Microsoft 365 Administrator (MS-102)

Duration: 5 Days

COURSE OUTLINE

Module 1: Implement and manage a Microsoft 365 tenant

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

Learning objectives

By the end of this module, you should 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 365 tenant meets your business needs.

Module 2: Manage users, licenses, and mail 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 mail contacts.

Learning objectives

By the end of this module, you should be able to:

- Identify which user identity model 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.
- Create and manage mail contacts from both the new Exchange admin center and Exchange Online PowerShell.

Module 3: Manage groups in Microsoft 365

This module provides instruction 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.

Learning objectives

By the end of this module, you should 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 instruction 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.

Learning objectives

By the end of this module, you should 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.

Learning objectives

By the end of this module, you should 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: Configure administrative roles in Microsoft 365

This module examines the key functionality that's available in the more commonly used Microsoft 365 admin roles. It also provides instruction on how to configure these roles.

Learning objectives

By the end of this module, you should be able to:

- Describe the Azure RBAC permission model used in Microsoft 365.
- Describe the most common Microsoft 365 admin roles.
- Identify the key tasks assigned to the common Microsoft 365 admin roles.
- Delegate admin roles to partners.
- Manage permissions using administrative units in Azure Active Directory.
- Elevate privileges to access admin centers by using Azure AD 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.

Learning objectives

By the end of this module, you should be able to:

- Monitor your organization's Microsoft 365 service health in the Microsoft 365 admin center.
- Develop an incident response plan to deal with incidents that may occur with your Microsoft 365 service.
- Request assistance from Microsoft to address technical, pre-sales, 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.

Learning objectives

By the end of this module, you should be able to:

- Describe the Microsoft 365 Apps for enterprise functionality.
- Configure the Readiness Toolkit.

- 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.

Module 9: Analyze 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.

Learning objectives

By the end of this module, you should be able to:

- Identify how Microsoft Viva Insights can help improve collaboration behaviors in your organization.
- Describe how the Personal insights app analyzes how you work.
- Describe how the Team insights app provides visibility into team work 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: 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 365.

Learning objectives

By the end of this module, you should 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 Azure AD Connect sync and Azure AD Connect Cloud Sync.
- Choose which directory synchronization best fits your environment and business needs.

Module 11: Implement directory synchronization tools

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

Learning objectives

By the end of this module, you should be able to:

- Configure Azure AD Connect and Azure AD Connect Cloud Sync prerequisites
- Set up Azure AD Connect and Azure AD Connect Cloud Sync
- Monitor synchronization services using Azure AD Connect Health

Module 12: Manage synchronized identities

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

Learning objectives

By the end of this module, you should be able to:

- Ensure users synchronize efficiently
- Manage groups with directory synchronization
- Use Azure AD 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 13: Manage secure user access in Microsoft 365

This module examines various password-related tasks for users and administrators, including.

- creating and configuring password policies
- configuring self-service password management
- configuring multifactor authentication
- implementing conditional access policies

Learning objectives

By the end of this module, you should be able to:

- Manage user passwords
- Describe pass-through authentication
- Enable multifactor authentication
- Describe self-service password management
- Implement Azure AD Smart Lockout

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

Learning objectives

By the end of this module, you should 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.

Learning objectives

By the end of this module, you should 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: Explore security solutions in Microsoft 365 Defender

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

Learning objectives

By the end of this module, you should 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 17: 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 show them what they can do to further reduce that risk.

Learning objectives

By the end of this module, you should be able to:

- Describe the benefits of Secure Score and what kind of services can be analyzed
- 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 18: Examine Privileged Identity Management

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.

Learning objectives

By the end of this module, you should 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
- Describe how Privileged Identity Management audit history enables you to see all the user assignments and activations within a given time period for all privileged roles
- Explain how Privileged Access Management provides granular access control over privileged admin tasks in Microsoft 365

Module 19: Examine Azure Identity Protection

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

Learning objectives

By the end of this module, you should 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 20: Examine Exchange Online Protection

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.

Learning objectives

By the end of this module, you should be able to:

- Describe how Exchange Online Protection analyzes email to provide anti-malware pipeline protection.
- List several mechanisms used by Exchange Online Protection to filter spam and malware.
- Describe other solutions administrators may implement to provide extra protection against phishing and spoofing.
- Understand how EOP provides protection against outbound spam

Module 21: Examine Microsoft Defender for Office 365

This module examines how Microsoft Defender for Office 365 extends EOP protection by filtering targeted attacks such as zero-day attacks in email attachments and Office documents, and time-of-click protection against malicious URLs.

Learning objectives

By the end of this module, you should 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.
- Unblock users who violated spam filtering policies so they can resume sending emails.

Module 22: 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.

Learning objectives

By the end of this module, you should be able to:

- Create and modify a Safe Attachments policy using Microsoft 365 Defender
- 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 23: 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.

Learning objectives

By the end of this module, you should be able to:

- Create and modify a Safe Links policy using Microsoft 365 Defender
- 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 23: Explore threat intelligence in Microsoft 365 Defender

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.

Learning objectives

By the end of this module, you should 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 Microsoft 365 Defender's Automated investigation and response process works.
- Describe how threat hunting enables security operators to identify cybersecurity threats.
- Describe how Advanced hunting in Microsoft 365 Defender proactively inspects events in your network to locate threat indicators and entities.

Module 24: 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 cyberthreats across all your Microsoft and third-party cloud services.

Learning objectives

By the end of this module, you should 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 25: 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 behavioral sensors, cloud security analytics, and threat intelligence.

Learning objectives

By the end of this module, you should 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 26: 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.

Learning objectives

By the end of this module, you should 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 27: 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.

Learning objectives

By the end of this module, you should 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 28: Explore archiving and records management 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.

Learning objectives

By the end of this module, you should 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.
- Learn how retention labels can be used to allow or block actions when documents and emails are declared records.
- Create your file plan for retention and deletion settings and actions.
- Determine when items should be marked as records by importing an existing plan (if you already have one) or create new retention labels. Restore deleted data in Exchange Online and SharePoint Online.

Module 29: Explore archiving and records management 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.

Learning objectives

By the end of this module, you should 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.
- Learn how retention labels can be used to allow or block actions when documents and emails are declared records.
- Create your file plan for retention and deletion settings and actions.
- Determine when items should be marked as records by importing an existing plan (if you already have one) or create new retention labels. Restore deleted data in Exchange Online and SharePoint Online.

Module 30: 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.

Learning objectives

By the end of this module, you should 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 31: Explore Microsoft Purview Message Encryption

This module introduces Microsoft Purview Message Encryption, an online service that's built on Microsoft Azure Rights Management and includes encryption, identity, and authorization policies to help organizations secure their email.

Learning objectives

By the end of this module, you should be able to:

- Describe the features of Microsoft Purview Message Encryption.
- Explain how Microsoft Purview Message Encryption works and how to set it up.
- Define mail flow rules that apply branding and encryption templates to encrypt email messages.
- Add organizational branding to encrypted email messages.
- Explain the extra capabilities provided by Microsoft Purview Advanced Message Encryption.

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.

Learning objectives

By the end of this module, you should 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 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.

Learning objectives

By the end of this module, you should 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.

Learning objectives

By the end of this module, you should 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.

Learning objectives

By the end of this module, you should 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.
- Describe what a DLP policy is and what it contains
- 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.

Learning objectives

By the end of this module, you should 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.

Learning objectives

By the end of this module, you should 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.
- Analyze 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.

Learning objectives

By the end of this module, you should 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.

Learning objectives

By the end of this module, you should be able to:

- Describe the overall process to create, configure, and publish sensitivity labels
- Identify the administrative permissions that must be assigned to compliance team members to implement sensitivity labels
- Develop a data classification framework that provides the foundation for your sensitivity labels
- Create and configure sensitivity labels
- Publish sensitivity labels by creating a label policy
- Identify the differences between removing and deleting sensitivity labels

WHO SHOULD ATTEND

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, students 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.