Microsoft 365 Security Administration Fast Track

Duration: 5 Days

Who should attend:

In this course you will learn how to secure user access to your organization's Microsoft 365 resources using the security & compliance features of Microsoft Entra ID, Microsoft Defender and Microsoft Purview as they pertain to Microsoft 365. This includes user password protection, multi-factor authentication, Identity Protection, Microsoft Entra Connect, and conditional access in Microsoft 365. You will also 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, Microsoft 365 Defender, and threat management. In the course you will learn about information protection technologies from Microsoft Purview. 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.

Pre-requisites:

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.

Content

Module 1: User and Group Management

This module explains how to manage user accounts and groups in Microsoft 365. The module sets the foundation for the remainder of the course.

Lessons

Microsoft 365 Security Administration Fast Track

- Identity and Access Management concepts
- Plan your identity and authentication solution
- User accounts and roles
- Password Management

Lab : Initialize your tenant – users and groups

- Set up your Microsoft 365 tenant
- Manage users and groups

Lab : Password management

- Configure Self-service password reset (SSPR) for user accounts in Entra ID
- Deploy Entra ID Smart Lockout

After completing this module, students will be able to:

- Create and manage user accounts.
- Describe and use Microsoft 365 admin roles.
- Plan for password policies and authentication.

Module 2: Identity Synchronization and Protection

This module explains concepts related to synchronizing identities for Microsoft 365. Specifically, it focuses on Microsoft Entra 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
- Entra ID Identity Protection

Lab : Implement Identity Synchronization

Microsoft 365 Security Administration Fast Track

- Set up your organization for identity synchronization

After completing this module, students will be able to:

- Explain directory synchronization.
- Plan directory synchronization.
- Describe and use Microsoft Entra Connect.
- Configure Microsoft Entra Connect Prerequisites.
- Manage users and groups with directory synchronization.
- Describe directory federation.
- Enable Entra ID 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

Lab : Use Conditional Access to enable MFA

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

Lab : Configure Privileged Identity Management

Microsoft 365 Security Administration Fast Track

- Manage Azure resources
- Assign directory roles
- Activate and deactivate PIM roles
- Directory roles
- PIM resource workflows
- View audit history for admin roles in PIM

After completing this module, students will be able to:

- Describe the concept of conditional access.
- Describe and use conditional access policies.
- Plan for device compliance.
- Configure conditional users and groups.
- Configure role based access control
- Describe the concepts of identity governance
- Configure and use 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

- Zero Trust
- Threat vectors and data breaches
- Security strategy and principles
- Microsoft security solutions
- Secure Score

Lab : Use Microsoft Secure Score

- Improve your secure score in the Microsoft 365 Defender Portal

Microsoft 365 Security Administration Fast Track

After completing this module, students will be able to:

- Describe several techniques attackers use to compromise user accounts through email.
- Describe techniques attackers use to gain control over resources.
- List the types of threats that can be avoided by using EOP and Microsoft Defender for Office 365.
- Describe the benefits of Secure Score and what kind of services can be analyzed.
- Describe how to use Secure Score to identify gaps in your current Microsoft 365 security posture.

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

Lab : Manage Microsoft 365 Security Services

- Implement Microsoft Defender Policies

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
- Configure Microsoft Defender for Identity.
- Configure Microsoft Defender for Endpoint.

Microsoft 365 Security Administration Fast Track

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 Microsoft Sentinel for Microsoft 365.

Lessons

- Security dashboard
- Threat investigation and response
- Microsoft Sentinel

Lab : Using Attack Simulator

- Conduct a simulated Spear phishing attack

After completing this module, students will be able to:

- Describe how Threat Explorer can be used to investigate threats and help to protect your tenant.
- Describe how the Security Dashboard gives C-level executives insight into top risks and trends.
- Use the attack simulator in Microsoft 365.
- Describe how Microsoft Sentinel can used for Microsoft 365.

Module 7: Microsoft Defender for Cloud Apps

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

- Defender for Cloud Apps
- Use Defender for Cloud Apps information

Microsoft 365 Security Administration Fast Track

After completing this module, students will be able to:

- Describe Defender for Cloud Apps.
- Explain how to deploy Defender for Cloud Apps.
- Control your Cloud Apps with Policies.
- Use the Cloud App Catalog.
- Manage cloud app permissions.

Module 8: Mobility

This module explains mobile application and device management.

Lessons

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

After completing this module, students will be able to:

- Describe how to manage mobile devices in the enterprise

Module 9: Microsoft Purview Compliance portal

This module explains the Microsoft Purview Compliance portal.

Lessons

- Microsoft Purview Compliance portal
- Protect your sensitive data with Microsoft Purview
- What is Compliance Manager?

Microsoft 365 Security Administration Fast Track

After completing this module, students will be able to:

- Understand the Microsoft Purview Compliance portal

Module 10: 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

- Archiving and retention in Exchange
- Retention in Microsoft 365
- Retention policies in the Microsoft Purview Compliance Portal
- Governance and records management
- Information protection concepts
- Sensitivity labels

Lab : Archiving and Retention

After completing this module, students will be able to:

- Configure archiving and retention in Microsoft 365.
- Plan and configure Records Management

Module 11: Microsoft 365 Encryption

This module explains information rights management in Exchange and SharePoint. The module also describes encryption technologies used to secure messages.

Lessons

Microsoft 365 Security Administration Fast Track

- Microsoft 365 Encryption
- Deploy message encryption in Microsoft Purview

Lab : Configure Purview Message Encryption

After completing this module, students will be able to:

- Describe the various Microsoft 365 Encryption Options.

Module 12: 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
- Building ethical walls in Exchange Online

Lab : Privileged Access Management

- Set up privileged access management and process a request

After completing this module, students will be able to:

- Explain and configure Insider Risk Management in Microsoft 365.
- Configure and approve privileged access requests for global administrators.
- Configure and use information barriers to conform to organizational regulations.
- Build ethical walls in Exchange Online
- Configure Customer Lockbox

Microsoft 365 Security Administration Fast Track

Module 13: 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 data subject requests.

Lessons

- eDiscovery
- Content Search
- Audit Log Investigations

Lab : Manage Search and Investigation

- Investigate your Microsoft 365 Data
- Respond to a data subject request using eDiscovery

After completing this module, students will be able to:

- Conduct content searches in Microsoft 365
- Perform and audit log investigation.
- Configure Microsoft 365 for audit logging.
- Use eDiscoveryInformation protection concepts