



Microsoft Identity and Access Administrator

Course Duration: 4 Days
Exam Reference: SC-300

Course Overview

This course trains professionals to design, implement, and operate an organization's Identity and Access Management (IAM) systems using Microsoft Entra ID. You will gain the knowledge to secure authentication and authorization, implement self-service capabilities, and create adaptive access controls based on Zero Trust principles. The course focuses on modernizing identity solutions, implementing hybrid identity, and ensuring identity governance across enterprise applications.

Prerequisites

You should be familiar with:

- Microsoft Azure
- Microsoft 365 services and workloads
- Active Directory Domain Services (AD DS)
- PowerShell and Kusto Query Language (KQL)

Course Objectives

Upon completion, you will be able to:

- Explore identity in Microsoft Entra ID and its role in Zero Trust.
- Implement an identity management solution for users, groups, and devices.
- Implement an Authentication and Access Management solution using MFA, Conditional Access, and Identity Protection.
- Implement Access Management for Apps, including SSO and application registration.
- Plan and implement an identity governance strategy using entitlement management, access reviews, and Privileged Access Management (PIM).



Contact Us



800.674.3550



2151 W. Hillsboro Blvd., Ste 210
Deerfield Beach, FL 33442

Connect With Us





Microsoft Identity and Access Administrator

Course Outline

Module 1: Explore identity in Microsoft Entra ID

- Define common identity terms and explain how they're used in the Microsoft Cloud
- Explore the common management tools and needs of an identity solution
- Review the goal of Zero Trust and how it's applied in the Microsoft Cloud
- Explore the available identity services in the Microsoft Cloud

Module 2: Implement an identity management solution

- Implement initial configuration of Microsoft Entra ID
- Create, configure, and manage identities
- Implement and manage external identities
- Implement and manage hybrid identity

Module 3: Implement an Authentication and Access Management solution

- Secure Microsoft Entra users with multifactor authentication
- Manage user authentication
- Plan, implement, and administer Conditional Access
- Manage Microsoft Entra Identity Protection
- Implement access management for Azure resources
- Deploy and Configure Microsoft Entra Global Secure Access

Module 4: Implement Access Management for Apps

- Plan and design the integration of enterprise apps for SSO
- Implement and monitor the integration of enterprise apps for SSO
- Implement app registration
- Register apps using Microsoft Entra ID

Module 5: Plan and implement an identity governance strategy

- Plan and implement entitlement management
- Plan, implement, and manage access review
- Plan and implement privileged access
- Monitor and maintain Microsoft Entra ID
- Explore the many features of Microsoft Entra Permissions Management



Microsoft Identity and Access Administrator

Module 6: Virtual Classroom Live Labs

- Lab : Manage user roles
- Lab : Working with tenant properties
- Lab : Assigning license using group membership
- Lab : Configure external collaboration settings
- Lab : Add guest users to the directory
- Lab : Add a federated identity provider
- Lab : Add hybrid identity with Azure AD Connect
- Lab : Enable sign-in and user-risk policies
- Lab : Configure an Azure AD Multi-factor Authentication registration policy
- Lab : Use Azure Key Vault for managed identities
- Lab : Implement and test a conditional access policy
- Lab : Manage Azure AD smart lockout values
- Lab : Assign Azure resource roles in Privileged Identity Management
- Lab : Azure AD authentication for Windows and Linux virtual machines
- Lab : Enable Azure AD self-service password reset
- Lab : Enable Azure AD Multi-factor Authentication
- Lab : Defender for Cloud Apps access policies
- Lab : Register an application
- Lab : Implement access management for apps
- Lab : Grant tenant-wide admin consent to an application
- Lab : Create access reviews for internal and external users
- Lab : Manage the lifecycle of external users in Azure AD Identity Governance settings
- Lab : Add terms of use and acceptance reporting
- Lab : Create and manage a catalog of resources in Azure AD entitlement management
- Lab : Configure Privileged Identity Management (PIM) for Azure AD roles
- Lab : Explore Microsoft Sentinel and use Kusto Queries for reviewing Azure AD data sources
- Lab : Monitor and manage your security posture with Identity Secure Score