Microsoft 365 Messaging

Course MS-203T00: 5 days Instructor Led

About this course

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.

Audience profile

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.

At course completion

After completing this course, students will be able to:
- Manage the transport pipeline in Microsoft 365
- Manage and troubleshoot mail flow in Microsoft 365
- Manage message security
- Manage compliance in Microsoft 365
- Manage your Microsoft 365 messaging environment
- Manage role-based permissions in Microsoft 365
- Manage recipient objects and resources in Microsoft 365
- Manage the hybrid deployment life cycle
- Manage mailbox migrations

Course Outline

Module 1: Manage the transport pipeline in Microsoft 365

In this module, you will learn about the different transport components of Exchange, how the message routing works, and how to configure the message flow for your organization. You will examine the tasks that messaging administrators must complete to configure message transport. You will review the message transport options and learn how to configure domains and connectors. You will also learn how to manage transport rules, which are a very powerful configuration to control the message flow in your organization.

Lessons

- Explore transport services
- Configure message transport
- Manage transport rules

Lab: Configure Message Transport

- Create Connectors

After completing this module, students will be able to:

- Describe the transport components of Exchange
- Plan an effective message routing for your organization
- Modify message flow for your organization
- Describe which transport agents exist and what they do
- Configure the different transport options
- Plan and set up domains for your organizations
- Understand how receive and send connectors work
- Understand what transport rules are
- Describe how transport rules are working
- Configure custom transport rules
- Describe how transport rules can be used for data loss prevention

Module 2: Manage and troubleshoot mail flow in Microsoft 365

In this module, you will examine the components of mail flow, and you will learn how to manage your mail flow, which is a crucial task for every Exchange administrator. You will study the differences between managing mail flow in Exchange Online, Exchange Server, and Exchange Hybrid deployments. From managing mail flow, you will transition to troubleshooting mail flow issues such as emails not being routed correctly in or outside your organization, or when secure connections cannot be established successfully. You will learn about the tools Microsoft provides to help you find the root cause of your issues and fix your mail flow. You will then transition from troubleshooting mail flow to troubleshooting transport issues, such as network-based issues, connector and agent issues, and architectural issues, as well as how to troubleshoot in coexistence. Finally, you will learn how to check event, protocol, and tracking logs when all troubleshooting for service availability and message transport has finished and an issue still persists, or if you must find historical data about issues in the past.

Lessons

- Manage mail flow
- Troubleshoot mail flow
- Troubleshoot transport issues
- Troubleshoot mail flow using logs

Lab: Conditional Mail Routing

- Create Mail Flow Rules

After completing this module, students will be able to:

- Manage mail flow in organizations
- Understand mail flow for Exchange Servers
- Manage mail flow for Exchange Online

- Describe and manage mail flow in hybrid environments
- Understand how to troubleshoot SMTP mail flow issues
- Describe how to troubleshoot issues with a shared namespace
- Describe how to troubleshoot encryption issues with TLS
- Understand how Alert policies can be used to troubleshoot mail flow issues
- Troubleshooting network-based issues
- Describe troubleshooting procedures for connector and agent issues
- Plan troubleshooting for architectural issues
- Understand how to perform troubleshooting in coexistence
- Create searches for the message tracking log
- Describe how to troubleshoot using the protocol logs
- Understand how to work with the event logging for Exchange

Module 3: Manage message security

In this module, you will learn about Microsoft Exchange Online Protection (EOP) features and functionality. You will also learn how to plan messaging routing for this service, which provides anti-malware and anti-spam policies that protect your organization against spam and malware and safeguards your organization from messaging policy violations. You will then review the anti-malware and anti-spam protection that Exchange Server and Online Protection provide, and you will learn how to configure SPAM and malware filters, policies, and settings to provide protection for your users. You will conclude the module by examining Defender for Office 365 and how it extends the protection provided by EOP by filtering targeted attacks that could pass through EOP's line of defenses, including advanced threats such as zero-day attacks in email attachments and Office documents and time-of-click protection against malicious URLs. You will learn how Defender for Office 365 protects users from advanced threats through features such as safe attachments and safe links, and how it generates reports which provide administrators with insight into attacks targeting their tenants through email.

Lessons

- Plan for message security
- Manage anti-malware and anti-spam policies
- Explore threat protection in Microsoft 365 Defender

Lab: Managing Messaging Hygiene

- Create Hygiene Filters

After completing this module, students will be able to:

- Explain the use and features of Exchange Online Protection
- Plan message routing for Exchange Online Protection
- Investigate the available EOP reports and logs
- Understand the different message header fields relevant for spam and spoofing protection
- Configure anti-spam and anti-malware filters in Exchange Server
- Using additional features for outbound spam filtering and quarantine
- Implementing protection features against phishing and spoofing

- Create transport rules for custom requirements
- Describe the features of Microsoft Defender for Office 365
- Describe the protection provided by Safe Attachment and Safe Links policies
- Understand the spoof intelligence features
- Describe how Microsoft Defender anti-phishing policies work
- Understand how to use the Configuration Analyzer
- Manage the Tenant Allow/Block list in Microsoft 365 Defender
- Understand the features of Advanced Hunting

Module 4: Manage compliance in Microsoft 365

This module begins by describing the different compliance features in Microsoft 365 that messaging administrators can use to comply with legal and regulatory requirements. This module supports compliance in Exchange by examining the compliance features available in the Exchange Admin Center for Exchange Server and hybrid deployments. Because of the complex retention requirements of modern messaging environments, this module focuses on how archiving is performed with Exchange so that you can provide an efficient and compliant environment to your users. You will also examine how additional archive storage is provided to your users, how messages are automatically processed and archived, and how audit logging in Exchange that provides information about administrator, delegate, and user actions in user mailboxes and your Exchange organization. Finally, because organizations must adhere to legal discovery requirements (related to organizational policy, compliance, or lawsuits), you will examine how eDiscovery for Microsoft Exchange can help you perform discovery searches for relevant content within mailboxes.

Lessons

- Explore messaging compliance in Microsoft 365
- Explore messaging compliance in Exchange
- Manage Exchange Online archiving and auditing
- Manage content search

Lab: Manage Messaging Compliance

- Manage Messaging Compliance

After completing this module, students will be able to:

- Describe different policy and compliance features for messaging
- Evaluate the Microsoft 365 permission model
- Plan retention policies for Exchange Online mailboxes
- Create message traces to understand the mail flow in your Exchange Online organization
- Describe litigation and in-place holds in Exchange Server
- Plan retention and deletion with Message Records Management (MRM)
- Investigate the message tracking log in your Exchange organization
- Describe what in-place archiving is and how it works
- Understand the differences between journaling and archiving
- Know what the mailbox and administrator audit logs are used for
- Understand content searches to search for messages in your organization

- Describe eDiscovery cases and in-place eDiscovery for Exchange

Module 5: Manage your Microsoft 365 messaging environment

This module begins with an examination on how to manage authentication for messaging. This module focuses on how to ensure that user accounts are well protected and secure, and how to deploy multiple security features that do not introduce unnecessary complexity in users' everyday work, which can result in lower business productivity and new security risks. You will then transition from messaging authentication to organizational settings, where you will learn how to configure settings that apply to the entire organization or to many users in the organization. Finally, you will examine how to configure organizational sharing.

Lessons

- Manage authentication for messaging
- Configure organizational settings
- Configure organizational sharing

After completing this module, students will be able to:

- Configure password policy options
- Configure self-service password management
- Implement multi-factor authentication
- Plan password policies
- Configure modern authentication in Exchange Online
- Configure workload policies and throttling
- Configure quota configurations
- Deploy Microsoft 365 Integrated Apps
- Provide an overview of Exchange federated delegation sharing features
- Describe federated sharing components
- Explain considerations for designing and implementing federation trusts and certificates
- Implement organization relationships
- Implement sharing policies

Module 6: Manage role-based permissions in Microsoft 365

This module examines how messaging administrators manage role-based permissions, which is an essential task for any messaging administrator. Since Exchange Server and Exchange Online both use the Role Based Access Control (RBAC) permission model, this module examines the basics of RBAC management. The module concludes by examining how a messaging administrator must plan and configure permissions carefully so as not to put their environment or their entire Active Directory at risk.

Lessons

- Manage administrator roles
- Manage user roles

- Analyze role-based permissions

Lab: Manage Roles and Permission Policies

- Manage Roles and Permission Policies

After completing this module, students will be able to:

- Describe how RBAC is used to assign roles to users
- Understand what management role group for administrative tasks are
- Assign the built-in management roles for administration
- Create custom management roles and assign them through role assignment policies to users
- Troubleshoot RBAC management roles
- Describe the built-in end-user roles
- Configure role assignment policies
- Create new custom roles and role assignment policies
- Understand the differences between shared permissions and split permissions
- Describe multi-forest permissions
- Identify the differences between the permission models

Module 7: Manage recipient objects and resources in Microsoft 365

This module examines some of the most common tasks that messaging administrators perform - creating and configuring email recipients, lists, and resources. This module examines the different types of Exchange Server recipients, including how they differ from each other. The module then focuses on the various tasks that require you to create and manage Exchange recipients in Exchange, including user mailboxes, resource mailboxes, public folder, shared mailboxes, mail contacts, and mail users. You will also learn how to manage permissions for recipients, and how to create and manage groups.

Lessons

- Explore the different types of Exchange recipients
- Create and manage Exchange recipients
- Manage email addresses, lists, and resources

Lab: Implement Public Folders

- Create Public Folders
- Manage Public Folders

Lab: Create Recipient Objects and Resources

- Create Exchange Recipients
- Create Groups

After completing this module, students will be able to:

- Describe the different recipient objects in Exchange
- Describe resource mailboxes
- Describe shared mailboxes
- Describe linked mailboxes
- Describe groups
- Describe public folders
- Create and manage Mailbox settings
- Create and manage Resource and Shared mailboxes
- Create and manage Mail contacts and mail users
- Create and manage Recipient permissions
- Create and manage Groups
- Create and manage public folders
- Describe address lists
- Explain how to configure address lists
- Describe address book policies
- Explain how to configure offline address books
- Describe email address policies

Module 8: Manage the hybrid deployment life cycle

In this module you will examine the requirements necessary to implement a hybrid deployment, and you will learn about the features and components that are required when implementing a hybrid deployment. This module examines all planning aspects that are required before running the Hybrid Configuration Wizard. This includes the configuration options of the HCW, as well as the details on Organization Configuration Transfer (OCT) and the Hybrid Agent. The module concludes with a review of the mail flow options for a hybrid deployment. This module also examines Edge Transport servers and their use in hybrid Exchange deployments. You will then learn about the requirements and best practices to configure a hybrid deployment, which is the first step for your Exchange organization, regardless of whether you want to connect your Exchange on-premises and Exchange Online organizations for long-term coexistence or as part of a cloud migration strategy. In this module, you will then examine how to manage a hybrid deployment and implement advanced hybrid functionality. You will cover the features that require a successful hybrid deployment such as OneDrive for Business attachment storage for on-premises mailboxes. This module concludes with an introduction to troubleshooting techniques for a hybrid deployment. You will learn how to troubleshoot directory synchronization issues including pass-through authentication (PTA) and single sign-on, Exchange transport, and client access troubleshooting as well as mailbox replication service troubleshooting.

Lessons

- Explore Exchange hybrid deployment requirement
- Plan and configure a hybrid deployment using the Hybrid Configuration Wizard
- Provide a gateway for Internet email using Edge Transport servers
- Implement advanced hybrid functionality
- Troubleshoot hybrid deployments

Lab: Deploy a Hybrid Environment

- Configure your Hybrid Deployment

Lab: Deploy a Hybrid Environment

- Test your Hybrid Deployment
- Troubleshoot your Hybrid Deployment

Lab: Prepare Azure AD for Hybrid Synchronization

- Prepare Azure AD for Hybrid Synchronization

After completing this module, students will be able to:

- Describe connection options that are available for connecting on-premises Exchange to Microsoft 365
- List and describe components of a hybrid Exchange deployment
- Describe Azure Active Directory Connect (Azure AD Connect)
- Identify Microsoft 365 identity options for Exchange hybrid
- Compare Exchange delegated federation vs. OAuth
- Plan for Exchange Hybrid configuration
- Describe Organization Configuration Transfer
- Explain Exchange Modern Hybrid and Hybrid Agent
- Plan mail flow options for a hybrid Exchange deployment
- Describe the prerequisites to run the Microsoft 365 Hybrid Configuration Wizard
- Explain best practices for implementing a hybrid Exchange deployment
- Describe the purpose and functionality of Edge Transport servers
- Explain the infrastructure requirements for Edge Transport servers
- Describe EdgeSync
- Plan for message flow with an Edge Transport server
- Manage a hybrid Exchange deployment
- Explain how to configure Oauth for a hybrid Exchange deployment
- Describe how to configure OneDrive for Business attachments for on-premises mailboxes
- Troubleshoot Directory synchronization
- Troubleshoot Pass-Through Authentication and Single Sign-On
- Troubleshoot Transport with Exchange Online
- Troubleshoot Client Access in a hybrid Exchange deployment
- Troubleshoot Mailbox Replication Service

Module 9: Manage mailbox migrations

This module examines the options that are available for migrating email to Exchange Online. This module summarizes the migration and co-existence options and recommends when to use which option. The module then examines the requirements for running an IMAP migration, the migration options that are available, and the steps that are performed during a migration. The module then examines how to plan and perform both a cutover and staged migration. It compares each of these two migration approaches, and you will learn about the requirements, planning activities, and

migration process for each option. The module concludes by examining important additional migration tasks, such as cross tenant migrations, and PST migrations.

Lessons

- Plan mailbox migrations
- Run IMAP migrations
- Run cutover and staged migrations
- Run advanced mailbox migrations

Lab: Plan a Mail Migration to Microsoft 365

- Paper-based classroom exercise - Plan a Mail Migration to Microsoft 365

After completing this module, students will be able to:

- 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
- Describe the requirements for an IMAP migration and how it's carried out
- Move mailbox data using an IMAP migration
- Describe the requirements for both cutover and staged migrations
- Identify the steps involved in running both cutover and staged migrations
- Create and manage migration batches in the Exchange Admin Center
- Import PST Files to Exchange Online mailboxes
- Perform a Cross-Tenant Migration
- Prepare target user objects for a cross-tenant migration