Microsoft 365 Administrator Essentials

Duration: *5 Day(s)*

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 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.

Review this course online at https://www.alta3.com/courses/MS-102T00

Objectives

- Design and configure Microsoft 365 tenant environments.
- Implement identity synchronization and manage user identities.
- Strengthen security using Microsoft Defender and compliance features.
- Administer data governance to meet regulatory standards.

Who Should Attend

- Aspiring Microsoft 365 Administrators
- Current IT Professionals
- System Administrators
- Technical Support Specialists

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.

Course Outline

Configure your Microsoft 365 tenant

1. Configure your Microsoft 365 experience
2. Manage users, licenses, and mail contacts in Microsoft 365
3. Manage groups in Microsoft 365
4. Add a custom domain in Microsoft 365
5. Configure client connectivity to Microsoft 365

Manage your Microsoft 365 tenant

6. Configure administrative roles in Microsoft 365
7. Manage tenant health and services in Microsoft 365
8. Deploy Microsoft 365 Apps for enterprise
9. Analyze your Microsoft 365 workplace data using Microsoft Viva Insights

Implement identity synchronization

10. Explore identity synchronization
11. Prepare for identity synchronization to Microsoft 365
12. Implement directory synchronization tools
13. Manage synchronized identities
14. Manage secure user access in Microsoft 365

Explore security metrics in Microsoft 365 Defender

15. Examine threat vectors and data breaches
16. Explore the Zero Trust security model
17. Explore security solutions in Microsoft 365 Defender
18. Examine Microsoft Secure Score
19. Examine Privileged Identity Management
20. Examine Azure Identity Protection

Manage your security services in Microsoft 365 Defender

21. Explore threat intelligence in Microsoft 365 Defender
22. Implement app protection by using Microsoft Defender for Cloud Apps
23. Implement endpoint protection by using Microsoft Defender for Endpoint
24. Implement threat protection by using Microsoft Defender for Office 365

Implement threat protection by using Microsoft 365 Defender

25. Explore threat intelligence in Microsoft 365 Defender
26. Implement app protection by using Microsoft Defender for Cloud Apps
27. Implement endpoint protection by using Microsoft Defender for Endpoint
28. Implement threat protection by using Microsoft Defender for Office 365

Explore data governance in Microsoft 365

29. Examine data governance solutions in Microsoft Purview
30. Explore archiving and records management in Microsoft 365
31. Explore retention in Microsoft 365
32. Explore Microsoft Purview Message Encryption

Implement compliance in Microsoft 365

33. Explore compliance in Microsoft 365
34. Implement Microsoft Purview Insider Risk Management
35. Implement Microsoft Purview Implementation Barriers
36. Explore Microsoft Purview Data Loss Prevention
37. Implement Microsoft Purview Data Loss Prevention

Manage compliance in Microsoft 365

38. Implement data classification of sensitive information
39. Explore sensitivity labels
40. Implement sensitivity labels