KOENIG
step forward

Microsoft
Solutions Partner
Microsoft Cloud
Training Services

MS-500: Microsoft 365 Security Administration

Duration: 32 Hours (4 Days)

Course Overview

The MS-500: Microsoft 365 Security Administration course is designed to provide comprehensive security administration training, enabling IT professionals to manage and secure Microsoft 365 enterprise environments. This course prepares learners for the ms-500 certification, highlighting the importance of Zero Trust Security principles, Identity and access management, Threat protection, Information protection, and Compliance features within Microsoft 365. Learners will gain hands-on experience through labs, enhancing their skills in configuring and managing Security and compliance solutions, responding to threats, and enforcing data governance. By mastering the content taught in the course, professionals will be equipped to implement and oversee Security and compliance solutions for Microsoft 365 and Hybrid environments, a crucial skill set for modern IT security administration roles.

Audience profile

The MS-500: Microsoft 365 Security Administration course is tailored for IT professionals seeking to secure Microsoft 365 enterprise environments.

- IT Security Specialists
- Systems Administrators
- Network Administrators
- IT Professionals with a focus on Microsoft 365
- Cybersecurity Analysts
- Security Engineers
- Compliance Officers
- Enterprise Architects
- Technical Support Staff specializing in Microsoft 365
- Identity and Access Management Consultants
- Cloud Solutions Architects
- Information Security Managers
- IT Managers and Directors looking to implement or oversee Microsoft 365 security solutions

Course Syllabus

Module 1: User and Group Protection

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

- Identity and Access Management Concepts
- Zero Trust Security
- User Accounts in Microsoft 365
- Administrator Roles and Security Groups in Microsoft 365
- Password Management in Microsoft 365

- Azure AD Identity Protection

Lab: Initialize your trial tenant

- Set up your Microsoft 365 tenant

Lab: Configure Privileged Identity Management

- Discover and Manage Azure Resources
- Assign Directory Roles
- Activate and Deactivate PIM Roles
- Directory Roles (General)
- PIM Resource Workflows
- View audit history for Azure AD roles in PIM

Module 2: Identity Synchronization

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

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

Lab: Implement Identity Synchronization

- Set up your organization for identity synchronization

Module 3: 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.

Lessons

- Conditional access
- Manage device access
- Role Based Access Control (RBAC)
- Solutions for external access

Lab: Use Conditional Access to enable MFA

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

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
- Security solutions in Microsoft 365
- Microsoft Secure Score

Lab: Use Microsoft Secure Score

- Improve your secure score in the Microsoft 365 Security Center

Module 5: Advanced 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, Azure Advanced Threat Protection and Windows Defender Advanced Threat Protection.

Lessons

- Exchange Online Protection
- Office 365 Advanced Threat Protection
- Manage Safe Attachments
- Manage Safe Links
- Azure Advanced Threat Protection
- Microsoft Defender Advanced Threat Protection

Lab: Manage Microsoft 365 Security Services

- Implement ATP Policies

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. The module also explains and configures Microsoft Advanced Threat Analytics.

Lessons

- Use the Security dashboard
- Microsoft 365 threat investigation and response
- Azure Sentinel for Microsoft 365
- Configuring Advanced Threat Analytics

Lab: Using Attack Simulator

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

Module 7: 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

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

Lab: Configure Azure AD for Intune

- Enable Device Management
- Configure Azure AD for Intune
- Create Intune Policies

Module 8: Information Protection

The module explains how to implement Azure Information Protection and Windows Information Protection.

Lessons

- Information Protection Concepts
- Azure Information Protection
- Advanced Information Protection
- Windows Information Protection

Lab: Implement Azure Information Protection and Windows Information Protection

- Implement Azure Information Protection
- Implement Windows Information Protection

Module 9: 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
- Secure Multipurpose Internet Mail Extension
- Office 365 Message Encryption

Lab: Configure Office 365 Message Encryption

- Configure Office 365 Message Encryption
- Validate Information Rights Management

Module 10: 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 Explained
- Data Loss Prevention Policies
- Custom DLP Policies
- Creating a DLP Policy to Protect Documents
- Policy Tips

Lab: Implement Data Loss Prevention policies

- Manage DLP Policies
- Test MRM and DLP Policies

Module 11: 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

- Cloud App Security Explained
- Using Cloud Application Security Information

Module 12: Compliance in Microsoft 365

This module focuses on data governance in Microsoft 365. The module will introduce you to Compliance Manager and discuss Global Data Protection Regulations (GDPR).

Lessons

- Plan for compliance requirements
- Build ethical walls in Exchange Online
- Manage Retention in Email
- Troubleshoot Data Governance

Module 13: 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 Microsoft 365 Compliance Center
- Archiving and Retention in Exchange
- In-place Records Management in SharePoint

Lab: Compliance and Retention

- Initialize Compliance
- Configure retention tags and policies

Module 14: Content Search and Investigation

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