

MS-500T00A: Microsoft 365 Security Administration

COURSE OVERVIEW

Learn how to secure your Microsoft 365 deployment and comply with industry data protections. This course focuses on securing user identity and access, threat protection, information protection and data governance. This course was designed for IT Professionals who manage and deploy security technologies for Microsoft 365 in their organization. The course is for the Microsoft 365 Security Administrator job role. It helps learners prepare for the Microsoft 365 Certified: Security Administrator Associate exam (MS-500).

WHO SHOULD ATTEND?

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 OUTCOMES

Delegates will gain the skills and knowledge 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.

KEY COURSE HIGHLIGHTS

At the end of the course, you will understand;

- 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.

All our courses are dual-certificate courses. At the end of the training, the delegates will receive two certificates.

1. A GTC end-of-course certificate
2. Continuing Professional Development (CPD) Certificate of completion with earned credits awarded