PEAK LEARNING www.PeakLearningLLC.com

MS-102: Microsoft 365 Administrator (16 hr)

Overview

This instructor led online training course aligns to the MS-102 exam and the Microsoft 365 Certified Administrator Expert certification. This training course includes a deep dive into deploying and implementing Microsoft 365 services, managing user identity and roles, managing access and authentication, and planning Office 365 workloads and applications. Exam Number: MS-102.

Skills Learned

After completing this online training course, students will be able to:

- Deploy and manage a Microsoft 365 tenant
- Implement and manage identity and access in EntraID
- Manage security and threats by using Microsoft 365 Defender
- Manage compliance by using Microsoft Purview

Audience Profile

- This course is for Microsoft 365 administrators.

Prerequisites

We recommend students have experience with all Microsoft 365 workloads and Azure Active Directory (Azure AD), part of Microsoft Entra, and have administered at least one of these. They also have a working knowledge of networking, server administration, DNS, and PowerShell.

For certification purposes, you're required to hold **one** of the following certifications before being able to earn the Microsoft 365 Certified Administrator Expert:

- Microsoft 365 Certified: Modern Desktop Administrator Associate
- Microsoft 365 Certified: Messaging Administrator Associate
- Microsoft 365 Certified: Teams Administrator Associate
- Microsoft Certified: Identity and Access Administrator Associate

Course Outline

01. Implement and manage a Microsoft 365 tenant

- Create a tenant
- Implement and manage domains
- Configure organizational settings, including security, privacy, and profile
- Identify and respond to service health issues
- Configure notifications in service health
- Monitor adoption and usage

02. Manage users and groups

- Create and manage users
- Create and manage guest users
- Create and manage contacts
- Create and manage groups, including Microsoft 365 groups
- Manage and monitor Microsoft 365 license allocations
- Perform bulk user management, including PowerShell

03. Manage roles in Microsoft 365

- Manage roles in Microsoft 365 and Azure AD
- Manage role groups for Microsoft Defender, Microsoft Purview, and Microsoft 365 workloads
- Manage delegation by using administrative units
- Implement privileged identity management for Azure AD roles

04. Implement and manage identity synchronization with Azure AD

- Prepare for identity synchronization by using IdFix
- Implement and manage directory synchronization by using Azure AD Connect cloud sync
- Implement and manage directory synchronization by using Azure AD Connect
- Monitor synchronization by using Azure AD Connect Health
- Troubleshoot synchronization, including Azure AD Connect and Azure AD Connect cloud sync

05. Implement and manage authentication

- Implement and manage authentication methods, including Windows Hello for Business, passwordless, tokens, and the Microsoft Authenticator app
- Implement and manage self-service password reset (SSPR)
- Implement and manage Azure AD Password Protection
- Implement and manage multi-factor authentication (MFA)
- Investigate and resolve authentication issues

06. Implement and manage secure access

- Plan for identity protection
- Implement and manage Azure AD Identity Protection
- Plan Conditional Access policies
- Implement and manage Conditional Access policies

07. Manage security reports and alerts by using the Microsoft 365 Defender portal

- Review and take actions to improve the Microsoft Secure Score in the Microsoft 365 Defender portal
- Review and respond to security incidents and alerts in Microsoft 365 Defender
- Review and respond to issues identified in security and compliance reports in Microsoft 365 Defender
- Review and respond to threats identified in threat analytics

08. Implement and manage email and collaboration protection with Microsoft Defender for Office 365

- Implement policies and rules in Defender for Office 365
- Review and respond to threats identified in Defender for Office 365, including threats and investigations
- Create and run campaigns, such as attack simulation
- Unblock users

09. Implement and manage endpoint protection by using Microsoft Defender for Endpoint

- Onboard devices to Defender for Endpoint
- Configure Defender for Endpoint settings
- Review and respond to endpoint vulnerabilities
- Review and respond to risks identified in the Microsoft Defender Vulnerability Management dashboard

10. Implement Microsoft Purview information protection and data lifecycle management

- Implement and manage sensitive info types by using keywords, keyword lists, or regular expressions
- Implement retention labels, retention label policies, and retention policies
- Implement sensitivity labels and sensitivity label policies

11. Implement Microsoft Purview data loss prevention (DLP)

- Implement DLP for workloads
- Implement Endpoint DLP
- Review and respond to DLP alerts, events, and reports