MS-102T00: Microsoft 365 Administrator Essentials

Course Duration: 5 Days

Class times: 9am-4pm

Course Level: Intermediate

Language: English

Mode of Training: Virtually Instructor-Led

Prerequisites

Job Role: Administrator

Related Exam: MS-102

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.

Course Outline

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.

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: 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.

Learning objectives

After completing this module, you should be able to:

- Identify how Microsoft Viva Insights can help improve collaboration behaviors in your organization.
- Discover the sources of data used in Microsoft Viva Insights.
- Explain the high-level insights available through Microsoft Viva Insights.
- Create custom analysis with Microsoft Viva Insights.
- Summarize tasks and considerations for setting up Microsoft Viva Insights and managing privacy.

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.

Learning objectives

By the end of this module, you should 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 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 12: 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, 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 13: Manage synchronized identities

This module examines how to manage user identities when Azure AD Connect is configured, 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
- Troubleshoot directory synchronization using various troubleshooting tasks and tools

Module 14: 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 entitlement packages
- 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
- Implement entitlement packages in Azure AD Identity Governance
- Implement conditional access policies
- Create and perform an access review

Module 15: 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 16: 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 17: 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 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 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 19: 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 Microsoft Identity Manager helps organizations manage the users, credentials, policies, and access within their organizations and hybrid environments
- Explain how Privileged Access Management provides granular access control over privileged admin tasks in Microsoft 365

Module 20: 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 21: 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 22: 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, 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 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.

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 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.

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 25: 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 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 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 27: Implement endpoint protection by using Microsoft Defender for Endpoint

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 28: Implement threat protection by using Microsoft Defender for Office 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.