Module Title : MS-500T01-A: Managing Microsoft 365 Identity and Access
Duration : 1 day

About this course

Help protect against credential compromise with identity and access management. In this course you will learn how to secure user access to your organization's resources. Specifically, this course covers user password protection, multi-factor authentication, how to enable Azure Identity Protection, how to configure Active Directory federation services, how to setup and use Azure AD Connect, and introduces you to Conditional Access. You will also learn about solutions for managing external access to your Microsoft 365 system.

Audience profile

This course is for the Microsoft 365 security administrator role. This role collaborates with the Microsoft 365 Enterprise Administrator, business stakeholders and other workload administrators to plan and implement security strategies and 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 has strong skills and experience with identity protection, information protection, threat protection, security management and data governance. This role focuses on the Microsoft 365 environment and includes hybrid environments.

At course completion

After completing this course, students should be able to:

- Administer user and group security in Microsoft 365.
- Manage passwords in Microsoft 365.
- Describe Azure Identity Protection features.
- Plan and implement Azure AD Connect.
- Manage synchronized identities.
- Plan implement federated identities.
- Describe and use conditional access.

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.

Prerequisites

Learners should start this course already having the following skills:

- 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.