APPLIED TECHNOLOGY ACADEMY

800.674.3550
Info@AppliedTechAc.com
AppliedTechnologyAcademy.com

Microsoft Identity and Access Administrator Training

Microsoft Authorized Training · Applied Technology Academy

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.

LEVEL	DURATION	EXPERIENCE	AVERAGE SALARY	LABS
Intermediate	**4 Days**	**1 year: Microsoft**	**$133,000**	**Yes**

Course Overview

- 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).

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

800.674.3550
Info@AppliedTechAc.com
AppliedTechnologyAcademy.com

  - 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
- **Module 6: Virtual Classroom Live Labs**
  - Manage user roles
  - Working with tenant properties
  - Assigning license using group membership
  - Configure external collaboration settings
  - Add guest users to the directory
  - Add a federated identity provider
  - Add hybrid identity with Azure AD Connect
  - Enable sign-in and user-risk policies
  - Configure an Azure AD Multi-factor Authentication registration policy
  - Use Azure Key Vault for managed identities
  - Implement and test a conditional access policy
  - Manage Azure AD smart lockout values
  - Assign Azure resource roles in Privileged Identity Management
  - Azure AD authentication for Windows and Linux virtual machines
  - Enable Azure AD self-service password reset
  - Enable Azure AD Multi-factor Authentication
  - Defender for Cloud Apps access policies
  - Register an application
  - Implement access management for apps
  - Grant tenant-wide admin consent to an application
  - Create access reviews for internal and external users
  - Manage the lifecycle of external users in Azure AD Identity Governance settings

- Add terms of use and acceptance reporting
- Create and manage a catalog of resources in Azure AD entitlement management
- Configure Privileged Identity Management (PIM) for Azure AD roles
- Explore Microsoft Sentinel and use Kusto Queries for reviewing Azure AD data sources
- Monitor and manage your security posture with Identity Secure Score

Intended Audience

- IT professionals responsible for managing identity, access, and security across cloud and hybrid environments.
- Identity and access administrators focused on providing secure authentication and authorization access to enterprise applications.
- Security engineers looking to specialize in Microsoft Entra ID (formerly Azure AD), zero trust, and identity governance.

System administrators managing Microsoft 365, Azure, or other Microsoft cloud services who need to strengthen their identity and access management skills.

Prerequisites

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

Follow-On Courses

- AZ305: Microsoft Azure Solutions Architect
- AZ500: Microsoft Azure Security Technologies

Ready to enroll? Call 800.674.3550 or email Info@AppliedTechAc.com — private team cohorts, GSA MAS purchasing, military credentialing funding, VA GI Bill and VR&E and student financing available.