PURPLE GRIFFON
The IT Service Management Training & Consultancy Specialists

Course Title: MS-102T00-A Microsoft 365 Administrator Essentials	**Course Duration**: 5.0 Days
Exam: Not Included	**Exam Type**: Proctored Exam
Qualification: Microsoft Certified: Microsoft 365 AdministratorInstructor-led training, hands-on labs	

Course Syllabus

1 - Configure your Microsoft 365 experience

- Explore your Microsoft 365 cloud environment
- Configure your Microsoft 365 organizational profile
- Manage your tenant subscriptions in Microsoft 365
- Integrate Microsoft 365 with customer engagement apps
- Complete your tenant configuration in Microsoft 365

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

- 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 Microsoft Entra ID
- Create and manage guest users
- Create and manage mail contacts

3 - Manage groups in Microsoft 365

- Examine groups in Microsoft 365
- Create and manage groups in Microsoft 365
- Create dynamic groups using Azure rule builder
- Create a Microsoft 365 group naming policy
- Create groups in Exchange Online and SharePoint Online

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

5 - Configure client connectivity to Microsoft 365

- Examine how automatic client configuration works
- Explore the DNS records required for client configuration

- Configure Outlook clients
- Troubleshoot client connectivity

6 - Configure administrative roles in Microsoft 365

- 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 Microsoft Entra ID
- Elevate privileges using Microsoft Entra Privileged Identity Management
- Examine best practices when configuring administrative roles

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
- Monitor tenant health using Microsoft 365 usage analytics
- Develop an incident response plan
- Request assistance from Microsoft

8 - Deploy Microsoft 365 Apps for enterprise

- 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 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

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

- Examine the analytical features of Microsoft Viva Insights
- Explore Personal insights
- Explore Team insights
- Explore Organization insights
- Explore Advanced insights

10 - Explore identity synchronization

- Examine identity models for Microsoft 365
- Examine authentication options for the hybrid identity model
- Explore directory synchronization

11 - Prepare for identity synchronization to Microsoft 365

- Plan your Microsoft Entra deployment
- Prepare for directory synchronization
- Choose your directory synchronization tool
- Plan for directory synchronization using Microsoft Entra Connect

- Plan for directory synchronization using Microsoft Entra Connect cloud sync

12 - Implement directory synchronization tools

- Configure Microsoft Entra Connect prerequisites
- Configure Microsoft Entra Connect
- Monitor synchronization services using Microsoft Entra Connect Health
- Configure Microsoft Entra Connect cloud sync prerequisites
- Configure Microsoft Entra Connect cloud sync

13 - Manage synchronized identities

- Manage users with directory synchronization
- Manage groups with directory synchronization
- Use Microsoft Entra Connect Sync Security Groups to help maintain directory synchronization
- Configure object filters for directory synchronization
- Explore Microsoft Identity Manager
- Troubleshoot directory synchronization

14 - Manage secure user access in Microsoft 365

- Manage user passwords
- Enable pass-through authentication
- Enable multifactor authentication
- Enable passwordless sign-in with Microsoft Authenticator
- Explore self-service password management
- Explore Windows Hello for Business
- Implement Microsoft Entra Smart Lockout
- Implement conditional access policies
- Explore Security Defaults in Microsoft Entra ID
- Investigate authentication issues using sign-in logs

15 - Examine threat vectors and data breaches

- 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 account breaches
- 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

16 - Explore the Zero Trust security model

- 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

17 - Explore security solutions in Microsoft 365 Defender

- 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

18 - Examine Microsoft Secure Score

- 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

19 - Examine Privileged Identity Management

- Explore Privileged Identity Management in Microsoft Entra ID
- Configure Privileged Identity Management
- Audit Privileged Identity Management
- Control privileged admin tasks using Privileged Access Management

20 - Examine Azure Identity Protection

- 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

21 - Examine Exchange Online Protection

- 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

22 - Examine Microsoft Defender for Office 365

- 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

23 - Manage Safe Attachments

- 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

24 - Manage Safe Links

- 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

25 - Explore threat intelligence in Microsoft 365 Defender

- 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

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

- 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

27 - Implement endpoint protection by using Microsoft Defender for Endpoint

- 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

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

- 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

29 - Examine data governance solutions in Microsoft Purview

- Explore data governance and compliance in Microsoft Purview
- Protect sensitive data with Microsoft Purview Information Protection
- Govern organizational data using Microsoft Purview Data Lifecycle Management
- Minimize internal risks with Microsoft Purview Insider Risk Management
- Explore Microsoft Purview eDiscovery solutions

30 - Explore archiving and records management in Microsoft 365

- Explore archive mailboxes in Microsoft 365

- Enable archive mailboxes in Microsoft 365
- Explore Microsoft Purview Records Management
- Implement Microsoft Purview Records Management
- Restore deleted data in Exchange Online
- Restore deleted data in SharePoint Online

31 - Explore retention in Microsoft 365

- Explore retention by using retention policies and retention labels
- Compare capabilities in retention policies and retention labels
- Define the scope of a retention policy
- Examine the principles of retention
- Implement retention using retention policies, retention labels, and eDiscovery holds
- Restrict retention changes by using Preservation Lock

32 - Explore Microsoft Purview Message Encryption

- Examine Microsoft Purview Message Encryption
- Configure Microsoft Purview Message Encryption
- Define mail flow rules to encrypt email messages
- Add organizational branding to encrypted email messages
- Explore Microsoft Purview Advanced Message Encryption

33 - Explore compliance in Microsoft 365

- Plan for security and compliance in Microsoft 365
- Plan your beginning compliance tasks in Microsoft Purview
- Manage your compliance requirements with Compliance Manager
- Examine the Compliance Manager dashboard
- Analyze the Microsoft Compliance score

34 - Implement Microsoft Purview Insider Risk Management

- Explore insider risk management
- Plan for insider risk management
- Explore insider risk management policies
- Create insider risk management policies
- Investigate insider risk management activities and alerts
- Explore insider risk management cases

35 - Implement Microsoft Purview Information Barriers

- Explore Microsoft Purview Information Barriers
- Configure information barriers in Microsoft Purview
- Examine information barriers in Microsoft Teams
- Examine information barriers in OneDrive
- Examine information barriers in SharePoint

36 - Explore Microsoft Purview Data Loss Prevention

- Examine Data Loss Prevention
- Explore Endpoint data loss prevention
- Examine DLP policies

- View DLP policy results
- Explore DLP reports

37 - Implement Microsoft Purview Data Loss Prevention

- Plan to implement Microsoft Purview Data Loss Protection
- Implement Microsoft Purview's default DLP policies
- Design a custom DLP policy
- Create a custom DLP policy from a template
- Configure email notifications for DLP policies
- Configure policy tips for DLP policies

38 - Implement data classification of sensitive information

- Explore data classification
- Implement data classification in Microsoft 365
- Explore trainable classifiers
- Create and retrain a trainable classifier
- View sensitive data using Content explorer and Activity explorer
- Detect sensitive information documents using Document Fingerprinting

39 - Explore sensitivity labels

- Manage data protection using sensitivity labels
- Explore what sensitivity labels can do
- Determine a sensitivity label's scope
- Apply sensitivity labels automatically
- Explore sensitivity label policies

40 - Implement sensitivity labels

- Plan your deployment strategy for sensitivity labels
- Examine the requirements to create a sensitivity label
- Create sensitivity labels
- Publish sensitivity labels
- Remove and delete sensitivity labels

Course Overview

This course provides IT professionals with the knowledge and skills required to administer Microsoft 365 environments. It covers tenant configuration, identity and access management, security and compliance, and management of core Microsoft 365 workloads including Exchange Online, SharePoint Online, Teams, and endpoint management. The course prepares learners for real-world administration tasks and the MS-102 certification exam.

Course Learning Outcomes

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.

Audience

Microsoft 365 administrators, IT administrators, systems engineers, support engineers, and professionals responsible for managing Microsoft 365 services

Entry-Level Requirements

Experience with Microsoft 365 workloads and basic knowledge of networking, identity, and security concepts recommended

Recommended Reading

Microsoft Learn: MS-102 Administrator Learning Path, Microsoft 365 documentation

What's Included

Instructor-led training, hands-on labs, course materials, exam preparation guide

Exam Information

This course prepares learners for the MS-102: Microsoft 365 Administrator Certification Exam. The exam measures the ability to manage Microsoft 365 tenants, identities, security and compliance, and Microsoft 365 workloads. It includes multiple-choice, scenario-based, and case study questions. Passing the exam earns the Microsoft Certified: Microsoft 365 Administrator credential.

What's Next

After completing MS-102, learners can advance to specialized Microsoft certifications such as SC-300 (Identity and Access Administrator), SC-400 (Information Protection Administrator), or MD-102 (Endpoint Administrator).

Additional Information

Prerequisites

- 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.