

Microsoft 365 Security Administration



Length: 5 days

Format: Bootcamp

Time: Day



About This Course

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.

Required Exams

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 ensure 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 Objectives

By completing this course, students will learn how to:

- * Administer user and group access in Microsoft 365.
- * Explain and manage Azure Identity Protection.
- * Plan and implement Azure AD Connect.
- * Manage synchronized user identities.
- * Explain and use conditional access.
- * Describe cyber-attack threat vectors.
- * Explain security solutions for Microsoft 365.
- * Use Microsoft Secure Score to evaluate and improve your security posture.
- * Configure various advanced threat protection services for Microsoft 365.
- * Plan for 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.
- * Explain and use sensitivity labels.

Outline

Module 1: User and Group Management

This module explains how to manage user accounts and groups in Microsoft 365. It introduces you to the Zero Trust concept as well as authentication. The module sets the foundation for the remainder of the course.

Lessons

- * Identity and Access Management concepts
- * The Zero Trust model
- * Plan your identity and authentication solution
- * User accounts and roles
- * Password Management

Module 2: Identity Synchronization and Protection

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

- * Plan directory synchronization
- * Configure and manage synchronized identities
- * Azure AD Identity Protection

Module 3: Identity and 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. We discuss identity governance as a concept and its components..

Lessons

- * Application Management
- * Identity Governance
- * Manage device access
- * Role Based Access Control (RBAC)
- * Solutions for external access
- * Privileged Identity Management

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
- * Microsoft security solutions
- * Secure Score

Module 5: 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, Microsoft Defender for Identity and Microsoft Defender for Endpoint..

Lessons

- * Exchange Online Protection (EOP)
- * Microsoft Defender for Office 365
- * Manage Safe Attachments
- * Manage Safe Links
- * Microsoft Defender for Identity
- * Microsoft Defender for Endpoint

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.

Lessons

- * Security dashboard
- * Threat investigation and response
- * Azure Sentinel
- * Advanced Threat Analytics

Module 7: Microsoft 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 your cloud applications.

Lessons

- * Deploy Cloud Application Security
- * Use cloud application security information

Module 8: 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

- * Mobile Application Management (MAM)

- * Mobile Device Management (MDM)
- * Deploy mobile device services
- * Enroll devices to Mobile Device Management

Module 9: Information Protection and Governance

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

- * Information protection concepts
- * Governance and Records Management
- * Sensitivity labels
- * 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 10: 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 (IRM)
- * Secure Multipurpose Internet Mail Extension (S-MIME)
- * Office 365 Message Encryption

Module 11: 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 fundamentals
- * Create a DLP policy

- * Customize a DLP policy
- * Create a DLP policy to protect documents
- * Policy tips

Module 12: Compliance Management

This module explains the Compliance center in Microsoft 365. It discusses the components of compliance score.

Lessons

- * Compliance center

Module 13: Insider Risk Management

This module focuses on insider risk related functionality within Microsoft 365. It covers not only Insider Risk Management in the compliance center but also information barriers and privileged access management as well.

Lessons

- * Insider Risk
- * Privileged Access
- * Information barriers
- * Information barriers

Module 14: Discover and Respond

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