MS-500T00: Microsoft 365 Security Administration

Course Duration: 4 Days

Class times: 9am-4pm

Course Level: Intermediate

Language: English

Mode of Training: Virtually Instructor-Led

Prerequisites

Job Role: Administrator

Related Exam: MS-500

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.

Course Outline

Module 1: Create, configure, and manage identities.

Access to cloud-based workloads needs to be controlled centrally by providing a definitive identity for each user and resource. You can ensure employees and vendors have just-enough access to do their job.

Learning objectives

At the end of this module, you'll be able to:

- Create, configure, and manage users.

- Create, configure, and manage groups.
- Manage licenses.
- Explain custom security attributes and automatic user provisioning.

Module 2: Explore identity synchronization.

This module examines identity synchronization using Azure AD Connect and explores the authentication and provisioning options that can be used and the inner workings of directory synchronization.

Learning objectives

By the end of this module, you'll be able to:

- Describe the Microsoft 365 authentication and provisioning options.
- Explain directory synchronization.
- Explain how Azure AD Connect enables coexistence between your on-premises Active Directory environment and Microsoft 365

Module 3: Implement and manage hybrid identity.

Creating a hybrid-identity solution to use your on-premises active directory can be challenging. Explore how to implement a secure hybrid-identity solution.

Learning objectives

By the end of this module, you will be able to:

- Plan, design, and implement Azure Active Directory Connect (AADC)
- Manage Azure Active Directory Connect (AADC)
- Manage password hash synchronization (PHS)
- Manage pass-through authentication (PTA)
- Manage seamless single sign-on (seamless SSO)
- Manage federation excluding manual ADFS deployments.
- Troubleshoot synchronization errors.

- Implement and manage Azure Active Directory Connect Health

Module 4: Implement and manage external identities.

Inviting external users to use company Azure resources is a great benefit, but you want to do it in a secure way. Explore how to enable secure external collaboration.

Learning objectives

By the end of this module, you will be able to:

- Manage external collaboration settings in Azure Active Directory
- Invite external users (individually or in bulk)
- Manage external user accounts in Azure Active Directory
- Configure identity providers (social and SAML/WS-fed)

Module 5: Manage secure user access in Microsoft 365

This module examines various password-related tasks for user and admin accounts, such as creating and configuring password policies, configuring self-service password management, configuring multifactor authentication, and implementing entitlement packages and conditional access policies.

Learning objectives

By the end of this module, you'll be able to:

- Manage user passwords.
- Describe pass-through authentication.
- Enable multifactor authentication.
- Describe self-service password management.
- Implement Azure AD Smart Lockout
- Implement entitlement packages in Azure AD Identity Governance
- Implement conditional access policies.
- Create and perform an access review.

Module 6: Manage user authentication.

There are multiple options for authentication in Azure AD. Learn how to implement and manage the right authentications for users based on business needs.

Learning objectives

By the end of this module, you will be able to:

- Administer authentication methods (FIDO2 / Passwordless)
- Implement an authentication solution based on Windows Hello for Business
- Configure and deploy self-service password reset.
- Deploy and manage password protection.
- Implement and manage tenant restrictions.

Module 7: Plan, implement, and administer Conditional Access

Conditional Access gives a fine granularity of control over which users can do specific activities, access which resources, and how to ensure data and systems are safe.

Learning objectives

By the end of this module, you will be able to:

- Plan and implement security defaults.
- Plan conditional access policies.
- Implement conditional access policy controls and assignments (targeting, applications, and conditions).
- Test and troubleshoot conditional access policies.
- Implement application controls.
- Implement session management.
- Configure smart lockout thresholds.

Module 8: Plan and implement privileged access.

Ensuring that administrative roles are protected and managed to increase your Azure solution security is a must. Explore how to use PIM to protect your data and resources.

Learning objectives

By the end of this module, you will be able to:

- Define a privileged access strategy for administrative users (resources, roles, approvals, and thresholds)
- Configure Privileged Identity Management for Azure AD roles.
- Configure Privileged Identity Management for Azure resources.
- Assign roles.
- Manage PIM requests.
- Analyze PIM audit history and reports.
- Create and manage emergency access accounts.

Module 9: Plan and implement entitlement management.

When new users or external users join your site, quickly assigning them access to Azure solutions is a must. Explore how to entitle users to access your site and resources.

Learning objectives

By the end of this module, you will be able to:

- Define catalogues.
- Define access packages.
- Plan, implement and manage entitlements.
- Implement and manage terms of use.
- Manage the lifecycle of external users in Azure AD Identity Governance settings.

Module 10: Manage Azure AD Identity Protection

Protecting a user's identity by monitoring their usage and sign-in patterns will ensure a secure cloud solution. Explore how to design and implement Azure AD Identity protection.

Learning objectives

By the end of this module, you will be able to:

- Implement and manage a user risk policy.
- Implement and manage sign-in risk policies.
- Implement and manage MFA registration policy.
- Monitor, investigate, and remediate elevated risky users

Module 11: Protect against threats with Microsoft Defender for Endpoint

Learn how Microsoft Defender for Endpoint can help your organization stay secure.

Learning objectives

In this module, you will learn how to:

- Define the capabilities of Microsoft Defender for Endpoint.
- Understand how to hunt threats within your network.
- Explain how Microsoft Defender for Endpoint can remediate risks in your environment.

Module 12: Deploy the Microsoft Defender for Endpoint environment.

Learn how to deploy the Microsoft Defender for Endpoint environment, including onboarding devices and configuring security.

Learning objectives

Upon completion of this module, the learner will be able to:

- Create a Microsoft Defender for Endpoint environment.
- Onboard devices to be monitored by Microsoft Defender for Endpoint
- Configure Microsoft Defender for Endpoint environment settings.

Module 13: Protect against malicious attacks and unauthorized access with Microsoft Edge

Microsoft Edge helps protect your network and devices from malicious attacks and helps prevent unauthorized access to, and leaks of, corporate data with Microsoft Defender SmartScreen and Microsoft Defender Application Guard.

Learning objectives

At the end of this module, you will be able to:

- Describe how Microsoft Edge is built for secure browsing.
- Use Microsoft Defender SmartScreen and Application Guard to protect against malicious attacks and unauthorized access.
- Manage Microsoft Edge security options through policies and controls in Microsoft Endpoint Manager

Module 14: Understand Microsoft 365 encryption.

Learn how Microsoft 365 encrypts data-at-rest and in-transit, securely manages encryption keys, and provides key management options to customers to meet their business needs and compliance obligations.

Learning objectives

Upon completion of this module, you should be able to:

- Explain how encryption mitigates the risk of unauthorized data disclosure.
- Describe Microsoft data-at-rest and data-in-transit encryption solutions.
- Explain how Microsoft 365 implements service encryption to protect customer data at the application layer.
- Understand the differences between Microsoft managed keys and customer managed keys for use with service encryption.

Module 15: Understand app management using Microsoft Intune

As part of application management, Microsoft Intune helps you configure apps, protect app data, manage app policy assignments, and implement app security rules.

Learning objectives

In this module, you will:

- Understand how your organization's apps can be configured and protected.
- Understand the app management lifecycle.
- Learn about the data protection framework using app protection policies.

Module 16: Manage device compliance.

This module examines device compliance policies, how organizations effectively use them, how to create policies and configure conditional users and groups, how to build Conditional Access policies, and how to monitor enrolled devices.

Learning objectives

By the end of this module, you'll be able to:

- Plan for device compliance by defining the rules and settings that must be configured on a device for it to be considered compliant.
- Configure conditional users and groups for deploying profiles, policies, and apps.
- Create Conditional Access policies to implement automated access control decisions for accessing your cloud apps.
- Monitor enrolled devices to control their Intune activities and compliance status.

Module 17: Remediate risks with Microsoft Defender for Office 365

Learn about the Microsoft Defender for Office 365 component of Microsoft 365 Defender.

Learning objectives

In this module, you will learn how to:

- Define the capabilities of Microsoft Defender for Office 365.
- Understand how to simulate attacks within your network.
- Explain how Microsoft Defender for Office 365 can remediate risks in your environment.

Module 18: Query, visualize, and monitor data in Microsoft Sentinel

This module describes how to query, visualize, and monitor data in Microsoft Sentinel.

Learning objectives

In this module you will:

- Visualize security data using Microsoft Sentinel Workbooks.
- Understand how queries work.
- Explore workbook capabilities.
- Create a Microsoft Sentinel Workbook.

Module 19: Create and manage sensitive information types.

Learn how to use sensitive information types to support your information protection strategy.

Learning objectives

After completing this module, you will be able to:

- Recognize the difference between built-in and custom sensitivity labels.
- Configure sensitive information types with exact data match-based classification.
- Implement document fingerprinting.
- Create custom keyword dictionaries.

Module 20: Apply and manage sensitivity labels.

Learn about how sensitivity labels are used to classify and protect business data while making sure that user productivity and their ability to collaborate are not hindered.

Learning objectives

After completing this module, you will be able to:

- Apply sensitivity labels to Microsoft Teams, Microsoft 365 groups, and SharePoint sites.
- Monitor label usage using label analytics.
- Configure on-premises labelling.

- Manage protection settings and marking for applied sensitivity labels.
- Apply protections and restrictions to email.
- Apply protections and restrictions to files.

Module 21: Prevent data loss in Microsoft Purview

Learn how to discover, classify, and protect sensitive and business-critical content throughout its lifecycle across your organization.

Learning objectives

When you finish with this module, you'll be able to:

- Discuss the data loss prevention solution and its benefits.
- Describe the data loss prevention configuration process.
- Explain what users will experience when the solution is implemented.

Module 22: Manage data loss prevention policies and reports in Microsoft 365

Learn how to manage data loss prevention policies and mitigate data loss prevention policy violations.

Learning objectives

After completing this module, you'll be able to:

- Review and analyze DLP reports.
- Manage permissions for DLP reports.
- Identify and mitigate DLP policy violations.
- Mitigate DLP violations in Microsoft Defender for Cloud Apps.

Module 23: Manage the data lifecycle in Microsoft Purview

Learn how to manage your content lifecycle using solutions to import, store, and classify business-critical data so you can keep what you need and delete what you don't.

Learning objectives

Upon completion of this module, you should be able to:

- Discuss the Data Lifecycle Management solution and its benefits.
- List the customer scenarios the Data Lifecycle Management solution addresses.
- Describe the Data Lifecycle Management configuration process.
- Explain what users will experience when the solution is implemented.
- Articulate deployment and adoption best practices.

Module 24: Manage data retention in Microsoft 365 workloads.

Learn how to manage retention for Microsoft 365, and how retention solutions are implemented in the individual Microsoft 365 services.

Learning objectives

After completing this module, you will be able to:

- Describe the retention features in Microsoft 365 workloads.
- Configure retention settings in Microsoft Teams, Yammer, and SharePoint Online.
- Recover content protected by retention settings.
- Regain protected items from Exchange Mailboxes.

Module 25: Manage records in Microsoft Purview

Learn how to use intelligent classification to automate and simplify the retention schedule for regulatory, legal, and business-critical records in your organization.

Learning objectives

Upon completion of this module, you should be able to:

- Discuss the Microsoft Purview Records Management solution and its benefits.
- List the customer scenarios the Microsoft Purview Records Management solution addresses.
- Describe the Microsoft Purview Records Management configuration process.

- Explain what users will experience when the solution is implemented.
- Articulate deployment and adoption best practices.

Module 26: Manage compliance in Microsoft 365 and Exchange Online

Learn how compliance works in an Exchange Online environment. Learn how to use retention and data loss prevention policies to keep the data and communications you're required to maintain, how to find that data and communications, and how to ensure you're ready for an audit.

Learning objectives

At the end of this module, you should be able to:

- Explain retention policies.
- Explain data loss prevention policies.
- Explain audit logs.
- Explain content search.

Module 27: Manage Microsoft Purview eDiscovery (Premium)

This module explores how to use Microsoft Purview eDiscovery (Premium) to preserve, collect, analyze, review, and export content that's responsive to an organization's internal and external investigations, and communicate with custodians involved in a case.

Learning objectives

By the end of this module, you'll be able to:

- Describe how Microsoft Purview eDiscovery (Premium) builds on eDiscovery (Standard).
- Describe the basic workflow of eDiscovery (Premium).
- Create and manage cases in eDiscovery (Premium).
- Manage custodians and non-custodial data sources.
- Analyze case content and use analytical tools to reduce the size of search result sets.

Module 28: Manage regulatory and privacy requirements with Microsoft Priva

Learn how to use Microsoft Priva to manage privacy risk policies and subject rights requests.

Learning objectives

Upon completion of this module, the learner will be able to:

- Create and manage risk management policies for data overexposure, data transfer, and data minimization.
- Investigate and remediate risk alerts.
- Send user notifications.
- Create and manage Subject Rights Requests
- Estimate and retrieve subject data.
- Review subject data.
- Create subject rights reports.

Module 29: Prepare Microsoft Purview Communication Compliance

Microsoft Purview Communication Compliance is a solution that helps organizations address code-of-conduct policy violations in company communications, while also assisting organizations in regulated industries meet specific supervisory compliance requirements. Communication Compliance uses machine learning to intelligently detect violations across different communication channels such as Microsoft Teams, Exchange Online, or Yammer messages.

Learning objectives

Upon completion of this module, you should be able to:

- List the enhancements in communication compliance over Office 365 Supervision policies, which it will replace.
- Explain how to identify and remediate code-of-conduct policy violations.
- List the prerequisites that need to be met before creating communication compliance policies.
- Describe the types of built-in, pre-defined policy templates.

Module 30: Manage insider risk in Microsoft Purview

Microsoft Purview Insider Risk Management helps organizations address internal risks, such as IP theft, fraud, and sabotage. Learn about insider risk management and how Microsoft technologies can help you detect, investigate, and take action on risky activities in your organization.

Learning objectives

Upon completion of this module, you should be able to:

- Explain how Microsoft Purview Insider Risk Management can help prevent, detect, and contain internal risks in an organization.
- Describe the types of built-in, pre-defined policy templates.
- List the prerequisites that need to be met before creating insider risk policies.
- Explain the types of actions you can take on an insider risk management case.

Module 31: Plan information barriers

Information barriers enable administrators to define policies to allow or prevent communications between groups of users in Microsoft Teams chats and channels. When information barrier policies are in place, people who should not communicate with other specific users won't be able to find, select, chat, or call those users. With information barriers, checks are in place to prevent unauthorized communication.

Learning objectives

Upon completion of this module, you should be able to:

- Describe how information barrier policies can help your organization maintain compliance with relevant industry standards and regulations and avoid potential conflicts of interest.
- List the types of situations when information barriers would be applicable.
- Explain the process of creating an information barrier policy.
- Explain how to troubleshoot unexpected issues after information barriers are in place.

Module 32: Implement privileged access management.

Privileged access management allows granular access control over privileged admin tasks in Office 365. Privileged access management requires users to request just-in-time access to complete elevated and privileged tasks through a highly scoped and time-bound approval workflow. This configuration gives users just-enough-access to perform the task at hand without risking exposure of sensitive data or critical configuration settings.

Learning objectives

Upon completion of this module, you should be able to:

- Explain the difference between privileged access management and privileged identity management.
- Describe the privileged access management process flow.
- Describe how to configure and enable privileged access management.

Module 33: Manage Customer Lockbox

Customer Lockbox supports requests to access data in Exchange Online, SharePoint Online, and OneDrive when Microsoft engineers need to access customer content to determine root cause and fix an issue. Customer Lockbox requires the engineer to request access from the customer as a final step in the approval workflow. This gives organizations the option to approve or deny these requests and provide direct-access control to the customer.

Learning objectives

Upon completion of this module, you should be able to:

- Describe the Customer Lockbox workflow.
- Explain how to approve or deny a Customer Lockbox request.
- Explain how you can audit actions performed by Microsoft engineers when access requests are approved.