

KOENIG SOLUTIONS · COURSE OUTLINE

MS-102T00: Microsoft 365 Administrator

Learn to configure, secure and manage Microsoft 365 tenants, identities, security and compliance across the enterprise.

40

MODULES

164

TOPICS

104

HANDS-ON ACTIVITIES

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 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.

Who Should Attend

Microsoft 365 Administrators

Identity Administrators

Security Administrators

Compliance Administrators

Messaging Administrators

LEARNING OBJECTIVES

- Configure tenant settings, users, groups and custom domains
- Configure client connectivity and deploy Microsoft 365 Apps for enterprise
- Assign administrative roles and manage delegated permissions
- Plan and implement directory synchronization with Microsoft Entra Connect
- Manage synchronized identities and secure user access with MFA
- Analyse threat vectors and evaluate Microsoft Secure Score
- Implement Microsoft Defender solutions for email, endpoints and cloud apps
- Implement data governance, retention, DLP and sensitivity labels

COURSE SYLLABUS

40 Modules, 164 Topics

01

8 Labs

Configure Your Microsoft 365 Experience

TOPICS

Microsoft 365 subscription and tenant · Set up your organizational profile · Manage your services and add-ins · Finalize your tenant

02

Manage Users, Licenses, and Mail Contacts in Microsoft 365

TOPICS

Understanding user identities · Creating and managing user accounts · Managing user licenses · Recovering deleted user accounts · Create and manage guest users · Create and manage mail contacts

03**4 Labs**

Manage Groups in Microsoft 365

TOPICS

- Creating and managing groups
- Creating dynamic groups using Azure rule builder
- Creating a Microsoft 365 group naming policy
- Creating groups in Exchange Online and SharePoint Online

04**2 Labs**

Add a Custom Domain in Microsoft 365

TOPICS

- 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

05

Configure Client Connectivity to Microsoft 365

TOPICS

- Understand how automatic client configuration works
- Understand which DNS records are required for automatic client configuration
- Configure Outlook clients
- Troubleshoot client connectivity

06**4 Labs**

Configure Administrative Roles in Microsoft 365

TOPICS

- Microsoft 365 permission model
- Microsoft 365 admin roles and best practices
- Assign admin roles to users in Microsoft 365
- Delegate admin roles to partners
- Manage permissions using administrative units in Microsoft Entra ID
- Elevate privileges

07**4 Labs**

Manage Tenant Health and Services in Microsoft 365

TOPICS

- Monitor the health of your Microsoft 365 services

MONITOR TENANT HEALTH USING:

- Microsoft 365 Adoption Score
- Microsoft 365 usage analytics
- Develop an incident response plan
- Request assistance from Microsoft

08**4 Labs**

Deploy Microsoft 365 Apps for Enterprise

TOPICS

- Validate app readiness using the Readiness Toolkit
- Microsoft 365 Apps for enterprise deployment options
- Manage cloud apps and app updates using the Microsoft 365 Apps admin center
- Control how often their users get new features by specifying the update channel

09

Analyze Your Microsoft 365 Workplace Data Using Microsoft Viva Insights

TOPICS

- The analytical features of Microsoft Viva Insights
- Personal insights
- Team insights
- Organization insights
- Advanced insights

10

Explore Identity Synchronization

TOPICS

Microsoft 365 identity models · Microsoft 365 authentication options · Directory synchronization

11

Prepare for Identity Synchronization to Microsoft 365

TOPICS

Directory synchronization · Microsoft Entra Connect Sync · Microsoft Entra Cloud Sync

12**5 Labs**

Implement Directory Synchronization Tools

TOPICS

- 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

13**6 Labs**

Manage Synchronized Identities

TOPICS

- Manage users with directory synchronization
- Manage groups with directory synchronization
- Use Microsoft Entra Connect Sync security groups
- Microsoft Identity Manager
- Troubleshoot directory synchronization

14**3 Labs**

Manage Secure User Access in Microsoft 365

TOPICS

- Password policies and authentication
- Microsoft Entra Pass-Through Authentication (PTA) and Multifactor authentication (MFA)
- Password less sign-in with Microsoft Authenticator
- Self-service Password Management and Windows Hello for Business
- Microsoft Entra Smart Lockout and Conditional access policies
- Microsoft Entra Security Defaults

15

Examine Threat Vectors and Data Breaches

TOPICS

Compromise user accounts through email · Gain control over resources · Compromise data

16

Explore the Zero Trust Security Model

TOPICS

- Effectively adapts to the complexity of the modern environment
- Embraces the mobile workforce
- Protects people, devices, apps, and data wherever they are located

19

Explore Security Solutions in Microsoft Defender XDR

TOPICS

Microsoft Defender for Office 365 · Microsoft Defender for Identity · Microsoft Defender for Endpoint · Microsoft 365 Threat Intelligence · Microsoft Defender for Cloud App Security

17

Examine Microsoft Secure Score

TOPICS

- Benefits of using Microsoft Secure Score
- Assessing your organization's security posture with Microsoft Secure Score
- Improving your secure score
- Tracking your Microsoft Secure Score history and meeting your goals

18

16 Activities

Examine Privileged Identity Management

TOPICS

Configure PIM for use in your organization · Audit PIM roles

19

Examine Microsoft Entra ID Protection

TOPICS

- Most security breaches take place when attackers gain access to an environment by stealing a user's identity
- Microsoft Entra ID uses adaptive machine learning algorithms and heuristics to detect anomalies and suspicious incidents that indicate potentially compromised identities
- Using this data, Microsoft Entra ID Protection generates reports and alerts that enable organizations to evaluate the detected issues and take appropriate mitigation or remediation actions

20

Examine Email Protection in Microsoft 365

TOPICS

- EOP technologies that block spam, bulk email, and malware before mail arrives in users' mailboxes
- EOP protection against phishing, spoofing, and outbound spam filtering

21

Enhance Your Email Protection Using Microsoft Defender for Office 365

TOPICS

- Climb the security ladder from EOP to Microsoft Defender for Office 365
- Expand EOP using Safe Attachments and Safe Links
- Manage spoofed intelligence
- Outbound spam filtering policies
- Unblock users from sending email

22

Lab

Manage Safe Attachments

TOPICS

- Creating and modifying a Safe Attachments policy in the Microsoft Defender portal
- Creating a Safe Attachments policy by using Windows PowerShell
- Configuring a Safe Attachments policy
- Implementing a transport rule to bypass Safe Attachments scanning

23

2 Labs

Manage Safe Links

TOPICS

- Creating and modifying a Safe Links policy in the Microsoft Defender portal
- Creating a Safe Links policy by using Windows PowerShell
- Configuring a Safe Links policy to take certain actions
- Implementing a transport rule to disable the Safe Links functionality
- **Exercise 2:** Implement a Safe Links policy

24**11 Labs**

Explore Threat Intelligence in Microsoft Defender XDR

TOPICS

Microsoft Intelligent Security Graph · How Microsoft Defender XDR uses alerts · Automated investigation and response · Threat hunting · Threat analytics and reports

25

Implement App Protection by Using Microsoft Defender for Cloud Apps

TOPICS

- Microsoft Defender for Cloud Apps features
- Deploying Microsoft Defender for Cloud Apps
- Controlling your Cloud Apps with policies
- Configuring Cloud Discovery in Microsoft Defender for Cloud Apps
- Troubleshooting Microsoft Defender for Cloud Apps

26

Implement Endpoint Protection by Using Microsoft Defender for Endpoint

TOPICS

Vulnerability management · Attack surface reduction · Next generation protection · Endpoint detection and response · Auto investigation and remediation

27**12 Activities**

Implement Threat Protection by Using Microsoft Defender for Office 365

TOPICS

- Microsoft Defender for Office 365 protection stack
- Threat Explorer
- Threat Tracker widgets and views

28

Examine Data Governance Solutions in Microsoft Purview

TOPICS

Data governance and compliance · Microsoft Purview Information Protection · Microsoft Purview Data Lifecycle Management · Microsoft Purview Insider Risk Management · Microsoft Purview eDiscovery solutions

29

Explore Archiving and Records Management in Microsoft 365

TOPICS

- Archive mailboxes in Microsoft 365
- Microsoft Purview Records Management
- Restore deleted data in Exchange and SharePoint

30

7 Labs

Explore Retention in Microsoft 365

TOPICS

- Retention policies and retention labels
- Principles of retention
- How organizations use Preservation Lock to restrict users

31

3 Labs

Explore Microsoft Purview Message Encryption

TOPICS

- Microsoft Purview Message Encryption
- Mail flow rules to encrypt email messages
- Organizational branding on encrypted email messages
- Microsoft Purview Advanced Message Encryption

32

Explore Compliance in Microsoft 365

TOPICS

- Planning for security and compliance in Microsoft 365 and Microsoft Purview
- Managing compliance requirements using Compliance Manager
- Analyzing the Microsoft Compliance Score

33

Implement Microsoft Purview Insider Risk Management

TOPICS

Insider risk management planning · Insider risk management policies · Insider risk management activities and alerts · Insider risk management cases

34

Implement Microsoft Purview Information Barriers

TOPICS

How to configure information barriers · Information barriers in Microsoft Teams · Information barriers in OneDrive · Information barriers in SharePoint Online

35

Explore Microsoft Purview Data Loss Prevention

TOPICS

DLP fundamentals in Exchange and SharePoint · Endpoint data loss prevention · DLP policies · DLP reporting tools

36**5 Labs**

Implement Microsoft Purview Data Loss Prevention

TOPICS

- Create a DLP implementation plan
- Implement Microsoft Purview's default DLP policies
- Create a custom DLP policy
- Create policy tips for users when a DLP rule applies
- Configure email notifications for DLP policies

37

Implement Data Classification of Sensitive Information

TOPICS

Data classification in Microsoft 365 · Trainable classifiers · Viewing sensitive data · Document fingerprinting

38

Explore Sensitivity Labels

TOPICS

Insider risk management policies · Insider risk management activities and alerts · Insider risk management cases

39**7 Labs**

Implement Sensitivity Labels

TOPICS

Sensitivity label requirements · Developing a data classification framework · How to create and publish sensitivity labels · How to remove and delete sensitivity labels

Practise What You Learn

#	MODULE	ACTIVITY
01	Configure Your Microsoft 365 Experience	LABS ■ Initialize your Microsoft 365 tenant ■ Obtain your Microsoft 365 credentials ■ Set up the Adatum's organization profile ■ Create a custom theme for Adatum's pilot project team ■ Enable Information Rights Management for SharePoint Online ■ Turn on Audit Logging to enable Alert policies ■ Install Microsoft Graph PowerShell ■ Run a PowerShell script to create and publish a sensitivity label
03	Manage Groups in Microsoft 365	LABS ■ Exercise 2: Manage users and groups ■ Create a user account for Adatum's Enterprise Administrator ■ Create and manage groups ■ Recover groups using PowerShell
04	Add a Custom Domain in Microsoft 365	LABS ■ Exercise 3: Add a custom domain ■ Add a custom domain
06	Configure Administrative Roles in Microsoft 365	LABS ■ Manage administration delegation ■ Assign Delegated Administrators in the Microsoft 365 admin center ■ Manage Delegated Administrators with Windows PowerShell ■ Verify Delegated Administration
07	Manage Tenant Health and Services in Microsoft 365	LABS ■ Exercise 2: Monitor and troubleshoot Microsoft 365 ■ Troubleshoot Mail Flow in Microsoft 365 ■ Monitor service health and analyze reports ■ Submit a Help request to Microsoft Support
08	Deploy Microsoft 365 Apps for Enterprise	LABS ■ Install Microsoft 365 Apps for enterprise ■ Verify how licensing affects installing Microsoft 365 Apps for enterprise ■ Verify how the global Office download setting affects installing Microsoft 365 Apps for enterprise ■ Perform a User-Driven Installation of Microsoft 365 Apps for enterprise

#	MODULE	ACTIVITY
12	Implement Directory Synchronization Tools	LABS ■ Exercise 1: Prepare for identity synchronization ■ Configure your UPN suffix ■ Prepare problem user accounts ■ Run the IdFix tool and fix identified issues ■ Prepare for Directory Synchronization
13	Manage Synchronized Identities	LABS ■ Exercise 2: Implement identity synchronization ■ Install Microsoft Entra Connect Sync and initiate synchronization ■ Create group accounts to test synchronization ■ Change group membership to test synchronization ■ Force a manual synchronization ■ Validate the results of directory synchronization
14	Manage Secure User Access in Microsoft 365	LABS ■ Exercise 3: Manage secure user access ■ Deploy Microsoft Entra Pass-Through Authentication ■ Deploy Microsoft Entra Smart Lockout
18	Examine Privileged Identity Management	PRIVILEGED ACCESS MANAGEMENT LABS ■ Exercise 1: PIM Administrator approval ■ Configure the Global Admin role to require approval ■ Assign an eligible group to the Global Admin role ■ Submit a request for the Global Admin role ■ Approve the request for the Global Admin role ■ PIM Self-approval ■ Create an eligible group for the Helpdesk Admin role ■ Configure the Helpdesk Admin role for self-approval ■ Self-activate the Helpdesk Admin role ■ Verify a PIM notification was issued ■ PIM Teammate approval ■ Create a group for the Intune Admin role ■ Configure the Intune Admin role to require approval ■ Submit a request for the Intune Admin role ■ Approve the request for the Intune Admin role ■ Verify a PIM notification was issued
22	Manage Safe Attachments	Labs: Create a Safe Attachment policy and turn on Microsoft Defender for Office 365
23	Manage Safe Links	LABS ■ Create a Safe Links policy ■ Validate the Safe Links policy

#	MODULE	ACTIVITY
24	Explore Threat Intelligence in Microsoft Defender XDR	LABS
		■ Prepare for Alert Policies
		■ Assign RBAC permissions for alert notification testing
		■ Implement a Mailbox Permission Alert
		■ Create a Mailbox Permission Alert
		■ Test the Mailbox Permission Alert
		■ Implement a SharePoint Permission Alert
		■ Create a SharePoint Permission Alert
		■ Test the SharePoint Permission Alert
		■ Test the Default eDiscovery Alert
27	Implement Threat Protection by Using Microsoft Defender for Office 365	ATTACK SIMULATION TRAINING LABS
		■ Conduct a Spear Phishing attack using Attack Simulation training
		■ Enable Multifactor Authentication for the Global Admin
		■ Configure and launch a Spear Phishing attack
		■ Conduct a Drive-by URL attack using Attack Simulation training
		■ Configure and launch a Drive-by URL attack
		■ Validate alert notifications and simulated attacks
		■ Validate the Mailbox Permission alert
		■ Validate the SharePoint Permission alert
		■ Validate the default eDiscovery alert
30	Explore Retention in Microsoft 365	LABS
		■ Exercise 1 - Initialize Compliance
		■ Create a security group for compliance testing
		■ Configure Mobile Device Management for compliance testing
		■ Exercise 2 - Configure In-Place Archiving and Retention Policies
		■ Activate In-Place Archiving for a new user's mailbox
		■ Create an email retention policy for test users
		■ Create an email retention policy for all users
31	Explore Microsoft Purview Message Encryption	LABS
		■ Exercise 3: Create message encryption rules
		■ Create a mail flow encryption rule using the Exchange admin center
		■ Create a mail flow encryption rule using Windows PowerShell

#	MODULE	ACTIVITY
		LABS
36	Implement Microsoft Purview Data Loss Prevention	■ Manage DLP Policies ■ Create a DLP policy with custom settings ■ Test the DLP Policy ■ Test the first DLP Policy rule ■ Test the second DLP Policy rule
39	Implement Sensitivity Labels	LABS ■ Implement Sensitivity labels ■ Install the Azure Information Protection Unified Labeling client ■ Create a sensitivity label ■ Assign your Sensitivity Label to a document ■ Verify your Sensitivity Label policy ■ Contingency table creation ■ Creating an Aspect Ratio Table

WHAT IS INCLUDED

Everything You Need to Succeed

- Koenig course material for every module
- Delivery by certified instructors and subject matter experts
- Hands-on exercises throughout the course
- Course completion certificate from Koenig

Who We Are

Established in 1993, Koenig Solutions is a globally recognised training provider with 35+ technology partnerships, 5,000+ training programmes and a network of certified instructors and subject matter experts, supporting individuals and enterprise teams worldwide.

Learn the Way That Suits You

Classroom Training

Live Online Classes (ILO)

Fly-Me-A-Trainer (FMAT)

Flexi (Self-Paced)

1-on-1 Training

Ready to Get Started?

Talk to a learning advisor about schedules, group training and customised delivery.

Visit koenig-solutions.com

✉ info@koenig-solutions.com