

Course No. 1936

Microsoft Identity and access administrator (SC-300)

IDENTITY & ACCESS MANAGEMENT
INFORMATION TECHNOLOGY & CYBERSECURITY

DURATION

5 Days

DELIVERY

Classroom



Course Overview

The Microsoft Identity and Access Administrator (SC-300) training course provides a comprehensive, practical foundation for professionals responsible for designing, implementing, administering, and securing identity and access environments using Microsoft security and identity technologies. The course focuses on the core responsibilities of an identity and access administrator, with particular emphasis on Microsoft Entra ID, identity lifecycle management, authentication, authorization, access governance, and secure access to organizational resources.

Effective identity and access management is a critical component of modern cybersecurity and digital transformation. Organizations increasingly operate across cloud, hybrid, and distributed environments where controlling who can access systems, applications, data, and infrastructure is essential to maintaining security and operational continuity. The Microsoft Identity and Access Administrator (SC-300) course enables participants to understand how identity can be used as a strategic security control while supporting business productivity and secure access.

The course develops practical capabilities in managing users, groups, identities, authentication methods, application access, privileged identities, and governance processes within Microsoft Entra ID. Participants explore approaches for strengthening authentication, implementing role-based access control, managing privileged access, configuring identity protection capabilities, and establishing appropriate access policies aligned with organizational requirements.

Designed for enterprise and institutional environments, the training is particularly relevant to organizations operating complex IT infrastructures, including government entities, ministries, banks and financial institutions, oil and gas organizations, and large corporations. The program connects technical identity administration with operational security, risk management, compliance requirements, and business continuity, helping participants apply identity and access management principles effectively within their professional environments.

Objectives

- Analyze the architecture and core capabilities of Microsoft Entra ID and establish how identity services support organizational cybersecurity and access management requirements.
- Develop practical approaches for managing users, groups, administrative roles, and identity objects throughout their operational lifecycle.

- Evaluate authentication requirements and apply appropriate authentication methods to strengthen secure access to organizational resources.
- Implement Microsoft Entra authentication and access controls that support secure and efficient user access across cloud and hybrid environments.
- Design role-based access control structures that align administrative privileges with organizational responsibilities and security principles.
- Assess application identity and access requirements and configure appropriate controls for enterprise applications and cloud services.
- Strengthen privileged identity management practices by applying appropriate controls for elevated administrative access and sensitive resources.
- Implement identity governance processes that support access reviews, entitlement management, lifecycle controls, and appropriate user access.
- Evaluate identity-related security risks and apply Microsoft Entra capabilities to identify, manage, and respond to suspicious identity activity.
- Apply access policies and security controls that support Zero Trust principles and reduce unnecessary or excessive access privileges.
- Align identity and access administration practices with organizational security, compliance, risk, and operational requirements through practical workplace scenarios.
- Assess the effectiveness of an organization's identity and access environment and develop an actionable improvement plan by the end of the course.

Who Should Attend

The Microsoft Identity and Access Administrator (SC-300) training course is designed for IT professionals responsible for identity administration, access management, cybersecurity, cloud infrastructure, systems administration, and enterprise technology operations. It is particularly suitable for Microsoft administrators, identity and access administrators, system administrators, network and infrastructure specialists, cloud administrators, cybersecurity professionals, security operations personnel, and IT support professionals involved in managing organizational identities and access.

The program is also valuable for IT managers, cybersecurity managers, infrastructure managers, cloud and digital transformation teams, information security specialists, and technical decision makers who need a stronger understanding of Microsoft identity and access capabilities. Professionals working in government organizations, financial institutions, oil and gas companies,

large enterprises, and organizations operating hybrid or cloud-based environments can use the course to strengthen identity security practices and improve control over access to critical systems, applications, and information.

Learning Outcomes

- Configure and manage core Microsoft Entra ID capabilities according to organizational identity and access requirements.
- Create and administer users, groups, administrative roles, and identity objects using appropriate management practices.
- Manage identity lifecycles and apply structured processes for provisioning, modifying, reviewing, and deprovisioning access.
- Configure and evaluate authentication methods that improve identity security while maintaining an effective user experience.
- Apply role-based access control to provide appropriate administrative permissions and reduce excessive privilege.
- Configure and manage access to enterprise applications while addressing application identity and authorization requirements.
- Implement privileged identity management practices for controlling and monitoring elevated administrative access.
- Apply identity governance capabilities, including access reviews and entitlement management, to improve control over organizational access.
- Configure and evaluate access policies based on users, applications, devices, locations, and organizational risk considerations.
- Identify common identity-related security risks and apply Microsoft Entra security capabilities to support detection and response.
- Apply Zero Trust concepts to identity and access management and evaluate their relevance to enterprise security architecture.
- Develop a practical identity and access improvement action plan based on an organization's operational, security, and governance requirements.

Course Outline

DAY 01

Microsoft Entra ID and Identity Management Foundations

- Introduction to modern identity and access management in enterprise environments
- Microsoft Entra ID architecture, components, and core capabilities
- Managing users, groups, organizational identities, and administrative accounts
- Identity lifecycle management and identity synchronization concepts

PRACTICAL APPLICATION OR DISCUSSION

Assessing an organization's current identity environment and identifying key access management requirements

DAY 02

Authentication, Authorization and Secure Access

- Authentication concepts and modern authentication approaches
- Managing authentication methods and authentication policies
- Multi-factor authentication and strengthening identity verification
- Role-based access control and administrative role management
- Access control principles, least privilege, and separation of administrative responsibilities

PRACTICAL APPLICATION OR DISCUSSION

Designing an authentication and authorization framework for a large enterprise environment

DAY 03

Application Access and Privileged Identity Management

- Managing application identities and enterprise application access
- Application registration and identity considerations for cloud applications
- Managing permissions, consent, and application access
- Privileged Identity Management and control of elevated administrative privileges

DAY 03 — CONTINUED

- Just-in-time access, privileged role activation, monitoring, and governance

PRACTICAL APPLICATION OR DISCUSSION

Developing a privileged access management model for sensitive enterprise systems

DAY 04

Identity Governance, Security and Zero Trust

- Identity governance principles and access lifecycle controls
- Access reviews and maintaining appropriate user access
- Entitlement management and controlled access to organizational resources
- Identity protection, risk-based identity controls, and suspicious activity considerations
- Applying Zero Trust principles to identity and access management

PRACTICAL APPLICATION OR DISCUSSION

Evaluating identity risks and developing controls for a government, financial, or oil and gas environment

DAY 05

Identity Security Strategy and Enterprise Implementation

- Designing an integrated identity and access management framework
- Aligning Microsoft Entra capabilities with cybersecurity, compliance, and operational requirements
- Reviewing administrative privileges, access policies, application permissions, and governance processes
- Identity security monitoring, continuous improvement, and operational management
- Developing an enterprise identity and access implementation roadmap

FINAL WORKSHOP, ACTION PLAN, OR IMPLEMENTATION EXERCISE

Build and present a practical Microsoft Identity and Access Administration strategy for a selected organizational environment



Register or Request More Information

Course page: <https://quest-training.com/courses/microsoft-identity-and-access-administrator-sc-300>

Website: <https://quest-training.com>

Email: info@quest-training.com

Phone: +905016771440

