

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.pass2lead.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 an Azure AD tenant

You configure User consent settings to allow users to provide consent to apps from verified publishers.

You need to ensure that the users can only provide consent to apps that require low impact permissions.

What should you do?

- A. Create an access package.
- B. Configure permission classifications.
- C. Create an enterprise application collection.
- D. Create an access review.

Correct Answer: B

QUESTION 2

You have a Microsoft 365 ES subscription that contains a user named User1. User1 is eligible for the Application administrator role.

User1 needs to configure a new connector group for an application proxy.

What should you do to activate the role for User1?

- A. the Microsoft Defender for Cloud Apps portal
- B. the Microsoft 365 admin center
- C. the Azure Active Directory admin center
- D. the Microsoft 365 Defender portal

Correct Answer: C

QUESTION 3

You need to sync the ADatum users. The solution must meet the technical requirements. What should you do?

- A. From the Microsoft Azure Active Directory Connect wizard, select Customize synchronization options.
- B. From PowerShell, run Set-ADSyncScheduler.
- C. From PowerShell, run Start-ADSyncSyncCycle.
- D. From the Microsoft Azure Active Directory Connect wizard, select Change user sign-in.

Correct Answer: A

You need to select Customize synchronization options to configure Azure AD Connect to sync the Adatum organizational unit (OU).

QUESTION 4

HOTSPOT

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

Name	Type	Directory synced
User1	Member	Yes
User2	Member	No
User3	Guest	No

For which users can you configure the Job title property and the Usage location property in Azure AD? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Job title property:

▼
User2 only
User1 and User2 only
User2 and User3 only
User1, User2, and User3

Usage location property:

▼
User2 only
User1 and User2 only
User2 and User3 only
User1, User2, and User3

Correct Answer:

Job title property:

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

Usage location property:

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

QUESTION 5

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

Name	Usage location	Department	Job title
User1	United States	Sales	Associate
User2	Finland	Sales	SalesRep
User3	Australia	Sales	Manager

You create a dynamic user group and configure the following rule syntax.

```
user.usageLocation -in ["US","AU"] -and (user.department -eq "Sales") -and -not (user.jobTitle -eq "Manager") -or (user.jobTitle -eq "SalesRep")
```

Which users will be added to the group?

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

Correct Answer: D

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:

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:

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

QUESTION 7

You have an Azure Active Directory (Azure AD) tenant named contoso.com.

You plan to bulk invite Azure AD business-to-business (B2B) collaboration users.

Which two parameters must you include when you create the bulk invite? Each correct answer presents part of the solution

NOTE: Each correct selection is worth one point.

- A. email address
- B. redirection URL
- C. username
- D. shared key
- E. password

Correct Answer: AB

Reference: <https://docs.microsoft.com/en-us/azure/active-directory/external-identities/tutorial-bulk-invite>

QUESTION 8

HOTSPOT

Your company has an Azure Active Directory (Azure AD) tenant named contoso.com. The company has a business partner named Fabrikam, Inc.

Fabrikam uses Azure AD and has two verified domain names of fabrikam.com and litwareinc.com. Both domain names are used for Fabrikam email addresses.

You plan to create an access package named package1 that will be accessible only to the users at Fabrikam.

You create a connected organization for Fabrikam.

You need to ensure that the package1 will be accessible only to users who have fabrikam.com email addresses.

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

NOTE: Each correct selection is worth one point.

Hot Area:

To allow access for users who have fabrikam.com email addresses, configure:

<input type="text"/>
An access package assignment in Identity Governance
An access package policy in Identity Governance
A conditional access policy in Azure AD
The External collaboration settings in Azure AD

To block access for users who have litwareinc.com email addresses, configure:

<input type="text"/>
An access package assignment in Identity Governance
An access package policy in Identity Governance
A conditional access policy in Azure AD
The External collaboration settings in Azure AD

Correct Answer:

To allow access for users who have fabrikam.com email addresses, configure:

<input type="text"/>
An access package assignment in Identity Governance
An access package policy in Identity Governance
A conditional access policy in Azure AD
The External collaboration settings in Azure AD

To block access for users who have litwareinc.com email addresses, configure:

<input type="text"/>
An access package assignment in Identity Governance
An access package policy in Identity Governance
A conditional access policy in Azure AD
The External collaboration settings in Azure AD

QUESTION 9

You need to configure the detection of multi-staged attacks to meet the monitoring requirements. What should you do?

- A. Customize the Azure Sentinel rule logic.
- B. Create a workbook.

- C. Add Azure Sentinel data connectors.
- D. Add an Azure Sentinel playbook.

Correct Answer: A

QUESTION 10

You need to resolve the issue of the sales department users. What should you configure for the Azure AD tenant?

- A. the User settings
- B. the Device settings
- C. the Access reviews settings
- D. Security defaults

Correct Answer: B

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 an Azure Active Directory (Azure AD) tenant that syncs to an Active Directory forest.

You discover that when a user account is disabled in Active Directory, the disabled user can still authenticate to Azure AD for up to 30 minutes.

You need to ensure that when a user account is disabled in Active Directory, the user account is immediately prevented from authenticating to Azure AD.

Solution: You configure pass-through authentication.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: A

Reference: <https://docs.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn>

QUESTION 12

DRAG DROP

You have an on-premises Microsoft Exchange organization that uses an SMTP address space of contoso.com.

You discover that users use their email address for self-service sign-up to Microsoft 365 services.

You need to gain global administrator privileges to the Azure Active Directory (Azure AD) tenant that contains the self-signed users.

Which four actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:

Actions	Answer Area
Sign in to the Microsoft 365 admin center.	
Create a self-signed user account in the Azure AD tenant.	
From the Microsoft 365 admin center, add the domain name.	⬅️ ➡️
Respond to the Become the admin message.	
From the Microsoft 365 admin center, remove the domain name.	⬆️ ⬇️
Create a TXT record in the contoso.com DNS zone.	

Correct Answer:

Actions

From the Microsoft 365 admin center, add the domain name.
From the Microsoft 365 admin center, remove the domain name.

Answer Area

	Create a self-signed user account in the Azure AD tenant.	
	Sign in to the Microsoft 365 admin center.	
⏪	Respond to the Become the admin message.	⏩
⏩		⏪
	Create a TXT record in the contoso.com DNS zone.	

QUESTION 13

HOTSPOT

You need to create the LWGroup1 group to meet the management requirements.

How should you complete the dynamic membership rule? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

(user.objectId -ne

"Guest"
"Member"
Null

) and (user.userType - eq

"Guest"
"Member"
Null

)

Correct Answer:

Answer Area

(user.objectId -ne

▼
"Guest"
"Member"
Null

) and (user.userType - eq

▼
"Guest"
"Member"
Null

)

QUESTION 14

You have an Azure AD tenant.

You open the risk detections report.

Which risk detection type is classified as a user risk?

- A. password spray
- B. anonymous IP address
- C. unfamiliar sign-in properties
- D. Azure AD threat intelligence

Correct Answer: D

QUESTION 15

You have a Microsoft 365 tenant.

In Azure Active Directory (Azure AD), you configure the terms of use.

You need to ensure that only users who accept the terms of use can access the resources in the tenant. Other users must be denied access.

What should you configure?

- A. an access policy in Microsoft Cloud App Security.
- B. Terms and conditions in Microsoft Endpoint Manager.
- C. a conditional access policy in Azure AD
- D. a compliance policy in Microsoft Endpoint Manager

Correct Answer: C

Reference: <https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/terms-of-use>

[SC-300 Practice Test](#)

[SC-300 Exam Questions](#)

[SC-300 Braindumps](#)