MICROSOFT 365 MESSAGING Course (MS–203)

This course examines the key elements of Microsoft 365 messaging administration, including message transport and mail flow, messaging security, hygiene, and compliance, messaging infrastructure, and hybrid messaging. This course is designed for persons who are aspiring to be Messaging Administrators in a Microsoft 365 deployment.

مروری بر دوره

The Messaging Administrator plans, deploys, configures, troubleshoots, and secures the messaging infrastructure in a hybrid and cloud enterprise environment. Responsibilities include managing recipients, mailboxes, transport, mail flow, administrative roles, threat protection, compliance, migrations, and client connectivity. To implement a secure hybrid topology that meets the business needs of a modern organization, the Messaging Administrator must collaborate with other workload administrators and the Microsoft 365 enterprise administrator. The Messaging Administrator should have a working knowledge of authentication types, licensing, and integration with Microsoft 365 applications.

آنچه خواهید آموخت

- Students will learn to,
- Manage mail flow
- Troubleshoot mail flow
- Manage mail flow rules
- Plan for message security
- Manage anti–malware and anti–spam policies
- Explore threat protection in Microsoft 365 Defender
- Explore messaging compliance in Microsoft 365
- Explore messaging compliance in Exchange
- Manage Exchange Online archiving and auditing
- Manage Content Search
- Manage authentication for messaging
- Configure organizational settings
- Configure organizational sharing
- Manage administrator roles
- Manage user roles
- Analyze role–based permissions
- Explore the different types of Exchange recipients
- Create and manage Exchange recipients

- Manage email addresses, lists, and resources
- Explore Exchange hybrid deployment requirements
- Plan and configure a hybrid deployment using the Hybrid Configuration Wizard
- Plan mailbox migrations
- Run mailbox migrations
- Troubleshoot hybrid deployments

سرفصل ها

Module 1: Manage mail flow

- Manage mail flow in Exchange organizations.
- Understand mail flow for Exchange Servers.
- Manage mail flow for Exchange Online.
- Describe and manage mail flow in hybrid environments.
- Configure message transport options.
- Configure SMTP domains (Remote and Accepted domains)
- Configure connectors

Module 2: Troubleshoot mail flow

- Understand how to troubleshoot SMTP mail flow issues.
- Describe how to troubleshoot issues with a shared namespace.
- Describe how to troubleshoot Transport Layer Security encryption issues.
- Troubleshoot network–based issues.
- Understand how the service health dashboard can be utilized to review active and ongoing service–related issues.
- Understand how Alert policies can be used to troubleshoot mail flow issues.

Module 3 : Manage mail flow rules

- Understand what mail flow rules are.
- Describe how mail flow rules work.
- Configure custom mail flow rules.

Module 4: Plan for message security

- Explain the use and features of Exchange Online Protection.
- Plan message routing for Exchange Online Protection.
- Investigate the available EOP reports and logs that enable organizations to monitor message hygiene.

- Define mail flow rules that apply encryption templates to encrypt email messages.

Module 5: Manage anti-malware and anti-spam policies

- Understand the different message header fields relevant for spam and spoofing protection.
- Configure anti-spam and anti-malware filters in Exchange Server.
- Manage extra features for outbound spam filtering and quarantine.
- Implement protection features against phishing and spoofing.
- Create transport rules for custom requirements.

Module 6: Explore threat protection in Microsoft 365 Defender

- Describe the threat protection features of Microsoft Defender for Office 365.
- Understand how the Configuration analyzer reviews threat protection policies and provides suggestions for improvement.
- Describe the protection provided by Safe Attachment and Safe Links policies.
- Understand the spoof intelligence features provided by Exchange Online Protection.
- Describe how Microsoft Defender anti-phishing policies work.
- Understand the process to manage the Tenant Allow/Block list in Microsoft 365 Defender.
- Run realistic attack scenarios using Attack Simulator to help identify vulnerable users before a real attack impacts your organization.

Module 7: Explore messaging compliance in Microsoft 365

- Describe different policy and compliance features for messaging.
- Evaluate the different administrator roles in Microsoft 365.
- Plan retention policies for Exchange Online mailboxes.
- Create message traces to understand the mail flow in your Exchange Online organization.
- Describe how sensitivity labels let you classify and protect your organization's data.
- Create and manage inactive mailboxes.

Module 8: Explore messaging compliance in Exchange

- Describe litigation and in-place holds in Exchange Server.
- Plan retention and deletion with Message Records Management (MRM).
- Analyze your Exchange organization's message tracking log.

Module 9: Manage Exchange Online archiving and auditing

- Describe what in-place archiving is and how it works.

- Understand the differences between journaling and archiving.
- Identify how mailbox and administrator audit logs are used.

Module 10: Manage Content Search

- Design content searches to search for messages in your organization.
- Describe eDiscovery cases and in–place eDiscovery for Exchange.

Module 11: Manage authentication for messaging

- Configure password policy options.
- Configure self–service password management.
- Implement multifactor authentication.
- Plan password policies.
- Configure modern authentication in Exchange Online.
- Configure conditional access policies.

Module 12: Configure organizational settings

- Configure workload policies and throttling.
- Configure quota configurations.
- Deploy Microsoft 365 Integrated apps.

Module 13: Configure organizational sharing

- Provide an overview of Exchange federated delegation sharing features.
- Describe federated sharing components.
- Identify considerations for designing and implementing federation trusts and certificates.
- Implement organization relationships.
- Implement sharing policies.

Module 14: Manage administrator roles

- Describe how RBAC is used to assign roles to users.
- Understand management role groups and their administrative tasks.
- Assign the built–in management roles for messaging administration.
- Create custom management roles and assign them through role assignment policies to users.
- Troubleshoot RBAC management roles.

- Describe how Privileged Identity Management enables you to manage, control, and monitor access to important resources in your organization.

Module 15: Manage user roles

- Describe the built–in end–user roles.
- Configure role assignment policies.
- Create new custom roles and role assignment policies.

Module 16: Analyze role–based permissions

- Identify the differences between shared permissions and split permissions.
- Describe multi–forest permissions.
- Identify the differences between the permission models.

Module 17: Explore the different types of Exchange recipients

- Describe the different recipient objects in Exchange.
- Examine how organizations use resource mailboxes.
- Compare shared mailboxes to linked mailboxes.
- Describe how recipients can be grouped together to improve collaboration.
- Examine how organization us public folders.

Module 18: Create and manage Exchange recipients

- Manage mailbox settings.
- Manage resource mailboxes and shared mailboxes.
- Create and manage mail contacts and mail users.
- Manage permissions for recipients.
- Create and manage groups.
- Create and manage public folders.

Module 19: Manage email addresses, lists, and resources

- Describe address lists.
- Create and manage address lists.
- Describe address book policies.
- Configure offline address books.
- Describe email address policies.

Module 20: Explore Exchange hybrid deployment requirements

- Describe connection options that are available for connecting on–premises Exchange to Microsoft 365.
- List and describe components of a hybrid deployment.
- Describe Azure Active Directory Connect (Azure AD Connect).
- Identify Microsoft 365 identity options for Exchange hybrid.
- Compare Exchange delegated federation to OAuth.

Module 21: Plan and configure a hybrid deployment using the Hybrid Configuration Wizard

- Plan for Exchange Hybrid configuration.
- Describe Organization Configuration Transfer.
- Explain Exchange Modern Hybrid and Hybrid Agent.
- Plan mail flow options for a hybrid deployment.
- Describe the prerequisites to run the Microsoft 365 Hybrid Configuration Wizard.
- Explain best practices for implementing a hybrid deployment.

Module 22: Plan mailbox migrations

- Describe the migration and coexistence strategies with Exchange Online.
- Describe considerations that affect which migration option to use.
- Determine whether DNS MX records must be changed during a mailbox migration.

Module 23: Run mailbox migrations

- Describe the requirements for an IMAP migration and how it's carried out.
- Move mailbox data using an IMAP migration.
- Plan for a cross–tenant mailbox migration.
- Prepare target user objects for a cross–tenant migration.

Module 24: Troubleshoot hybrid deployments

- Troubleshoot directory synchronization.
- Troubleshoot pass–through authentication and single sign–on.
- Troubleshoot transport with Exchange Online.
- Troubleshoot client access in coexistence.
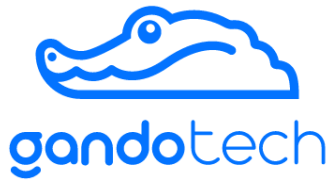- Troubleshoot the Mailbox Replication service.

مدارک مرتبط

🌐 info@gandotech.com

📍 Lisbon, Sintra, Mirante St, No3, 2/C

📱 +351 911970800

✉ P.Code: 27 45-039