MS-500: Microsoft 365 Security Administration

(4 Day)

Overview

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.

Job role: Administrator

Skills gained

- Administer user and group access in Microsoft 365.
- Describe and manage Azure Identity Protection features.
- Plan and implement Azure AD Connect.
- Manage synchronized 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.
- Configure various advanced threat protection services for Microsoft 365.
- Configure Advanced Threat Analytics.
- Plan and deploy secure mobile devices.
- Implement information rights management.
- Secure messages in Office 365.
- Configure Data Loss Prevention policies.
- Deploy and manage Cloud App Security.
- Implement Windows information protection for devices.
- Plan and deploy a data archiving and retention system.
- Create and manage an eDiscovery investigation.
- Manage GDPR data subject requests.

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.

Course Outline

Module 1: User and Group Protection

- 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

Module 2: Identity Synchronization

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

Module 3: Access Management

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

Module 4: Security in Microsoft 365

- Threat vectors and data breaches
- Security strategy and principles
- Security solutions in Microsoft 365
- Microsoft Secure Score

Module 5: Advanced Threat Protection

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

Module 6: Threat Management

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

Module 7: Mobility

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

Module 8: Information Protection

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

Module 9: Rights Management and Encryption

- Information Rights Management
- Secure Multipurpose Internet Mail Extension
- Office 365 Message Encryption

Module 10: Data Loss Prevention

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

Module 11: Cloud Application Security

- Cloud App Security Explained
- Using Cloud Application Security Information

Module 12: Compliance in Microsoft 365

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

Module 13: Archiving and Retention

- 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

Module 14: Content Search and Investigation

- Content Search
- Audit Log Investigations
- Advanced eDiscovery