microsoft 365 Threat Intelligence provides admins with evidence-based knowledge and actionable advice that can be used to make informed decisions about protecting and responding to cyber-attacks against their tenants.

Lessons

- Introduction
- Explore Microsoft Intelligent Security Graph
- Explore alert policies in Microsoft 365
- Run automated investigations and responses
- Explore threat hunting with Microsoft Threat Protection
- Explore advanced threat hunting in Microsoft Defender XDR
- Explore threat analytics in Microsoft 365
- Identify threat issues using Microsoft Defender reports
- Knowledge check
- Summary

After completing the course, delegates will be able to:

- Describe how threat intelligence in Microsoft 365 is powered by the Microsoft Intelligent Security Graph.
- Create alerts that can identify malicious or suspicious events.
- Understand how the automated investigation and response process works in Microsoft Defender XDR.
- Describe how threat hunting enables security operators to identify cybersecurity threats.
- Describe how Advanced hunting in Microsoft Defender XDR proactively inspects events in your network to locate threat indicators and entities.

Module 26: Implement app protection by using Microsoft Defender for Cloud Apps

This module examines how to implement Microsoft Defender for Cloud Apps, which identifies and combats cyber threats across all your Microsoft and third-party cloud services.

Lessons

- Introduction
- Explore Microsoft Defender Cloud Apps
- Deploy Microsoft Defender for Cloud Apps
- Configure file policies in Microsoft Defender for Cloud Apps
- Manage and respond to alerts in Microsoft Defender for Cloud Apps
- Configure Cloud Discovery in Microsoft Defender for Cloud Apps
- Troubleshoot Cloud Discovery in Microsoft Defender for Cloud Apps
- Knowledge check
- Summary

After completing the course, delegates will be able to:

- Describe how Microsoft Defender for Cloud Apps provides improved visibility into network cloud activity and increases the protection of critical data across cloud applications.
- Explain how to deploy Microsoft Defender for Cloud Apps.
- Control your cloud apps with file policies.
- Manage and respond to alerts generated by those policies.
- Configure and troubleshoot Cloud Discovery.

Module 27: Implement endpoint protection by using Microsoft Defender for Endpoint

This module examines how Microsoft Defender for Endpoint helps enterprise networks prevent, detect, investigate, and respond to advanced threats by using endpoint behavioural sensors, cloud security analytics, and threat intelligence.

Lessons

- Introduction
- Explore Microsoft Defender for Endpoint
- Configure Microsoft Defender for Endpoint in Microsoft Intune
- Onboard devices in Microsoft Defender for Endpoint
- Manage endpoint vulnerabilities with Microsoft Defender Vulnerability Management
- Manage device discovery and vulnerability assessment
- Reduce your threat and vulnerability exposure
- Knowledge check
- Summary

After completing the course, delegates will be able to:

- Describe how Microsoft Defender for Endpoint helps enterprise networks prevent, detect, investigate, and respond to advanced threats.
- Onboard supported devices to Microsoft Defender for Endpoint.
- Implement the Threat and Vulnerability Management module to effectively identify, assess, and remediate endpoint weaknesses.
- Configure device discovery to help find unmanaged devices connected to your corporate network.
- Lower your organization's threat and vulnerability exposure by remediating issues based on prioritized security recommendations.

Module 28: Implement threat protection by using Microsoft Defender for Office 365

This module examines the Microsoft Defender for Office 365 protection stack and its corresponding threat intelligence features, including Threat Explorer, Threat Trackers, and Attack simulation training.

Lessons

- Introduction

- Explore the Microsoft Defender for Office 365 protection stack
- Examine the security policies and rules used in Microsoft Defender for Office 365
- Investigate security attacks by using Threat Explorer
- Identify cybersecurity issues by using Threat Trackers
- Prepare for attacks with Attack simulation training
- Knowledge check
- Summary

After completing the course, delegates will be able to:

- Describe the protection stack provided by Microsoft Defender for Office 365.
- Understand how Threat Explorer can be used to investigate threats and help to protect your tenant.
- Describe the Threat Tracker widgets and views that provide you with intelligence on different cybersecurity issues that might affect your company.
- Run realistic attack scenarios using Attack Simulator to help identify vulnerable users before a real attack impacts your organization.

Module 29: Examine data governance solutions in Microsoft Purview

This module introduces Microsoft Purview, which is designed to meet the challenges of today's decentralized, data-rich workplace by providing a comprehensive set of solutions that help organizations govern, protect, and manage their entire data estate.

Lessons

- Introduction
- Explore data governance and compliance in Microsoft Purview
- Protect sensitive data with Microsoft Purview Information Protection
- Govern organizational data using Microsoft Purview Data Lifecycle Management
- Minimize internal risks with Microsoft Purview Insider Risk Management
- Explore Microsoft Purview eDiscovery solutions
- Knowledge check
- Summary

After completing the course, delegates will be able to:

- Protect sensitive data with Microsoft Purview Information Protection.
- Govern organizational data using Microsoft Purview Data Lifecycle Management.
- Minimize internal risks with Microsoft Purview Insider Risk Management.
- Explain the Microsoft Purview eDiscovery solutions.

Module 30: Explore data management practices in Microsoft 365

This module examines how Microsoft 365 supports data governance by enabling organizations to archive content by using archive mailboxes and manage their high-value content for legal, business, or regulatory obligations by implementing records management.

Lessons

- Introduction
- Explore archive mailboxes in Microsoft 365
- Enable archive mailboxes in Microsoft 365
- Restore deleted data in Exchange Online
- Restore deleted data in SharePoint Online
- Knowledge check
- Summary

After completing the course, delegates will be able to:

- Enable and disable an archive mailbox in the Microsoft Purview compliance portal and through Windows PowerShell.
- Run diagnostic tests on an archive mailbox.
- Restore deleted data in Exchange Online and SharePoint Online.

Module 31: Explore retention in Microsoft 365

This module examines how data can be retained and ultimately removed in Microsoft 365 by using data retention policies and data retention labels in retention policies.

Lessons

- Introduction
- Explore retention by using retention policies and retention labels
- Compare capabilities in retention policies and retention labels
- Define the scope of a retention policy
- Examine the principles of retention
- Implement retention using retention policies, retention labels, and eDiscovery holds
- Restrict retention changes by using Preservation Lock
- Knowledge check
- Summary

After completing the course, delegates will be able to:

- Explain how a retention policies and retention labels work.
- Identify the capabilities of both retention policies and retention labels.
- Select the appropriate scope for a policy depending on business requirements.
- Explain the principles of retention.
- Identify the differences between retention settings and eDiscovery holds.
- Restrict retention changes by using preservation lock.

Module 32: Explore compliance in Microsoft 365

This module explores the tools Microsoft 365 provides to help ensure an organization's regulatory compliance, including the Microsoft Purview compliance portal, Compliance Manager, and the Microsoft compliance score.

Lessons

- Introduction
- Plan for security and compliance in Microsoft 365
- Plan your beginning compliance tasks in Microsoft Purview
- Manage your compliance requirements with Compliance Manager
- Examine the Compliance Manager dashboard
- Analyse the Microsoft Compliance score
- Knowledge check
- Summary

After completing the course, delegates will be able to:

- Describe how Microsoft 365 helps organizations manage risks, protect data, and remain compliant with regulations and standards.
- Plan your beginning compliance tasks in Microsoft Purview.
- Manage your compliance requirements with the Compliance Manager.
- Manage compliance posture and improvement actions using the Compliance Manager dashboard.
- Explain how an organization's compliance score is determined.

Module 33: Implement Microsoft Purview Insider Risk Management

This module examines how Microsoft Purview Insider Risk Management helps organizations minimize internal risks by enabling them to detect, investigate, and act on malicious and inadvertent activities.

Lessons

- Introduction

- Explore insider risk management
- Plan for insider risk management
- Explore insider risk management policies
- Create insider risk management policies
- Investigate insider risk management activities and alerts
- Explore insider risk management cases
- Knowledge check
- Summary

After completing the course, delegates will be able to:

- Describe insider risk management functionality in Microsoft 365.
- Develop a plan to implement the Microsoft Purview Insider Risk Management solution.
- Create insider risk management policies.
- Manage insider risk management alerts and cases.

Module 34: Implement Microsoft Purview Information Barriers

This module examines how Microsoft Purview uses information barriers to restrict communication and collaboration in Microsoft Teams, SharePoint Online, and OneDrive for Business.

Lessons

- Introduction
- Explore Microsoft Purview Information Barriers
- Configure information barriers in Microsoft Purview
- Examine information barriers in Microsoft Teams
- Examine information barriers in OneDrive
- Examine information barriers in SharePoint
- Knowledge check
- Summary

After completing the course, delegates will be able to:

- Describe how information barriers can restrict or allow communication and collaboration among specific groups of users.
- Describe the components of an information barrier and how to enable information barriers.
- Understand how information barriers help organizations determine which users to add or remove from a Microsoft Team, OneDrive account, and SharePoint site.
- Describe how information barriers prevent users or groups from communicating and collaborating in Microsoft Teams, OneDrive, and SharePoint.

Module 35: Explore Microsoft Purview Data Loss Prevention

This module examines the data loss prevention features in Microsoft 365 that help organizations identify, monitor, report, and protect sensitive data through deep content analysis while helping users understand and manage data risks.

Lessons

- Introduction
- Examine data loss prevention for workloads
- Explore Endpoint data loss prevention
- Examine DLP policies
- Explore adaptive protection in Data Loss Prevention (Preview)
- View DLP policy results
- Knowledge check
- Summary

After completing the course, delegates will be able to:

- Describe how Data Loss Prevention (DLP) is managed in Microsoft 365.
- Understand how DLP in Microsoft 365 uses sensitive information types and search patterns.
- Describe how Microsoft Endpoint DLP extends the DLP activity monitoring and protection capabilities to devices.
- Describe what a DLP policy is and what it contains.
- Understand how adaptive protection integrates Insider Risk Management with DLP.
- View DLP policy results using both queries and reports.

Module 36: Implement Microsoft Purview Data Loss Prevention

This module examines how organizations can use Microsoft Purview Data Loss Prevention to help protect sensitive data and define the protective actions that organizations can take when a DLP rule is violated.

Lessons

- Introduction
- Plan to implement Microsoft Purview Data Loss Protection
- Implement Microsoft Purview's default DLP policies
- Design a custom DLP policy
- Create a custom DLP policy from a template
- Configure email notifications for DLP policies
- Configure policy tips for DLP policies
- Knowledge check
- Summary

After completing the course, delegates will be able to:

- Create a data loss prevention implementation plan.
- Implement Microsoft 365's default DLP policy.
- Create a custom DLP policy from a DLP template and from scratch.
- Create email notifications and policy tips for users when a DLP rule applies.
- Create policy tips for users when a DLP rule applies
- Configure email notifications for DLP policies

Module 37: Implement data classification of sensitive information

This module introduces you to data classification in Microsoft 365, including how to create and train classifiers, view sensitive data using Content explorer and Activity explorer, and implement Document Fingerprinting.

Lessons

- Introduction
- Explore data classification
- Implement data classification in Microsoft 365
- Explore trainable classifiers
- Create and retrain a trainable classifier
- View sensitive data using Content explorer and Activity explorer
- Detect sensitive information documents using Document Fingerprinting
- Knowledge check
- Summary

After completing the course, delegates will be able to:

- Explain the benefits and pain points of creating a data classification framework.
- Identify how data classification of sensitive items is handled in Microsoft 365.
- Understand how Microsoft 365 uses trainable classifiers to protect sensitive data.
- Create and then retrain custom trainable classifiers.
- Analyse the results of your data classification efforts in Content explorer and Activity explorer.
- Implement Document Fingerprinting to protect sensitive information being sent through Exchange Online.

Module 38: Explore sensitivity labels

This module examines how sensitivity labels from the Microsoft Information Protection solution let you classify and protect your organization's data, while making sure that user productivity and collaboration isn't hindered.

Lessons

- Introduction

- Manage data protection using sensitivity labels
- Explore what sensitivity labels can do
- Determine a sensitivity label's scope
- Apply sensitivity labels automatically
- Explore sensitivity label policies
- Knowledge check
- Summary

After completing the course, delegates will be able to:

- Describe how sensitivity labels let you classify and protect your organization's data
- Identify the common reasons why organizations use sensitivity labels
- Explain what a sensitivity label is and what they can do for an organization
- Configure a sensitivity label's scope
- Explain why the order of sensitivity labels in your admin center is important
- Describe what label policies can do.

Module 39: Implement sensitivity labels

This module examines the process for implementing sensitivity labels, including applying proper administrative permissions, determining a deployment strategy, creating, configuring, and publishing labels, and removing and deleting labels.

Lessons

- Introduction
- Plan your deployment strategy for sensitivity labels
- Enable sensitivity labels for files in SharePoint and OneDrive
- Examine the requirements to create a sensitivity label
- Create sensitivity labels
- Publish sensitivity labels
- Remove and delete sensitivity labels
- Module assessment
- Summary

After completing the course, delegates will be able to:

- Create a deployment strategy for implementing sensitivity labels that satisfies your organization's requirements.
- Enable sensitivity labels in SharePoint Online and OneDrive so they can use encrypted files.
- Create and configure sensitivity labels.
- Publish sensitivity labels by creating a label policy.
- Identify the differences between removing and deleting sensitivity labels.

ASSOCIATED CERTIFICATIONS & EXAM

This course will prepare delegates to write the Microsoft MS-102: Microsoft 365 Administrator exam.