CISSP | CEH | PKI | SECURITY

MS-500: Microsoft 365 Security Administration

$2,595.00

- 4 Days

Upcoming Dates

Jan 07 - Jan 10
Mar 31 - Apr 03
Jun 23 - Jun 26

Course Description

Day 1: Managing Microsoft 365 Identity and Access (MS-500T01-A)

Help protect against credential compromise with identity and access management. In this course you will learn how to secure user access to your organization's resources. Specifically, this course covers user password protection, multi-factor authentication, how to enable Azure Identity Protection, how to configure Active Directory federation services, how to setup and use Azure AD Connect, and introduces you to Conditional Access. You will also learn about solutions for managing external access to your Microsoft 365 system.

Day 2: Implementing Microsoft 365 Threat Protection (MS-500T02-A)

Threat protection helps stop damaging attacks with integrated and automated security. In this course 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 for them. You will learn about Secure Score, Exchange Online protection, Azure Advanced Threat Protection, Windows Defender Advanced Threat Protection, and how to use Microsoft 365 Threat Intelligence. It also discusses securing mobile devices and applications. The goal of this course is to help you configure your Microsoft 365 deployment to achieve your desired security posture.

Day 3: Implementing Microsoft 365 Information Protection (MS-500T03-A)

Information protection is the concept of locating and classifying data anywhere it lives. In this course you will learn about information protection technologies that help secure your Microsoft 365 environment. Specifically, this course discusses information rights managed content, message encryption, as well as labels, policies and rules that support data loss prevention and information protection. Lastly, the course explains the deployment of Microsoft Cloud App Security.

Day 4: Administering Microsoft 365 Built-in Compliance (MS-500T04-A)

Internal policies and external requirements for data retention and investigation may be necessary for your organization. In this course you will learn about archiving and retention in Microsoft 365 as well as data governance and how to conduct content searches and investigations. Specifically, 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. The course also helps your organization prepare for Global Data Protection Regulation (GDPR).

Course Outline

Day 1: Managing Microsoft 365 Identity and Access (MS-500T01-A)

Course Outline

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

Day 2: Implementing Microsoft 365 Threat Protection (MS-500T02-A)

Course Outline

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

Day 3: Implementing Microsoft 365 Information Protection (MS-500T03-A)

Course Outline

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.

Day 4: Administering Microsoft 365 Built-in Compliance (MS-500T04-A)

Course Outline

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

Audience

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.

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

What You Will Learn

Day 1: Managing Microsoft 365 Identity and Access (MS-500T01-A)

After completing this course, students should 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.

Day 2: Implementing Microsoft 365 Threat Protection (MS-500T02-A)

After completing this course, students will be able to:

- 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.

Day 3: Implementing Microsoft 365 Information Protection (MS-500T03-A)

After completing this course, learners should be able to:

- 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.

Day 4: Administering Microsoft 365 Built-in Compliance (MS-500T04-A)

After completing this course, learners should be able to:

- 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.