Managing Microsoft 365 Identity and Access (MS-500T01)

Modality: Virtual Classroom

Duration: 1 Day

SATV Value: 1

When you register without the Master Subscription Program in all Microsoft 500 series training (500T01, 500T02 ..... and 500T04), you can obtain a Free Official Exam Voucher for the Microsoft 500 Exam (except transactions utilizing Training Vouchers / SATV). When you are registered in the Master Subscription, this program does not include an Exam Voucher but you can apply to buy the Official Exam Voucher individually.

About this course:

Help secure your access and identity control against credential compromises. In this program, you'll discover how to protect user access to the resources of your organization. This course primarily covers the protection of user passwords, multi-factor authentication, how to allow Azure Identity Security, how to set up ADFS, how to use and configure Azure Active Directory Connect, and teaches you to Conditional Access. You'll also hear about options for external access control to your Office 365 program.

A system administrator for Office 365 Skills has an annual salary of $65,187 per annum.

Course Objective:

· Microsoft 365 manages passwords.

· Prepare and deploy Azure Active Directory Connect

· Prepare and deploy federated identities

· In MS 365 manage user and group security

· Define the features of Azure Identity Protection

· Managing synchronized identities.

· Use and describe conditional access

Audience:

This program is for the Security Administrator position for MS 365. This position works with the MS 365 Enterprise Administrator, business partners and other workload managers to prepare and execute security initiatives and make sure that the solutions are in line with the organization's regulations and policies.

The position efficiently and effectively secures enterprise environments for MS 365. Responsibilities include resolving threats to the MS 365 network, maintaining, implementing, and tracking security and enforcement solutions. They respond to events, inquiries, and data governance compliance.

The MS 365 Security Manager is experienced with MS 365 workloads and has good identity protection, privacy protection, threat detection, compliance management, and data management expertise and experience. This position focuses on the environment for MS 365, which incorporates hybrid environments.

Prerequisite:

· Office 365 experience

· Fundamental knowledge of computer networks

· Fundamental understanding of MS Azure

· Fundamental knowledge of authentication and authorization

· Windows 10 devices experience

· Working expertise of Mobile device Management

Course Outline:

Module 1: User and Group Security

This module explains how to manage user accounts and groups in Microsoft 365. It introduces you to Privileged Identity Management in Azure AD as well as Identity Protection. The module sets the foundation for the remainder of the course.

Lessons

- User Accounts in Microsoft 365
- Administrator Roles and Security Groups in Microsoft 365
- Password Management in Microsoft 365
- Azure AD Identity Protection

Lab : Managing your Microsoft 365 Identity environment

- Setting up your lab environment
- Managing your Microsoft 365 identity environment using the Microsoft 365 admin center
- Assign service administrators

After completing this module, students should be able to:

- Describe the user identities in Microsoft 365.
- Create user accounts from both the Microsoft 365 admin center and in Windows PowerShell.
- Describe and use Microsoft 365 admin roles.
- Describe the various types of group available in Microsoft 365.
- Plan for password policies and authentication.
- Implement Multi-factor authentication in Office 365.
- Describe Azure Identity Protection and what kind of identities can be protected.
- Describe how to enable Azure Identity Protection.
- Identify vulnerabilities and risk events.

Module 2: Identity Synchronization

This module explains concepts related to synchronizing identities. Specifically, it focuses on Azure AD Connect and managing directory synchronization to ensure the right people are connecting to your Microsoft 365 system.

Lessons

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

Lab : Implementing Identity Synchronization

- Setting up your organization for identity synchronization

After completing this module, students should be able to:

- Describe the Microsoft 365 authentication options.
- Explain directory synchronization.
- Plan directory synchronization.
- Describe and plan Azure AD Connect.
- Configure Azure AD Connect Prerequisites.
- Set up Azure AD Connect.
- Manage users with directory synchronization.
- Manage groups with directory synchronization.
- Use Azure AD Connect Sync Security Groups.

Module 3: Federated Identities

This module is all about Active Directory Federation Services (AD FS). Specifically, you will learn how to plan and manage AD FS to achieve the level of access you want to provide users from other directories.

Lessons

- Introduction to Federated Identities
- Planning an AD FS Deployment
- Implementing AD FS

After completing this module, students should be able to:

- Describe claims-based authentication and federation trusts.
- Describe how AD FS works.
- Plan an AD FS environment including best practices, high availability, and capacity planning.
- Plan Active Directory Federation Services in Microsoft Azure.
- Install and configure a Web Application Proxy for AD FS.
- Configure AD FS by using Azure AD Connect.

Module 4: Access Management

This module describes 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.

Lessons

- Conditional Access
- Managing Device Access
- Role Based Access Control (RBAC)
- Solutions for External Access

After completing this module, students should be able to:

- Describe the concept of conditional access.
- Describe conditional access policies.
- Plan for device compliance.
- Configure conditional users and groups.
- Configure RBAC.
- Distinguish between Azure RBAC and Azure AD administrative roles.
- Manage External Access.
- Explain Licensing Guidance for Azure AD B2B Collaboration.