SC-300 Study Guide

Microsoft Identity and Access Administrator Exam Resources

PURPOSE

The following resources have been assembled to help you prepare for the SC-300 Microsoft Identity and Access Administrator learning track during Microsoft Certification Week.

Use this guide to understand what knowledge is needed to complete the exam and as a learning tool to help you understand areas where you feel you need additional training. It is not required that you leverage all the resources in this guide to participate in Microsoft Certification Week.

AUDIENCE

All Pax8 Partners

Table of Contents

SC-300: Exam Resources

Audience Profile for the Exam

The Microsoft Identity and Access Administrator designs, implements, and operates an organization's identity and access management systems by using Azure Active Directory (Azure AD). They manage tasks such as providing secure authentication and authorization access to enterprise applications. The administrator provides seamless experiences and self-service management capabilities for all users.

Adaptive access and governance are core elements to the role. This role is also responsible for troubleshooting, monitoring, and reporting for the identity and access environment.

The Identity and Access Administrator may be a single individual or a member of a larger team. This role 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.

Preparing with an Azure and M365 Subscription

It is highly recommended when preparing for a Microsoft exam, that you have had some level of hands-on experience with the services within the objectives. Microsoft courses have a GitHub repository for labs that are recommended and available to the public.

- Azure Free Trial: Create your Azure free account today | Microsoft Azure
- Suggested Lab Guides: https://github.com/MicrosoftLearning/AZ-900T0x-MicrosoftAzureFundamentals

The lab guides can be found at this link: https://github.com/MicrosoftLearning
Microsoft offers trial subscriptions for both Azure and Microsoft 365

Creating an Azure free subscription
Create your Azure free account today | Microsoft Azure

Creating a Microsoft 365 trial subscription
If you are new to Microsoft 365 and Azure, getting hands on experience is important not just for exam preparation, but also for professional development. If you are getting certified as a way to open doors to new job opportunities, you must understand the administration portals and how to work within them. This book will provide some exercises that will get you familiar with how to work within Microsoft 365 and Azure Active Directory. In order to follow along with the steps, it is recommended that you have a subscription to Microsoft 365 and Azure Active Directory Premium. The steps to create these in as a thirty (30) day trial are provided below.

Office 365 or Microsoft 365 trial subscription
Many of the features and capabilities discussed within the exam objectives require an enterprise level license within Microsoft 365. The enterprise licenses are the E3 and E5 licenses. Microsoft offers thirty (30) day trial licenses of these, so as you prepare for the exam, you can create this trial subscription and be able to follow along with the exercises. To get started, navigate to this link and select "try for free" under the Office 365 E5 plan: https://www.microsoft.com/en-us/microsoft-365/enterprise/compare-office-365-plans

Follow the steps to create an account. If you have already created an account previously, you may need to use a different email address to obtain the free trial.
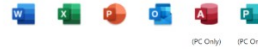
Microsoft

Thank you for choosing Office 365 E5

1. **Let's set up your account**
   Enter your work or school email address, we'll check if you need to create a new account for Office 365 E5.
   Email
   [   ]
   This is required
   [Next]

2. Tell us about yourself

3. Create your business identity

4. You're all set

What is Office 365 E5

Fully installed Office apps for PC and Mac

(PC Only)   (PC Only)

Premium services

Other benefits
- Unlimited personal cloud storage with qualifying plans
- Email hosting with 100 GB mailbox
- Online & desktop versions of Office applications
- Free FastTrack deployment support with 150+ seats

Trial highlights

25 licenses, 30-day free trial

Azure Active Directory Premium subscription
In addition to the Office 365 E5 trial subscription, you will need access to an Azure Active Directory Premium license for many of the advanced identity and access features that are discussed within the exam objectives. The best way to obtain these features is through an Enterprise Mobility + Security E5license. Microsoft also offers this as a thirty (30) day free trial.
To get started, navigate to this link and select "try now" under the Enterprise Mobility + Security E5 plan:
https://www.microsoft.com/en-us/microsoft-365/enterprise-mobility-security/compare-plans- and-pricing
This is an add-on license to Microsoft 365, so you should enter the same email address that you used to sign up for the Office 365 E5 subscription.

Exam Objectives

The following are the learning objectives for the exam. In line with each objective are links to Microsoft documentation around the specific concept or service. In addition to the documentation, there are also online courses from Microsoft Learn and the Microsoft Partner virtual training series available for additional learning resources. Access to the exam objectives can be found on Microsoft
Learn: https://docs.microsoft.com/en-us/learn/certifications/exams/sc-300

Objective: Implement an Identity Management Solution (25-30%)

Implement Initial Configuration of Azure Active Directory
- Configure and manage Azure AD directory roles
  Understand roles in Azure Active Directory
  Configure and manage Azure Active Directory roles
- Configure and manage custom domains
  Add a custom domain name to Azure Active Directory
  Configure and manage custom domains
- Configure and manage device registration options
  Configure and manage device registration
- Configure delegation by using administrative units
  Administrative units in Azure Active Directory
- Configure tenant-wide settings
  Configuration in a tenant
  Configure tenant-wide setting

Create, Configure, and Manage Identities
- Create, configure, and manage users
  Create, configure, and manage users
  Create and manage users
- Create, configure, and manage groups
  Create, configure, and manage groups
  Create and manage groups

- Manage licenses
  [Manage licenses](#)

Implement and Manage External Identities
- Manage external collaboration settings in Azure Active Directory
  [Manage external collaboration](#)
  [Manage external collaboration settings in Azure AD](#)
- Invite external users (individually or in bulk)
  [Invite external users – individually and in bulk](#)
  [Exercise: Invite guest users bulk](#)
  [Demo: Invite guest users to the app](#)
- Manage external user accounts in Azure Active Directory
  [Manage external user accounts in Azure AD](#)
- Configure identity providers (social and SAML/WS-fed)
  [Configure identity providers](#)

Implement and Manage Hybrid Identity
- Implement and manage Azure Active Directory Connect (AADC)
  [Plan, design, and implement Azure Active Directory Connect (AADC)](#)
  [Getting started with Azure AD Connect using express settings](#)
- Implement and manage Password Hash Synchronization (PHS)
  [What is password hash synchronization with Azure AD?](#)
  [Implement & manage password hash synchronization (PHS)](#)
- Implement and manage Pass-Through Authentication (PTA)
  [What is Azure AD Pass-through Authentication?](#)
  [Implement manage pass-through authentication (PTA)](#)
- Implement and manage seamless Single Sign-On (SSO)
  [Azure Active Directory Seamless Single Sign-On](#)
  [Manage pass-through authentication & seamless single sign-on](#)
- Implement and manage Federation excluding manual ADFS deployments
  [Implement and manage federation](#)
- Implement and manage Azure Active Directory Connect Health
  [Implement Azure Active Directory Connect Health](#)
  [Manage Azure Active Directory Connect Health](#)
- Troubleshoot synchronization errors
  [Trouble-shoot synchronization errors](#)

Objective: Implement an Authentication and Access Management Solution (25- 30%)

Plan and Implement Azure Multifactor Authentication (MFA)
- Plan Azure MFA deployment (excluding MFA Server)
  [What is Azure AD Multi-Factor Authentication?](#)
  [Plan your multi-factor authentication deployment](#)
- Implement and manage Azure MFA settings
  [Configure Azure AD MFA settings](#)
- Manage MFA settings for users
  [Configure users](#)

Manage User Authentication
- Administer authentication methods (FIDO2 / Passwordless)
  [Passwordless authentication options for Azure AD](#)
  [Administer FIDO2 and passwordless authentication methods](#)
- Implement an authentication solution based on Windows Hello for Business
  [Windows Hello for Business & authentication](#)
  [Implement authentication based on Windows Hello for Business](#)
- Configure and deploy self-service password reset
  [Deploy SSPR](#)
  [Configure & deploy self-service password reset](#)
- Deploy and manage password protection
  [Deploy on-premises Azure AD password protection](#)

[Deploy & manage password protection](#)
- Implement and manage tenant restrictions
[Use tenant restrictions to manage access to SaaS cloud apps](#)
[Implement & manage tenant restrictions](#)

Plan, Implement, and Administer Conditional Access
- Plan and implement security defaults
[Plan security defaults](#)
[Work with security defaults](#)
- Plan conditional access policies
[Conditional access policy](#)
- Implement conditional access policy controls and assignments (targeting, applications, and conditions)
- [Implement conditional access policies roles & assignments](#)
- Testing and troubleshooting conditional access policies
[Test & troubleshoot conditional access policies](#)
- Implement application controls
[Implement application controls](#)
- Implement session management
[Implement session management](#)
- Configure smart lockout thresholds
[Configure smart lockout thresholds](#)

Manage Azure AD Identity Protection

- Implement and manage a user risk policy
- [Implement & manage user risk policy](#)
[Enable user risk policy](#)
- Implement and manage sign-in risk policies
[Enable sign-in risk policy](#)
- Implement and manage MFA registration policy
- [Azure AD Multi-Factor Authentication registration policy](#) [Configure Azure AD MFA registration policy](#)
- Monitor, investigate, and remediate elevated risky users
- [Monitor, investigate, & remediate elevated risky users](#)

Objective: Implement Access Management for Apps (10-15%)

Plan, Implement and Monitor the Integration of Enterprise Apps for Single Sign-on (SSO)
- Implement and configure consent settings
[Configure how end-users consent to applications](#)
[Implement and configure consent settings](#)
- Discover apps by using MCAS or ADFS app report
[Discover apps by using MCAS & ADFS report](#)
- Design and implement access management for apps
[Exercise: Implement access management for apps](#)
- Design and implement app management roles
[Design & implement app management roles](#)
- Monitor and audit access/sign-on to Azure Active Directory integrated enterprise applications
[Monitor & audit access to Azure AD integrated apps](#)
- Implement token customizations
[Implement token customizations](#)
- Integrate on-premises apps by using Azure AD application proxy
[Add an on-premises app through Application Proxy in Azure AD](#)
[Integrate on-premises apps by using Azure AD app proxy](#)
- Integrate custom SaaS apps for SSO
[Integrate custom SaaS apps for single sign-onIntegrate Azure AD SSO with SaaS apps](#)

- Configure pre-integrated (gallery) SaaS apps
  Configure pre-integrated gallery SaaS apps
- Implement application user provisioning
  What is automated SaaS app user provisioning in Azure AD?
  Implement application user provisioning

On-Demand Training from Microsoft Learn

New to the cloud? Azure fundamentals is a six-part series that teaches you basic cloud concepts, provides a streamlined overview of many Azure services, and guides you with hands-on exercises to deploy your very first services for free.

- Azure Fundamentals part 1: Describe core Azure Concepts
- Azure Fundamentals part 2: Describe core Azure Services
- Azure Fundamentals part 3: Describe core solutions and management tools on Azure
- Azure Fundamentals part 4: Describe general security and network security features
- Azure Fundamentals part 5: Describe identity, governance, privacy, and compliance features
- Azure Fundamentals part 6: Describe Azure cost management and service level agreements

Virtual Training Series

This online course will provide foundational level knowledge of cloud services and how those services are provided with Microsoft Azure. The course can be taken as an optional first step in learning about cloud services and Microsoft Azure, before taking further Microsoft Azure or Microsoft cloud services courses.

All Virtual Training Series: http://aka.ms/vts