MS-500T00: Microsoft® 365 Security Administration

Duration: 4 Days
Method: Instructor-Led Training (ILT) | Live Online Training

Course Description

In this course, participants will learn to implement, manage, and monitor security and compliance solutions for Microsoft 365 and hybrid environments. This course will teach participants to secure Microsoft 365 enterprise environments, respond to threats, perform investigations, and enforce data governance. This course will also teach participants to plan and implement security strategies that comply with their organization's policies and regulations. Lastly, participants will become familiar with Microsoft 365 workloads and gain skills and experience in identity protection, information protection, threat protection, security management, and data governance.

Target Audience

This course is intended for:
- IT Professionals
- Persons who are aspiring to the Microsoft 365 Security Administration role.

Prerequisites

To attend this course, candidates must have:
- 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 Objectives

Upon successful completion of this course, attendees will be able 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.

Course Topics

Module 1: User and Group Management

- 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

- Plan Directory Synchronization
- Configure and Manage Synchronized Identities
- Azure AD Identity Protection

Course Topics *Continued*

Module 3: Identity and Access Management
- 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
- Threat Vectors and Data Breaches
- Security Strategy and Principles
- Microsoft Security Solutions
- Secure Score

Module 5: Threat Protection
- 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
- Security Dashboard
- Threat Investigation and Response
- Azure Sentinel
- Advanced Threat Analytics

Module 7: Microsoft Cloud Application Security
- Deploy Cloud Application Security
- Use Cloud Application Security Information

Module 8: Mobility
- Mobile Application Management (MAM)
- Mobile Device Management (MDM)
- Deploy Mobile Device Services
- Enrol Devices to Mobile Device Management

Tel: 876-978-1107 / 876-978-1486
WhatsApp: 876-978-9353
E-Mail: training@RWTTS.com | **Website:** www.RWTTS.com

Microsoft Partner

Course Topics *Continued*

Module 9: Information Protection and Governance
- Information Protection Concepts
- Governance and Records Management
- Sensitivity Labels
- Archiving in Microsoft 365
- Retention in Microsoft 365
- Retention Policies in The Microsoft 365 Compliance Centre
- Archiving and Retention in Exchange
- In-Place Records Management in SharePoint

Module 10: Rights Management and Encryption
- Information Rights Management (IRM)
- Secure Multipurpose Internet Mail Extension (S-MIME)
- Office 365 Message Encryption

Module 11: Data Loss Prevention (DLP)
- 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
- Compliance Centre

Module 13: Insider Risk Management
- Insider Risk
- Privileged Access
- Information Barriers
- Building Ethical Walls in Exchange Online

Module 14: Discover and Respond
- Content Search
- Audit Log Investigations
- Advanced eDiscovery

LABS INCLUDED