Exam SC-300 – Microsoft Identity and Access Administrator

Exam SC-300: Microsoft Identity and Access Administrator

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.

Part of the requirements for: Microsoft Certified: Identity and Access Administrator Associate
Related exams: none
Important: See details
Go to Certification Dashboard

Table of Contents

SC-300 part 1: Implement an identity management solution

Unit 1: Implement initial configuration of Azure Active Directory

Introduction

https://docs.microsoft.com/en-us/learn/modules/implement-initial-configuration-of-azure-active-directory/1-introduction

Unit 2: Configure and manage Azure Active Directory roles

https://docs.microsoft.com/en-us/learn/modules/implement-initial-configuration-of-azure-active-directory/2-configure-manage-roles

Unit 3: Exercise manage users roles

https://docs.microsoft.com/en-us/learn/modules/implement-initial-configuration-of-azure-active-directory/3-exercise-manage-users-roles

Unit 4: Configure and manage custom domains

https://docs.microsoft.com/en-us/learn/modules/implement-initial-configuration-of-azure-active-directory/4-configure-manage-custom-domains

Unit 5: Configure and manage device registration

https://docs.microsoft.com/en-us/learn/modules/implement-initial-configuration-of-azure-active-directory/5-configure-manage-device-registration

- Azure AD registered devices
- Azure AD joined devices
- Hybrid Azure AD joined devices

Unit 6: Configure delegation by using administrative units

https://docs.microsoft.com/en-us/learn/modules/implement-initial-configuration-of-azure-active-directory/6-configure-delegation-administrative-units

- Plan your administrative units
- Delegate administration in Azure Active Directory
- Plan for Delegation
- Define roles
- Delegate app administration
- Delegate app ownership
- Develop a security plan
- Establish emergency accounts

- Secure your administrator roles

Unit 7: Configure tenant-wide setting

https://docs.microsoft.com/en-us/learn/modules/implement-initial-configuration-of-azure-active-directory/7-configure-tenant-wide-options

- Configure tenant-wide user settings
- Member and guest users
- Sign in with LinkedIn
- Manage security defaults
- Configure the external user options
- Configure tenant properties for the directory

Unit 8: Exercise - setting tenant-wide properties

https://docs.microsoft.com/en-us/learn/modules/implement-initial-configuration-of-azure-active-directory/8-exercise-set-tenant-wide-properties

Unit 9: Knowledge check

Check your knowledge

1. A domain name is included as part of a user name or email address for users and groups. Can a domain name also be included as part of an application or other resource?

- (●) Yes, a domain name can be included as part of an application or other resource if the domain name is owned by the organization that contains the resource. ✓

  Correct. When an organization that contains and application or other resources, the domain can be included if it is owned by the same organization.

- ( ) A domain name can be included as part of the app ID URI for an application, but cannot be included as part of other resources.
- ( ) No, a domain name cannot be included as part of an application or other resource.

2. The proliferation of many types of devices and bring your own device (BYOD) concept require IT professionals to accommodate two rather different goals. One goal is to allow users to be productive wherever and anytime. What is the other goal?

- ( ) Provide antimalware apps for a various devices.
- ( ) Establish baseline security guidelines for users.
- (●) Protect the organization's assets. ✓

  Correct. Identity is new perimeter is a common security phrase these days, meaning that validation or both people and devices are required to protect company assets.

3. Azure AD guest users have restricted directory permissions. Which of the following answers best describes guest users capabilities?

3. Azure AD guest users have restricted directory permissions. Which of the following answers best describes guest users capabilities?

- (●) They can manage their own profile, change their own password, and add other B2B guests to groups. ✕

  Sorry, that's incorrect. Azure AD guest users cannot add other B2B guests to groups.

- ( ) They can manage their own profile, change their own password, and retrieve some information about other users, groups, and apps.
- ( ) They can manage their own profile, change their own password, and identify group members or other directory objects.

Unit 10: Summary and Resources

Now that you have reviewed this module, you should be able to:

- Configure and manage Azure Active Directory roles.
- Configure and manage custom domains.
- Configure and manage device registration options.
- Configure delegation by using administrative units.
- Configure tenant-wide settings

Use these resources to discover more.

- Information about which roles manage Azure resources and which roles manage Azure AD resources is available at Classic subscription administrator roles, Azure roles, and Azure AD roles.
- For more information about roles, see Understand Azure role definitions.
- For information about how to use PIM, see Privileged Identity Management.
- The following step-by-step guides provide information on how you can use Conditional Access to configure equivalent policies to those policies enabled by security defaults:
  - Require MFA for administrators
  - Require MFA for Azure management
  - Block legacy authentication
  - Require MFA for all users
  - Require Azure AD MFA registration - Requires Azure AD Identity Protection part of Azure AD Premium P2.

SC-300 Part 2 Implement an Authentication and Access Management solution

Unit 1: Introduction

https://docs.microsoft.com/en-us/learn/modules/secure-aad-users-with-mfa/1-introduction

Unit 2: What is Azure AD Multi-Factor Authentication?

https://docs.microsoft.com/en-us/learn/modules/secure-aad-users-with-mfa/2-azure-multi-factor-authentication

rotecting your cloud assets is one of the primary goals for security group. One of the primary ways unauthorized users get access to systems is by obtaining a valid username/password combination. Azure can help mitigate this with several features of Azure Active Directory including:

- **Password complexity rules**. This will force users to generate hard(er)-to-guess passwords.
- **Password expiration rules**. You can force users to change their passwords on a periodic basis (and avoid using previous-used passwords).
- **Self-service password reset (SSPR)**. This allows users to self-serve and reset their password if they have forgotten it without involving an IT department.
- **Azure AD Identity Protection**. To help protect your organization's identities, you can configure risk-based policies that automatically respond to risky behaviors. These policies can either automatically block the behaviors or initiate remediation, including requiring password changes.
- **Azure AD password protection**. You can block commonly used and compromised passwords via a globally banned-password list.
- **Azure AD smart lockout**. Smart lockout helps lock out malicious hackers who are trying to guess your users' passwords or use brute-force methods to get in. It recognizes sign-ins coming from valid users and treats them differently than the ones of malicious hackers and other unknown sources.
- **Azure AD Application Proxy**. You can provision security-enhanced remote access to on-premises web applications.
- **Single sign-on (SSO)** access to your applications. This includes thousands of pre-integrated SaaS apps.
- **Azure AD Connect**. Create and manage a single identity for each user across your hybrid enterprise, keeping users, groups, and devices in sync.

These are all great options which deter someone *guessing* or brute-forcing a password. However, sometimes passwords are obtained through social engineering, or poor physical security practices (like putting your password on a sticky note under your keyboard!). In these cases, the above features won't stop an intrusion. Instead, security administrators will want to turn to **Azure AD Multi-Factor Authentication (MFA)**.

What is Azure AD MFA?

Azure AD Multi-Factor Authentication (MFA) supplies added security for your identities by requiring two or more elements for full authentication.

These elements fall into three categories:

- **Something you know** - which might be a password or the answer to a security question.
- **Something you possess** - which might be a mobile app that receives a notification or a token-generating device.
- **Something you are** - which typically is a biometric property, such as a fingerprint or face scan used on many mobile devices.

Using Azure AD MFA increases identity security by limiting the impact of credential exposure. To fully authenticate, a malicious hacker who has a user's password would also need their phone or their fingerprint. Authentication with only a single factor is insufficient, and without authentication from Azure AD MFA, a malicious hacker is unable to use those credentials to authenticate. You should enable Azure AD MFA wherever possible, because it adds enormous benefits to security.

Azure AD MFA is the Microsoft two-step verification solution. Azure AD MFA helps safeguard access to data and applications while meeting user demand for a simple sign-in process. It delivers strong authentication via a range of verification methods, including phone call, text message, or mobile app verification. The security of Azure AD

MFA lies in its layered approach. Compromising multiple authentication factors presents a significant challenge for malicious hackers. Even if a malicious hacker manages to learn the user's password, it is useless without also possessing the trusted device. If the user loses the device, a person who finds it won't be able to use it without the user's password.

How to get Multi-Factor Authentication?

Multi-Factor Authentication comes as part of the following offerings:

- **Azure Active Directory Premium** or **Microsoft 365 Business** - Both of these offerings support Azure AD Multi-Factor Authentication using security defaults to require multi-factor authentication.
- **Azure AD Free** or standalone **Microsoft 365** licenses - Use security defaults that require multi-factor authentication for your users and administrators.
- **Azure Active Directory Global Administrators** - A subset of Azure AD Multi-Factor Authentication capabilities are available as a means to protect global administrator accounts.

Unit 3:

Unit 3: Plan your multi-factor authentication deployment

Before starting a deployment of Azure AD Multi-Factor Authentication, there are several things you should decide.

First, consider rolling out MFA in waves. Start with a small group of pilot users to evaluate the complexity of your environment and identify any setup issues or unsupported apps or devices. Then broaden that group over time and evaluating the results with each pass until your entire company is enrolled.

Next, make sure to create a full communication plan. Azure AD MFA has several user interaction requirements including a registration process. Keep users informed every step of the way and let them know what they are required to do, important dates, and how to get answers to questions if they have trouble. Microsoft provides communication templates including posters, and email templates to help draft your communications.

Azure AD MFA policies

Azure AD Multi-factor Authentication is enforced with **Conditional Access** policies. Conditional Access policies are IF-THEN statements. **IF** a user wants to access a resource, **THEN** they must complete an action. For example, a payroll manager wants to access the payroll application and is required to perform multi-factor authentication to access it. Other common access requests that might require MFA include:

- IF a specific cloud application is accessed
- IF a user is accessing a specific network
- IF a user is accessing a specific client application
- IF a user is registering a new device

Deciding supported authentication methods

When you turn on Azure AD MFA, you can choose the authentication methods you want to make available. You should always support more than one method so users have a backup option in case their primary method is unavailable. You can choose from the following methods:

DECIDING SUPPORTED AUTHENTI

Method	Description
Mobile App Verification code	A mobile authentication app such as the Microsoft Authenticator app can be used to retrieve an OATH which is then entered into the sign-in interface. This code is changed every 30 seconds and the app wo is limited. Note that this approach doesn't work in China on Android devices.
Call to a phone	Azure can call a supplied phone number. The user then approves the authentication using the keypad. backup method.
Text message to a phone	A text message with a verification code can be sent to a mobile phone. The user then enters the verifi sign-in interface to complete the authentication.

Administrators can enable one or more of the options above and then users can opt-in to each support authentication method they want to use.

Selecting an authentication method

Finally, you must decide how users will register their selected methods. The easiest approach is to use **Azure Active Directory Identity Protection**. If your organization

has licenses for Identity Protection, you can configure it to prompt users to register for MFA the next time they sign in.

Users can also be prompted to register for MFA when they try to use an application or service that requires multi-factor authentication. Finally, you can enforce registration using a Conditional Access policy applied to an Azure group containing all users in your organization. This approach requires some manual work to periodically review the group to remove registered users. There are some useful scripts in the documentation to automate some of this process.

Unit 4: Exercise - Enable Azure AD Multi-Factor Authentication

https://docs.microsoft.com/en-us/learn/modules/secure-aad-users-with-mfa/4-exercise-mfa

References

https://docs.microsoft.com/en-us/search/?terms=sc-300%20exam&category=Learn