- **Vendor:** Microsoft
- **Exam Code:** SC-300
- **Exam Name:** Microsoft Identity and Access Administrator
- **New Updated Questions from Braindump2go (Updated in April/2023)**

QUESTION 107
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 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 AD, you create an assignment for the Insights at administrator role.
Does this meet the goal?

A. Yes
B. No

Answer: B

QUESTION 108
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 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

Answer: A
Explanation:
https://docs.microsoft.com/en-us/azure/azure-monitor/alerts/action-groups#configure-notifications

QUESTION 109
Due to a recent company acquisition, you have inherited a new Azure tenant with 1 subscription associated that you have the manage. The security has been neglected and you are looking for a quick and easy way to enable various security settings like requiring users to Register for Multi-factor authentication, blocking legacy authentication protocols, and protecting privileged activities like access to the Azure portal. What is the best way to enforce these settings with

the least amount of administrative effort.

A. Enable Security Defaultsright
B. Configure Conditional Access Policies
C. Configuring an Azure Policy
D. Utilize Active Directory Sign-In Logs

Answer: A

QUESTION 110
You recently created a new Azure AD Tenant for your organization, Lead2pass Inc and you were assigned a default domain of whizlabs.onmicorosft.com. You want to use your own custom domain of whizlabs.com. You added the custom domain via the Azure portal and now you have to validate that you are the owner of the custom domain through your registrar. What type of record will you need to add to your domain registrar?

A. TXT record
B. A record
C. CNAME record
D. CAA record

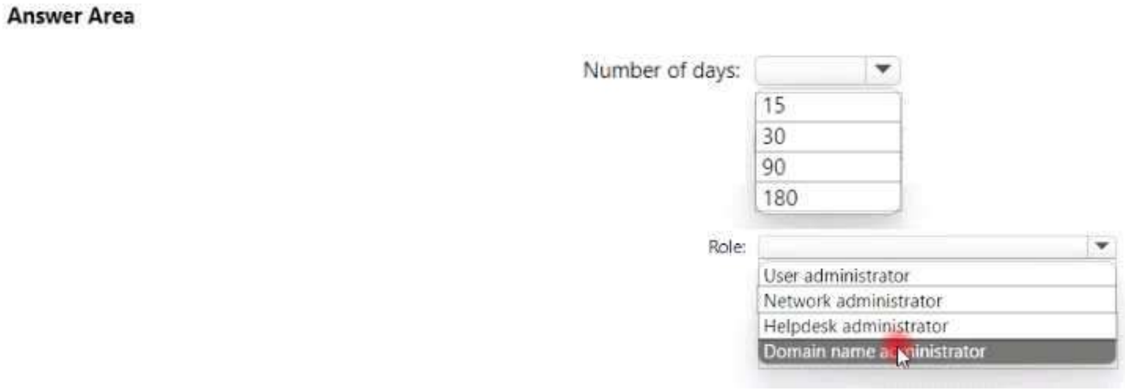
Answer: A

QUESTION 111
You are looking to improve your organizations security posture after hearing about breaches and hacks of other organizations on the news. You have been looking into Azure Identity Protection and you are commissioning a team to begin implementing this service. This team will need full access to Identity Protection but would not need to reset passwords. You should follow the principle of least privilege. What role should you grant this new team?

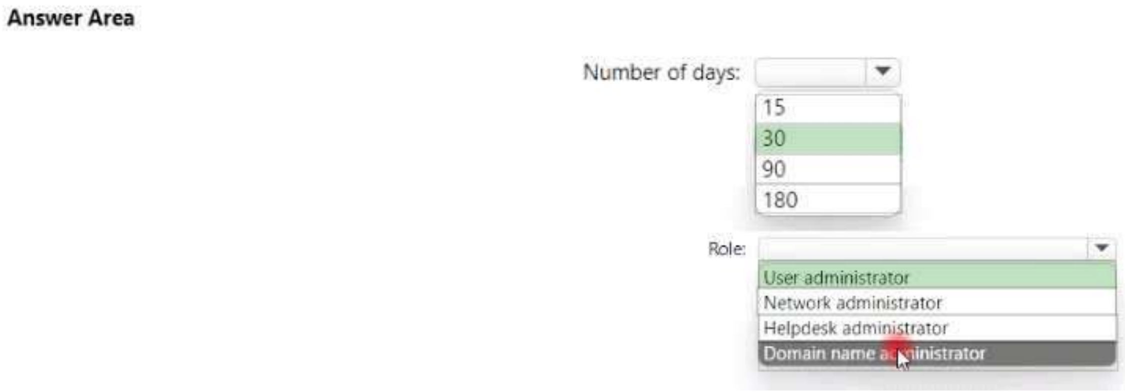
A. Security Operator
B. Global Administrator
C. Security Administratorright
D. HelpDesk Administrator

Answer: C

QUESTION 112
Hotspot Question
You have an Azure Active Directory (Azure AD) tenant that contains a user named User1. An administrator deletes User1. You need to identity the following:
- How many days after the account of User1 is deleted can you restore the account?
- Which is the least privileged role that can be used to restore User1?
What should you identify? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



Answer:



Answer Area

Number of days:
15
[✓ 30]
90
180

Role:
[✓ User administrator]
Network administrator
Helpdesk administrator
Domain name administrator

QUESTION 113

Drag and Drop Question

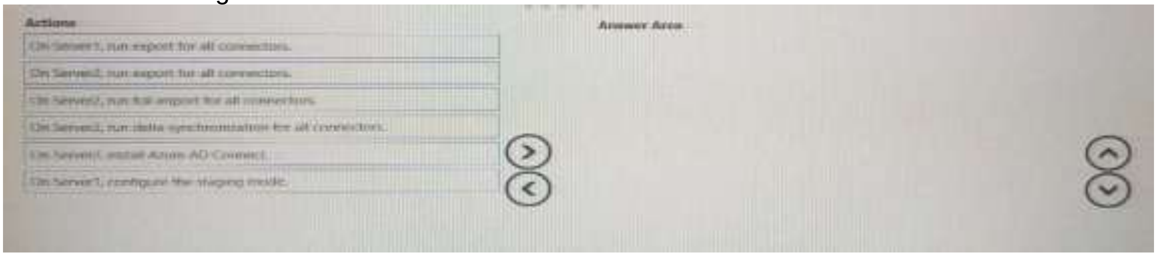
Your network contains an Active Directory forest named contoso.com that is linked to an Azure Active Directory (Azure AD) tenant named contoso.com by using Azure AD Connect.

Attire AD Connect is installed on a server named Server 1.

You deploy a new server named Server? that runs Windows Server 2019.

You need to implement a failover server for Azure AD Connect. The solution must minimize how long it takes to fail over if Server1 fails.

Which three 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.



Actions

On Server1, run export for all connectors.

On Server2, run export for all connectors.

On Server2, run full import for all connectors.

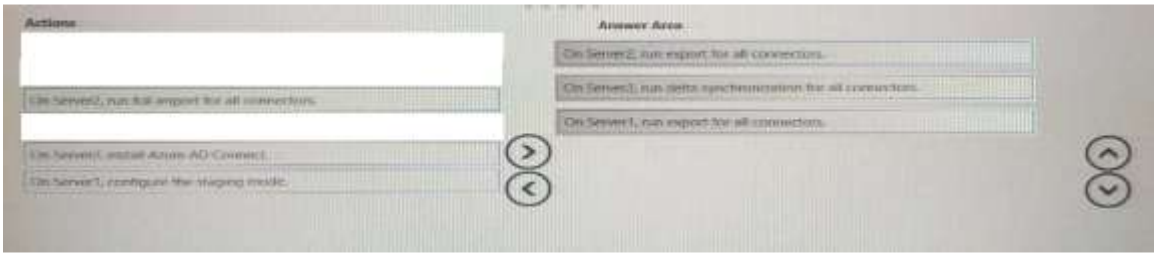
On Server2, run delta synchronization for all connectors.

On Server2, install Azure AD Connect.

On Server1, configure the staging mode.

Answer Area

Answer:



Actions

On Server2, run full import for all connectors.

On Server2, install Azure AD Connect.

On Server1, configure the staging mode.

Answer Area

On Server2, run export for all connectors.

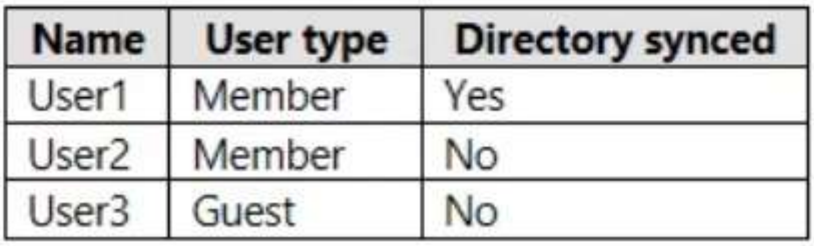
On Server1, run delta synchronization for all connectors.

On Server1, run export for all connectors.

QUESTION 114

Hotspot Question

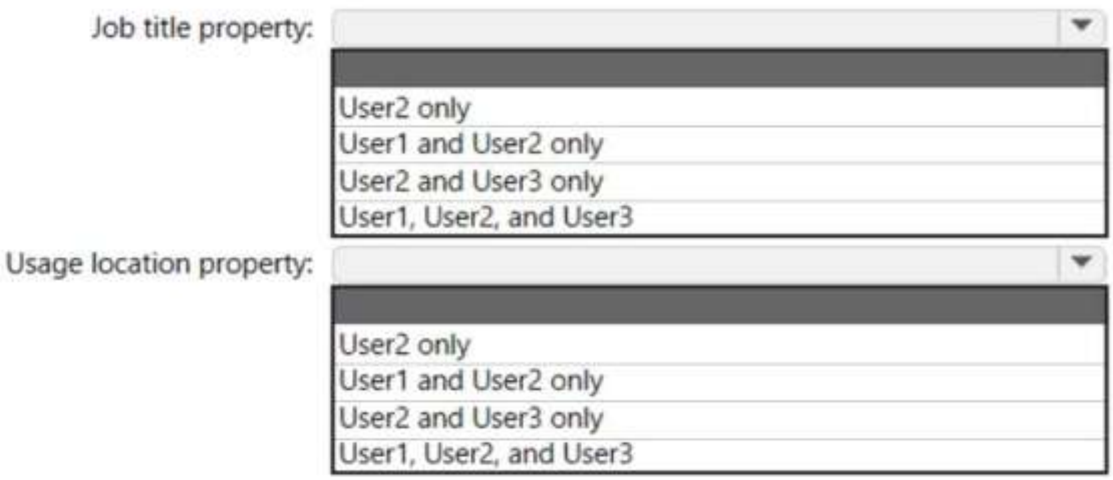
You have an Azure Active Directory (Azure AD) tenant that contains the users shown in the following table.



Name	User 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.



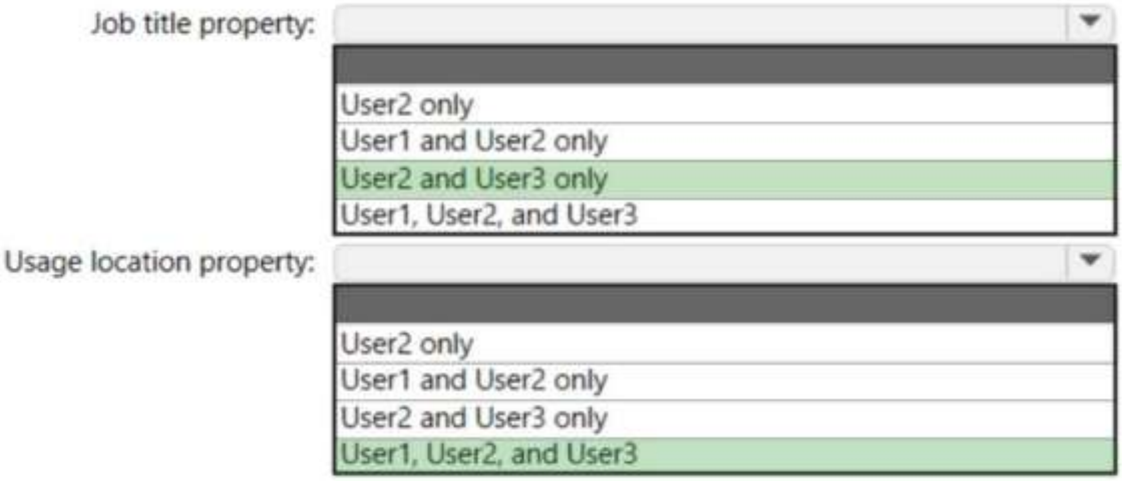
Job title property:

- 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

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]

Explanation:
Box 1: User2 and User3 only
Job title property for directory synched users cannot be updated from Azure AD.
Box 2: User1, User2, and User3
Invite users with Azure Active Directory B2B collaboration, Update user's name and usage location.
To assign a license, the invited user's Usage location must be specified. Admins can update the invited user's profile on the Azure portal.
1. Go to Azure Active Directory > Users and groups > All users. If you don't see the newly created user, refresh the page.
2. Click on the invited user, and then click Profile.
3. Update First name, Last name, and Usage location.
4. Click Save, and then close the Profile blade.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-users-profile-azure-portal
https://docs.microsoft.com/en-us/power-platform/admin/invite-users-azure-active-directory-b2b-collaboration#update-users-name-and-usage-location

QUESTION 115
You are the lead cloud administrator for Lead2pass Inc. and you just hired a new employee that will be in charge of Azure AD Support issues. This new employee needs the ability to reset the passwords for all types of users when requested, including users with the user admin, global admin, or password admin roles. You need to ensure that you follow the principle of least privilege when granting access. What role should you grant the new employee?

A. Password Admin

B. Global Admin
C. Security Admin
D. User Admin

Answer: B

QUESTION 116
Your organization is considering allowing employees to work remotely and to use their own devices to access many of the organizations resources. However, to help protect against potential data loss, your organization needs to ensure that only approved applications can be used to access the company data. What can you configure to meet this requirement?

A. Privileged Identity Management
B. Conditional Access Policiesright
C. RBAC roles
D. Azure Security Center

Answer: B

QUESTION 117
Your organization is looking to tighten its security posture when it comes to Azure AD users passwords. There has been reports on local news recently of various organizations having user identities compromised due to using weak passwords or passwords that resemble the organization name or local sports team names. You want to provide protection for your organization as well as supplying a list of common words that are not acceptable passwords. What should you configure.

A. Azure AD Password Protectionright
B. Azure AD Privileged Identity Management
C. Azure Defender for Passwords
D. Azure AD Multi-factor Authentication

Answer: A

QUESTION 118
You have hired a new Azure Engineer that will be responsible for managing all aspects of enterprise applications and app registrations. This engineer will not need to manage anything application proxy related. You need to grant the proper role to the engineer to perform his job duties while maintaining the principle of least privilege. What role should you grant?

A. Global Administrator
B. Application Administrator
C. Cloud Application Administratorright
D. Enterprise Administrator

Answer: C

QUESTION 119
You have a Microsoft 365 tenant.
You currently allow email clients that use Basic authentication to conned to Microsoft Exchange Online.
You need to ensure that users can connect t to Exchange only run email clients that use Modern authentication protocols.
You need to ensure that use Modern authentication.
What should you implement?

A. a compliance policy in Microsoft Endpoint Manager
B. a conditional access policy in Azure Active Directory (Azure AD)

C. an application control profile in Microsoft Endpoint Manager
D. an OAuth policy in Microsoft Cloud App Security

Answer: C

QUESTION 120
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 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 create a data collection rule.
Does this meet the goal?

A. Yes
B. No

Answer: B
Explanation:
Data Collection Rules (DCRs) define the data collection process in Azure Monitor. DCRs specify what data should be collected, how to transform that data, and where to send that data. Some DCRs will be created and managed by Azure Monitor to collect a specific set of data to enable insights and visualizations.
Reference:
https://learn.microsoft.com/en-us/azure/azure-monitor/essentials/data-collection-rule-overview>

QUESTION 121
You have a Microsoft 365 subscription that contains the following:
- An Azure Active Directory (Azure AD) tenant that has an Azure Active Directory Premium P2 license
- A Microsoft SharePoint Online site named Site1
- A Microsoft Teams team named Team1

You need to create an entitlement management workflow to manage Site1 and Team1.
What should you do first?

A. Configure an app registration.
B. Create an Administrative unit.
C. Create an access package.
D. Create a catalog.

Answer: C
Explanation:
All access packages must be put in a container called a catalog. A catalog defines what resources you can add to your access package. If you don't specify a catalog, your access package will be put into the general catalog.
https://learn.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-access-package-create

QUESTION 122
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 Account lockout settings for multi-factor authentication (MFA).
Does this meet the goal?

A. Yes
B. No

Answer: B

QUESTION 123
Your organization is a 100% Azure cloud based organization with no on-premise resources. You recently completed an acquisition of another company that is 100% on-premise with no cloud premise. You need to immediately provide your cloud users with access to a few of the acquired companies on-premise web applications. What service can you implement to ensure Azure Active Directory can still be used to authenticate to the on-premise applications?

A. Azure Active Directory Connect
B. Azure Security Center
C. Azure Active Directory Application Proxyright
D. Azure Active Directory Domain Services

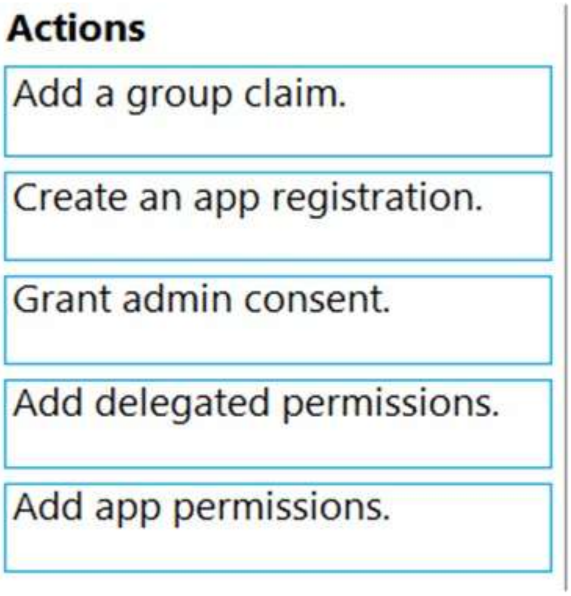
Answer: C

QUESTION 124
Your organization is working with a new consulting firm to help with the design, development, and deployment of a new IT service. The consultants will be joining your organization at various points throughout the project and will not know what permissions they need or who to request the access from. As the Cloud Administrator, what can you implement to ensure consultants can easily request and get all of the access they need to do their job?

A. Azure Arm Templates
B. Azure Blueprints
C. Azure Policies
D. Azure AD Entitlement Management

Answer: D

QUESTION 125
Drag and Drop Question
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.



Actions

Add a group claim.

Create an app registration.

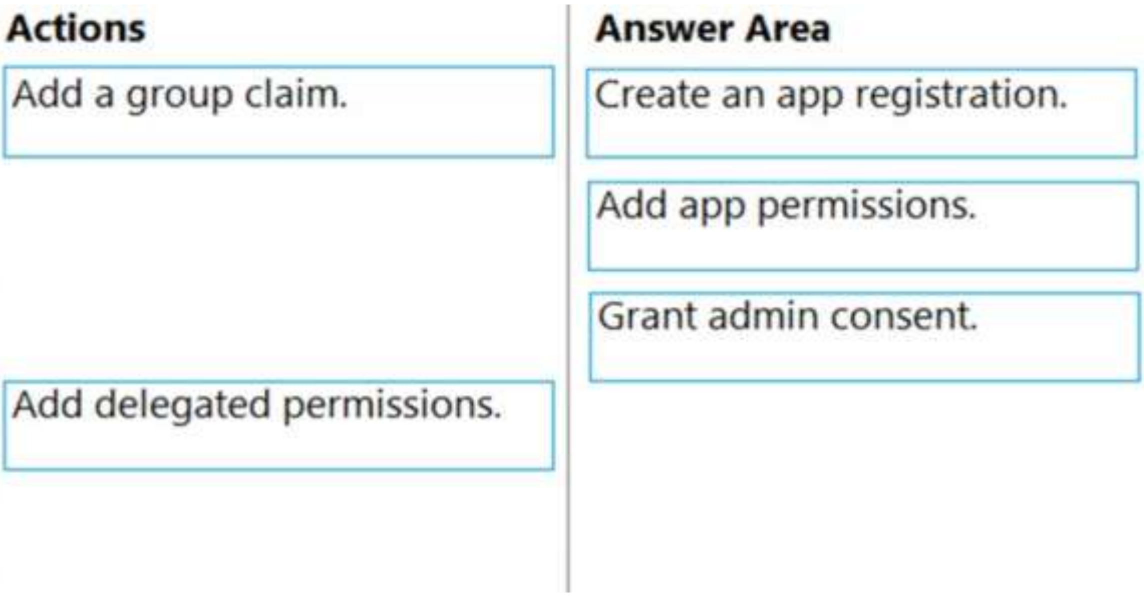
Grant admin consent.

Add delegated permissions.

Add app permissions.

Answer Area

Answer:



Actions

Add a group claim.

Add delegated permissions.

Answer Area

Create an app registration.

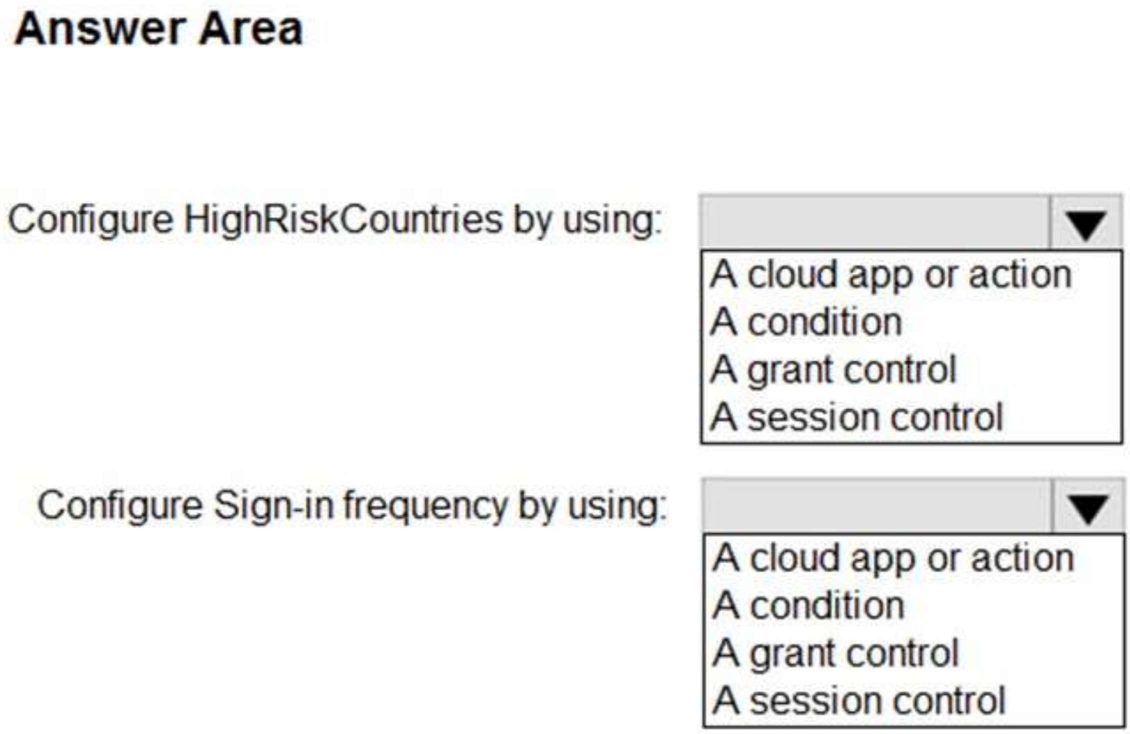
Add app permissions.

Grant admin consent.

Explanation:
1. Create an app registration:
Your app must be registered with the Microsoft identity platform and be authorized by either a user or an administrator for access to the Microsoft Graph resources it needs.
2. Add app permissions:
After the consents to permissions for your app, your app can acquire access tokens that represent the app's permission to access a resource in some capacity. Encoded inside the access token is every permission that your app has been granted for that resource.
3. Grant admin consent:
Higher-privileged permissions require administrator consent.
Reference:
https://docs.microsoft.com/en-us/graph/permissions-reference

QUESTION 126
Hotspot Question
You have a Microsoft 36S 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.



Answer Area

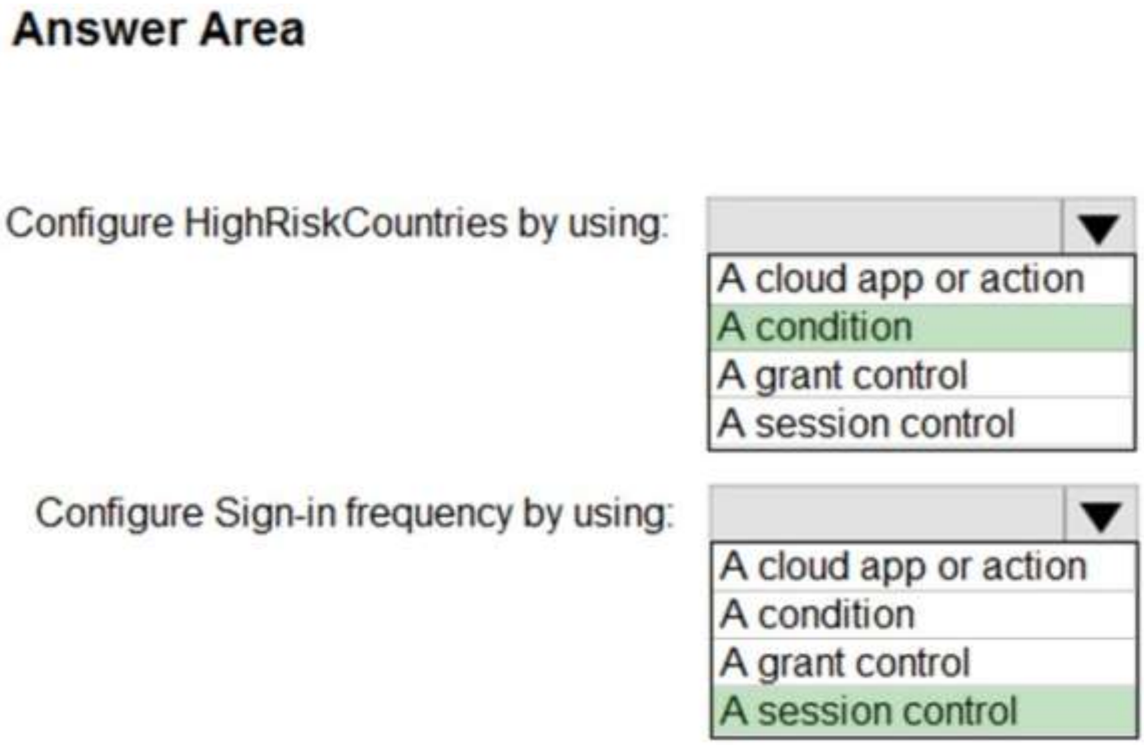
Configure HighRiskCountries by using: ▼

- 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

Answer:



Answer Area

Configure HighRiskCountries by using: ▼

- A cloud app or action
- [✓ A condition]
- A grant control
- A session control

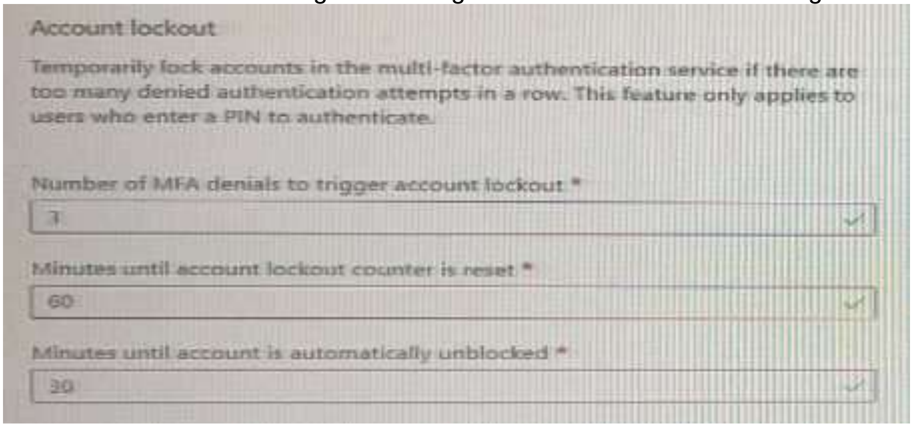
Configure Sign-in frequency by using: ▼

- A cloud app or action
- A condition
- A grant control
- [✓ A session control]

Explanation:
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 127

Hotspot Question
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

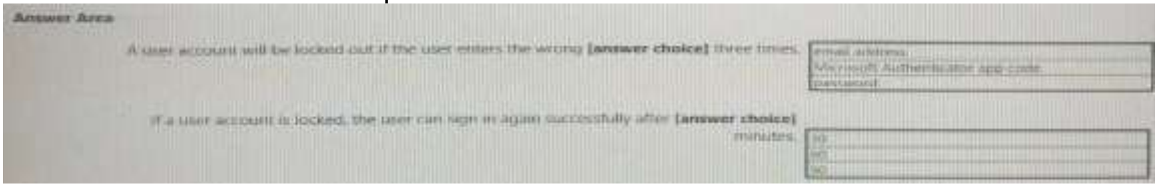
Temporarily lock accounts in the multi-factor authentication service if there are too many denied authentication attempts in a row. This feature only applies to users who enter a PIN to authenticate.

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.

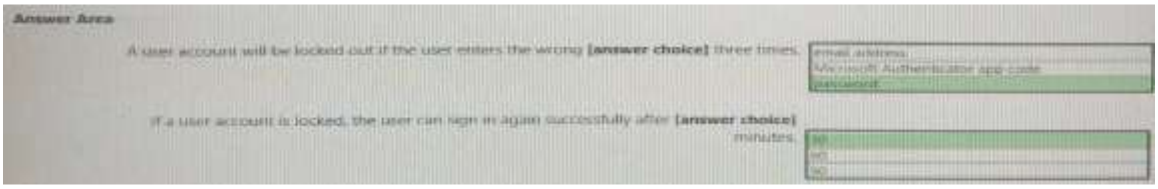


Answer Area

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

Answer:



Answer 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

QUESTION 128
You have a Microsoft 365 tenant.
All users have mobile phones and laptops.
The users frequently work from remote locations that do not have Wi-Fi access or mobile phone connectivity.
While working from the remote locations, the users connect their laptop to a wired network that has internet access.
You plan to implement multi-factor authentication (MFA).
Which MFA authentication method can the users use from the remote location?

A. a notification through the Microsoft Authenticator app
B. email
C. security questions
D. a verification code from the Microsoft Authenticator app

Answer: D
Explanation:
The Authenticator app can be used as a software token to generate an OATH verification code. After entering your username and password, you enter the code provided by the Authenticator app into the sign-in interface.
Incorrect Answers:
A: A notification through the Microsoft Authenticator app requires connectivity to send the verification code to the device requesting the logon.
B: An email requires network connectivity.
C: Security questions are not used as an authentication method but can be used during the self-service password reset (SSPR) process.
Reference:

https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-authenticator-app#verification-code-from-mobile-app

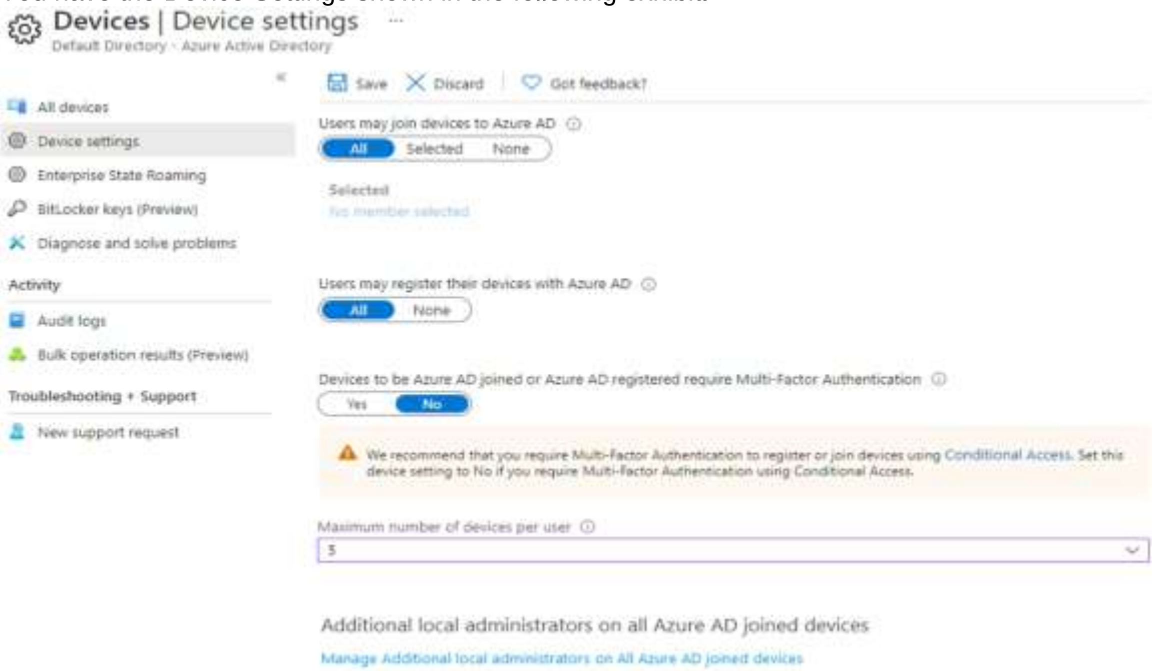
QUESTION 129

Hotspot Question

You have an Azure Active Directory (Azure AD) tenant that has an Azure Active Directory Premium Plan 2 license. The tenant contains the users shown in the following table.

Name	Role
Admin1	Cloud device administrator
Admin2	Device administrator
User1	**None**

You have the Device Settings shown in the following exhibit.



Devices | Device settings ...

Default Directory · Azure Active Directory

Users may join devices to Azure AD ⓘ

● All ○ Selected ○ None

Selected

No member selected

Users may register their devices with Azure AD ⓘ

● All ○ None

Devices to be Azure AD joined or Azure AD registered require Multi-Factor Authentication ⓘ

○ Yes ● No

⚠ We recommend that you require Multi-Factor Authentication to register or join devices using Conditional Access. Set this device setting to No if you require Multi-Factor Authentication using Conditional Access.

Maximum number of devices per user ⓘ

5

Additional local administrators on all Azure AD joined devices

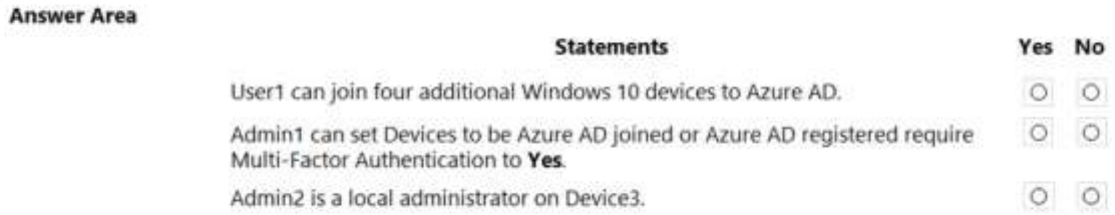
Manage Additional local administrators on All Azure AD joined devices

User1 has the devices shown in the following table.

Name	Operating system	Device identity
Device1	Windows 10	Azure AD joined
Device2	iOS	Azure AD registered
Device3	Windows 10	Azure AD registered
Device4	Android	Azure AD registered

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

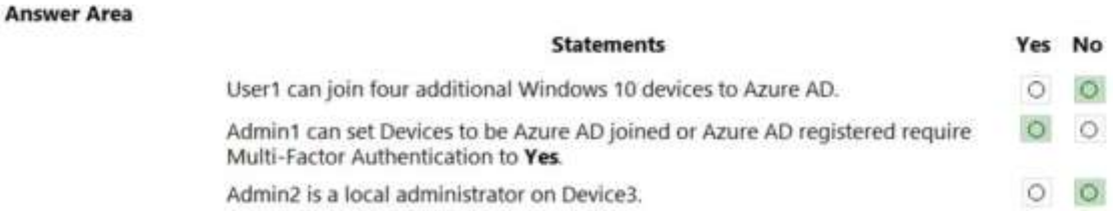
NOTE: Each correct selection is worth one point.



Answer Area

Statements	Yes	No
User1 can join four additional Windows 10 devices to Azure AD.	○	○
Admin1 can set Devices to be Azure AD joined or Azure AD registered require Multi-Factor Authentication to **Yes**.	○	○
Admin2 is a local administrator on Device3.	○	○

Answer:



Answer Area

Statements	Yes	No
User1 can join four additional Windows 10 devices to Azure AD.	○	●
Admin1 can set Devices to be Azure AD joined or Azure AD registered require Multi-Factor Authentication to **Yes**.	●	○
Admin2 is a local administrator on Device3.	○	●

Explanation:
Box 1: No
Maximum number of devices: This setting enables you to select the maximum number of Azure AD joined or Azure AD registered devices that a user can have in Azure AD.
Box 2: Yes
You must be assigned one of the following roles to view or manage device settings in the Azure portal:

- Global Administrator
- Cloud Device Administrator
- Global Reader
- Directory Reader

Box 3: No
Additional local administrators on Azure AD joined devices (Device is Registered not Joined)
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/devices/device-management-azure-portal

QUESTION 130
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 use Azure Monitor to analyze Azure Active Directory (Azure AD) activity logs.
You receive more than 100 email alerts each day for failed Azure AD user sign-in attempts.
You need to ensure that a new security administrator receives the alerts instead of you.
Solution: From Azure AD, you create an assignment for the Insights administrator role.
Does this meet the goal?

A. Yes
B. No

Answer: B
Explanation:
Permissions should be given to a Security Administrator.
Insights Administrator is an administrator Ofc365 Viva app. (Employee Experience Platform).
https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#security-administrator

QUESTION 131
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 use Azure Monitor to analyze Azure Active Directory (Azure AD) activity logs.
You receive more than 100 email alerts each day for failed Azure AD user sign-in attempts.
You need to ensure that a new security administrator receives the alerts instead of you.
Solution: From Azure AD, you modify the Diagnostics settings.
Does this meet the goal?

A. Yes

B. No

Answer: B
Explanation:
Action group change is needed.