



SC-300^{Q&As}

Microsoft Identity and Access Administrator

Pass Microsoft SC-300 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.pass4itsure.com/sc-300.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Microsoft
Official Exam Center

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers





QUESTION 1

You have a Microsoft 365 E5 subscription.

Users authorize third-party cloud apps to access their data.

You need to configure an alert that will be triggered when an app requires high permissions and is authorized by more than 20 users.

Which type of policy should you create in the Microsoft Defender for Cloud Apps portal?

- A. anomaly detection policy
- B. OAuth app policy
- C. access policy
- D. activity policy

Correct Answer: B

<https://learn.microsoft.com/en-us/defender-cloud-apps/app-permission-policy>

Reason :In addition to the existing investigation of OAuth apps connected to your environment, you can set permission policies so that you get automated notifications when an OAuth app meets certain criteria. For example, you can automatically be alerted when there are apps that require a high permission level and were authorized by more than 50 users.

QUESTION 2

HOTSPOT

You have an Azure Active Directory (Azure AD) tenant that has multi-factor authentication (MFA) enabled.

The account lockout settings are configured as shown in the following exhibit.

Account lockout

Temporarily lock accounts in the multi-factor authentication service if there are too many denied authentication attempts in a row. This feature only applies to users who enter a PIN to authenticate.

Number of MFA denials to trigger account lockout *

3

Minutes until account lockout counter is reset *

60

Minutes until account is automatically unblocked *

30

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic. NOTE: Each correct selection is worth one point.



Hot Area:

A user account will be locked out if the user enters the wrong [answer choice] three times

Email address
Microsoft Authenticator app code
password

If a user account is locked, the user can Sign in again successfully after [answer Choice] minutes.

30
60
90

Correct Answer:

A user account will be locked out if the user enters the wrong [answer choice] three times

Email address
Microsoft Authenticator app code
password

If a user account is locked, the user can Sign in again successfully after [answer Choice] minutes.

30
60
90

QUESTION 3

You have an Azure Active Directory (Azure AD) tenant named conto.so.com that has Azure AD Identity Protection enabled. You need to Implement a sign-in risk remediation policy without blocking access. What should you do first?

- A. Configure access reviews in Azure AD.
- B. Enforce Azure AD Password Protection.
- C. implement multi-factor authentication (MFA) for all users.
- D. Configure self-service password reset (SSPR) for all users.

Correct Answer: C

MFA and SSPR are both required. However, MFA is required first.

Reference: <https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-remediate-unblock> <https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-sspr-deployment>



QUESTION 4

HOTSPOT

You need to implement the planned changes and technical requirements for the marketing department.

What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

To configure user access:

<input type="text"/>
An access package
An access review
A conditional access policy

To enable collaboration with fabrikam.com:

<input type="text"/>
An accepted domain
A connected organization
A custom domain name

Correct Answer:

Answer Area

To configure user access:

<input type="text"/>
An access package
An access review
A conditional access policy

To enable collaboration with fabrikam.com:

<input type="text"/>
An accepted domain
A connected organization
A custom domain name

Reference: <https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-organization>

**QUESTION 5**

You have an Azure subscription that contains an Azure SQL database named db1.

You deploy an Azure App Service web app named App1 that provides product information to users that connect to App1 anonymously.

You need to provide App1 with access to db1. The solution must meet the following requirements:

1.

Credentials must only be available to App1.

2.

Administrative effort must be minimized. Which type of credentials should you use?

- A. a system-assigned managed identity
- B. an Azure Active Directory (Azure AD) user account
- C. a SQL Server account
- D. a user-assigned managed identity

Correct Answer: A

QUESTION 6

You have a Microsoft 365 subscription that contains a user named User1.

You need to ensure that User1 can create access reviews for Azure AD roles. The solution must use the principal of least privilege.

Which role should you assign to User1?

- A. Privileged role administrator
- B. Identify Governance administrator
- C. User administrator
- D. User Access Administrator

Correct Answer: B

QUESTION 7**HOTSPOT**

You have a Microsoft 365 tenant.



You create a named location named HighRiskCountries that contains a list of high-risk countries.

You need to limit the amount of time a user can stay authenticated when connecting from a high-risk country.

What should you configure in a conditional access policy? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Configure HighRiskCountries by using:

<input type="checkbox"/>	A cloud app or action
<input type="checkbox"/>	A condition
<input type="checkbox"/>	A grant control
<input type="checkbox"/>	A session control

Configure Sign-in frequency by using:

<input type="checkbox"/>	A cloud app or action
<input type="checkbox"/>	A condition
<input type="checkbox"/>	A grant control
<input type="checkbox"/>	A session control

Correct Answer:

Configure HighRiskCountries by using:

<input type="checkbox"/>	A cloud app or action
<input checked="" type="checkbox"/>	A condition
<input type="checkbox"/>	A grant control
<input type="checkbox"/>	A session control

Configure Sign-in frequency by using:

<input type="checkbox"/>	A cloud app or action
<input type="checkbox"/>	A condition
<input type="checkbox"/>	A grant control
<input checked="" type="checkbox"/>	A session control

QUESTION 8

HOTSPOT

You have an Azure Active Directory (Azure AD) tenant that contains an administrative unit named Department1.



Department1 has the users shown in the Users exhibit. (Click the Users tab.)

Dashboard > ContosoAzureAD > Department1 Administrative Unit

Department1 Administrative Unit | Users (Preview)

ContosoAzureAD - Azure Active Directory

+ Add member | Remove member | Bulk operations | Refresh | Columns | Preview features | Got feedback?

This page includes previews available for your evaluation. View previews →

Search users | Add filters

2 users found

Name	User principal name	User type	Directory synced
<input type="checkbox"/> US User1	User1@m365x629615.onmicrosoft.com	Member	No
<input type="checkbox"/> US User2	User2@m365x629615.onmicrosoft.com	Member	No

Department1 has the groups shown in the Groups exhibit. (Click the Groups tab.)

Dashboard > ContosoAzureAD > Department1 Administrative Unit

Department1 Administrative Unit | Groups

ContosoAzureAD - Azure Active Directory

+ Add | Remove | Refresh | Columns | Preview features | Got feedback?

Search groups | Add filters

Name	Group Type	Membership Type
<input type="checkbox"/> GR Group1	Security	Assigned
<input type="checkbox"/> GR Group2	Security	Assigned

Department1 has the user administrator assignments shown in the Assignments exhibit. (Click the Assignments tab.)
The members of Group2 are shown in the Group2 exhibit. (Click the Group2 tab.)

Dashboard > ContosoAzureAD > Identity Governance > Privileged Identity Management > ContosoAzureAD >

User Administrator | Assignments

Privileged Identity Management | Azure AD roles

+ Add assignments | Settings | Refresh | Export | Got feedback?

Eligible assignments | Active assignments | Expired assignments

Search by member name or principal name

Name	Principal name	Type	Scope
User Administration			
Admin1	Admin1@m365x629615.onmicrosoft.com	User	Department1 Administrative Unit (Administrative unit)
Admin2	Admin2@m365x629615.onmicrosoft.com	User	Directory



Dashboard > ContosoAzureAD > Groups > Group2

Group2 | Members

Group

» [+ Add members](#) [Remove](#) [Refresh](#) [Bulk operations](#) [Columns](#) [Preview features](#) [Got feedback?](#)

This page includes previews available for your evaluation. [View previews](#) →

Direct members

Name	User type
<input type="checkbox"/>  User3	Member
<input type="checkbox"/>  User4	Member

For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
Admin1 can reset the passwords of User3 and User4.	<input type="radio"/>	<input type="radio"/>
Admin1 can add User1 to Group 2	<input type="radio"/>	<input type="radio"/>
Admin 2 can reset the password of User1.	<input type="radio"/>	<input type="radio"/>

Correct Answer:



Answer Area

Statements	Yes	No
Admin1 can reset the passwords of User3 and User4.	<input type="radio"/>	<input checked="" type="radio"/>
Admin1 can add User1 to Group 2	<input checked="" type="radio"/>	<input type="radio"/>
Admin 2 can reset the password of User1.	<input checked="" type="radio"/>	<input type="radio"/>

QUESTION 9

You have 2,500 users who are assigned Microsoft Office 365 Enterprise E3 licenses. The licenses are assigned to individual users.

From the Groups blade in the Azure Active Directory admin center, you assign Microsoft 365 Enterprise E5 licenses to the users.

You need to remove the Office 365 Enterprise E3 licenses from the users by using the least amount of administrative effort.

What should you use?

- A. the Identity Governance blade in the Azure Active Directory admin center
- B. the Set-AzureAdUser cmdlet
- C. the Licenses blade in the Azure Active Directory admin center
- D. the Set-WindowsProductKey cmdlet

Correct Answer: C

You can unassign licenses from users on either the Active users page, or on the Licenses page. The method you use depends on whether you want to unassign product licenses from specific users or unassign users licenses from a specific

product.

Note:

There are several versions of this question in the exam. The question has two possible correct answers:

1.



the Licenses blade in the Azure Active Directory admin center

2.

the Set-MsolUserLicense cmdlet

Other incorrect answer options you may see on the exam include the following:

1.

the Administrative units blade in the Azure Active Directory admin center

2.

the Groups blade in the Azure Active Directory admin center

3.

the Set-AzureAdGroup cmdlet

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/admin/manage/remove-licenses-from-users?view=o365-worldwide>

QUESTION 10

You have an Azure subscription that contains the custom roles shown in the following table.

Name	Type
Role1	Azure Active Directory (Azure AD) role
Role2	Azure subscription role

You need to create a custom Azure subscription role named Role3 by using the Azure portal. Role3 will use the baseline permissions of an existing role. Which roles can you clone to create Role3?

- A. Role2 only
- B. built-in Azure subscription roles only
- C. built-in Azure subscription roles and Role2 only
- D. built-in Azure subscription roles and built-in Azure AD roles only
- E. Role1, Role2 built-in Azure subscription roles, and built-in Azure AD roles

Correct Answer: C



QUESTION 11

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while

others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have a Microsoft 365 tenant.

You have 100 IT administrators who are organized into 10 departments.

You create the access review shown in the exhibit. (Click the Exhibit tab.)



Create an access review

Access reviews allow reviewers to attest to whether users still need to be in a role.

Review name *

Description ⓘ

Start date *

Frequency

Duration (in days) ⓘ

End ⓘ Never End by Occurrences

Number of times

End date

Users

Scope Everyone

Review role membership (permanent and eligible) *
Application Administrator and 72 others

Reviewers

Reviewers

(Preview) Fallback reviewers ⓘ
Megan Bowen

Upon completion settings

Start

You discover that all access review requests are received by Megan Bowen.

You need to ensure that the manager of each department receives the access reviews of their respective department.

Solution: You add each manager as a fallback reviewer.

Does this meet the goal?



A. Yes

B. No

Correct Answer: B

Reference: <https://docs.microsoft.com/en-us/azure/active-directory/governance/create-access-review>

QUESTION 12

You have an Azure Active Directory (Azure AD) tenant that contains the users shown in the following table.

Name	Group
User1	Group1
User2	Group1
User3	Group2
User4	Group2
User5	None

You have an administrative unit named Au1. Group1, User2, and User3 are members of Au1.

User5 is assigned the User administrator role for Au1.

For which users can User5 reset passwords?

A. User1, User2, and User3

B. User1 and User2 only

C. User3 and User4 only

D. User2 and User3 only

Correct Answer: D

QUESTION 13

HOTSPOT

A user named User1 attempts to sign in to the tenant by entering the following incorrect passwords:

1.

Pa55w0rd12



2.

Pa55w0rd12

3.

Pa55w0rd12

4.

Pa55w.rd12

5.

Pa55w.rd123

6.

Pa55w.rd123

7.

Pa55w.rd123

8.

Pa55word12

9.

Pa55word12 10.Pa55word12 11.Pa55w.rd12

You need to identify how many sign-in attempts were tracked for User1, and how User1 can unlock her account before the 300-second lockout duration expires.

What should identify? To answer, select the appropriate

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

Tracked sign-in attempts:

	▼
4	
5	
10	
11	

Unlock by:

	▼
Clearing the browser cache	
Signing in by using inPrivate browsing mode	
Performing a self-service password reset (SSPR)	

Correct Answer:

Answer Area

Tracked sign-in attempts:

	▼
4	
5	
10	
11	

Unlock by:

	▼
Clearing the browser cache	
Signing in by using inPrivate browsing mode	
Performing a self-service password reset (SSPR)	

Reference: <https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-sspr-deployment>

[Latest SC-300 Dumps](#)

[SC-300 Practice Test](#)

[SC-300 Study Guide](#)