Course Outline

MS-500: Microsoft 365 Security Administration

Course Summary

Description

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. Students 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.

Students will also 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. Student 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).

Objectives

After taking 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.
- 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.

Topics

- User and Group Security
- Identity Synchronization
- Federated Identities
- Access Management
- Security in Microsoft 365
- Advanced Threat Protection
- Threat Intelligence
- Information Protection
- Data Loss Prevention
- Cloud Application Security
- Archiving and Retention
- Data Governance in Microsoft 365
- Managing Search and Investigations

Course Summary (cont'd)

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.

Duration

Five days

Course Outline

MS-500: Microsoft 365 Security Administration

Course Outline

I. 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.

A. User Accounts in Microsoft 365
B. Administrator Roles and Security Groups in Microsoft 365
C. Password Management in Microsoft 365
D. 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

II. 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.

A. Introduction to Identity Synchronization
B. Planning for Azure AD Connect
C. Implementing Azure AD Connect
D. Managing Synchronized Identities

Lab : Implementing Identity Synchronization

- Setting up your organization for identity synchronization

III. 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.

A. Introduction to Federated Identities
B. Planning an AD FS Deployment
C. Implementing AD FS

IV. 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.

A. Conditional Access
B. Managing Device Access
C. Role Based Access Control (RBAC)
D. Solutions for External Access

V. 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.

A. Threat Vectors and Data Breaches
B. Security Solutions for Microsoft 365
C. Microsoft Secure Score

VI. 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.

A. Exchange Online Protection
B. Office 365 Advanced Threat Protection
C. Managing Safe Attachments
D. Managing Safe Links
E. Azure Advanced Threat Protection
F. 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

VII. 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.

D. Microsoft 365 Threat Intelligence
E. Using the Security Dashboard
F. Configuring Advanced Threat Analytics
G. Lab : Advanced Threat Analytics
H. Enabling and installing the ATA Center

Course Outline

MS-500: Microsoft 365 Security Administration

Course Outline (cont'd)

VIII. 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.

A. Plan for Mobile Application Management
B. Plan for Mobile Device Management
C. Deploy Mobile Device Management
D. Enroll Devices to Mobile Device Management

IX. 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.

A. Information Rights Management
B. Secure Multipurpose Internet Mail Extension
C. Office 365 Message Encryption
D. Azure Information Protection
E. Advanced Information Protection
F. Windows Information Protection

Lab : Data Loss Prevention

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

X. 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.

A. Data Loss Prevention Explained
B. Data Loss Prevention Policies
C. Custom DLP Policies
D. Creating a DLP Policy to Protect Documents
E. Policy Tips

Lab : Data Loss Prevention

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

XI. 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.

A. Cloud Application Security Explained
B. Using Cloud Application Security Information
C. Office 365 Cloud App Security

XII. Archiving and Retention

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

A. Archiving in Microsoft 365
B. Retention in Microsoft 365
C. Retention Policies in the Security and Compliance Center
D. Archiving and Retention in Exchange
E. 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

XIII. 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.

A. Planning Security and Compliance Needs
B. Building Ethical Walls in Exchange Online
C. Manage Retention in Email
D. Troubleshooting Data Governance
E. Analytics and Telemetry
F. Repair retention policies that do not run as expected.

XIV. 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.

A. Searching for Content in the Security and Compliance Center
B. Audit Log Investigations
C. Advanced eDiscovery

Lab : eDiscovery

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