MS-MS500T00: MICROSOFT 365 SECURITY ADMINISTRATION

DURATION	LEVEL	TECHNOLOGY	DELIVERY METHOD	TRAINING CREDITS
4 Days	Intermediate	Microsoft 365	Instructor-led	NA

INTRODUCTION

In this course you will learn how to secure user access to your organization's resources. The course covers user password protection, multi-factor authentication, how to enable Azure Identity Protection, how to setup and use Azure AD Connect, and introduces you to conditional access in Microsoft 365. You will learn about threat protection technologies that help protect your Microsoft 365 environment. Specifically, you will learn about threat vectors and Microsoft's security solutions to mitigate threats. You will learn about Secure Score, Exchange Online protection, Azure Advanced Threat Protection, Windows Defender Advanced Threat Protection, and threat management. In the course you will learn about information protection technologies that help secure your Microsoft 365 environment. The course discusses information rights managed content, message encryption, as well as labels, policies and rules that support data loss prevention and information protection. Lastly, you will learn about archiving and retention in Microsoft 365 as well as data governance and how to conduct content searches and investigations. This course covers data retention policies and tags, in-place records management for SharePoint, email retention, and how to conduct content searches that support eDiscovery investigations.

AUDIENCE PROFILE

The Microsoft 365 Security administrator collaborates with the Microsoft 365 Enterprise Administrator, business stakeholders and other workload administrators to plan and implement security strategies and to 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 hybrid environments. This role has strong skills and experience with identity protection, information protection, threat protection, security management and data governance.

PREREQUISTES

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.

COURSE OBJECTIVES

After completing this course, students will be able to:

- Administer user and group access in Microsoft 365.
- Explain and manage Azure Identity Protection.
- Plan and implement Azure AD Connect.
- Manage synchronized user identities.
- Explain and use conditional access.
- Describe cyber-attack threat vectors.
- Explain security solutions for Microsoft 365.

COURSE CONTENT

Module 1: User and Group Management

This module explains how to manage user accounts and groups in Microsoft 365. It introduces you to the Zero Trust concept as well as authentication. The module sets the

foundation for the remainder of the course.

Lessons

- Identity and Access Management concepts
- The Zero Trust model
- Plan your identity and authentication solution
- User accounts and roles
- Password Management

Lab: Initialize your tenant - users and groups

- Set up your Microsoft 365 tenant
- Manage users and groups

Lab: Password management

- Configure Self-service password reset (SSPR) for user accounts in Azure AD
- Deploy Azure AD Smart Lockout

After completing this module, students will be able to:

- Create and manage user accounts.
- Describe and use Microsoft 365 admin roles.
- Plan for password policies and authentication.
- Describe the concepts of Zero Trust security.
- Explain the Zero Trust model.

Module 2: Identity Synchronization and Protection

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

Lessons

- Plan directory synchronization
- Configure and manage synchronized identities
- Azure AD Identity Protection

Lab: Implement Identity Synchronization

- Set up your organization for identity synchronization

After completing this module, students will be able to:

- Explain directory synchronization.
- Plan directory synchronization.
- Describe and use Azure AD Connect.
- Configure Azure AD Connect Prerequisites.
- Manage users and groups with directory synchronization.
- Describe Active Directory federation.
- Enable Azure Identity Protection

Module 3: Identity and Access Management

This module explains 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. We discuss identity governance as a concept and its components.

Lessons

- Application Management
- Identity Governance
- Manage device access
- Role Based Access Control (RBAC)
- Solutions for external access
- Privileged Identity Management

Lab: Use Conditional Access to enable MFA

- MFA Authentication Pilot (require MFA for specific apps)
- MFA Conditional Access (complete an MFA roll out)

Lab: Configure Privileged Identity Management

- Manage Azure resources
- Assign directory roles
- Activate and deactivate PIM roles
- Directory roles
- PIM resource workflows
- View audit history for Azure AD roles in PIM

After completing this module, students will be able to:

- Describe the concept of conditional access.
- Describe and use conditional access policies.
- Plan for device compliance.
- Configure conditional users and groups.
- Configure role based access control
- Describe the concepts of identity governance
- Configure and use Privileged Identity Management

Module 4: Security in Microsoft 365

This module explains the various cyber-attack threats that exist. It then introduces you to the Microsoft solutions used to mitigate 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 strategy and principles
- Microsoft security solutions
- Secure Score

Lab: Use Microsoft Secure Score

- Improve your secure score in the Microsoft 365 Security Center

After completing this module, students will be able to:

- Describe several techniques attackers use to compromise user accounts through email.
- Describe techniques attackers use to gain control over resources.
- List the types of threats that can be avoided by using EOP and Microsoft Defender for Office 365.
- Describe the benefits of Secure Score and what kind of services can be analyzed.
- Describe how to use Secure Score to identify gaps in your current Microsoft 365 security posture.

Module 5: Threat Protection

This module explains the various threat protection technologies and services available for Microsoft 365. The module covers message protection through Exchange Online Protection, Microsoft Defender for Identity and Microsoft Defender for Endpoint.

Lessons

- Exchange Online Protection (EOP)
- Microsoft Defender for Office 365
- Manage Safe Attachments
- Manage Safe Links
- Microsoft Defender for Identity
- Microsoft Defender for Endpoint

Lab: Manage Microsoft 365 Security Services

- Implement Microsoft Defender Policies

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
- Configure Microsoft Defender for Identity.
- Configure Microsoft Defender for Endpoint.

Module 6: Threat Management

This module explains Microsoft Threat Management which provides you with the tools to evaluate and address cyber threats and formulate responses. You will learn how to use the Security dashboard and Azure Sentinel for Microsoft 365.

Lessons

- Security dashboard

- Threat investigation and response
- Azure Sentinel
- Advanced Threat Analytics

Lab: Using Attack Simulator

- Conduct a simulated Spear phishing attack
- Conduct simulated password attacks

After completing this module, students will be able to:

- 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 and trends.
- Describe what Advanced Thread Analytics (ATA) is and what requirements are needed to deploy it.
- Configure Advanced Threat Analytics.
- Use the attack simulator in Microsoft 365.
- Describe how Azure Sentinel can used for Microsoft 365.

Module 7: Microsoft Cloud Application Security

This module focuses on cloud application security in Microsoft 365. The module will explain cloud discovery, app connectors, policies, and alerts. You will learn how these features work to secure you cloud applications.

Lessons

- Deploy Cloud Application Security
- Use cloud application security information

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.
- Use the Cloud App Catalog.
- Use the Cloud Discovery dashboard.
- Manage cloud app permissions.

Module 8: Mobility

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

Lessons

- Mobile Application Management (MAM)
- Mobile Device Management (MDM)
- Deploy mobile device services
- Enroll devices to Mobile Device Management

Lab: Device Management

- Enable Device Management
- Configure Azure AD for Intune
- Create compliance and conditional access policies

After completing this module, students will be able to:

- Describe mobile application considerations.
- Manage devices with MDM.
- Configure Domains for MDM.
- Manage Device Security Policies.
- Enrol devices to MDM.
- Configure a Device Enrolment Manager Role.

Module 9: Information Protection and Governance

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

Lessons

- Information protection concepts
- Governance and Records Management
- Sensitivity labels
- Archiving in Microsoft 365
- Retention in Microsoft 365
- Retention policies in the Microsoft 365 Compliance Center
- Archiving and retention in Exchange
- In-place records management in SharePoint

Lab : Archiving and Retention

- Initialize compliance
- Configure retention tags and policies

After completing this module, students will be able to:

- Configure sensitivity labels.
- Configure archiving and retention in Microsoft 365.
- Plan and configure Records Management

Module 10: Rights Management and Encryption

This module explains information rights management in Exchange and SharePoint. The module also describes encryption technologies used to secure messages.

Lessons

- Information Rights Management (IRM)
- Secure Multipurpose Internet Mail Extension (S-MIME)
- Office 365 Message Encryption

Lab: Configure Office 365 Message Encryption

- Configure Office 365 Message Encryption
- Validate Information Rights Management

After completing this module, students will be able to:

- Describe the various Microsoft 365 Encryption Options.
- Describe the use of S/MIME.
- Describe and enable Office 365 Message Encryption.

Module 11: Data Loss Prevention

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

Lessons

- Data loss prevention fundamentals
- Create a DLP policy
- Customize a DLP policy
- Create a DLP policy to protect documents
- Policy tips

Lab: Implement Data Loss Prevention policies

- Manage DLP Policies
- Test MRM and DLP Policies

After completing this module, students will be able to:

- Describe Data Loss Prevention (DLP).
- Use policy templates to implement DLP policies for commonly used information.
- 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.
- Explain how SharePoint Online creates crawled properties from documents.

Module 12: Compliance Management

This module explains the Compliance center in Microsoft 365. It discusses the components of compliance score.

Lessons

- Compliance center

After completing this module, students will be able to:

- Describe how to use compliance score to make organizational decisions.
- Describe how assessments are used to determine compliance score.

Module 13: Insider Risk Management

This module focuses on insider risk related functionality within Microsoft 365. It covers not only Insider Risk Management in the compliance center but also information barriers

and privileged access management as well.

Lessons

- Insider Risk
- Privileged Access
- Information barriers
- Building ethical walls in Exchange Online

Lab: Privileged Access Management

- Set up privileged access management and process a request

After completing this module, students will be able to:

- Explain and configure Insider Risk Management in Microsoft 365.
- Configure and approve privileged access requests for global administrators.
- Configure and use information barriers to conform to organizational regulations.
- Build ethical walls in Exchange Online
- Configure Customer Lockbox

Module 14: Discover and Respond

This module focuses on content search and investigations. The module 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

- Content Search
- Audit Log Investigations
- Advanced eDiscovery

Lab: Manage Search and Investigation

- Investigate your Microsoft 365 Data
- Conduct a Data Subject Request

After completing this module, students will be able to:

- Conduct content searches in Microsoft 365
- Perform and audit log investigation.
- Configure Microsoft 365 for audit logging.
- Use Advanced eDiscovery

ASSOCIATED CERTIFICATIONS & EXAM

This course will prepare delegates to write the Microsoft MS-500: Microsoft 365 Security Administration exam