

**Microsoft Identity and Access Administrator (SC-300)**

**Course Number:** MOC-SC-300
**Duration:** 4 days

**Overview**

This Microsoft Identity and Access Administrator (SC-300) training class teaches teams how to implement identity management solutions based on Microsoft Azure AD and its connected identity technologies. Attendees learn how to use identity content for Azure AD, enterprise application registration, conditional access, identity governance, and other identity tools. This course prepares students for the [SC-300 exam](https://docs.microsoft.com/en-us/learn/certifications/exams/SC-300) for which every attendee receives a voucher.

For information on Privileged Identity Management in Azure Read our tutorial on [How To Use PIM in Microsoft Azure to Improve Security](file:////library/how-to-articles/azure-pim).

**Prerequisites**

All students must have:

* Knowledge of security best practices and industry security requirements such as defense in depth, least privileged access, shared responsibility, and zero trust model.
* Familiarity with identity concepts such as authentication, authorization, and active directory.
* Some experience deploying Azure workloads. Because this course does not cover the basics of Azure administration but builds on that knowledge by adding security-specific information, students should have taken [Microsoft Azure Administrator Training (AZ-104)](file:////training/microsoft-azure-administrator) or have the equivalent knowledge.
* Some experience with Windows and Linux operating systems. Experience with scripting languages is helpful but not required. Course labs may use PowerShell and the CLI.

**Materials**

All Microsoft training students receive Microsoft official courseware.

For all Microsoft Official Courses taught in their entirety that have a corresponding certification exam, an exam voucher is included for each participant.

**Software Needed on Each Student PC**

Attendees will not need to install any software on their computers for this class. The class will be conducted in a remote environment that Accelebrate will provide; students will only need a local computer with a web browser and a stable Internet connection. Any recent version of Microsoft Edge, Mozilla Firefox, or Google Chrome will work well.

**Objectives**

* Implement initial configuration of Azure Active Directory
* Manage external collaboration settings in Azure Active Directory
* Configure identity providers (social and SAML/WS-fed)
* Manage Seamless Single Sign-On (Seamless SSO)
* Create and manage a resource catalog with Azure AD entitlement
* Implement application registration and configure permissions
* Configure Privileged Identity Management for Azure AD roles and Azure resources
* Work with the Azure Active Directory

**Outline**

* Explore Identity in Azure AD
	+ 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 Azure AD Business to Business
	+ Compare Microsoft identity providers
	+ Define identity licensing
	+ Explore authentication
	+ Discuss authorization
	+ Explain auditing in identity
* Implement Initial Configuration of Azure Active Directory
	+ Configure company brand
	+ Configure and manage Azure Active Directory roles
	+ Manage user roles
	+ Configure delegation by using administrative units
	+ Analyze Azure AD role permissions
	+ Configure and manage custom domains
	+ Configure tenant-wide setting
	+ Setting tenant-wide properties
	+ Create, configure, and manage identities
	+ Create, configure, and manage users
	+ Assign licenses to users
	+ Restore or remove deleted users
	+ Create, configure, and manage groups
	+ Add groups in Azure Active Directory
	+ Configure and manage device registration
	+ Manage licenses
	+ Change group license assignments
	+ Change user license assignments
	+ Create custom security attributes
	+ Explore automatic user creation
* Create, Configure, and Manage Identities
	+ Create, configure, and manage users
	+ Assign licenses to users
	+ Restore or remove deleted users
	+ Create, configure, and manage groups
	+ Add groups in Azure Active Directory
	+ Configure and manage device registration
	+ Manage licenses
	+ Change group license assignments
	+ Describe guest access and Business to Business accounts3 min
	+ Manage external collaboration
	+ Configure external collaboration
	+ Invite external users - individually and in bulk
	+ Add guest users to directory
	+ Invite guest users bulk
	+ Manage guest users in Azure Active Directory
	+ Manage external user accounts in Azure Active Directory
	+ Manage external users in Microsoft 365 workloads
	+ Explore dynamic groups
	+ Implement cross-tenant access controls
	+ Configure identity providers
	+ Implement and manage Entra Verified ID
	+ Change user license assignments
	+ Create custom security attributes
	+ Explore automatic user creation
	+ Implement and Manage External Identities
* Implement and Manage Hybrid Identity
	+ Plan, design, and implement Azure Active Directory Connect
	+ Implement manage password hash synchronization (PHS)
	+ Implement manage pass-through authentication (PTA)
	+ Manage pass-through authentication and Seamless Single Sign-On (SSO)
	+ Implement and manage federation
	+ Trouble-shoot synchronization errors
	+ Implement Azure Active Directory Connect Health
	+ Manage Azure Active Directory Connect Health
* Secure Azure Active Directory Users with Multi-Factor Authentication
	+ What is Azure AD Multi-Factor Authentication?
	+ Plan your multi-factor authentication deployment
	+ Enable Azure AD Multi-Factor Authentication
	+ Configure multi-factor authentication methods
* Manage User Authentication
	+ Administer FIDO2 and passwordless authentication methods
	+ Explore the Authenticator app and OATH tokens
	+ Implement an authentication solution based on Windows Hello for Business
	+ Configure and deploy self-service password reset
	+ Deploy and manage password protection
	+ Configure smart lockout thresholds
	+ Manage Azure Active Directory smart lockout values
	+ Implement Kerberos and certificate-based authentication in Azure AD
	+ Configure Azure AD user authentication for virtual machines
* Plan, Implement, and Administer Conditional Access
	+ Plan security defaults
	+ Work with security defaults
	+ Plan Conditional Access policies
	+ Implement Conditional Access policy controls and assignments
	+ Implement Conditional Access policies roles and assignments
	+ Test and troubleshoot Conditional Access policies
	+ Implement application controls
	+ Implement session management
	+ Configure authentication session controls
	+ Implement continuous access evaluation
* Manage Azure AD Identity Protection
	+ Review identity protection basics
	+ Implement and manage user risk policy
	+ Exercise enable sign-in risk policy
	+ Exercise configure Azure Active Directory multi-factor authentication registration policy
	+ Monitor, investigate, and remediate elevated risky users
	+ Implement security for workload identities
	+ Explore Microsoft Defender for Identity
* 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 Entra Permissions Management (CloudKnox)
* 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
	+ Implement access management for apps
	+ Design and implement app management roles
	+ Create a custom role to manage app registration
	+ Configure pre-integrated gallery SaaS apps
	+ Implement and manage policies for OAuth apps
* Implement and Monitor the Integration of Enterprise Apps for SSO
	+ Implement token customizations
	+ Implement and configure consent settings
	+ Integrate on-premises apps by using Azure Active Directory application proxy
	+ Integrate custom SaaS apps for single-sign-on
	+ Implement application user provisioning
	+ Monitor and audit access to Azure Active Directory integrated applications
	+ Create and manage application collections
* Implement App Registration
	+ Plan your line of business application registration strategy
	+ Implement application registration
	+ Register an application
	+ Configure application permission
	+ Grant tenant-wide admin consent to an application
	+ Implement application authorization
	+ Add app roles to applications and receive tokens
	+ Manage and monitor applications with App governance
* Plan and Implement Entitlement Management
	+ Define access packages
	+ Create and manage a resource catalog with Azure AD entitlement
	+ Configure entitlement management
	+ Add terms of use acceptance report
	+ Manage the lifecycle of external users with Azure AD identity governance
	+ Configure and manage connected organizations
	+ Review per-user entitlements
* Plan, Implement, and Manage Access Review
	+ Plan for access reviews18 min
	+ Create access reviews for groups and apps12 min
	+ Create and configure access review programs3 min
	+ Monitor access review findings4 min
	+ Automate access review management tasks2 min
	+ Configure recurring access reviews
* Plan and Implement Privileged Access
	+ Define a privileged access strategy for administrative users10 min
	+ Configure Privileged Identity Management for Azure resources2 min
	+ Configure Privileged Identity Management for Azure Active Directory roles10 min
	+ Assign Azure Active Directory roles in Privileged Identity Management10 min
	+ Assign Azure resource roles in Privileged Identity Management8 min
	+ Plan and configure Privileged Access Groups3 min
	+ Analyze Privileged Identity Management audit history and reports8 min
	+ Create and manage emergency access accounts
* Monitor and Maintain Azure Active Directory
	+ Analyze and investigate sign-in logs to troubleshoot access issues
	+ Review and monitor Azure Active Directory audit logs
	+ Connect data from Azure Active Directory to Microsoft Sentinel
	+ Export logs to third-party security information and event management system
	+ Analyze Azure Active Directory workbooks and reporting
	+ Monitor security posture with Identity Secure Score
* Conclusion