Course Title: SC-300T00-A Microsoft Identity and Access Administrator [Cloud Slice Provided]	**Course Duration**: 4.0 Days
Exam: Not Included	**Exam Type**: Proctored Exam
Qualification: SC-300 Completion Certificate	

Course Syllabus

1 - Explore identity in Microsoft Entra ID

- Explain the identity landscape
- Explore zero trust with identity
- Discuss identity as a control plane
- Explore why we have identity
- Define identity administration
- Contrast decentralized identity with central identity systems
- Discuss identity management solutions
- Explain Microsoft Entra Business to Business
- Compare Microsoft identity providers
- Define identity licensing
- Explore authentication
- Discuss authorization
- Explain auditing in identity

2 - Implement initial configuration of Microsoft Entra ID

- Configure company brand
- Configure and manage Microsoft Entra roles
- Configure delegation by using administrative units
- Analyze Microsoft Entra role permissions
- Configure and manage custom domains
- Configure tenant-wide setting

3 - Create, configure, and manage identities

- Create, configure, and manage users
- Create, configure, and manage groups
- Configure and manage device registration
- Manage licenses
- Create custom security attributes
- Explore automatic user creation

4 - Implement and manage external identities

- Describe guest access and Business to Business accounts

- Manage external collaboration
- Invite external users - individually and in bulk
- Demo - manage guest users in Microsoft Entra ID
- 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

5 - Implement and manage hybrid identity

- Plan, design, and implement Microsoft Entra Connect
- Implement manage password hash synchronization (PHS)
- Implement manage pass-through authentication (PTA)
- Demo - Manage pass-through authentication and seamless single sign-on (SSO)
- Implement and manage federation
- Trouble-shoot synchronization errors
- Implement Microsoft Entra Connect Health
- Manage Microsoft Entra Health

6 - Secure Microsoft Entra users with multifactor authentication

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

7 - Manage user authentication

- Administer FIDO2 and passwordless authentication methods
- Explore Authenticator app and OATH tokens
- Implement an authentication solution based on Windows Hello for Business
- 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

8 - Plan, implement, and administer Conditional Access

- Plan security defaults
- Plan Conditional Access policies
- Implement Conditional Access policy controls and assignments
- Test and troubleshoot Conditional Access policies
- Implement application controls
- Implement session management
- Implement continuous access evaluation

9 - Manage Microsoft Entra Identity Protection

- Review identity protection basics
- Implement and manage user risk policy
- Monitor, investigate, and remediate elevated risky users
- Implement security for workload identities
- Explore Microsoft Defender for Identity

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
- Explore Microsoft Entra Permissions Management

11 - Plan and design the integration of enterprise apps for SSO

- Discover apps by using Microsoft Defender for Cloud Apps and Active Directory Federation Services app report
- Configure connectors to apps
- Design and implement app management roles
- Configure preintegrated gallery SaaS apps
- Implement and manage policies for OAuth apps

12 - Implement and monitor the integration of enterprise apps for SSO

- Implement token customizations
- Implement and configure consent settings
- Integrate on-premises apps with Microsoft Entra application proxy
- Integrate custom SaaS apps for single sign-on
- Implement application-based user provisioning
- Monitor and audit access to Microsoft Entra integrated enterprise applications
- Create and manage application collections

13 - Implement app registration

- Plan your line of business application registration strategy
- Implement application registration
- Register an application
- Configure permission for an application
- Grant tenant-wide admin consent to applications
- Implement application authorization
- Manage and monitor application by using app governance

14 - Plan and implement entitlement management

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

15 - Plan, implement, and manage access review

- Plan for access reviews
- Create access reviews for groups and apps
- Create and configure access review programs
- Monitor access review findings
- Automate access review management tasks

- Configure recurring access reviews

16 - Plan and implement privileged access

- Define a privileged access strategy for administrative users
- Configure Privileged Identity Management for Azure resources
- Plan and configure Privileged Access Groups
- Analyze Privileged Identity Management audit history and reports
- Create and manage emergency access accounts

17 - Monitor and maintain Microsoft Entra ID

- Analyze and investigate sign-in logs to troubleshoot access issues
- Review and monitor Microsoft Entra audit logs
- Export logs to third-party security information and event management system
- Analyze Microsoft Entra workbooks and reporting
- Monitor security posture with Identity Secure Score

Course Overview

This course prepares IT professionals to design, implement, and manage identity and access solutions using Microsoft Entra ID (Azure AD), conditional access, authentication methods, and governance. Learners gain practical experience through Cloud Slice labs in securing enterprise identities, managing privileged access, and monitoring authentication activity in real-world Microsoft environments.

Course Learning Outcomes

By the end of this course, learners will be able to design and implement identity management solutions, configure and manage secure authentication and authorization methods, implement conditional access and identity protection policies, monitor and report on access and authentication, manage hybrid identities, and enforce governance and compliance standards in Microsoft environments. Learners gain the expertise needed to ensure secure access and identity management for enterprise systems.

Audience

IT professionals, security administrators, system administrators, identity and access specialists, and anyone responsible for managing enterprise identities and access in Microsoft 365 and Azure

Entry-Level Requirements

Experience with Microsoft 365 or Azure administration recommended; understanding of networking, security, and cloud concepts is beneficial

Recommended Reading

Microsoft Learn SC-300 learning path, Microsoft Entra ID and Azure AD documentation, Exam Ref SC-300 Microsoft Identity and Access Administrator

What's Included

Instructor-led training, hands-on labs, course materials, exam preparation guide

Exam Information

This course prepares learners for the SC-300: Microsoft Identity and Access Administrator certification exam. The exam measures skills in designing, implementing, and operating identity and access management solutions in Microsoft 365 and Azure environments. It includes multiple-choice, scenario-based, and case-study questions reflecting real-world identity management tasks. Successful candidates earn the Microsoft Certified: Identity and Access Administrator Associate credential.

What's Next

After completing SC-300, learners can advance to SC-400 (Information Protection Administrator), SC-200 (Security Operations Analyst), or pursue advanced Azure security and identity architecture roles.

Additional Information

Prerequisites

- SC-900T00: Microsoft Security, Compliance, and Identity Fundamentals
- AZ-104T00 - Microsoft Azure Administrator