

Microsoft Identity and Access Administrator (SC-300T00)

Duration: 4 days

Audience: Professionnel TI

Who is this training for?

This course is for the Identity and Access Administrators who are planning to take the associated certification exam, or who are performing identity and access administration tasks in their day-to-day job. This course would also be helpful to an administrator or engineer that wants to specialize in providing identity solutions and access management systems for Azure-based solutions; playing an integral role in protecting an organization.

Training objectives

By the end of this course, students will be able to:

- Design, implement, and operate identity and access management (IAM) solutions using Microsoft Entra ID
- Configure and manage secure authentication and authorization for enterprise applications
- Provide seamless user experiences and self-service capabilities across the organization
- Implement adaptive access policies and identity governance strategies to protect organizational resources
- Monitor, troubleshoot, and report on identity and access environments to ensure reliability and compliance
- Collaborate effectively with cross functional roles to drive strategic identity initiatives within the organization

Summary

The Microsoft Identity and Access Administrator course explores how to design, implement, and operate an organization's identity and access management systems by using Microsoft Entra ID. Learn to manage tasks such as providing secure authentication and authorization access to enterprise applications. You will also learn to provide seamless experiences and self-service management

capabilities for all users. Finally, learn to create adaptive access and governance of your identity and access management solutions ensuring you can troubleshoot, monitor, and report on your environment. The Identity and Access Administrator may be a single individual or a member of a larger team. Learn how this role collaborates with many other roles in the organization to drive strategic identity projects. The end goal is to provide you knowledge to modernize identity solutions, to implement hybrid identity solutions, and to implement identity governance.

Course outline

Learning Path 1 — Explore identity in Microsoft Entra ID

- Module 1 — Explore identity in Microsoft Entra ID

Learning Path 2 — Implement an identity management solution using Microsoft Entra ID

- Module 1 — Implement initial configuration of Microsoft Entra ID
- Module 2 — Create, configure, and manage identities
- Module 3 — Implement and manage external identities
- Module 4 — Implement and manage hybrid identity

Learning Path 3 — Implement an authentication and access management solution

- Module 1 — Secure Microsoft Entra users with multifactor authentication
- Module 2 — Manage user authentication
- Module 3 — Plan, implement, and administer Conditional Access
- Module 4 — Manage Microsoft Entra Identity Protection
- Module 5 — Implement access management for Azure resources
- Module 6 — Deploy and configure Microsoft Entra Global Secure Access

Learning Path 4 — Implement access management for apps

- Module 1 — Plan and design the integration of enterprise apps for SSO
- Module 2 — Implement and monitor the integration of enterprise apps for SSO
- Module 3 — Implement app registration

- Module 4 — Register apps using Microsoft Entra ID

Learning Path 5 — Plan and implement an identity governance strategy

- Module 1 — Plan and implement entitlement management
- Module 2 — Plan, implement, and manage access reviews
- Module 3 — Plan and implement privileged access
- Module 4 — Monitor and maintain Microsoft Entra ID

Approach and methodology

Practical and structured approach combining focused theory and guided workshops. Participants gradually administer Microsoft identities and access through real-world exercises inspired by professional scenarios, promoting immediate application of learning.

They learn how to manage identities, secure access, implement authentication and governance with Microsoft Entra ID.

Led by a Microsoft certified trainer (MCT), the training focuses on interactivity and the development of directly transferable technical skills to effectively protect resources and users in a professional context.

Prerequisites

Students

should have the following knowledge and experience before attending this course:

- Understand security best practices and industry security requirements such as defense in depth, least privileged access, role-based access control, shared responsibility, and zero trust model.
- Be familiar with identity providers like Microsoft Entra ID, Microsoft Entra Domain Services, or other authentication providers.
- Have some experience deploying Azure workloads.
-

Have experience with Windows and/or Linux operating systems and minor scripting language experience.

- Have experience with PowerShell and the CLI.

Recommendations

Optional prerequisites:

- General familiarity with Microsoft Entra ID
- Practical understanding of enterprise app integration and SSO concepts
- Basic knowledge of identity governance (entitlement management, access reviews)
- Awareness of Zero Trust principles and adaptive access strategies
- Prior exposure to multifactor authentication (MFA) concepts

Certifications

[Microsoft Certified: Identity and Access Administrator Associate](#)

Legal notices

© AFI Expertise inc.