MS-500 Microsoft 365 Security Administrator

About this course
This four-MOC packaged set is aligned to Microsoft 365 Exam: Microsoft 365 Security Administrator contains courseware that helps prepare students for Exams MS-500. Passing this exam is required to earn the Microsoft 365 Security Administrator certification. The individual courses included in this packaged set are:
MS-500T01
MS-500T02
MS-500T03
MS-500T04

Audience profile
This course is for the Microsoft 365 security administrator role. This role collaborates with the Microsoft 365 Enterprise Administrator, business stakeholders and other workload administrators to plan and implement security strategies and ensures that the solutions comply with the policies and regulations of the organization.

This role proactively secures Microsoft 365 enterprise environments. Responsibilities include responding to threats, implementing, managing and monitoring security and compliance solutions for the Microsoft 365 environment. They respond to incidents, investigations and enforcement of data governance.

The Microsoft 365 Security administrator is familiar with Microsoft 365 workloads and has strong skills and experience with identity protection, information protection, threat protection, security management and data governance. This role focuses on the Microsoft 365 environment and includes hybrid environments.

At course completion
After completing this course, students will be able to:

- Administer user and group security in Microsoft 365.
- Manage passwords in Microsoft 365.
- Describe Azure Identity Protection features.
- Plan and implement Azure AD Connect.
- Manage synchronized identities.
- Plan implement federated identities.
- Describe and use conditional access.
- Describe cyber-attack threat vectors.
- Describe security solutions for Microsoft 365
- Use Microsoft Secure Score to evaluate your security posture.
- Use the Security Dashboard in the Microsoft Security & Compliance center.
- Configure various advanced threat protection services for Microsoft 365.
- Configure Advanced Threat Analytics.
- Plan and deploy Mobile Device Management.
- Implement information rights management.
- Secure messages in Office 365.
- Configure Data Loss Prevention policies.
- Deploy and manage Cloud App Security.
- Implement Azure information protection for Microsoft 365.
- Implement Windows information protection for devices.

- Plan and deploy a data archiving and retention system.
- Perform assessments in Compliance Manager.
- Manage email retention through Exchange.
- Conduct an audit log investigation.
- Create and manage an eDiscovery investigation.
- Manage GDPR data subject requests.

Course Outline

Day 1

Module 1: User and Group Security

This module explains how to manage user accounts and groups in Microsoft 365. It introduces you to Privileged Identity Management in Azure AD as well as Identity Protection. The module sets the foundation for the remainder of the course.

Lessons

- User Accounts in Microsoft 365
- Administrator Roles and Security Groups in Microsoft 365
- Password Management in Microsoft 365
- Azure AD Identity Protection

Lab: Managing your Microsoft 365 Identity environment

- Setting up your lab environment
- Managing your Microsoft 365 identity environment using the Microsoft 365 admin center
- Assign service administrators

After completing this module, students should be able to:

- Describe the user identities in Microsoft 365.
- Create user accounts from both the Microsoft 365 admin center and in Windows PowerShell.
- Describe and use Microsoft 365 admin roles.
- Describe the various types of group available in Microsoft 365.
- Plan for password policies and authentication.
- Implement Multi-factor authentication in Office 365.
- Describe Azure Identity Protection and what kind of identities can be protected.
- Describe how to enable Azure Identity Protection.
- Identify vulnerabilities and risk events.

Module 2: Identity Synchronization

This module explains concepts related to synchronizing identities. Specifically, it focuses on Azure AD Connect and managing directory synchronization to ensure the right people are connecting to your Microsoft 365 system.

Lessons

- Introduction to Identity Synchronization
- Planning for Azure AD Connect
- Implementing Azure AD Connect
- Managing Synchronized Identities

Lab: Implementing Identity Synchronization

- Setting up your organization for identity synchronization

After completing this module, students should be able to:

- Describe the Microsoft 365 authentication options.

- Explain directory synchronization.
- Plan directory synchronization.
- Describe and plan Azure AD Connect.
- Configure Azure AD Connect Prerequisites.
- Set up Azure AD Connect.
- Manage users with directory synchronization.
- Manage groups with directory synchronization.
- Use Azure AD Connect Sync Security Groups.

Module 3: Federated Identities
This module is all about Active Directory Federation Services (AD FS). Specifically, you will learn how to plan and manage AD FS to achieve the level of access you want to provide users from other directories.
Lessons
- Introduction to Federated Identities
- Planning an AD FS Deployment
- Implementing AD FS

After completing this module, students should be able to:
- Describe claims-based authentication and federation trusts.
- Describe how AD FS works.
- Plan an AD FS environment including best practices, high availability, and capacity planning.
- Plan Active Directory Federation Services in Microsoft Azure.
- Install and configure a Web Application Proxy for AD FS.
- Configure AD FS by using Azure AD Connect.

Module 4: Access Management
This module describes Conditional Access for Microsoft 365 and how it can be used to control access to resources in your organization. The module also explains Role Based Access Control (RBAC) and solutions for external access.
Lessons
- Conditional Access
- Managing Device Access
- Role Based Access Control (RBAC)
- Solutions for External Access

After completing this module, students should be able to:
- Describe the concept of conditional access.
- Describe conditional access policies.
- Plan for device compliance.
- Configure conditional users and groups.
- Configure RBAC.
- Distinguish between Azure RBAC and Azure AD administrative roles.
- Manage External Access.
- Explain Licensing Guidance for Azure AD B2B Collaboration.

Day 2
Module 1: Security in Microsoft 365
This module starts by explaining the various cyber-attack threats that exist. It then introduces you to the Microsoft solutions to thwart those threats. The module finishes with an explanation of Microsoft Secure Score and how it can be used to evaluate and report your organizations security posture.

Lessons

- Threat Vectors and Data Breaches
- Security Solutions for Microsoft 365
- Microsoft Secure Score

After completing this module, students will be able to:

- Describe several techniques hackers use to compromise user accounts through email.
- Describe techniques hackers use to gain control over resources.
- List the types of threats that can be avoided by using Exhange Online Protection and Office 365 ATP.
- Describe how Microsoft 365 Threat Intelligence can be beneficial to your organization's security officers and administrators.
- Describe the benefits of Secure Score and what kind of services can be analyzed.
- Describe how to use the tool to identify gaps between your current state and where you would like to be with regards to security.

Module 2: Advanced Threat Protection

This module explains the various threat protection technologies and services available in Microsoft 365. Specifically, the module covers message protection through Exchange Online Protection, Azure Advanced Threat Protection and Windows Defender Advanced Threat Protection.

Lessons

- Exchange Online Protection
- Office 365 Advanced Threat Protection
- Managing Safe Attachments
- Managing Safe Links
- Azure Advanced Threat Protection
- Windows Defender Advanced Threat Protection

Lab: Advanced Threat Protection

- Setting up your lab environment
- Editing an ATP Safe Links policy and creating a Safe Attachment policy

After completing this module, students will be able to:

- Describe the anti-malware pipeline as email is analyzed by Exchange Online Protection.
- Describe how Safe Attachments is used to block zero-day malware in email attachments and documents.
- Describe how Safe Links protect users from malicious URLs embedded in email and documents that point to malicious websites.
- Configure Azure Advanced Threat Protection.
- Configure Windows Defender ATP.
- Integrate Windows Defender ATP with Azure ATP.

Module 3: Threat Intelligence

This module explains Microsoft Threat Intelligence which provides you with the tools to evaluate and address cyber threats. You will learn how to use the Security Dashboard in the Microsoft 365 Security and Compliance Center. It also explains and configures Microsoft Advanced Threat Analytics.

Lessons

- Microsoft 365 Threat Intelligence
- Using the Security Dashboard
- Configuring Advanced Threat Analytics

Lab: Advanced Threat Analytics

- Enabling and installing the ATA Center

After completing this module, students will be able to:

- Describe how threat intelligence in Microsoft 365 is powered by the Microsoft Intelligent Security Graph.
- Describe how Threat Explorer can be used to investigate threats and help to protect your tenant.
- Describe how the Security Dashboard gives C-level executives insight into top risks, global trends, protection quality, and the organization's exposure to threats.
- Describe how the Security dashboard can be used as a launching point to enable security analysts to drill down for more details by using Threat Explorer.
- Describe what Advanced Thread Analytics (ATA) is and what requirements are needed to deploy it.
- Configure Advanced Threat Analytics.

Module 4: Mobility

This module is all about securing mobile devices and applications. You will learn about Mobile Device Management and how it works with Intune. You will also learn about how Intune and Azure AD can be used to secure mobile applications.

Lessons

- Plan for Mobile Application Management
- Plan for Mobile Device Management
- Deploy Mobile Device Management
- Enroll Devices to Mobile Device Management

After completing this module, students will be able to:

- Describe mobile application considerations.
- Use Intune to manage mobile applications.
- Manage devices with MDM.
- Compare MDM for Office 365 and Intune.
- Configure Domains for MDM.
- Manage Device Security Policies.
- Define Corporate Device Enrollment Policy.
- Enroll devices to MDM.
- Configure a Device Enrollment Manager Role.

Day 3

Module 1: Information Protection

This module explains information rights management in Exchange and SharePoint. It also describes encryption technologies used to secure messages. The module introduces how to implement Azure Information Protection and Windows Information Protection.

Lessons

- Information Rights Management
- Secure Multipurpose Internet Mail Extension
- Office 365 Message Encryption
- Azure Information Protection
- Advanced Information Protection
- Windows Information Protection

Lab: Data Loss Prevention

- Create and license users in your organization
- Configure MDM auto-enrollment
- Configure AIP and WIP

After completing this module, students will be able to:

- Describe the different Microsoft 365 Encryption Options.
- Describe the use of S/MIME.
- Describe how Office 365 Message Encryption works.
- Configure labels and policies for Azure Information Protection.
- Configure the advance AIP service settings for Rights Management Services (RMS) templates.
- Plan a deployment of Windows Information Protection policies.

Module 2: Data Loss Prevention

This module is all about data loss prevention in Microsoft 365. You will learn about how to create policies, edit rules, and customize user notifications.

Lessons

- Data Loss Prevention Explained
- Data Loss Prevention Policies
- Custom DLP Policies
- Creating a DLP Policy to Protect Documents
- Policy Tips

Lab: Data Loss Prevention

- Create and license users in your organization
- Create a DLP policy
- Testing DLP Policies

After completing this module, learners should be able to:

- Describe Data Loss Prevention (DLP).
- Recognize how actions and conditions work together for DLP.
- Use policy templates to implement DLP policies for commonly used information.
- Describe the different built-in templates for a DLP policies.
- Configure the correct rules for protecting content.
- Describe how to modify existing rules of DLP policies.
- Configure the user override option to a DLP rule.
- Describe how to work with managed properties for DLP policies.
- Explain how SharePoint Online creates crawled properties from documents.
- Describe the user experience when a user creates an email that contains sensitive information.

Module 3: Cloud Application Security

This module is all about cloud app security for Microsoft 365. The module will explain cloud discovery, app connectors, policies, and alerts.

Lessons

- Cloud Application Security Explained
- Using Cloud Application Security Information
- Office 365 Cloud App Security

After completing this module, students will be able to:

- Describe Cloud App Security.
- Explain how to deploy Cloud App Security.
- Control your Cloud Apps with Policies.
- Troubleshoot Cloud App Security.
- Use the Cloud App Catalog.
- Use the Cloud Discovery Dashboard.
- Prepare for Office 365 Cloud App Security.
- Manage cloud app permissions.

Day 4

Module 1: Archiving and Retention

This module explains concepts related to retention and archiving of data for Microsoft 365 including Exchange and SharePoint.

Lessons

- Archiving in Microsoft 365
- Retention in Microsoft 365
- Retention Policies in the Security and Compliance Center
- Archiving and Retention in Exchange
- In-place Records Management in SharePoint

Lab: Archiving and Retention

- Create and license users in your organization
- Configure Retention Tags and Policies
- MRM Retention Policies

After completing this module, you should be able to:

- Describe Data Governance in Microsoft 365.
- Describe the difference between In-Place Archive and Records Management.
- Explain how data is archived in Exchange.
- Recognize the benefits of In Place Records Management in SharePoint.
- Explain the difference between Message Records Management (MRM) in Exchange and Retention in Security and Compliance center.
- Explain how a retention policy works.
- Create a retention policy.
- Enable and disable In-Place Archiving.
- Create useful retention tags.

Module 2: Data Governance in Microsoft 365

This module focuses on data governance in Microsoft 365. The module will introduce you to Compliance Manager and discuss GDPR.

Lessons

- Planning Security and Compliance Needs
- Building Ethical Walls in Exchange Online
- Manage Retention in Email
- Troubleshooting Data Governance
- Analytics and Telemetry

After completing this module, you should be able to:

- Plan security and compliance roles.
- Describe what you need to consider for GDPR.
- Describe what an ethical wall in Exchange is and how it works.
- Work with retention tags in mailboxes
- Describe retention policies with email messages and email folders
- Explain how the retention age of elements is calculated.
- Repair retention policies that do not run as expected.

Module 3: Managing Search and Investigations

This module is focused on content searching and investigations. Specifically, it covers how to use eDiscovery to conduct advanced investigations of Microsoft 365 data. It also covers audit logs and discusses GDPR data subject requests.

Lessons

- Searching for Content in the Security and Compliance Center

- Audit Log Investigations
- Advanced eDiscovery

Lab: eDiscovery

- Create and license users in your organization
- Investigate your Microsoft 365 Data

After completing this module, you should be able to:

- Describe how to use content search.
- Designing your content search.
- Configuring search permission filtering.
- Describe what the audit log is and the permissions that are necessary to search the Office 365 audit log.
- Configure Audit Policies.
- Enter criteria for searching the audit log.
- Export search results to a CSV file.
- Describe what Advanced eDiscovery is and what requirements are needed.
- Analyze data in Advanced eDiscovery.
- Viewing the Advanced eDiscovery event log.
- Use Express Analytics.

Prerequisites

Learners should start this course already having the following skills:

- Basic conceptual understanding of Microsoft Azure
- Experience with Windows 10 devices
- Experience with Office 365
- Basic understanding of authorization and authentication
- Basic understanding of computer networks
- Working knowledge of managing mobile devices