MICROSOFT 365 ADMINISTRATOR ESSENTIALS (MS-102)

5 days

COURSE OVERVIEW

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.

TARGET AUDIENCE

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.

Job role: Administrator

COURSE 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.

Recommended prerequisites:

- M-MD102 - Managing Endpoints

COURSE CONTENT

1- Configure your Microsoft 365 experience

- Introduction
- Configure your Microsoft 365 experience
- Manage your tenant subscriptions in Microsoft 365
- Integrate Microsoft 365 with customer engagement apps
- Complete your tenant configuration in Microsoft 365
- Knowledge check
- Summary

2- Manage users, contacts, and licenses in Microsoft 365

- 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 Azure Active Directory
- Create and manage guest users
- Create and manage contacts
- Summary

3- Manage groups in Microsoft 365

- Introduction
- Examine groups in Microsoft 365
- Create and manage groups in Microsoft 365
- Create groups in Exchange Online and SharePoint Online
- Knowledge check
- Summary

4- Add a custom domain in Microsoft 365

- 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

5- Configure client connectivity to Microsoft 365

- Introduction
- Examine how automatic client configuration works
- Explore the DNS records required for client configuration
- Configure Outlook clients
- Troubleshoot client connectivity
- Knowledge check
- Summary

6- Configure administrative roles in Microsoft 365

- Introduction

- Explore the Microsoft 365 permission model
- Explore the Microsoft 365 admin roles
- Assign admin roles to users in Microsoft 365
- Delegate admin roles to partners
- Manage permissions using administrative units in Azure Active Directory
- Elevate privileges using Azure AD Privileged Identity Management
- Knowledge check
- Summary

7- Manage tenant health and services in Microsoft 365

- 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
- Develop an incident response plan
- Request assistance from Microsoft
- Knowledge check
- Summary

8- Deploy Microsoft 365 Apps for enterprise

- Introduction
- Explore Microsoft 365 Apps for enterprise functionality
- Explore your app compatibility by using the Readiness Toolkit
- Complete a self-service installation of Microsoft 365 Apps for enterprise
- Deploy Microsoft 365 Apps for enterprise with Microsoft Endpoint 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 center
- Knowledge check
- Summary

9- Analyze your Microsoft 365 workplace data using Microsoft Viva Insights

- Introduction
- Examine the analytical features of Microsoft Viva Insights
- Create custom analysis with Microsoft Viva Insights

- Configure Microsoft Viva Insights
- Examine Microsoft 365 data sources used in Microsoft Viva Insights
- Prepare organizational data in Microsoft Viva Insights
- Knowledge check
- Summary

10- Explore identity synchronization

- Introduction
- Examine authentication options in Microsoft 365
- Examine provisioning options in Microsoft 365
- Explore directory synchronization
- Explore Azure AD Connect
- Knowledge check
- Summary

11- Prepare for identity synchronization to Microsoft 365

- Introduction
- Plan your Azure Active Directory deployment
- Prepare for directory synchronization
- Choose your directory synchronization tool
- Plan for directory synchronization using Azure AD Connect
- Plan for directory synchronization using Azure AD Connect Cloud Sync
- Knowledge check
- Summary

12- Implement directory synchronization tools

- Introduction
- Configure Azure AD Connect prerequisites
- Configure Azure AD Connect
- Monitor synchronization services using Azure AD Connect Health
- Configure Azure AD Connect Cloud Sync prerequisites
- Configure Azure AD Connect Cloud Sync
- Knowledge check
- Summary

13- Manage synchronized identities

- Introduction
- Manage users with directory synchronization

- 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
- Knowledge check
- Summary

14- Manage secure user access in Microsoft 365

- Introduction
- Manage user passwords
- Enable pass-through authentication
- Enable multi-factor authentication
- Explore self-service password management
- Implement Azure AD Smart Lockout
- Implement entitlement packages in Azure AD Identity Governance
- Implement conditional access policies
- Create and run an access review
- Investigate authentication issues using sign-in logs
- Knowledge check
- Summary

15- Examine threat vectors and data breaches

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 how an account breach compromises a user account
- 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

16- Explore the Zero Trust security model

- 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

17- Explore security solutions in Microsoft 365 Defender

- Introduction
- Enhance your email security using Exchange Online Protection and 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 Cloud App Security
- Review the security reports in Microsoft 365 Defender
- Knowledge check
- Summary

18- Examine Microsoft Secure Score

- 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

19- Examine Privileged Identity Management

- Introduction
- Explore Privileged Identity Management in Azure AD
- Configure Privileged Identity Management
- Audit Privileged Identity Management
- Explore Microsoft Identity Manager
- Control privileged admin tasks using Privileged Access Management
- Knowledge check

- Summary

20- Examine Azure Identity Protection

- Introduction
- Explore Azure Identity Protection
- Enable the default protection policies in Azure Identity Protection
- Explore the vulnerabilities and risk events detected by Azure Identity Protection
- Plan your identity investigation
- Knowledge check
- Summary

21- Examine Exchange Online Protection

- 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

22- Examine Microsoft Defender for Office 365

- 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
- Unblock users from sending email
- Knowledge check
- Summary

23- Manage Safe Attachments

- 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

24- Manage Safe Links

- Introduction
- Protect users from malicious URLs by using Safe Links
- Create Safe Links policies using Microsoft 365 Defender
- 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

25- Explore threat intelligence in Microsoft 365 Defender

- 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 365 Defender
- Explore threat analytics in Microsoft 365
- Identify threat issues using Microsoft Defender reports
- Knowledge check
- Summary

26- Implement app protection by using Microsoft Defender for Cloud Apps

- 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

27- Implement endpoint protection by using Microsoft Defender for Endpoint

- 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

28- Implement threat protection by using Microsoft Defender for Office 365

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