Study guide for Exam SC-300: Microsoft Identity and Access Administrator

Purpose of this document

This study guide should help you understand what to expect on the exam and includes a summary of the topics the exam might cover and links to additional resources. The information and materials in this document should help you focus your studies as you prepare for the exam.

Useful links	Description
Review the skills measured as of February 1, 2023	This list represents the skills measured AFTER the date provided. Study this list if you plan to take the exam AFTER that date.
Review the skills measured prior to February 1, 2023	Study this list of skills if you take your exam PRIOR to the date provided.
Change log	You can go directly to the change log if you want to see the changes that will be made on the date provided.
How to earn the certification	Some certifications only require passing one exam, while others require passing multiple exams.
Certification renewal	Microsoft associate, expert, and specialty certifications expire annually. You can renew by passing a **free** online assessment on Microsoft Learn.
Your Microsoft Learn profile	Connecting your certification profile to Microsoft Learn allows you to schedule and renew exams and share and print certificates.
Exam scoring and score reports	A score of 700 or greater is required to pass.
Exam sandbox	You can explore the exam environment by visiting our exam sandbox.
Request accommodations	If you use assistive devices, require extra time, or need modification to any part of the exam experience, you can request an accommodation.

Useful links	Description
Take a practice test	Are you ready to take the exam or do you need to study a bit more?

Updates to the exam

Our exams are updated periodically to reflect skills that are required to perform a role. We have included two versions of the Skills Measured objectives depending on when you are taking the exam.

We always update the English language version of the exam first. Some exams are localized into other languages, and those are updated approximately eight weeks after the English version is updated. Although Microsoft makes every effort to update localized versions as noted, there may be times when the localized versions of an exam are not updated on this schedule. Other available languages are listed in the **Schedule Exam** section of the **Exam Details** webpage. If the exam isn't available in your preferred language, you can request an additional 30 minutes to complete the exam.

Note

The bullets that follow each of the skills measured are intended to illustrate how we are assessing that skill. Related topics may be covered in the exam.

Note

Most questions cover features that are general availability (GA). The exam may contain questions on Preview features if those features are commonly used.

Skills measured as of February 1, 2023

Audience profile

The Microsoft identity and access administrator designs, implements, and operates an organization’s identity and access management systems by using Microsoft Azure Active Directory (Azure AD), part of Microsoft Entra. They configure and manage authentication and authorization of identities for users, devices, Azure resources, and applications.

The identity and access administrator provides seamless experiences and self-service management capabilities for all users. They ensure that identity is verified explicitly to support Zero Trust principles. They automate management of Azure AD by using PowerShell and analyze events by using Kusto Query Language (KQL). They are also responsible for troubleshooting, monitoring, and reporting for the identity and access environment.

The identity and access administrator collaborates with many other roles in the organization to drive strategic identity projects, to modernize identity solutions, to implement hybrid identity solutions, and to implement identity governance. They should be familiar with Azure and Microsoft 365 services and workloads.

- Implement identities in Azure AD (20–25%)

- Implement authentication and access management (25–30%)
- Implement access management for applications (15–20%)
- Plan and implement identity governance in Azure AD (20–25%)

Implement identities in Azure AD (20–25%)

Configure and manage an Azure AD tenant

- Configure and manage Azure AD roles
- Configure delegation by using administrative units
- Analyze Azure AD role permissions
- Configure and manage custom domains
- Configure tenant-wide settings

Create, configure, and manage Azure AD identities

- Create, configure, and manage users
- Create, configure, and manage groups
- Configure and manage device join and registration, including writeback
- Assign, modify, and report on licenses

Implement and manage external identities

- Manage external collaboration settings in Azure AD
- Invite external users, individually or in bulk
- Manage external user accounts in Azure AD
- Configure identity providers, including SAML or WS-Fed

Implement and manage hybrid identity

- Implement and manage Azure AD Connect
- Implement and manage Azure AD Connect cloud sync
- Implement and manage Password Hash Synchronization (PHS)
- Implement and manage Pass-Through Authentication (PTA)
- Implement and manage seamless Single Sign-On (SSO)
- Implement and manage Federation, excluding manual AD FS deployments
- Implement and manage Azure AD Connect Health
- Troubleshoot synchronization errors

Implement authentication and access management (25–30%)

Plan, implement, and manage Azure Multifactor Authentication (MFA) and self-service password reset

- Plan Azure MFA deployment, excluding MFA Server
- Configure and deploy self-service password reset

- Implement and manage Azure MFA settings
- Manage MFA settings for users
- Extend Azure AD MFA to third party and on-premises devices
- Monitor Azure AD MFA activity

Plan, implement, and manage Azure AD user authentication

- Plan for authentication
- Implement and manage authentication methods
- Implement and manage Windows Hello for Business
- Implement and manage password protection and smart lockout
- Implement certificate-based authentication in Azure AD
- Configure Azure AD user authentication for Windows and Linux virtual machines on Azure

Plan, implement, and manage Azure AD conditional access

- Plan conditional access policies
- Implement conditional access policy assignments
- Implement conditional access policy controls
- Test and troubleshoot conditional access policies
- Implement session management
- Implement device-enforced restrictions
- Implement continuous access evaluation
- Create a conditional access policy from a template

Manage Azure AD Identity Protection

- Implement and manage a user risk policy
- Implement and manage sign-in risk policy
- Implement and manage MFA registration policy
- Monitor, investigate and remediate risky users
- Implement security for workload identities

Implement access management for Azure resources

- Assign Azure roles
- Configure custom Azure roles
- Create and configure managed identities
- Use managed identities to access Azure resources
- Analyze Azure role permissions
- Configure Azure Key Vault RBAC and policies

Implement access management for applications (15–20%)

Manage and monitor application access by using Microsoft Defender for Cloud Apps

- Discover and manage apps by using Microsoft Defender for Cloud Apps
- Configure connectors to apps
- Implement application-enforced restrictions
- Configure conditional access app control
- Create access and session policies in Microsoft Defender for Cloud Apps
- Implement and manage policies for OAUTH apps

Plan, implement, and monitor the integration of Enterprise applications

- Configure and manage user and admin consent
- Discover apps by using ADFS application activity reports
- Design and implement access management for apps
- Design and implement app management roles
- Monitor and audit activity in enterprise applications
- Design and implement integration for on-premises apps by using Azure AD application proxy
- Design and implement integration for SaaS apps
- Provision and manage users, groups, and roles on Enterprise applications
- Create and manage application collections

Plan and implement application registrations

- Plan for application registrations
- Implement application registrations
- Configure application permissions
- Implement application authorization
- Plan and configure multi-tier application permissions
- Manage and monitor applications by using App governance

Plan and implement identity governance in Azure AD (20–25%)

Plan and implement entitlement management

- Plan entitlements
- Create and configure catalogs
- Create and configure access packages
- Manage access requests
- Implement and manage terms of use
- Manage the lifecycle of external users in Azure AD Identity Governance settings
- Configure and manage connected organizations

- Review per-user entitlements by using Azure AD Entitlement management

Plan, implement, and manage access reviews

- Plan for access reviews
- Create and configure access reviews for groups and apps
- Create and configure access review programs
- Monitor access review activity
- Respond to access review activity, including automated and manual responses

Plan and implement privileged access

- Plan and manage Azure roles in Privileged Identity Management (PIM), including settings and assignments
- Plan and manage Azure resources in PIM, including settings and assignments
- Plan and configure Privileged Access groups
- Manage PIM requests and approval process
- Analyze PIM audit history and reports
- Create and manage break-glass accounts

Monitor Azure AD

- Design a strategy for monitoring Azure AD
- Review and analyze sign-in, audit, and provisioning logs by using the Azure Active Directory admin center
- Configure diagnostic settings, including Log Analytics, storage accounts, and Event Hub
- Monitor Azure AD by using Log Analytics, including KQL queries
- Analyze Azure AD by using workbooks and reporting in the Azure Active Directory admin center
- Monitor and improve the security posture by using the Identity Secure Score

Study resources

We recommend that you train and get hands-on experience before you take the exam. We offer self-study options and classroom training as well as links to documentation, community sites, and videos.

Study resources	Links to learning and documentation
Get trained	Choose from self-paced learning paths and modules or take an instructor-led course
Find documentation	Azure Active Directory documentation Azure identity & access security best practices External Identities documentation Azure AD Multi-Factor Authentication overview

Study resources	Links to learning and documentation
	Microsoft Defender for Cloud documentation | Microsoft Docs Identity Governance - Azure Active Directory What is Privileged Identity Management? What is Azure Active Directory monitoring? Microsoft security documentation
Ask a question	Microsoft Q&A | Microsoft Docs
Get community support	Security, compliance, and identity community hub
Follow Microsoft Learn	Microsoft Learn - Microsoft Tech Community
Find a video	Exam Readiness Zone Browse other Microsoft Learn shows

Change log

Key to understanding the table: The topic groups (also known as functional groups) are in bold typeface followed by the objectives within each group. The table is a comparison between the two versions of the exam skills measured and the third column describes the extent of the changes.

Skill area prior to February 1, 2023	Skill area as of February 1, 2023	Change
Audience profile	Audience profile	No change
Implement identities in Azure AD	**Implement identities in Azure AD**	No change
Configure and manage an Azure AD tenant	Configure and manage an Azure AD tenant	No change
Create, configure and manage Azure AD identities	Create, configure and manage Azure AD identities	No change
Implement and manage external identities	Implement and manage external identities	Minor
Implement and manage hybrid identity	Implement and manage hybrid identity	No change

Skill area prior to February 1, 2023	Skill area as of February 1, 2023	Change
Implement authentication and access management	**Implement authentication and access management**	No change
Plan, implement, and manage Azure Multifactor Authentication (MFA) and self-service password reset	Plan, implement, and manage Azure Multifactor Authentication (MFA) and self-service password reset	No change
Plan, implement, and manage Azure AD user authentication	Plan, implement, and manage Azure AD user authentication	No change
Plan, implement, and manage Azure AD conditional access	Plan, implement, and manage Azure AD conditional access	No change
Manage Azure AD Identity Protection	Manage Azure AD Identity Protection	No change
Implement access management for Azure resources	Implement access management for Azure resources	No change
Implement access management for applications	**Implement access management for applications**	No change
Manage and monitor application access by using Microsoft Defender for Cloud Apps	Manage and monitor application access by using Microsoft Defender for Cloud Apps	No change
Plan, implement, and monitor the integration of Enterprise applications	Plan, implement, and monitor the integration of Enterprise applications	No change
Plan and implement application registrations	Plan and implement application registrations	No change
Plan and implement identity governance in Azure AD	**Plan and implement identity governance in Azure AD**	No change
Plan and implement entitlement management	Plan and implement entitlement management	No change
Plan, implement, and manage access reviews	Plan, implement, and manage access reviews	No change
Plan and implement privileged access	Plan and implement privileged access	No change
Monitor Azure AD	Monitor Azure AD	No change

Skills measured prior to February 1, 2023

- Implement identities in Azure AD (20–25%)
- Implement authentication and access management (25–30%)
- Implement access management for applications (15–20%)
- Plan and implement identity governance in Azure AD (20–25%)

Implement identities in Azure AD (20–25%)

Configure and manage an Azure AD tenant

- Configure and manage Azure AD roles
- Configure delegation by using administrative units
- Analyze Azure AD role permissions
- Configure and manage custom domains
- Configure tenant-wide settings

Create, configure, and manage Azure AD identities

- Create, configure, and manage users
- Create, configure, and manage groups
- Configure and manage device join and registration, including writeback
- Assign, modify, and report on licenses

Implement and manage external identities

- Manage external collaboration settings in Azure AD
- Invite external users, individually or in bulk
- Manage external user accounts in Azure AD
- Configure identity providers, including SAML or WS-fed

Implement and manage hybrid identity

- Implement and manage Azure AD Connect
- Implement and manage Azure AD Connect cloud sync
- Implement and manage Password Hash Synchronization (PHS)
- Implement and manage Pass-Through Authentication (PTA)
- Implement and manage seamless Single Sign-On (SSO)
- Implement and manage Federation, excluding manual AD FS deployments
- Implement and manage Azure AD Connect Health
- Troubleshoot synchronization errors

Implement authentication and access management (25–30%)

Plan, implement, and manage Azure Multifactor Authentication (MFA) and self-service password reset

- Plan Azure MFA deployment, excluding MFA Server
- Configure and deploy self-service password reset
- Implement and manage Azure MFA settings
- Manage MFA settings for users
- Extend Azure AD MFA to third party and on-premises devices
- Monitor Azure AD MFA activity

Plan, implement, and manage Azure AD user authentication

- Plan for authentication
- Implement and manage authentication methods
- Implement and manage Windows Hello for Business
- Implement and manage password protection and smart lockout
- Implement certificate-based authentication in Azure AD
- Configure Azure AD user authentication for Windows and Linux virtual machines on Azure

Plan, implement, and manage Azure AD conditional access

- Plan conditional access policies
- Implement conditional access policy assignments
- Implement conditional access policy controls
- Test and troubleshoot conditional access policies
- Implement session management
- Implement device-enforced restrictions
- Implement continuous access evaluation
- Create a conditional access policy from a template

Manage Azure AD Identity Protection

- Implement and manage a user risk policy
- Implement and manage sign-in risk policy
- Implement and manage MFA registration policy
- Monitor, investigate and remediate risky users
- Implement security for workload identities

Implement access management for Azure resources

- Assign Azure roles
- Configure custom Azure roles
- Create and configure managed identities

- Use managed identities to access Azure resources
- Analyze Azure role permissions
- Configure Azure Key Vault RBAC and policies

Implement access management for applications (15–20%)

Manage and monitor application access by using Microsoft Defender for Cloud Apps

- Discover and manage apps by using Microsoft Defender for Cloud Apps
- Configure connectors to apps
- Implement application-enforced restrictions
- Configure conditional access app control
- Create access and session policies in Microsoft Defender for Cloud Apps
- Implement and manage policies for OAUTH apps

Plan, implement, and monitor the integration of Enterprise applications

- Configure and manage user and admin consent
- Discover apps by using ADFS application activity reports
- Design and implement access management for apps
- Design and implement app management roles
- Monitor and audit activity in enterprise applications
- Design and implement integration for on-premises apps by using Azure AD Application Proxy
- Design and implement integration for SaaS apps
- Provision and manage users, groups, and roles on Enterprise applications
- Create and manage application collections

Plan and implement application registrations

- Plan for application registrations
- Implement application registrations
- Configure application permissions
- Implement application authorization
- Plan and configure multi-tier application permissions
- Manage and monitor applications by using App governance

Plan and implement identity governance in Azure AD (20–25%)

Plan and implement entitlement management

- Plan entitlements
- Create and configure catalogs
- Create and configure access packages
- Manage access requests

- Implement and manage terms of use
- Manage the lifecycle of external users in Azure AD Identity Governance settings
- Configure and manage connected organizations
- Review per-user entitlements by using Azure AD Entitlement management

Plan, implement, and manage access reviews

- Plan for access reviews
- Create and configure access reviews for groups and apps
- Create and configure access review programs
- Monitor access review activity
- Respond to access review activity, including automated and manual responses

Plan and implement privileged access

- Plan and manage Azure roles in Privileged Identity Management (PIM), including settings and assignments
- Plan and manage Azure resources in PIM, including settings and assignments
- Plan and configure Privileged Access groups
- Manage PIM requests and approval process
- Analyze PIM audit history and reports
- Create and manage break-glass accounts

Monitor Azure AD

- Design a strategy for monitoring Azure AD
- Review and analyze sign-in, audit, and provisioning logs by using the Azure Active Directory admin center
- Configure diagnostic settings, including Log Analytics, storage accounts, and Event Hub
- Monitor Azure AD by using Log Analytics, including KQL queries
- Analyze Azure AD by using workbooks and reporting in the Azure Active Directory admin center
- Monitor and improve the security posture by using the Identity Secure Score