

MS- 102 Microsoft 365 Administrator

Course Summary:

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.

Prerequisites:

- Students should have completed a role-based administrator training collection such as Messaging, Teamwork, Security and Compliance, or Collaboration.
- Students should have a proficient understanding of DNS and basic functional experience with Microsoft 365 services.
- Students must have a proficient understanding of general IT practices.
- Students should have a working knowledge of PowerShell.

Table of Contents

Module 1: Configure your Microsoft 365 experience

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

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

Module 2: Manage users, licenses, and mail contacts in Microsoft 365

- 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

Module 3: Manage groups in Microsoft 365

- 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

Labs:

- Exercise 2: Manage users and groups
- Create a user account for Adatum's Enterprise Administrator
- Create and manage groups
- Recover groups using PowerShell

Module 4: Add a custom domain in Microsoft 365

- 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 Labs
- Exercise 3: Add a custom domain
- Add a custom domain

Module 5: Configure client connectivity to Microsoft 365

- Understand how automatic client configuration works

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

Module 6: Configure administrative roles in Microsoft 365

- 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

Labs:

- Manage administration delegation
- Assign Delegated Administrators in the Microsoft 365 admin center
- Manage Delegated Administrators with Windows PowerShell
- Verify Delegated Administration

Module 7: Manage tenant health and services in Microsoft 365

- 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 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

Module 8: Deploy Microsoft 365 Apps for enterprise

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

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

Module 10: Explore identity synchronization

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

Module 11: Prepare for identity synchronization to Microsoft 365

- Directory synchronization
- Microsoft Entra Connect Sync

- Microsoft Entra Cloud Sync

Module 12: Implement directory synchronization tools

- 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

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

Module 13: Manage synchronized identities

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

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

Module 14: Manage secure user access in Microsoft 365

- 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

Labs:

- Exercise 3: Manage secure user access
- Deploy Microsoft Entra Pass-Through Authentication
- Deploy Microsoft Entra Smart Lockout

Module 15: Examine threat vectors and data breaches

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

Module 16: Explore the Zero Trust security model

- Effectively adapts to the complexity of the modern environment
 - Embraces the mobile workforce
 - Protects people, devices, apps, and data wherever they are located
- Module 19: Explore security solutions in Microsoft Defender XDR

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

Module 17: Examine Microsoft Secure Score

- 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

Module 18: Examine Privileged Identity Management

- Configure PIM for use in your organization
- Audit PIM roles
- 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

Module 19: Examine Microsoft Entra ID Protection

- 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

Module 20: Examine email protection in Microsoft 365

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

Module 21: Enhance your email protection using Microsoft Defender for Office 365

- 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

Module 22: Manage Safe Attachments

- 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

Labs:

- Create a Safe Attachment policy and turn on Microsoft Defender for Office 365

Module 23: Manage Safe Links

- 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

Labs:

- Create a Safe Links policy
- Validate the Safe Links policy

Module 24: Explore threat intelligence in Microsoft Defender XDR

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

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
- Review the Default eDiscovery Alert
- Test the Default eDiscovery Alert

Module 25: Implement app protection by using Microsoft Defender for Cloud Apps

- 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

Module 26: Implement endpoint protection by using Microsoft Defender for Endpoint

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

Module 27: Implement threat protection by using Microsoft Defender for Office 365

- Microsoft Defender for Office 365 protection stack
- Threat Explorer

- Threat Tracker widgets and views
- 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
- Validate the simulated Spear Phishing attack
- Validate the simulated Drive-by URL attack
- Disable Multifactor Authentication for the Global Admin

Module 28: Examine data governance solutions in Microsoft Purview

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

Module 29: Explore archiving and records management in Microsoft 365

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

Module 30: Explore retention in Microsoft 365

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

Module 31: Explore Microsoft Purview Message Encryption

- Microsoft Purview Message Encryption
- Mail flow rules to encrypt email messages
- Organizational branding on encrypted email messages
- Microsoft Purview Advanced 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 32: Explore compliance in Microsoft 365

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

Module 33: Implement Microsoft Purview Insider Risk Management

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

Module 34: Implement Microsoft Purview Information Barriers

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

Module 35: Explore Microsoft Purview Data Loss Prevention

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

Module 36: Implement Microsoft Purview Data Loss Prevention

- 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

Labs:

- 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

Module 37: Implement data classification of sensitive information

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

Module 38: Explore sensitivity labels

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

Module 39: Implement sensitivity labels

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