



Microsoft 365 Administrator Essentials (MS-102)

Description

Do you want to effectively manage users, secure your data, and optimize services within your Microsoft 365 environment? Our **Microsoft 365 Administrator Essentials (MS-102)** training will help you master the essential tools to manage your subscriptions, configure custom domains, and ensure identity synchronization within your organization.

You will learn how to maximize security and compliance while ensuring user connectivity. Benefit from official, practical, and comprehensive content that will help you enhance your skills and achieve optimal management of your infrastructure.

Course Content

Module 1: Configure your Microsoft 365 experience

- Configure your Microsoft 365 experience
- Manage your tenant subscriptions in Microsoft 365
- Integrate Microsoft 365 with customer engagement apps
- Complete your tenant configuration in Microsoft 365

Module 2: Manage users, contacts, and licenses 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 Azure Active Directory
- Create and manage guest users
- Create and manage contacts

Module 3: Manage groups in Microsoft 365

- Examine groups in Microsoft 365
- Create and manage groups in Microsoft 365
- Create groups in Exchange Online and SharePoint Online

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

Module 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

Module 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 Azure Active Directory
- Elevate privileges using Azure AD Privileged Identity Management

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

Module 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

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

- Examine the analytical features of Microsoft Viva Insights
- Create custom analysis with Microsoft Viva Insights
- Configure Microsoft Viva Insights
- Examine Microsoft 365 data sources used in Microsoft Viva Insights
- Prepare organizational data in Microsoft Viva Insights

Module 10: Explore identity synchronization

- Examine identity models for Microsoft 365

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

Module 11: Prepare for identity synchronization to Microsoft 365

- Plan your Azure Active Directory deployment
- Prepare for directory synchronization
- Choose your directory synchronization tool
- Plan for directory synchronization using Azure AD Connect
- Plan for directory synchronization using Azure AD Connect Cloud Sync

Module 12: Implement directory synchronization tools

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

Module 13: Manage synchronized identities

- Manage users with directory synchronization
- Manage groups with directory synchronization
- Use Azure AD Connect Sync Security Groups to help maintain directory
- Configure object filters for directory synchronization
- Troubleshoot directory synchronization

Module 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 Azure AD Smart Lockout
- Implement conditional access policies
- Explore security defaults in Azure AD
- Investigate authentication issues using sign-in logs

Module 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 how an account breach compromises a user account
- 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

Module 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

Module 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

Module 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

Module 19: Examine Privileged Identity Management

- Explore Privileged Identity Management in Azure AD
- Configure Privileged Identity Management
- Audit Privileged Identity Management
- Explore Microsoft Identity Manager
- Control privileged admin tasks using Privileged Access Management

Module 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

Module 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

Module 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

Module 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

Module 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

Module 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

Module 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

Module 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

Module 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

Lab / Exercises

- Official Microsoft Labs

Documentation

- Access to Microsoft Learn (online learning content)

Exam

- This course prepares for the certification **MS-102: Microsoft 365 Administrator**
- If you wish to take this exam, please select it when you add the course to your basket

Participant profiles

- This course is designed for people aspiring to the role of Microsoft 365 administrator who have already completed at least one of the role-based Microsoft 365 administrator certification paths

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

Objectives

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

Description

Microsoft 365 Administrator Essentials (MS-102) Training

Niveau

Intermédiaire

Classroom Registration Price (CHF)

3900

Virtual Classroom Registration Price (CHF)

3650

Duration (in Days)

5

Reference

MS-102T00