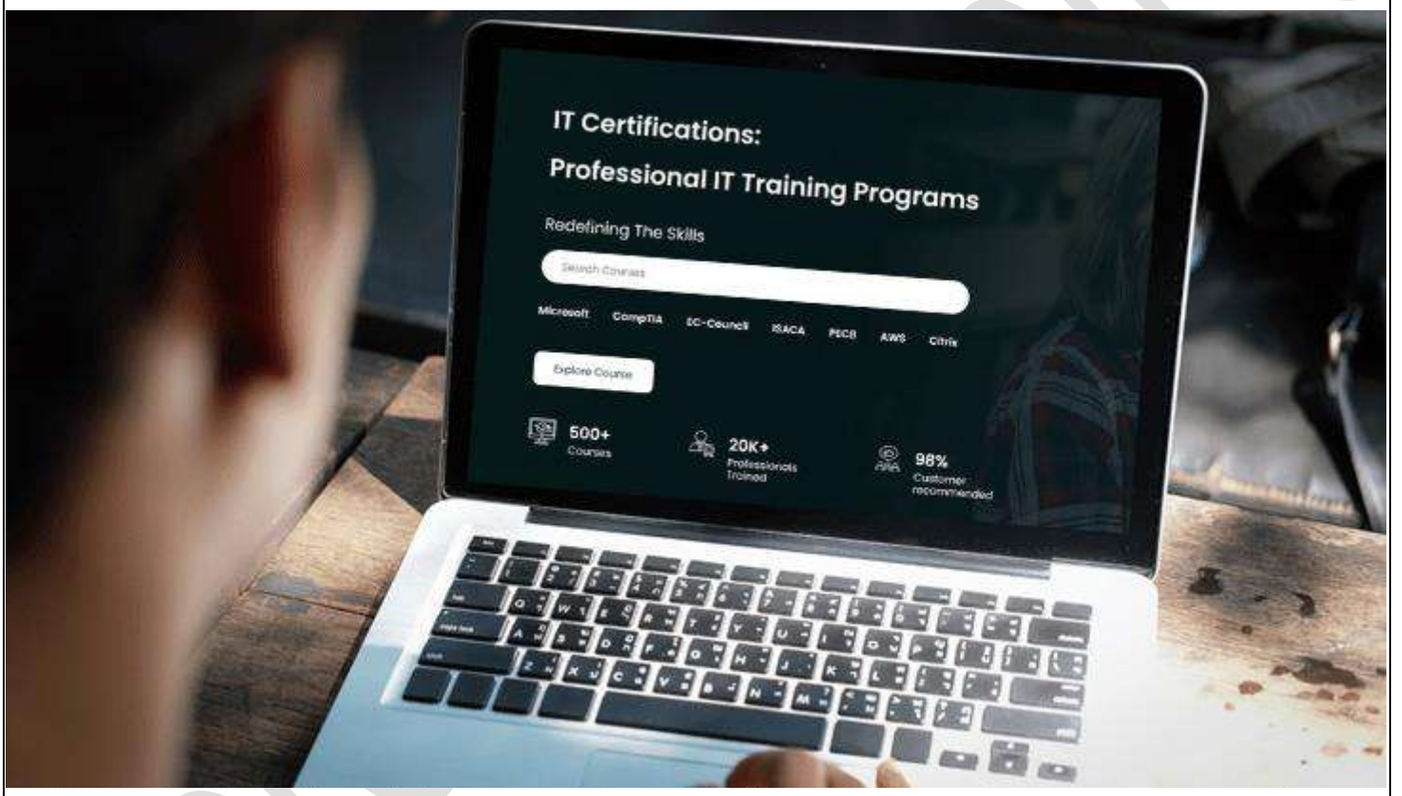
MICROTEK LEARNING | Redefining The Skills



MS-102T00: MICROSOFT 365 ADMINISTRATOR ESSENTIALS TRAINING

Duration: 5 Days

Course Description

Three crucial aspects of Microsoft 365 administration are covered in the MS-102T00: Microsoft 365 Administrator Essentials course: Microsoft 365 tenancy management, Microsoft 365 security and compliance, and Microsoft 365 identity synchronization.

You can configure your Microsoft 365 tenant in Microsoft 365 tenant management.

This includes setting up your organizational profile, tenant subscription choices, component services, user accounts and licenses, security groups, and administrative responsibilities. After that, you switch to establishing Microsoft 365, with an emphasis on setting up Office client connectivity. Finally, you look at how Microsoft 365 Apps for enterprise deployments may be managed via user-driven client installations.

Following a thorough analysis of Microsoft 365 identity synchronization, with an emphasis on Azure Active Directory Connect and Connect Cloud Sync, the MS-102T00: Microsoft 365 Administrator Essentials training concludes. You learn how to set up and manage synchronized identities, multifactor authentication, and self-service password management for Microsoft 365 password management. You also learn how to plan for and implement each of these directory synchronization choices.

In Microsoft 365 security management, you start by looking at the typical categories of attack vectors and data breaches that enterprises today must deal with. Then, you learn how Microsoft 365's security solutions deal with each of these risks. Azure Active Directory Identity Protection and the Microsoft Secure Score are introduced to you.

The next step is to learn how to handle the Microsoft 365 security services, such as safe attachments, safe links, and Exchange Online Protection. Finally, you are exposed to numerous reports that track the security state of an organization.

After that, you switch from security services to threat intelligence by utilizing Microsoft 365 Defender, Microsoft Defender for Cloud Apps, and Microsoft Defender for Endpoints.

Once you are familiar with the security features of Microsoft 365, you can look at the main aspects of compliance management for Microsoft 365. Data archiving and retention, Microsoft Purview message encryption, and data loss prevention (DLP) are all covered in the opening section of this document.

Then you go into more detail on archiving and retention, paying close attention to DLP policies, information barriers, and insider risk management in Microsoft's purview. Next, you look at how to use data classification and sensitivity labels to achieve these compliance features.

Training Exclusives

- Live instructor-led interactive sessions with Microsoft Certified Trainers (MCT).
- Access to Microsoft Official Courseware (MOC).
- Real-time Virtual Lab Environment.
- Experience 24*7 Learner Support.
- Self-paced learning and flexible schedules.

Who should attend this course?

- Microsoft 365 Administrator

What you will learn

- Configure your Microsoft 365 experience
- Manage users, contacts, and licenses in Microsoft 365
- Manage groups in Microsoft 365
- Add a custom domain in Microsoft 365
- Configure client connectivity to Microsoft 365
- Configure administrative roles in Microsoft 365
- Manage tenant health and services in Microsoft 365
- Deploy Microsoft 365 Apps for enterprise
- Analyze your Microsoft 365 workplace data using Microsoft Viva Insights
- Explore identity synchronization
- Prepare for identity synchronization to Microsoft 365
- Implement directory synchronization tools
- Manage synchronized identities
- Manage secure user access in Microsoft 365
- Examine threat vectors and data breaches
- Explore the Zero Trust security model
- Explore security solutions in Microsoft 365 Defender
- Examine Microsoft Secure Score
- Examine Privileged Identity Management
- Examine Azure Identity Protection
- Examine Exchange Online Protection
- Examine Microsoft Defender for Office 365
- Manage Safe Attachments
- Manage Safe Links
- Explore threat intelligence in Microsoft 365 Defender
- Implement app protection by using Microsoft Defender for Cloud Apps
- Implement endpoint protection by using Microsoft Defender for Endpoint
- Implement threat protection by using Microsoft Defender for Office 365

Prerequisites

Required

- MS-203T00: Microsoft 365 Messaging

-OR-

- SC-300T00: Microsoft Identity and Access Administrator

-OR-

- MS-500T00: Microsoft 365 (M365) Security Administration

-OR-

- MS-700T00: Managing Microsoft Teams (Teams Administrator)

Recommended

- 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.

What Exam Do I Need To Get Certified?

- MS-102: Microsoft 365 Administrator

Curriculum

Module 1: Configure your Microsoft 365 experience.

- Configure your company's organization profile, which is essential for setting up your company's tenant
- Maintain minimum subscription requirements for your company.
- Manage your services and add-ins by assigning more licenses, purchasing more storage, and so on
- Create a checklist that enables you to confirm your Microsoft 365 tenant meets your business needs

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

- Identify which user identity model is best suited for your organization
- Create user accounts from both the Microsoft 365 admin center and Windows PowerShell
- Manage user accounts and licenses in Microsoft 365
- Recover deleted user accounts in Microsoft 365
- Perform bulk user maintenance in Azure Active Directory

Module 3: Manage groups in Microsoft 365

- Describe the various types of groups available in Microsoft 365
- Create and manage groups using the Microsoft 365 admin center and Windows PowerShell
- Create and manage groups in Exchange Online and SharePoint Online

Module 4: Add a custom domain in Microsoft 365

- Identify the factors that must be considered when adding a custom domain to Microsoft 365
- Plan the DNS zones used in a custom domain
- Plan the DNS record requirements for a custom domain
- Add a custom domain to your Microsoft 365 deployment

Module 5: Configure client connectivity to Microsoft 365

- Describe how Outlook uses Autodiscover to connect an Outlook client to Exchange Online.
- Identify the DNS records needed for Outlook and other Office-related clients to automatically locate the services in Microsoft 365 using the Autodiscover process
- Describe the connectivity protocols that enable Outlook to connect to Microsoft 365
- Identify the tools that can help you troubleshoot connectivity issues in Microsoft 365 deployments.

Module 6: Configure administrative roles in Microsoft 365

- Describe the Azure RBAC permission model used in Microsoft 365
- Describe the most common Microsoft 365 admin roles
- Identify the key tasks assigned to the common Microsoft 365 admin roles
- Delegate admin roles to partners
- Manage permissions using administrative units in Azure Active Directory
- Elevate privileges to access admin centers by using Azure AD Privileged Identity Management

Module 7: Manage tenant health and services in Microsoft 365

- Monitor your organization's Microsoft 365 service health in the Microsoft 365 admin center

- Develop an incident response plan to deal with incidents that may occur with your Microsoft 365 service
- Request assistance from Microsoft to address technical, pre-sales, billing, and subscription support issues

Module 8: Deploy Microsoft 365 Apps for enterprise

- Describe the Microsoft 365 Apps for enterprise functionality
- Configure the Readiness Toolkit
- Plan a deployment strategy for Microsoft 365 Apps for enterprise
- Complete a user-driven installation of Microsoft 365 Apps for enterprise
- Deploy Microsoft 365 Apps for enterprise with Microsoft Endpoint Configuration Manager
- Identify the mechanisms for managing centralized deployments of Microsoft 365 Apps for enterprise
- Deploy Microsoft 365 Apps for enterprise with the Office Deployment Toolkit
- Describe how to manage Microsoft 365 Apps for enterprise updates
- Determine which update channel and application method applies for your organization

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

- Identify how Microsoft Viva Insights can help improve collaboration behaviors in your organization
- Discover the sources of data used in Microsoft Viva Insights
- Explain the high-level insights available through Microsoft Viva Insights
- Create custom analysis with Microsoft Viva Insights
- Summarize tasks and considerations for setting up Microsoft Viva Insights and managing privacy

Module 10: Explore identity synchronization

- Describe the Microsoft 365 authentication and provisioning options
- Explain directory synchronization
- Explain how Azure AD Connect enables coexistence between your on-premises Active Directory environment and Microsoft 365

Module 11: Prepare for identity synchronization to Microsoft 365

- Identify the tasks necessary to configure your Azure Active Directory environment
- Plan directory synchronization to synchronize your on-premises Active Directory objects to Azure AD
- Identify the features of Azure AD Connect Sync and Azure AD Connect Cloud Sync
- Choose which directory synchronization best fits your environment and business needs

Module 12: Implement directory synchronization tools

- Configure Azure AD Connect and Azure AD Connect Cloud Sync prerequisites
- Set up Azure AD Connect and Azure AD Connect Cloud Sync
- Monitor synchronization services using Azure AD Connect Health

Module 13: Manage synchronized identities

- Ensure users synchronize efficiently
- Manage groups with directory synchronization
- Use Azure AD Connect Sync Security Groups to help maintain directory synchronization.
- Configure object filters for directory synchronization
- Troubleshoot directory synchronization using various troubleshooting tasks and tools

Module 14: Manage secure user access in Microsoft 365

- Manage user passwords

- Describe pass-through authentication
- Enable multifactor authentication
- Describe self-service password management
- Implement Azure AD Smart Lockout
- Implement entitlement packages in Azure AD Identity Governance
- Implement conditional access policies
- Create and perform an access review

Module 15: Examine threat vectors and data breaches

- Describe techniques hackers use to compromise user accounts through email
- Describe techniques hackers use to gain control over resources
- Describe techniques hackers use to compromise data
- Mitigate an account breach
- Prevent an elevation of privilege attack
- Prevent data exfiltration, data deletion, and data spillage

Module 16: Explore the Zero Trust security model

- Describe the Zero Trust approach to security in Microsoft 365
- Describe the principles and components of the Zero Trust security model
- Describe the five steps to implementing a Zero Trust security model in your organization
- Explain Microsoft's story and strategy around Zero Trust networking

Module 17: Explore security solutions in Microsoft 365 Defender

- Identify the features of Microsoft Defender for Office 365 that enhance email security in a Microsoft 365 deployment
- Explain how Microsoft Defender for Identity identifies, detects, and investigates advanced threats, compromised identities, and malicious insider actions directed at your organization
- Explain how Microsoft Defender for Endpoint helps enterprise networks prevent, detect, investigate, and respond to advanced threats
- Describe how Microsoft 365 Threat Intelligence can be beneficial to your organization's security officers and administrators
- Describe how Microsoft Cloud App Security enhances visibility and control over your Microsoft 365 tenant through three core areas

Module 18: Examine Microsoft Secure Score

- Describe the benefits of Secure Score and what kind of services can be analyzed.
- Describe how to collect data using the Secure Score API
- Describe how to use the tool to identify gaps between your current state and where you would like to be regarding security
- Identify actions that increase your security by mitigating risks
- Explain where to look to determine the threats each action mitigates and the impact it has on users

Module 19: Examine Privileged Identity Management

- Describe how Privileged Identity Management enables you to manage, control, and monitor access to important resources in your organization
- Configure Privileged Identity Management for use in your organization
- Describe how Privileged Identity Management audit history enables you to see all the user assignments and activations within a given time period for all privileged roles
- Explain how Microsoft Identity Manager helps organizations manage the users, credentials, policies, and access within their organizations and hybrid environments

- Explain how Privileged Access Management provides granular access control over privileged admin tasks in Microsoft 365

Module 20: Examine Azure Identity Protection

- Describe Azure Identity Protection (AIP) and what kind of identities can be protected.
- Enable the three default protection policies in AIP
- Identify the vulnerabilities and risk events detected by AIP
- Plan your investigation in protecting cloud-based identities
- Plan how to protect your Azure Active Directory environment from security breaches

Module 21: Examine Exchange Online Protection

- Describe how Exchange Online Protection analyzes email to provide anti-malware pipeline protection
- List several mechanisms used by Exchange Online Protection to filter spam and malware
- Describe other solutions administrators may implement to provide extra protection against phishing and spoofing
- Understand how EOP provides protection against outbound spam

Module 22: Examine Microsoft Defender for Office 365

- Describe how the Safe Attachments feature in Microsoft Defender for Office 365 blocks zero-day malware in email attachments and documents
- Describe how the Safe Links feature in Microsoft Defender for Office 365 protects users from malicious URLs embedded in email and documents that point to malicious websites
- Create outbound spam filtering policies
- Unblock users who violated spam filtering policies so they can resume sending emails

Module 23: Manage Safe Attachments

- Create and modify a Safe Attachments policy using Microsoft 365 Defender
- Create a Safe Attachments policy by using PowerShell
- Configure a Safe Attachments policy
- Describe how a transport rule can disable a Safe Attachments policy
- Describe the end-user experience when an email attachment is scanned and found to be malicious

Module 24: Manage Safe Links

- Create and modify a Safe Links policy using Microsoft 365 Defender
- Create a Safe Links policy using PowerShell
- Configure a Safe Links policy
- Describe how a transport rule can disable a Safe Links policy
- Describe the end-user experience when Safe Links identifies a link to a malicious website embedded in email, and a link to a malicious file hosted on a website

Module 25: Explore threat intelligence in Microsoft 365 Defender

- Describe how threat intelligence in Microsoft 365 is powered by the Microsoft Intelligent Security Graph
- Create alerts that can identify malicious or suspicious events
- Understand how the Microsoft 365 Defender's Automated investigation and response process works
- Describe how threat hunting enables security operators to identify cybersecurity threats
- Describe how Advanced hunting in Microsoft 365 Defender proactively inspects events in your network to locate threat indicators and entities

Module 26: Implement app protection by using Microsoft Defender for Cloud Apps

- Describe how Microsoft Defender for Cloud Apps provides improved visibility into network cloud activity and increases the protection of critical data across cloud applications
- Explain how to deploy Microsoft Defender for Cloud Apps
- Control your cloud apps with file policies
- Manage and respond to alerts generated by those policies
- Configure and troubleshoot Cloud Discovery

Module 27: Implement endpoint protection by using Microsoft Defender for Endpoint

- Describe how Microsoft Defender for Endpoint helps enterprise networks prevent, detect, investigate, and respond to advanced threats
- Onboard supported devices to Microsoft Defender for Endpoint
- Implement the Threat and Vulnerability Management module to effectively identify, assess, and remediate endpoint weaknesses
- Configure device discovery to help find unmanaged devices connected to your corporate network
- Lower your organization's threat and vulnerability exposure by remediating issues based on prioritized security recommendations

Module 28: Implement threat protection by using Microsoft Defender for Office 365

- Describe the protection stack provided by Microsoft Defender for Office 365
- Understand how Threat Explorer can be used to investigate threats and help to protect your tenant
- Describe the Threat Tracker widgets and views that provide you with intelligence on different cybersecurity issues that might affect your company
- Run realistic attack scenarios using Attack Simulator to help identify vulnerable users before a real attack impacts your organization

For any query Contact Us – Microtek Learning