Microsoft Identity and Access Administrator (SC-300)

Description

Expand your skills with Microsoft Entra and Azure

In a constantly evolving digital world, identity management has become a strategic priority. The Microsoft Identity and Access Administrator (SC-300) training offers you essential expertise in using Microsoft Entra, Azure, and Microsoft 365. Through this course, you will learn how to design, deploy, and manage modern identity and access management solutions.

By completing this SC-300 training, you will be able to ensure secure access to enterprise applications while providing a seamless user experience through streamlined authentication. You will discover how to implement effective governance with Microsoft Entra ID, integrate Microsoft Entra Identity Verification, and manage external identities with Microsoft Entra External ID. You will also master troubleshooting, monitoring, and reporting techniques for hybrid and cloud environments.

A certification training to boost your career

The Microsoft Identity and Access Administrator (SC-300) course also prepares you for the official certification exam. You will be able to validate your skills by implementing best practices for identity administration and security using Azure and Microsoft 365.

Course Content
Module 1: Explore identity in Microsoft Entra ID

- Explain the identity landscape
- Explore Zero Trust with identity
- Discuss identity as a control plane
- Discover why we need identity
- Define identity administration
- Contrast decentralized vs centralized identity systems
- Discuss identity management solutions
- Explain Microsoft Entra Business to Business
- Compare Microsoft identity providers
- Define identity license management
- Explore authentication
- Discuss authorization
- Explain auditing in identity

Module 2: Implement initial configuration of Microsoft Entra ID

- Configure company branding
- Configure and manage Microsoft Entra roles
- Configure delegation using administrative units
- Analyze Microsoft Entra role permissions
- Configure and manage custom domains
- Configure tenant-wide settings

Module 3: Create, configure, and manage identities

- Create, configure, and manage identities
- Create, configure, and manage groups
- Configure and manage device enrollment
- Manage licenses
- Create custom security attributes
- Explore automated user creation

Module 4: Implement and manage external identities

- Describe guest access and business-to-business accounts
- Manage external collaboration
- Invite external users: individually and in bulk
- Manage external user accounts in Microsoft Entra ID
- Manage external users in Microsoft 365 workloads
- Implement and manage Microsoft Entra Verified ID
- Configure identity providers
- Implement cross-tenant access controls

Module 5: Implement and manage hybrid identities

- Plan, design, and implement Microsoft Entra Connect
- Implement and manage password hash synchronization (PHS)
- Implement and manage pass-through authentication (PTA)
- Implement and manage federation
- Troubleshoot synchronization errors
- Implement Microsoft Entra Connect Health
- Manage Microsoft Entra Health

Module 6: Secure Microsoft Entra users with multi-factor authentication

- What is Microsoft Entra multi-factor authentication?
- Plan your multi-factor authentication deployment
- Configure multi-factor authentication methods

Module 7: Manage user authentication

- Administer FIDO2 and passwordless authentication methods
- Explore Authenticator app and OATH tokens
- Implement Windows Hello for Business authentication
- Deploy and manage password protection
- Configure smart lockout thresholds
- Implement Kerberos and certificate-based authentication in Microsoft Entra ID
- Configure Microsoft Entra user authentication for virtual machines

Module 8: Plan, implement, and administer conditional access

- Plan default security settings
- Plan conditional access policies
- Implement policy assignments and controls
- Test and troubleshoot conditional access policies
- Implement application controls
- Implement session management
- Implement continuous access evaluation

Module 9: Manage Microsoft Entra Identity Protection

- Review Identity Protection fundamentals
- Implement and manage user risk policies
- Monitor, investigate, and remediate risky users
- Implement security for workload identities
- Explore Microsoft Defender for Identity

Module 10: Implement access management for Azure resources

- Assign Azure roles
- Configure custom Azure roles
- Create and configure managed identities
- Access Azure resources with managed identities
- Analyze Azure role permissions
- Configure Azure Key Vault RBAC policies
- Retrieve objects from Azure Key Vault
- Discover Microsoft Entra Permissions Management

Module 11: Deploy and configure Microsoft Entra Secure Global Access

- Explore Secure Global Access
- Deploy and configure Microsoft Entra Internet Access
- Deploy and configure Microsoft Entra Private Access
- Learn to use the dashboard for Secure Global Access
- Create remote networks for Secure Global Access
- Use conditional access with Secure Global Access
- Explore Secure Global Access logging and monitoring options

Module 12: Plan and design enterprise app integration for single sign-on

- Discover applications with Microsoft Defender for Cloud Apps and the AD FS Application Report
- Configure app connectors
- Design and implement application management roles

- Configure gallery-integrated SaaS apps
- Implement and manage OAuth app policies

Module 13: Implement and monitor enterprise app integration for single sign-on

- Implement token customizations
- Implement and configure consent settings
- Integrate on-premises apps using Microsoft Entra Application Proxy
- Integrate custom SaaS apps for single sign-on
- Implement app-based user provisioning
- Monitor and audit enterprise app access in Microsoft Entra
- Create and manage application collections

Module 14: Implement application registration

- Plan your application registration strategy
- Implement application registration
- Register an application
- Configure app permissions
- Grant tenant-wide admin consent to applications
- Implement application authorization
- Manage and monitor apps using application governance

Module 15: Register applications using Microsoft Entra ID

- Plan an application registration
- Explore application objects and service principals
- Create application registrations
- Configure application authentication
- Configure API permissions
- Create application roles

Module 16: Plan and implement entitlement management

- Define access packages
- Configure entitlement management
- Configure and manage connected organizations
- Review entitlements per user

Module 17: Plan, implement, and manage access reviews

- Plan access reviews
- Create access reviews for groups and applications
- Create and configure programmatic access reviews
- Monitor access review results
- Automate access review management tasks
- Configure recurring access reviews

Module 18: Plan and implement privileged access
Module 19: Monitor and manage Microsoft Entra ID

- Analyze and review sign-in logs to troubleshoot access issues
- Review and monitor Microsoft Entra audit logs

- Export logs to a third-party SIEM system
- Analyze Microsoft Entra workbooks and reports
- Monitor security posture with secure score for identity

Module 20: Explore Microsoft Entra Permissions Management features

- A comprehensive experience for all cloud environments
- Get overall insights in the Permissions Management dashboard
- Dive deeper into analysis using the Analytics tab
- Gain better understanding with the Reports tab
- Analyze historical data with the Audit tab
- Take corrective action with the Remediation tab
- Adopt a proactive management approach with continuous monitoring
- Manage access to Microsoft Entra Permissions Management
- Complete example

Lab / Exercises

- This course provides you with exclusive access to the official Microsoft lab, enabling you to practice your skills in a professional environment.

Documentation

- Access to Microsoft Learn, Microsoft's online learning platform, offering interactive resources and educational content to deepen your knowledge and develop your technical skills.

Exam

- This course prepares you to the SC-300: Microsoft Identity and Access Administrator exam.

Participant profiles

- Identity and access administrators
- Cybersecurity engineers
- Cloud solutions consultants
- Microsoft Azure solutions architects
- Access governance managers

Prerequisites

- Understand the fundamentals of Microsoft Azure and Microsoft 365
- Master the basic concepts of cybersecurity
- Have a basic understanding of identity and access administration

Objectives

- Implement identity management with Microsoft Entra ID
- Configure multi-factor authentication and conditional access
- Manage external access with Microsoft Entra External ID
- Monitor, troubleshoot, and oversee access to resources
- Implement identity governance
- Deploy secure hybrid identity solutions
- Integrate Microsoft Entra Identity Verification
- Protect applications with secure access policies

Description
Microsoft Identity and Access Administrator (SC-300)
Niveau
Intermédiaire
Classroom Registration Price (CHF)
3200
Virtual Classroom Registration Price (CHF)
3000
Duration (in Days)
4
Reference
SC-300T00