



# SC-300<sup>Q&As</sup>

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 that contains a Microsoft SharePoint Online site named Site1. Site1 hosts PDF files.

You need to prevent users from printing the files directly from Site1.

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

- A. activity policy
- B. access policy
- C. file policy
- D. session policy

Correct Answer: D

---

### QUESTION 2

You create a conditional access policy that blocks access when a user triggers a high-severity sign-in alert. You need to test the policy under the following conditions:

1.

A user signs in from another country.

2.

A user triggers a sign-in risk. What should you use to complete the test?

- A. the Conditional Access What If tool
- B. sign-ins logs in Azure Active Directory (Azure AD)
- C. the activity logs in Microsoft Defender for Cloud Apps
- D. access reviews in Azure Active Directory (Azure AD)

Correct Answer: A

---

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

Name	Role
User1	Conditional Access administrator
User2	Authentication administrator
User3	Security administrator
User4	Security operator

You plan to implement Azure AD Identity Protection.

Which users can configure the user risk policy, and which users can view the risky users report? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Configure the user risk policy:

User3 only
User3 and User4 only
User1, User2, and User3 only
User1, User3, and User4 only
User1, User2, User3, and User4

View the risky users report:

User3 only
User3 and User4 only
User1, User2, and User3 only
User1, User3, and User4 only
User1, User2, User3, and User4

Correct Answer:

Configure the user risk policy:

User3 only
User3 and User4 only
User1, User2, and User3 only
User1, User3, and User4 only
User1, User2, User3, and User4

View the risky users report:

User3 only
User3 and User4 only
User1, User2, and User3 only
User1, User3, and User4 only
User1, User2, User3, and User4

**QUESTION 5**

You have the Azure resources show in the following table.



Name	Description
User1	User account
Group1	Security group that uses the Dynamic user membership type
VM1	Virtual machine with a system-assigned managed identity
App1	Enterprise application
RG1	Resource group

Which identities can you assign the Contributor role for RG1?

- A. User1 only
- B. User1 and Group1 only
- C. User1 and VM1 only
- D. User1, VM1, and App1 only
- E. User1, Group1, VM1, and App1

Correct Answer: E

---

### QUESTION 6

#### 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:



## Answer Area

Configure HighRiskCountries by using:

	▼
A cloud app or action	
A condition	
A grant control	
A session control	

Configure Sign-in frequency by using:

	▼
A cloud app or action	
A condition	
A grant control	
A session control	

Correct Answer:



## Answer Area

Configure HighRiskCountries by using:

	▼
A cloud app or action	
A condition	
A grant control	
A session control	

Configure Sign-in frequency by using:

	▼
A cloud app or action	
A condition	
A grant control	
A session control	

Reference: <https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition>

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-session>

### QUESTION 7

#### HOTSPOT

You have an Azure Active Directory (Azure AD) tenant that has Security defaults disabled.

You are creating a conditional access policy as shown in the following exhibit.



# New

Conditional access policy

Control user access based on conditional access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Control user access based on users and groups assignment for all users, specific groups of users, directory roles, or external guest users. [Learn more](#)

Name \*

## Assignments

Users and groups ⓘ >  
 Specific users included

Cloud apps or actions ⓘ >  
 All cloud apps

Conditions ⓘ >  
 0 conditions selected

## Access controls

Grant ⓘ >  
 0 controls selected

Session ⓘ >  
 0 controls selected

## Include

Exclude

- None
- All users
- Select users and groups

All guest users (preview) ⓘ

Directory roles (preview) ⓘ

Users and groups

Select ⓘ >

1 user

 User1  
 user1@sk200922outlook.onm... ⓘ

Enable policy

Report-only  On  Off

Create

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:

### Answer Area

To ensure that User1 is prompted for multi-factor authentication (MFA) when accessing Cloud apps, you must configure the **[answer choice]**.

- Conditions settings
- Enable policy setting
- Grant settings
- Sessions settings
- Users and groups setting

To ensure that User1 is prompted for authentication every eight hours, you must configure the **[answer choice]**.

- Conditions settings
- Enable policy setting
- Grant settings
- Sessions settings
- Users and groups setting

Correct Answer:

### Answer Area

To ensure that User1 is prompted for multi-factor authentication (MFA) when accessing Cloud apps, you must configure the **[answer choice]**.

- Conditions settings
- Enable policy setting
- Grant settings
- Sessions settings
- Users and groups setting

To ensure that User1 is prompted for authentication every eight hours, you must configure the **[answer choice]**.

- Conditions settings
- Enable policy setting
- Grant settings
- Sessions settings
- Users and groups setting

### QUESTION 8

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



Name	Member of
User1	Group1
User2	Group2
User3	Group3

The tenant has the authentication methods shown in the following table.

Method	Target	Enabled
FIDO2	Group2	Yes
Microsoft Authenticator app	Group1	Yes
SMS	Group3	Yes

Which users will sign in to cloud apps by matching a number shown in the app with a number shown on their phone?

- A. User1 only
- B. User2 only
- C. User3 only
- D. User1 and User2 only
- E. User2 and User3 only

Correct Answer: A

### QUESTION 9

You configure a new Microsoft 365 tenant to use a default domain name of contosso.com.

You need to ensure that you can control access to Microsoft 365 resource-, by using conditional access policy.

What should you do first?

- A. Disable the User consent settings.
- B. Disable Security defaults.
- C. Configure a multi-factor authentication (MFA) registration policy1.
- D. Configure password protection for Windows Server Active Directory.

Correct Answer: B

**QUESTION 10**

You need implement the planned changes for application access to organizational data. What should you configure?

- A. authentication methods
- B. the User consent settings
- C. access packages
- D. an application proxy

Correct Answer: D

---

**QUESTION 11**

You have a Microsoft 365 ES subscription that user Microsoft Defender for Cloud Apps and Yammer.

You need prevent users from signing in to Yammer from high-risk locations.

What should you do in the Microsoft Defender for Cloud Apps portal?

- A. Create an access Policy.
- B. Create an activity policy.
- C. Unsanction Yammer.
- D. Create an anomaly detection policy.

Correct Answer: A

---

**QUESTION 12**

You have a Microsoft 365 tenant.

The Azure Active Directory (Azure AD) tenant syncs to an on-premises Active Directory domain.

You plan to create an emergency-access administrative account named Emergency1.

Emergency1 will be assigned the Global administrator role in Azure AD. Emergency1 will be used in the event of Azure AD functionality failures and on-premises infrastructure failures.

You need to reduce the likelihood that Emergency1 will be prevented from signing in during an emergency.

What should you do?

- A. Configure Azure Monitor to generate an alert if Emergency1 is modified or signs in.



- B. Require Azure AD Privileged Identity Management (PIM) activation of the Global administrator role for Emergency1.
- C. Configure a conditional access policy to restrict sign-in locations for Emergency1 to only the corporate network.
- D. Configure a conditional access policy to require multi-factor authentication (MFA) for Emergency1.

Correct Answer: A

---

### QUESTION 13

You need to modify the settings of the User administrator role to meet the technical requirements. Which two actions should you perform for the role? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

- A. Select Require justification on activation.
- B. Set all assignments to Active.
- C. Set all assignments to Eligible.
- D. Modify the Expire eligible assignments after setting.
- E. Select Require ticket information on activation.

Correct Answer: AC

---

### QUESTION 14

You need to track application access assignments by using Identity Governance. The solution must meet the delegation requirements. What should you do first?

- A. Modify the User consent settings for the enterprise applications.
- B. Create a catalog.
- C. Create a program.
- D. Modify the Admin consent requests settings for the enterprise applications.

Correct Answer: B

Reference: <https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlementmanagement-overview>

---

### QUESTION 15

#### HOTSPOT

You have a Microsoft 365 tenant that contains a group named Group1 as shown in the Group1 exhibit. (Click the Group1 tab.)



```
PS C:\> Get-AzureADGroup -searchstring "group1" | Get-AzureADGroupowner

ObjectID                               DisplayName  UserPrincipalName  UserType
-----
a7f7d405-636f-4493-b971-5c2b7a131b1c Admin        admin@m365x629615.onmicrosoft.com Member

PS C:\> Get-AzureADGroup -searchstring "group1" | GetAzureADGroupMember | ft displayname_

DisplayName
-----
User1
User4
Group3
```

You create an enterprise application named App1 as shown in the App1 Properties exhibit. (Click the App1 Properties tab.)

Dashboard > ContosoAzureAD > Enterprise applications > App1

**App1** Properties  
Enterprise Application

Save Discard Delete Got feedback?

Enabled for users to sign-in?  Yes  No

Name

Homepage URL

Logo

User access URL

Application ID

Object ID

Terms of Service Url

Privacy Statement Url

Reply URL

User assignment required?  Yes  No

Visible to users?  Yes  No

You configure self-service for App1 as shown in the App1 Self-service exhibit. (Click the App1 Self-service tab.)



Dashboard > ContosoAzureAD > Enterprise applications > App1

## App1 | Self-service

Enterprise application

Overview

Deployment Plan

Manage

Properties

Owners

Roles and administrators (Pre...

Users and groups

Single sign-on

Provisioning

Application proxy

Self-service

Security

Conditional Access

Permissions

Save Discard

Allow users to request access to this application?  Yes  No

To which group should assigned users be added?

Require approval before granting access to this application?  Yes  No

Who is allowed to approve access to this application?

To which role should users be assigned in this application?

## Select approvers

Search

User1  
User1@m365x629615.onmicrosoft.com  
Selected

User2  
User2@m365x629615.onmicrosoft.com

User3  
User3@m365x629615.onmicrosoft.com

User4  
User4@m365x629615.onmicrosoft.com

### Selected approvers

User1  
User1@m365x629615.onmicrosoft.com

Remove

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
The members of Group3 can access App1 without first being approved by User1.	<input type="radio"/>	<input type="radio"/>
After you configure self-service for App1, the owner of Group1 is User1.	<input type="radio"/>	<input type="radio"/>
App1 appears in the Microsoft Office 365 app launcher of User4.	<input type="radio"/>	<input type="radio"/>

Correct Answer:



## Answer Area

Statements	Yes	No
The members of Group3 can access App1 without first being approved by User1.	<input type="radio"/>	<input checked="" type="radio"/>
After you configure self-service for App1, the owner of Group1 is User1.	<input type="radio"/>	<input checked="" type="radio"/>
App1 appears in the Microsoft Office 365 app launcher of User4.	<input type="radio"/>	<input checked="" type="radio"/>

No No No

a) When you assign a group to an application, only users in the group will have access. The assignment does not cascade to nested groups. b) Tested in lab, existing owners will be replaced. Also direct assignment (resource owner) is path of least privilege. (replicated in test) c) Application setting "\\visible to users\\" is set to No, then no users see this application on their My Apps portal and O365 launcher.

Reference a) <https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/assign-user-or-group-access-portal>

b) maybe <https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-manage-groups> c)

<https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/application-properties#visible-to-users>

[Latest SC-300 Dumps](#)

[SC-300 PDF Dumps](#)

[SC-300 Practice Test](#)