



# 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.geekcert.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

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.

All users must use the Microsoft Authenticator app for multi-factor authentication (MFA) when accessing Microsoft 365 services. Some users report that they received an MFA prompt on their Microsoft Authenticator app without initiating a sign-in request.

You need to block the users automatically when they report an MFA request that they did not initiate. Solution: From the Azure portal, you configure the Notifications settings for multi-factor authentication (MFA). Does this meet the goal?

A. Yes

B. No

Correct Answer: B

You need to configure the fraud alert settings.

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

---

## QUESTION 2

### HOTSPOT

You have a Microsoft 365 tenant.

You configure a conditional access policy as shown in the Conditional Access policy exhibit. (Click the Conditional Access policy tab.)



Conditional access policy

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

Name \*

Require MFA for all users ✓

Assignments

Users and groups ⓘ >

All users

Cloud apps or actions ⓘ >

All cloud apps

Conditions ⓘ >

1 condition selected

Access controls

Grant ⓘ >

0 controls selected

Session ⓘ >

0 controls selected

Enable policy

Report-only On Off

Create

Control user access enforcement to block or grant access. [Learn more](#)

☐ Block access

☒ Grant access

☒ Require multi-factor authentication ⓘ

☐ Require device to be marked as compliant ⓘ

☐ Require Hybrid Azure AD joined device ⓘ

☐ Require approved client app ⓘ

[See list of approved client apps](#)

☐ Require app protection policy ⓘ

[See list of policy protected client apps](#)

☐ Require password change (Preview) ⓘ

For multiple controls

☒ Require all the selected controls

☐ Require one of the selected controls

Select

You view the User administrator role settings as shown in the Role setting details exhibit. (Click the Role setting details tab.)



Privileged Identity Management > ContosoAzureAD > User Administrator >

## Role setting details - User Administrator

Privileged Identity Management | Azure AD roles

Edit

### Activation

| Setting                                  | State                |
|--|----------------------|
| Activation maximum duration (hours)      | 8 hour(s)            |
| Require justification on activation      | Yes                  |
| Require ticket information on activation | No                   |
| On activation, require Azure MFA         | Yes                  |
| Require approval to activate             | Yes                  |
| Approvers                                | 1 Member(s), 0 Group |

### Assignment

| Setting  | State      |
|--|------------|
| Allow permanent eligible assignment                            | No         |
| Expire eligible assignments after                              | 15 day(s)  |
| Allow permanent active assignment                              | No         |
| Expire active assignments after                                | 1 month(s) |
| Require Azure Multi-Factor Authentication on active assignment | No         |
| Require justification on active assignment                     | No         |

You view the User administrator role assignments as shown in the Role assignments exhibit. (Click the Role assignments tab.)

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     | Membership |
|--------------------|------------------------------------|------|-----------|------------|
| User Administrator |                                    |      |           |            |
| Admin1             | Admin1@m365x629615.onmicrosoft.com | User | Directory | Direct     |
| Admin2             | Admin2@m365x629615.onmicrosoft.com | User | Directory | Direct     |
| Admin3             | Admin3@m365x629615.onmicrosoft.com | User | Directory | Direct     |

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





Hot Area:

|  | Yes                   | No                    |
|--|-----------------------|-----------------------|
| Before Admin1 can perform a task that requires the User administrator role, an approver must approve The activation request.   | <input type="radio"/> | <input type="radio"/> |
| Admin2 can request activation of the User Administrator role for a period of two hours.  | <input type="radio"/> | <input type="radio"/> |
| If Admin3 connects to the Azure Active Directory admin Center, and then activates the User administrator role, Admin3 will be prompted to authenticate by using Multi-factor authentication (MFA) twice. | <input type="radio"/> | <input type="radio"/> |

Correct Answer:

|  | Yes                              | No                               |
|--|----------------------------------|----------------------------------|
| Before Admin1 can perform a task that requires the User administrator role, an approver must approve The activation request.   | <input checked="" type="radio"/> | <input type="radio"/>            |
| Admin2 can request activation of the User Administrator role for a period of two hours.  | <input checked="" type="radio"/> | <input type="radio"/>            |
| If Admin3 connects to the Azure Active Directory admin Center, and then activates the User administrator role, Admin3 will be prompted to authenticate by using Multi-factor authentication (MFA) twice. | <input type="radio"/>            | <input checked="" type="radio"/> |

---

### QUESTION 3

#### 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](#) →

[+ Add filters](#)

2 users found

|                          | Name  | User principal name               | User type | Directory synced |
|--------------------------|-------|-----------------------------------|-----------|------------------|
| <input type="checkbox"/> | User1 | User1@m365x629615.onmicrosoft.com | Member    | No               |
| <input type="checkbox"/> | 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?](#)[+ Add filters](#)

|                          | Name   | Group Type | Membership Type |
|--------------------------|--------|------------|-----------------|
| <input type="checkbox"/> | Group1 | Security   | Assigned        |
| <input type="checkbox"/> | 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](#)

| 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 4

You have an Azure Active Directory (Azure AD) tenant.

You open the risk detections report.

Which risk detection type is classified as a user risk?

- A. impossible travel
- B. anonymous IP address
- C. atypical travel
- D. leaked credentials

Correct Answer: D

Reference: <https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks>

### QUESTION 5

You have an Azure Active Directory (Azure AD) tenant that contains the following objects:

1.  
A device named Device1
2.  
Users named User1, User2, User3, User4, and User5
- 3.





Groups named Group1, Group2, Group3, Group4, and Group5 The groups are configured as shown in the following table.

| Name   | Type          | Membership type | Members                      |
|--------|---------------|-----------------|------------------------------|
| Group1 | Security      | Assigned        | User1, User3, Group2, Group3 |
| Group2 | Security      | Dynamic User    | User2                        |
| Group3 | Security      | Dynamic Device  | Device1                      |
| Group4 | Microsoft 365 | Assigned        | User4                        |
| Group5 | Microsoft 365 | Dynamic User    | User5                        |

To which groups can you assign a Microsoft Office 365 Enterprise E5 license directly?

- A. Group1 and Group4 only
- B. Group1, Group2, Group3, Group4, and Group5
- C. Group1 and Group2 only
- D. Group1 only
- E. Group1, Group2, Group4, and Group5 only

Correct Answer: B

Reference: <https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/licensing-group-advanced>

[SC-300 PDF Dumps](#)

[SC-300 VCE Dumps](#)

[SC-300 Exam Questions](#)