SC-300Q&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.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

You have a Microsoft 365 tenant.

The Azure Active Directory (Azure AD) tenant contains the groups shown in the following table.

Name	Type
Group1	Security
Group2	Distribution
Group3	Microsoft 365
Group4	Mail-enabled security

In Azure AD. you add a new enterprise application named Appl. Which groups can you assign to App1?

A. Group1 and Group

B. Group2 only

C. Group3 only

D. Group1 only

E. Group1 and Group4

Correct Answer: C

QUESTION 2

You have an Azure Active Directory (Azure AD) tenant that contains a user named User1 and the conditional access policies shown in the following table.

Name	Status	Conditional access requirement
CAPolicy1	On	Users connect from a trusted IP address.
CAPolicy2	On	Users' devices are marked as compliant.
CAPolicy3	Report-only	The sign-in risk of users is low.

You need to evaluate which policies will be applied to User1 when User1 attempts to sign-in from various IP addresses. Which feature should you use?

A. Access reviews

B. Identity Secure Score

C. The What If tool

D. the Microsoft 365 network connectivity test tool

Correct Answer: C

QUESTION 3

You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint Online site named Site1.

You need to be notified if a user downloads more than 50 files in one minute from Site1.

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

A. session policy

B. activity policy

C. file policy

D. anomaly detection policy

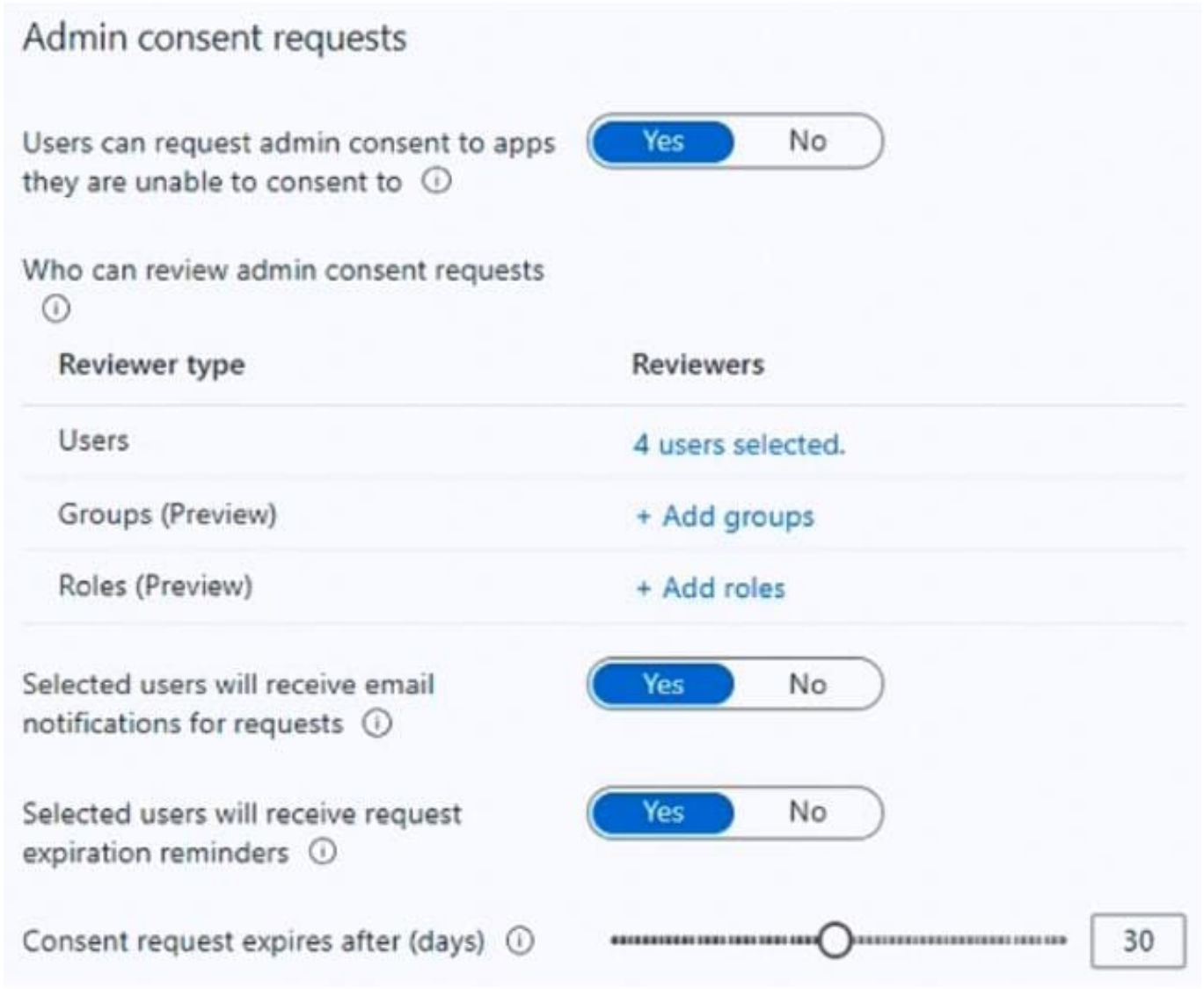
Correct Answer: B

QUESTION 4

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

Name	Role
Admin1	Cloud application administrator
Admin2	Application administrator
Admin3	Security administrator
User1	None

You add an enterprise application named App1 to Azure AD and set User1 as the owner of App1. App1 requires admin consent to access Azure AD before the app can be used. You configure the Admin consent requests settings as shown in the following exhibit.



Admin1, Admin2, Admin3, and User

Correct Answer: D

QUESTION 5

You have an Azure AD tenant that contains a user named User1.

User1 needs to manage license assignments and reset user passwords.

Which role should you assign to User1?

A. Helpdesk administrator

B. Billing administrator

C. License administrator

D. User administrator

Correct Answer: D

QUESTION 6

DRAG DROP

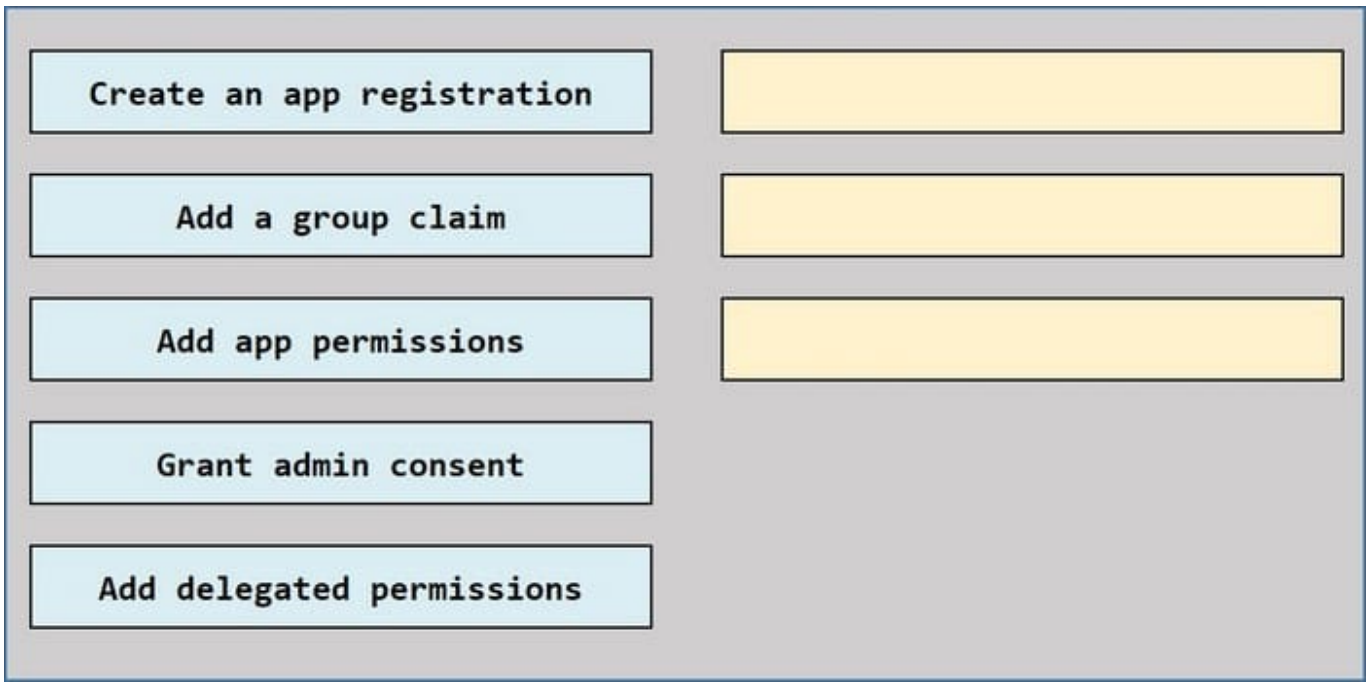
Your company has an Azure Active Directory (Azure AD) tenant named contoso.com.

The company is developing a web service named App1.

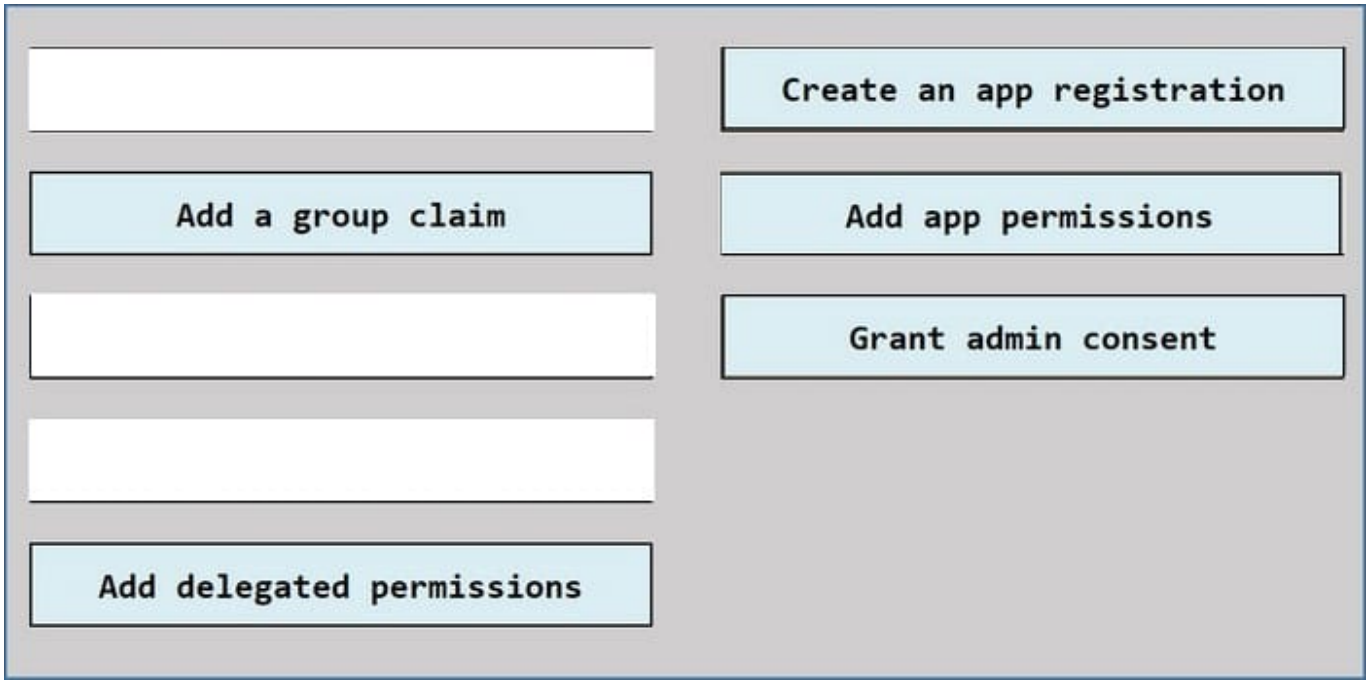
You need to ensure that App1 can use Microsoft Graph to read directory data in contoso.com.

Which three actions should yon 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:



Correct Answer:



QUESTION 7

You have a Microsoft 365 E5 subscription.

You create a user named User1.

You need to ensure that User1 can update the status of Identity Secure Score improvement actions.

Solution: You assign the Exchange Administrator role to User1.

Does this meet the goal?

A. Yes

B. No

Correct Answer: A

QUESTION 8

You have a Microsoft 365 subscription. The subscription contains users that use Microsoft Outlook 2016 and Outlook 2013 clients.

You need to implement tenant restrictions. The solution must minimize administrative effort.

What should you do first?

A. Configure the Outlook 2013 clients to use modern authentication.

B. Upgrade the Outlook 2013 clients to Outlook 2016.

C. From the Exchange admin center, configure Organization Sharing.

D. Upgrade all the Outlook clients to Outlook 2019.

Correct Answer: B

QUESTION 9

You have an Azure Active Directory (Azure AD) tenant that uses Azure AD Identity Protection and contains the resources shown in the following table.

Name	Type	Configuration
Risk1	User risk policy	Users that have a high severity risk must reset their password upon next sign-in.
User1	User	*Not applicable*

Azure Multi-factor Authentication (MFA) is enabled for all users.

User1 triggers a medium severity alert that requires additional investigation.

You need to force User1 to reset his password the next time he signs in.

The solution must minimize administrative effort.

What should you do?

A. Reconfigure the user risk, policy to trigger on medium or low severity.

B. Mark User1 as compromised.

C. Reset the Azure MIFA registration for User1.

D. Configure a sign-in risk policy.

Correct Answer: B

QUESTION 10

You use Azure Monitor to analyze Azure Active Directory (Azure AD) activity logs.

Yon receive more than 100 email alerts each day for tailed Azure Al) user sign-in attempts.

You need to ensure that a new security administrator receives the alerts instead of you.

Solution: From Azure monitor, you modify the action group.

Does this meet the goal?

A. Yes

B. No

Correct Answer: A

QUESTION 11

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

You create an enterprise application collection named HR Apps that has the following settings:

1.

Applications: Appl. App?, App3

2.

Owners: Admin 1

3.

Users and groups: HRUsers

AH three apps have the following Properties settings:

1.

Enabled for users to sign in: Yes

2.

User assignment required: Yes

3.

Visible to users: Yes

Users report that when they go to the My Apps portal, they only sue App1 and App2-You need to ensure that the users can also see App3. What should you do from App3? What should you do from App3?

A. From Users and groups, add HRUsers.

B. Prom Properties, change User assignment required to No.

C. From Permissions, review the User consent permissions.

D. From Single sign on, configure a sign-on method.

Correct Answer: A

Reference: https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/assign-user-or-group-access-portal https://docs.microsoft.com/en-us/azure/active-directory/user-help/my-applications-portal-workspaces

QUESTION 12

HOTSPOT

You have an Azure Active Directory (Azure AD) tenant that contains Azure AD Privileged Identity Management (PIM) role settings for the User administrator role as shown in the following exhibit.

... ContosoAzureAD > Identity Governance > Privileged Identity Management > ContosoAzureAD > User Administrator >

Role setting details - User Administrator

Privileged Identity Management | Azure AD roles

Edit

Activation

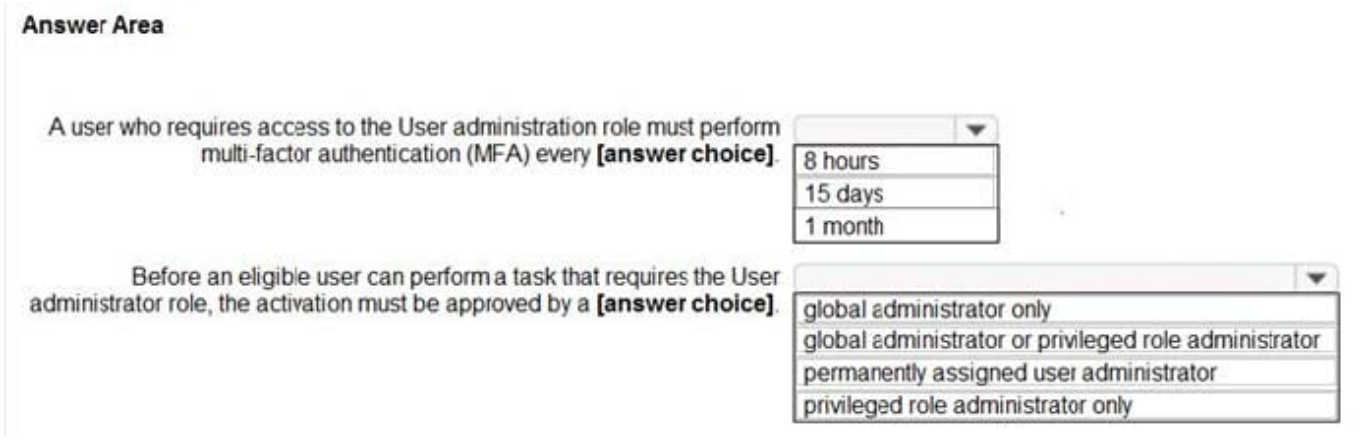
SETTING	STATE
Activation maximum duration (hours)	8 hour(s)
Require justification on activation	Yes
Require ticket information on activation	No
On activation, require Azure MFA	Yes
Require approval to activate	Yes
Approvers	None

Assignment

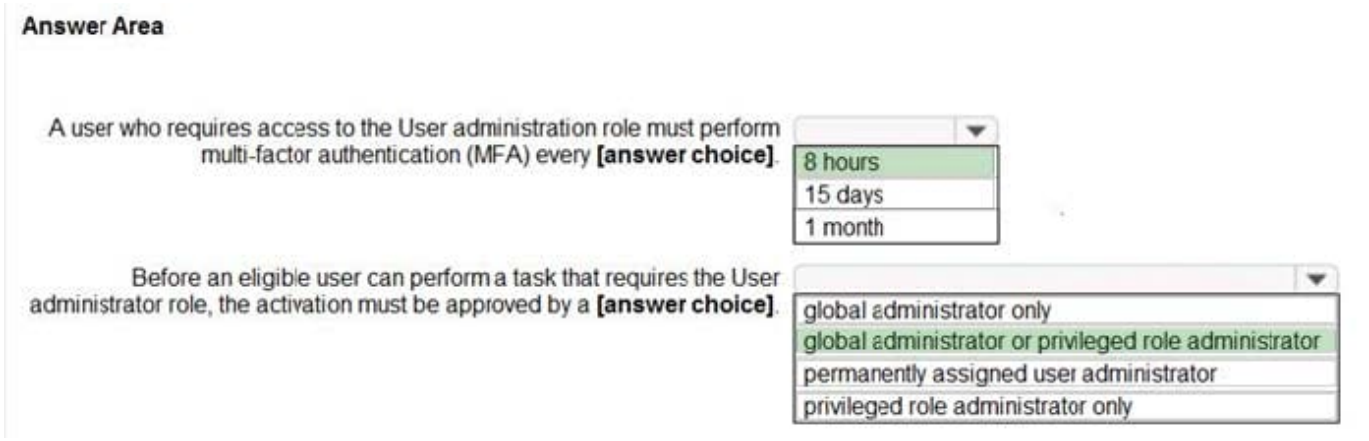
SETTING	STATE
Allow permanent eligible assignment	No
Expire eligible assignments after	15 day(s)
Allow permanent active assignment	No
Expire active assignments after	1 month(s)
Require Azure Multi-Factor Authentication on active assignment	No
Require justification on active assignment	No

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:



Correct Answer:



QUESTION 13

HOTSPOT

You have a Microsoft 365 tenant.

You need to Identity users who have leaked credentials. The solution must meet the following requirements:

Identity sign-ms by users who are suspected of having leaked credentials.

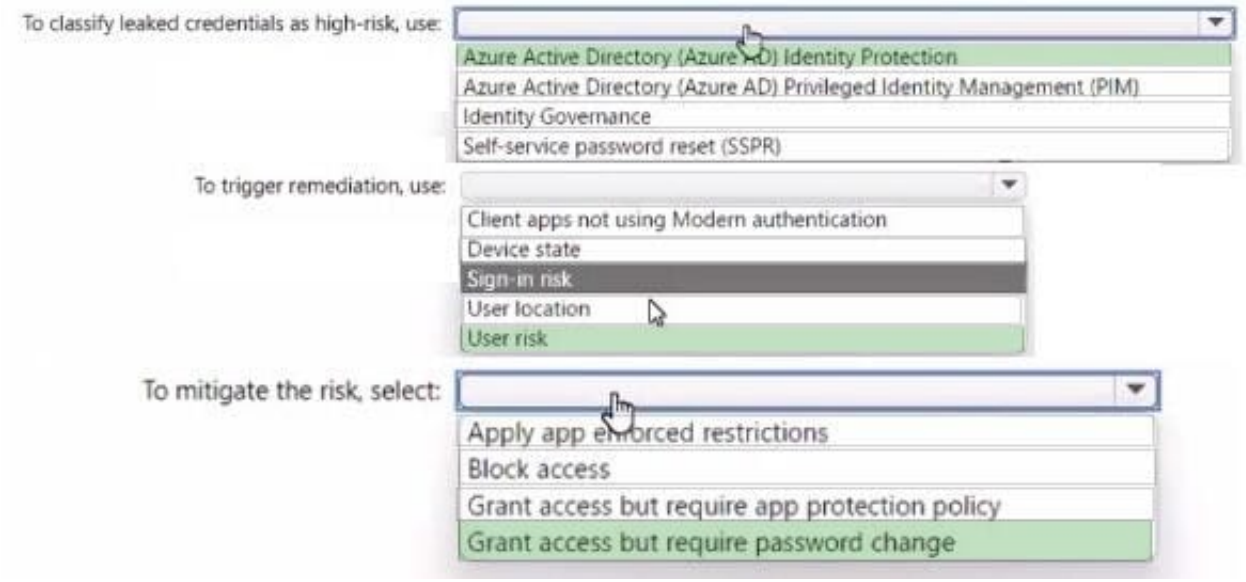
Flag the sign-ins as a high-risk event.

Immediately enforce a control to mitigate the risk, while still allowing the user to access applications.

What should you use? To answer, select the appropriate options m the answer area.

Hot Area:

Correct Answer:



QUESTION 14

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

You need to bulk create 25 new user accounts by uploading a template file.

Which properties are required in the template file?

A. displayName, identityIssuer, usageLocation, and userType

B. accountEnabled, givenName, surname, and userPrincipalName

C. accountEnabled, displayName, userPrincipalName, and passwordProfile

D. accountEnabled, passwordProfile, usageLocation, and userPrincipalName

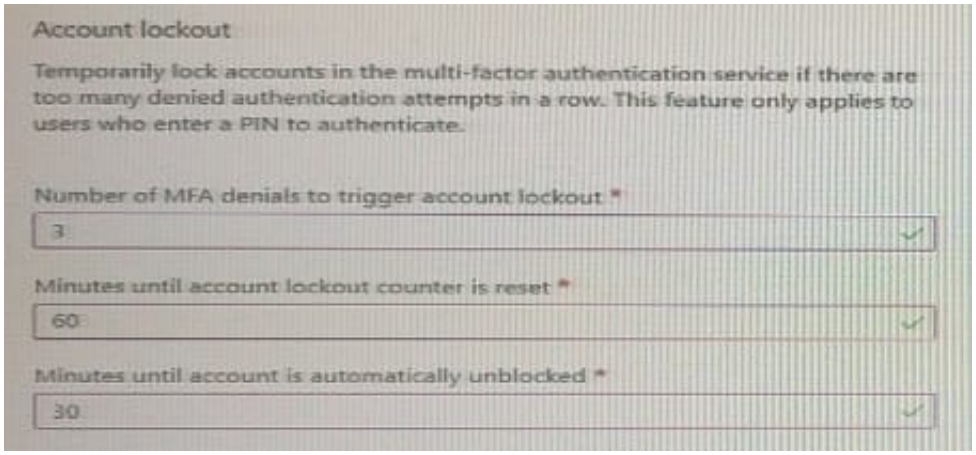
Correct Answer: C

QUESTION 15

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.



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