MS-MS102T00: MICROSOFT 365 ADMINISTRATOR

DURATION	LEVEL	TECHNOLOGY	DELIVERY METHOD	CERTIFICATION
5 Days	Intermediate	Microsoft 365	Instructor-led	MS-102 Exam

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

There are no formal prerequisites but is designed for experienced Microsoft 365 administrators with hands-on tenant management experience, working knowledge of Entra ID, networking fundamentals, and PowerShell.

COURSE OBJECTIVES

After completing this course, students will be able to:

- Deploy and manage a Microsoft 365 tenant, including users, licenses, services, and admin roles.
- Implement and manage identity and access using Microsoft Entra ID.
- Configure client connectivity and manage Microsoft 365 Apps for enterprise.
- Secure the Microsoft 365 environment using Microsoft Defender XDR.
- Implement compliance, data protection, and governance using Microsoft Purview.
- Monitor tenant health, service availability, and operational performance.

COURSE CONTENT

Module 1: Configure your Microsoft 365 tenant

This learning path provides instruction on how to configure your Microsoft 365 tenant, including your organizational profile, tenant subscriptions, user accounts and licenses, groups, custom domains, and client connectivity.

Module 1.1: Configure your Microsoft 365 experience

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

Module 1.2: 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.

Module 1.3: 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.

Module 1.4: 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.

Module 1.5: 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.

Module 2: Manage your Microsoft 365 tenant

This learning path provides instruction on how to manage your Microsoft 365 tenant, including administrative roles, tenant health and services, Microsoft 365 Apps for enterprise, and workplace analytics using Microsoft Viva Insights.

Module 2.1: 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.

Module 2.2: 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.

Module 2.3: 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.

Module 2.4: 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.

Module 3: Implement identity synchronization

This learning path examines how organizations should plan for and implement identity synchronization in a hybrid Microsoft 365 deployment. You learn how to implement Microsoft Entra Connect Sync and Microsoft Entra Cloud Sync, and how to manage synchronized identities.

Module 3.1: 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.

Module 3.2: 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.

Module 3.3: 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.

Module 3.4: 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.

Module 4: Manage identity and access in Microsoft 365

This learning path examines the threat vectors and data breaches organizations face today in their cybersecurity landscape, and the wide range of security solutions that Microsoft 365 provides to combat those threats.

Module 4.1: 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.

Module 4.2: 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.

Module 4.3: 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.

Module 4.4: 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.

Module 4.5: 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.

Module 4.6: Examine Privileged Identity Management in Microsoft Entra ID

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

Module 4.7: Examine Microsoft Entra ID Protection

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

Module 5: Manage your security services in Microsoft Defender XDR

This learning path examines how to manage the Microsoft 365 security services, with a special focus on security reporting and managing the Safe Attachments and Safe Links features in Microsoft Defender for Office 365.

Module 5.1: 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.

Module 5.2: 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.

Module 5.3: 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.

Module 5.4: 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.

Module 6: Implement threat protection by using Microsoft Defender XDR

This learning path examines how to manage the Microsoft 365 threat intelligence features that provide organizations with insight and protection against the internal and external cyber-attacks that threaten their tenants.

Module 6.1: 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.

Module 6.2: 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.

Module 6.3: 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.

Module 6.4: 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.

Module 7: Explore data governance in Microsoft 365

This learning path introduces you to the data governance features of Microsoft 365, which serve regulatory compliance, can facilitate eDiscovery, and are part of a business strategy to protect the integrity of the data estate.

Module 7.1: 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.

Module 7.2: 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 restore deleted data in Exchange Online and SharePoint Online.

Module 7.3: 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.

Module 8: Implement compliance in Microsoft 365

This learning path provides instruction on implementing the Microsoft 365 data governance features, including how to calculate your compliance readiness, implement compliance solutions, and create information barriers, DLP policies, and policy tips.

Module 8.1: 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.

Module 8.2: 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.

Module 8.3: 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.

Module 8.4: 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.

Module 8.5: 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.

Module 9: Manage compliance in Microsoft 365

This learning path provides instruction on managing the Microsoft 365 data governance features, including how to implement retention in email, sensitivity labels, and Windows Information Protection, and how to troubleshoot data loss prevention issues.

Module 9.1: 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.

Module 9.2: 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.

Module 9.3: 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.

ASSOCIATED CERTIFICATIONS & EXAM

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