Microsoft Security

SC-300T00: Microsoft Identity and Access Administrator

$2,595.00

- 4 Days

Upcoming Dates

Aug 18 - Aug 21
Oct 14 - Oct 17

Course Description

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 (Formerly Azure AD). 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

Implement an identity management solution

Learn to create and manage your initial Azure Entra ID (formerly Azure AD) implementation and configure the users, groups, and external identities you will use to run your solution.

Lessons

- Implement Initial configuration of Azure Entra ID (formerly Azure AD)
- Create, configure, and manage identities
- Implement and manage external identities
- Implement and manage hybrid identity

Labs

- Manage user roles
- Setting tenant-wide properties
- Assign licenses to users
- Restore or remove deleted users
- Add groups in Azure Entra ID (formerly Azure AD)
- Change group license assignments
- Change user license assignments
- Configure external collaboration
- Add guest users to the directory
- Explore dynamic groups

After completing this Learning Path, students will be able to:

- Deploy an initial Azure Entra ID (formerly Azure AD) with custom settings
- Manage both internal and external identities
- Implement a hybrid identity solution

Implement an authentication and access management solution

Implement and administer your access management using Azure Entra ID. Use MFA, conditional access, and identity protection to manage your identity solution.

Lessons

- Secure Azure Entra user with MFA
- Manage user authentication
- Plan, implement, and administer conditional access
- Manage Azure Entra identity (formerly Azure AD) protection
- Implement access management for Azure resources

Labs

- Enable Azure Entra (formerly Azure AD) MFA
- Configure and deploy self-service password reset (SSPR)
- Work with security defaults
- Implement conditional access policies, roles, and assignments
- Configure authentication session controls
- Manage Azure Entra smart lockout values
- Enable sign-in risk policy
- Configure Azure Entral MFA (formerly Azure AD) authentication registration policy

After completing this Learning Path, students will be able to:

- Configure and manage user authentication including MFA
- Control access to resources using conditional access
- Use Azure Entra Identity Protection to protect your organization

Implement access management for Apps

Explore how applications can and should be added to your identity and access solution with application registration in Azure Entra (formerly Azure AD).

Lessons

- Plan and design the integration of enterprise for SSO
- Implement and monitor the integration of enterprise apps for SSO

- Implement app registration

  Labs

- Implement access management for apps
- Create a custom role to management app registration
- Register an application
- Grant tenant-wide admin consent to an application
- Add app roles to applications and receive tokens

  After completing this Learning Path, students will be able to:

- Register a new application to your Azure Entra ID (formerly Azure AD)
- Plan and implement SSO for enterprise application
- Monitor and maintain enterprise applications

Plan and implement an identity governance strategy

Design and implement identity governance for your identity solution using entitlement, access reviews, privileged access, and monitoring your Azure Entra ID (formerly Azure AD)

  Lessons

- Plan and implement entitlement management
- Plan, implement, and manage access reviews
- Plan and implement privileged access
- Monitor and maintain Entra ID

  Labs

- Create and manage a resource catalog with Azure Entra entitlement
- Add terms of use acceptance report
- Manage the lifecycle of external users with Azure Entra identity governance
- Create access reviews for groups and apps
- Configure PIM for Azure Entra ID (formerly Azure AD) roles
- Assign Azure Entra ID (formerly Azure AD) role in PIM
- Assign Azure resource roles in PIM
- Connect data from Azure Entra to Azure Sentinel

  After completing this Learning Path, students will be able to:

- Manage and maintain Azure Entra from creation to solution
- Use access reviews to maintain your Azure Entra
- Grant access to users with entitlement management

Audience

The audience for this course is Identity and Access Management professional 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 engineer that wants to specialize in providing identity and access for Azure-based digital solutions; and plays an integral role in protecting an organization's data.

Prerequisites

Before attending this course, students must have:

- 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. This course does not cover the basics of Azure administration, instead the course content builds on that knowledge by adding identity and security specific information.
- Have experience with Windows and/or Linux operating systems and minor scripting language experience. This course touches on the use of PowerShell and the CLI.

What You Will Learn