MS-102: Microsoft 365 Administrator Essentials

Microsoft - Microsoft 365

- **Nível:** Intermédio
- **Duração:** 35h

Sobre o curso

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.

Destinatários

This course is designed for persons aspiring to the Microsoft 365 Administrator role

Pré-requisitos

Before attending this course, students must have:

- 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.

Programa

- 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
- Examine data governance solutions in Microsoft Purview
- Explore archiving and records management in Microsoft 365
- Explore retention in Microsoft 365
- Explore Microsoft Purview Message Encryption
- Explore compliance in Microsoft 365
- Implement Microsoft Purview Insider Risk Management
- Implement Microsoft Purview Information Barriers
- Explore Microsoft Purview Data Loss Prevention
- Implement Microsoft Purview Data Loss Prevention
- Implement data classification of sensitive information
- Explore sensitivity labels
- Implement sensitivity labels

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

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

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

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

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

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

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

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 Endpoint 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

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

Explore identity synchronization

- Examine authentication options in Microsoft 365
- Examine provisioning options in Microsoft 365
- Explore directory synchronization
- Explore Azure AD Connect

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

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

Manage synchronized identities

- Manage users with directory synchronization
- 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

Manage secure user access in Microsoft 365

- Manage user passwords
- Enable pass-through authentication
- Enable multi-factor authentication
- Explore self-service password management
- Implement Azure AD Smart Lockout
- Implement entitlement packages in Azure AD Identity Governance
- Implement conditional access policies
- Create and run an access review
- Investigate authentication issues using sign-in logs

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Examine data governance solutions 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.
- Explain the Microsoft Purview eDiscovery solutions.

Explore archiving and records management in Microsoft 365

- Enable and disable an archive mailbox in the Microsoft Purview compliance portal and through Windows PowerShell.
- Run diagnostic tests on an archive mailbox.
- Learn how retention labels can be used to allow or block actions when documents and emails are declared records.
- Create your file plan for retention and deletion settings and actions.
- Determine when items should be marked as records by importing an existing plan (if you already have one) or create new retention labels.
- Restore deleted data in Exchange Online and SharePoint Online.

Explore retention in Microsoft 365

- Explain how a retention policies and retention labels work.
- Identify the capabilities of both retention policies and retention labels.
- Select the appropriate scope for a policy depending on business requirements.
- Explain the principles of retention.
- Identify the differences between retention settings and eDiscovery holds.
- Restrict retention changes by using preservation lock.

Explore Microsoft Purview Message Encryption

- Describe the features of Microsoft Purview Message Encryption.
- Explain how Microsoft Purview Message Encryption works and how to set it up.
- Define mail flow rules that apply branding and encryption templates to encrypt email messages.
- Add organizational branding to encrypted email messages.
- Explain the extra capabilities provided by Microsoft Purview Advanced Message Encryption.

Explore compliance in Microsoft 365

- Describe how Microsoft 365 helps organizations manage risks, protect data, and remain compliant with regulations and standards.
- Plan your beginning compliance tasks in Microsoft Purview.
- Manage your compliance requirements with Compliance Manager.
- Manage compliance posture and improvement actions using the Compliance Manager dashboard.
- Explain how an organization’s compliance score is determined.

Implement Microsoft Purview Insider Risk Management

- Describe insider risk management functionality in Microsoft 365.
- Develop a plan to implement the Microsoft Purview Insider Risk Management solution.
- Create insider risk management policies.
- Manage insider risk management alerts and cases.

Implement Microsoft Purview Information Barriers

- Describe how information barriers can restrict or allow communication and collaboration among specific groups of users.
- Describe the components of an information barrier and how to enable information barriers.
- Understand how information barriers help organizations determine which users to add or remove from a Microsoft Team, OneDrive account, and
- SharePoint site.
- Describe how information barriers prevent users or groups from communicating and collaborating in Microsoft Teams, OneDrive, and SharePoint.

Explore Microsoft Purview Data Loss Prevention

- Describe how Data Loss Prevention (DLP) is managed in Microsoft 365
- Understand how DLP in Microsoft 365 uses sensitive information types and search patterns
- Describe how Microsoft Endpoint DLP extends the DLP activity monitoring and protection capabilities.
- Describe what a DLP policy is and what it contains
- View DLP policy results using both queries and reports

Implement Microsoft Purview Data Loss Prevention

- Create a data loss prevention implementation plan. Implement Microsoft 365’s default DLP policy.
- Create a custom DLP policy from a DLP template and from scratch.
- Create email notifications and policy tips for users when a DLP rule applies.
- Create policy tips for users when a DLP rule applies
- Configure email notifications for DLP policies

Implement data classification of sensitive information

- Explain the benefits and pain points of creating a data classification framework.
- Identify how data classification of sensitive items is handled in Microsoft 365.
- Understand how Microsoft 365 uses trainable classifiers to protect sensitive data.
- Create and then retrain custom trainable classifiers.
- Analyze the results of your data classification efforts in Content explorer and Activity explorer.
- Implement Document Fingerprinting to protect sensitive information being sent through Exchange Online.

Explore sensitivity labels

- Describe how sensitivity labels let you classify and protect your organization’s data
- Identify the common reasons why organizations use sensitivity labels
- Explain what a sensitivity label is and what they can do for an organization
- Configure a sensitivity label’s scope
- Explain why the order of sensitivity labels in your admin center is important
- Describe what label policies can do

Implement sensitivity labels

- Describe the overall process to create, configure, and publish sensitivity labels
- Identify the administrative permissions that must be assigned to compliance team members to implement sensitivity labels
- Develop a data classification framework that provides the foundation for your sensitivity labels
- Create and configure sensitivity labels
- Publish sensitivity labels by creating a label policy
- Identify the differences between removing and deleting sensitivity labels