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.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

QUESTION 1

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 User Administrator role to User1.

Does this meet the goal?

A. Yes

B. No

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 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 have an Azure subscription that contains an Azure SQL database named db1.

You deploy an Azure App Service web app named App1 that provides product information to users that connect to App1 anonymously.

You need to provide App1 with access to db1. The solution must meet the following requirements:

1.

Credentials must only be available to App1.

2.

Administrative effort must be minimized. Which type of credentials should you use?

A. a system-assigned managed identity

B. an Azure Active Directory (Azure AD) user account

C. a SQL Server account

D. a user-assigned managed identity

Correct Answer: A

QUESTION 4

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

1.

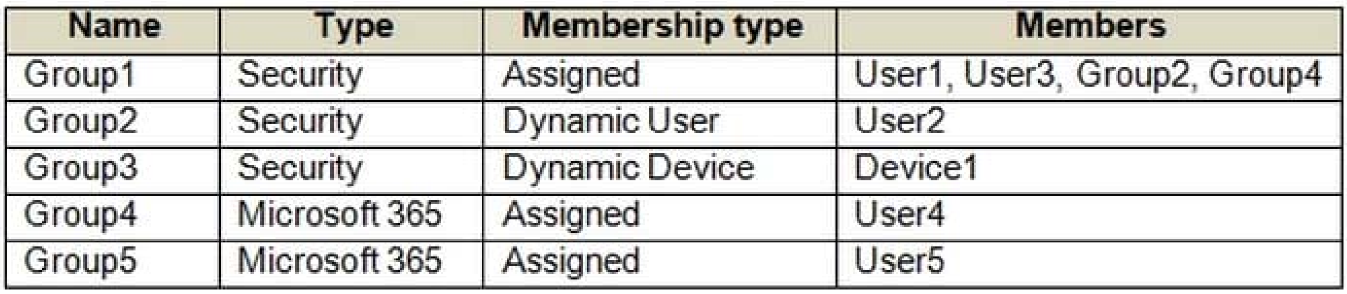
A device named Device1

2.

Users named User1, User2, User3, User4, and User5

3.

Five groups named Group1, Group2, Group3, Ciroup4, and Group5 The groups are configured as shown in the following table.



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

How many licenses are used if you assign the Microsoft Office 365 Enterprise E5 license to Group1?

A. 0

B. 2

C. 3

D. 4

Correct Answer: B

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

QUESTION 5

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Cloud Apps and Conditional Access policies.

You need to block access to cloud apps when a user is assessed as high risk.

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

A. access policy

B. OAuth app policy

C. anomaly detection policy

D. activity policy

Correct Answer: A

QUESTION 6

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 7

You need to meet the planned changes and technical requirements for App1. What should you implement?

A. a policy set in Microsoft Endpoint Manager

B. an app configuration policy in Microsoft Endpoint Manager

C. an app registration in Azure AD

D. Azure AD Application Proxy

Correct Answer: C

Reference: https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-register-app

QUESTION 8

HOTSPOT

Your company has a Microsoft 365 tenant.

All users have computers that run Windows 10 and are joined to the Azure Active Directory (Azure AD) tenant.

The company subscribes to a third-party cloud service named Service1. Service1 supports Azure AD authentication and authorization based on OAuth. Service1 is published to the Azure AD gallery.

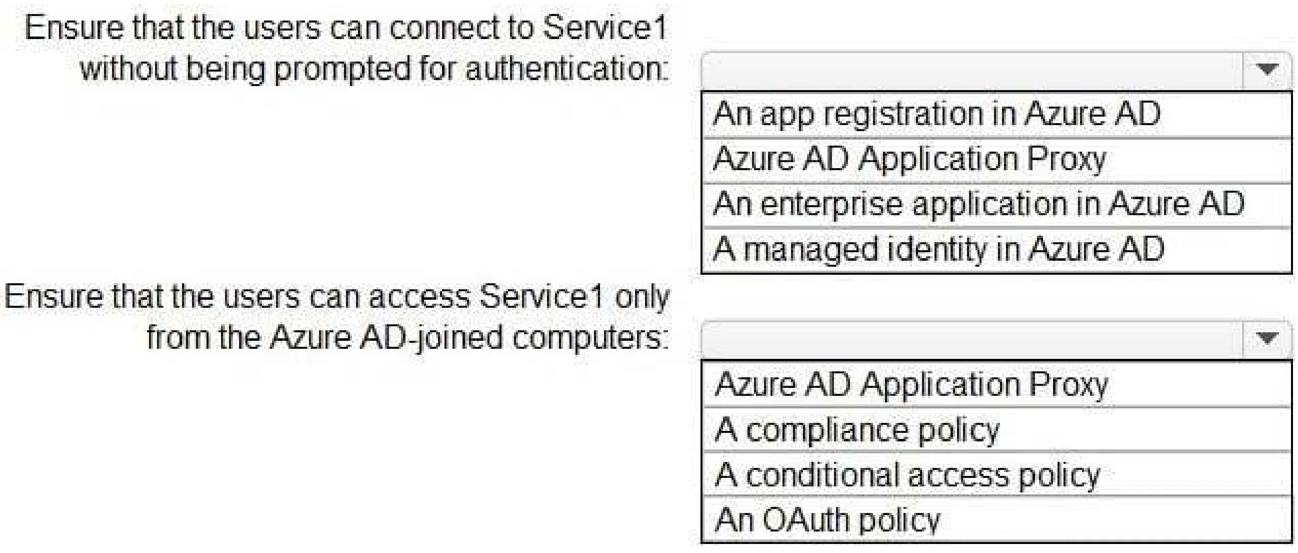
You need to recommend a solution to ensure that the users can connect to Service1 without being prompted for authentication. The solution must ensure that the users can access Service1 only from Azure AD-joined computers. The solution

must minimize administrative effort.

What should you recommend for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



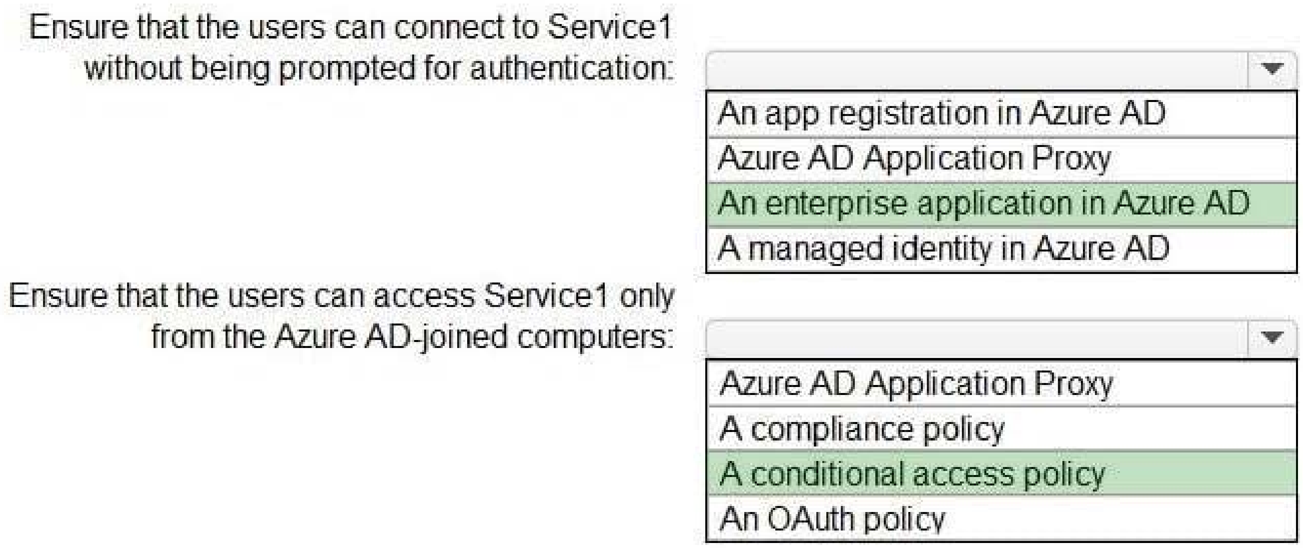
Ensure that the users can connect to Service1 without being prompted for authentication:

- An app registration in Azure AD
- Azure AD Application Proxy
- An enterprise application in Azure AD
- A managed identity in Azure AD

Ensure that the users can access Service1 only from the Azure AD-joined computers:

- Azure AD Application Proxy
- A compliance policy
- A conditional access policy
- An OAuth policy

Correct Answer:



Ensure that the users can connect to Service1 without being prompted for authentication:

- An app registration in Azure AD
- Azure AD Application Proxy
- [✓ An enterprise application in Azure AD]
- A managed identity in Azure AD

Ensure that the users can access Service1 only from the Azure AD-joined computers:

- Azure AD Application Proxy
- A compliance policy
- [✓ A conditional access policy]
- An OAuth policy

Reference: https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-how-applications-are-added https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/require-managed-devices

QUESTION 9

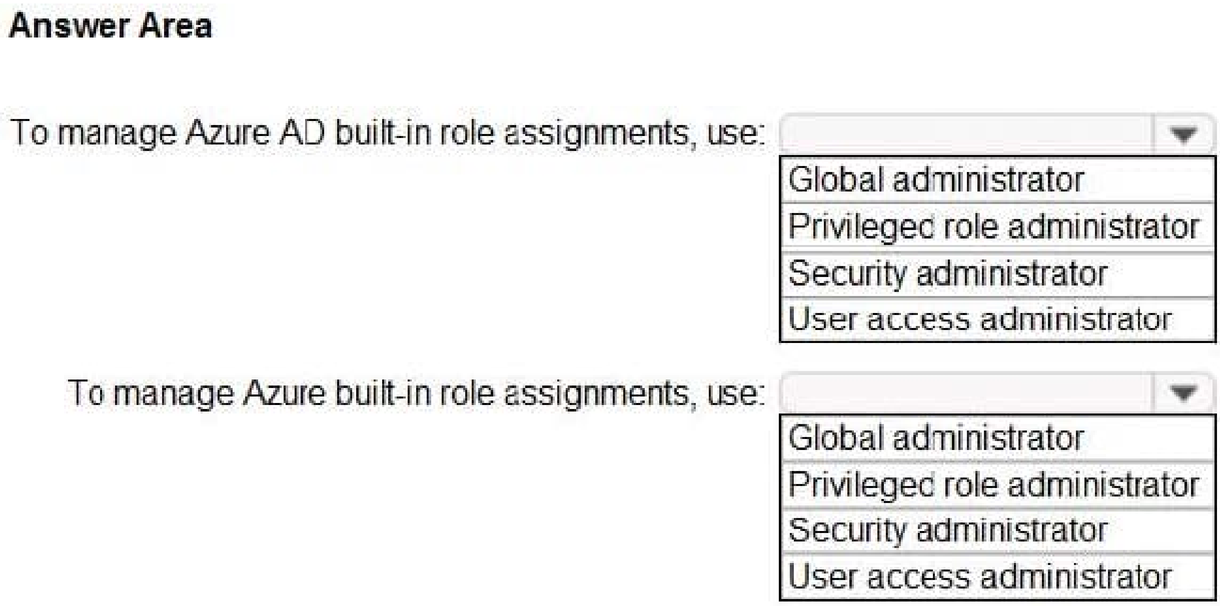
HOTSPOT

You need to identify which roles to use for managing role assignments. The solution must meet the delegation requirements.

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

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

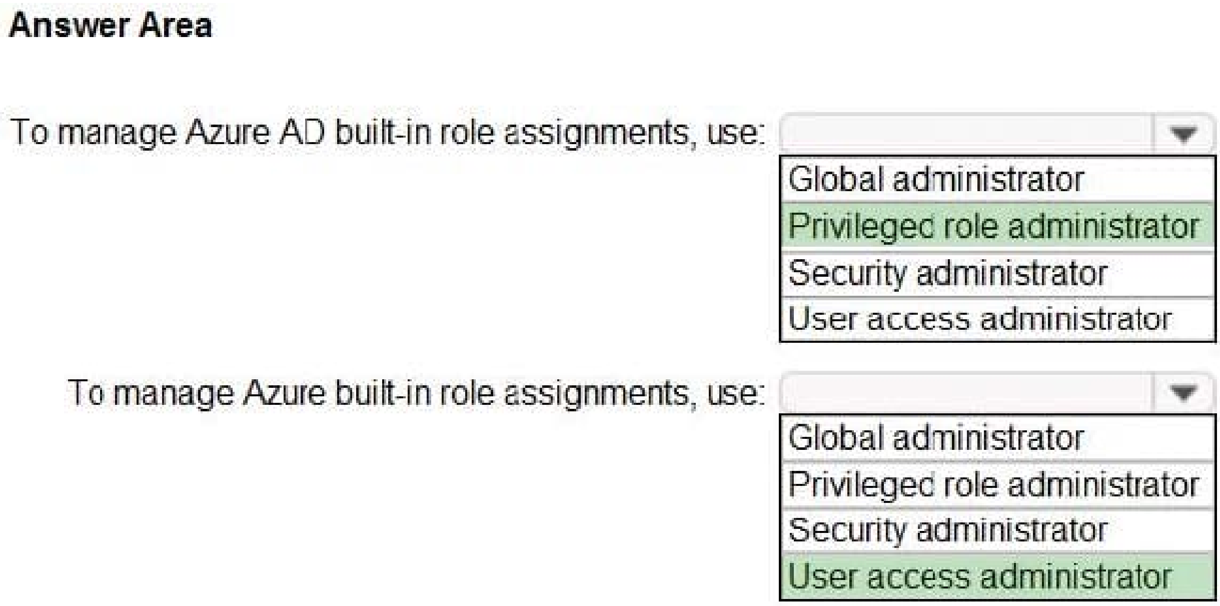
To manage Azure AD built-in role assignments, use:

- Global administrator
- Privileged role administrator
- Security administrator
- User access administrator

To manage Azure built-in role assignments, use:

- Global administrator
- Privileged role administrator
- Security administrator
- User access administrator

Correct Answer:



Answer Area

To manage Azure AD built-in role assignments, use:

- Global administrator
- [✓ Privileged role administrator]
- Security administrator
- User access administrator

To manage Azure built-in role assignments, use:

- Global administrator
- Privileged role administrator
- Security administrator
- [✓ User access administrator]

Reference: https://docs.microsoft.com/en-us/azure/role-based-access-control/role-assignments-portal
https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference

QUESTION 10

You have a Microsoft 365 tenant.

All users have computers that run Windows 10. Most computers are company-owned and joined to Azure Active Directory (Azure AD). Some computers are user-owned and are only registered in Azure AD.

You need to prevent users who connect to Microsoft SharePoint Online on their user-owned computer from downloading or syncing files. Other users must NOT be restricted.

Which policy type should you create?

A. a Microsoft Cloud App Security activity policy that has Microsoft Office 365 governance actions configured

B. an Azure AD conditional access policy that has session controls configured

C. an Azure AD conditional access policy that has client apps conditions configured

D. a Microsoft Cloud App Security app discovery policy that has governance actions configured

Correct Answer: B

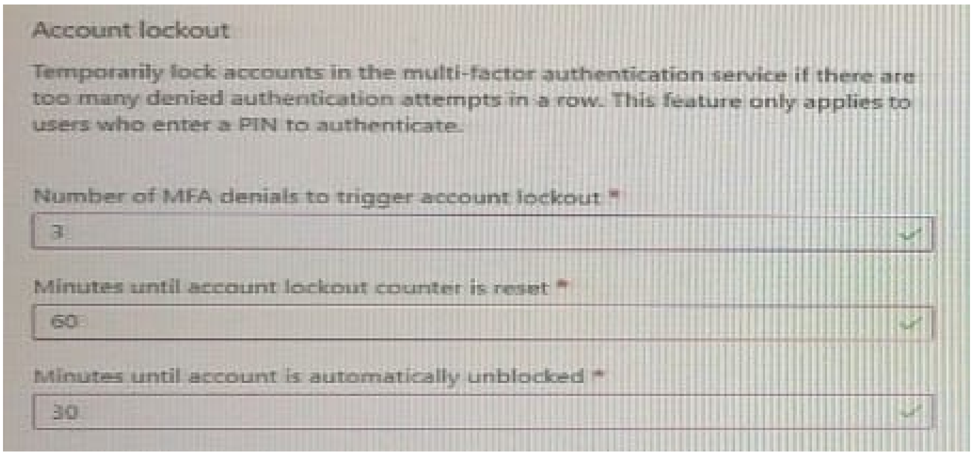
Reference: https://docs.microsoft.com/en-us/cloud-app-security/proxy-intro-aad

QUESTION 11

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.



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 *

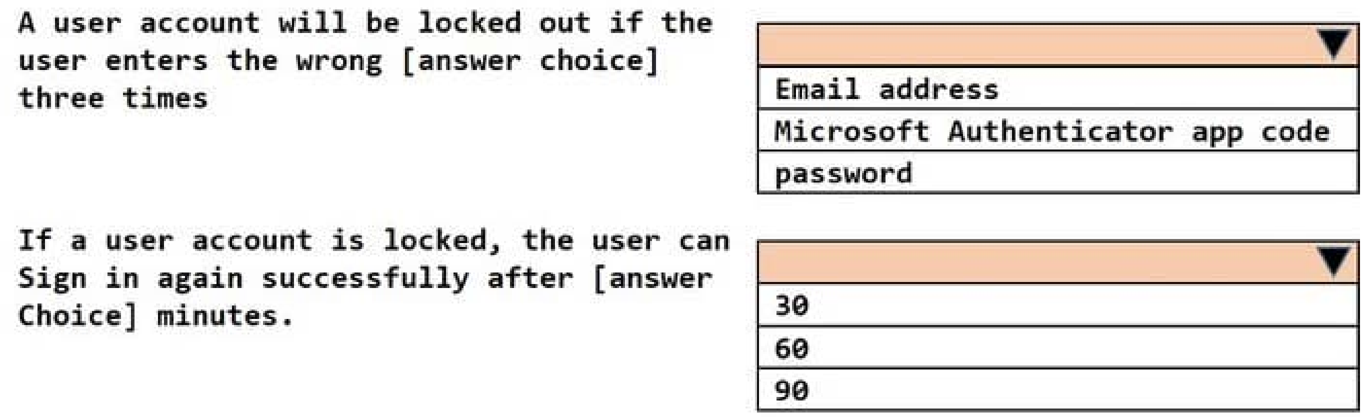
60

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.

Hot Area:



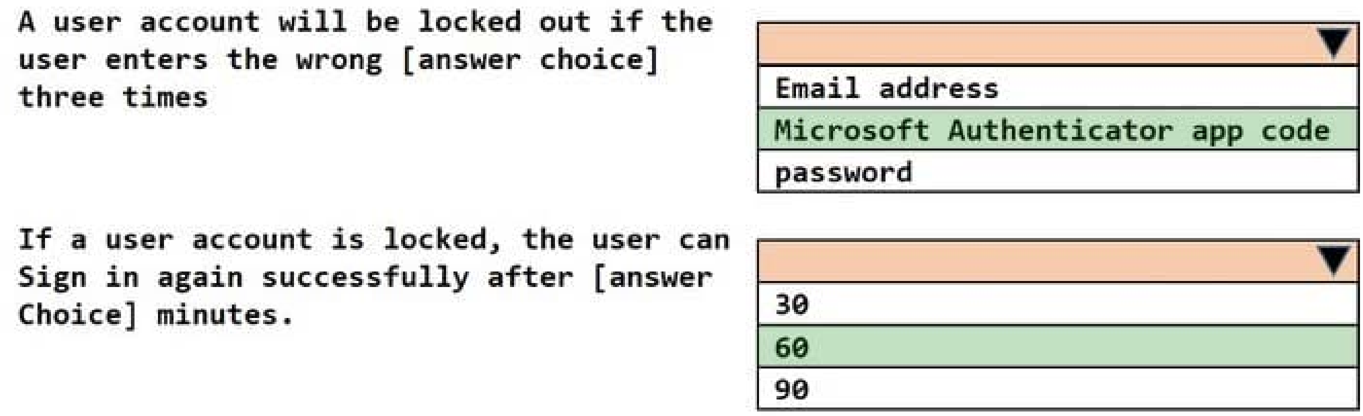
A user account will be locked out if the user enters the wrong [answer choice] three times

- 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

QUESTION 12

You have a Microsoft 365 tenant.

All users have mobile phones and Windows 10 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 laptops 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. voice

B. Windows Hello for Business

C. email

D. security questions

Correct Answer: B

QUESTION 13

HOTSPOT

You have a Microsoft 365 tenant.

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

1.

Identify sign-ins by users who are suspected of having leaked credentials.

2.

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

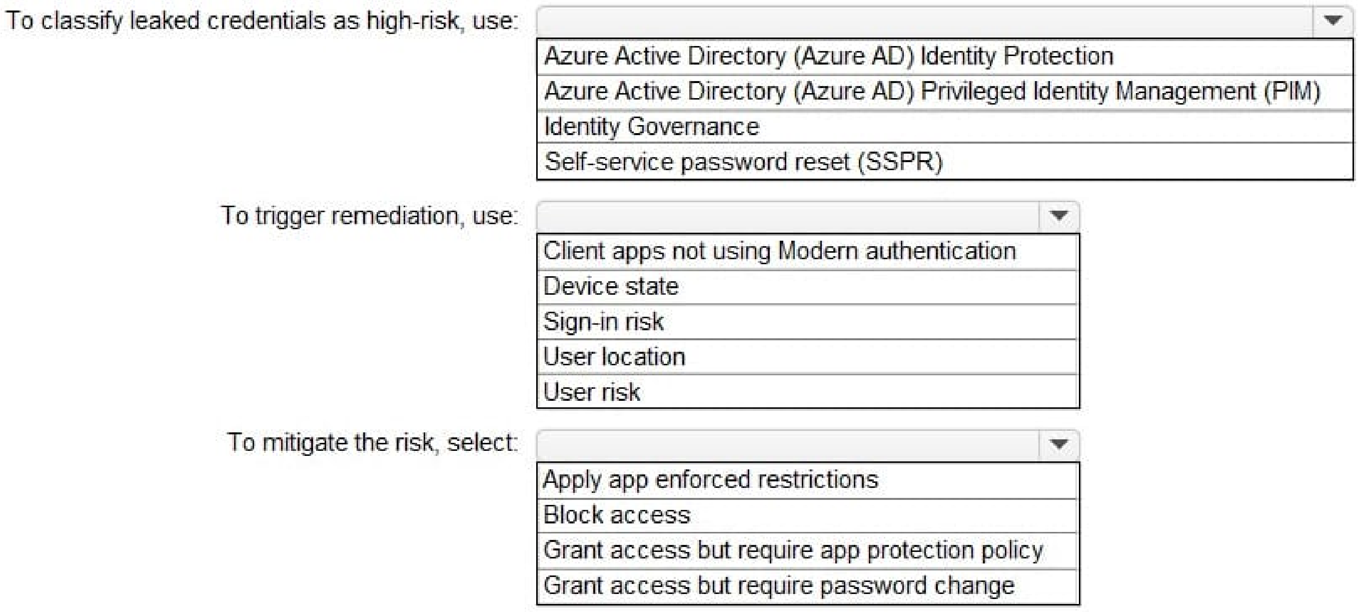
3.

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 in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



To classify leaked credentials as high-risk, use:

- Azure Active Directory (Azure AD) Identity Protection
- Azure Active Directory (Azure AD) Privileged Identity Management (PIM)
- Identity Governance
- Self-service password reset (SSPR)

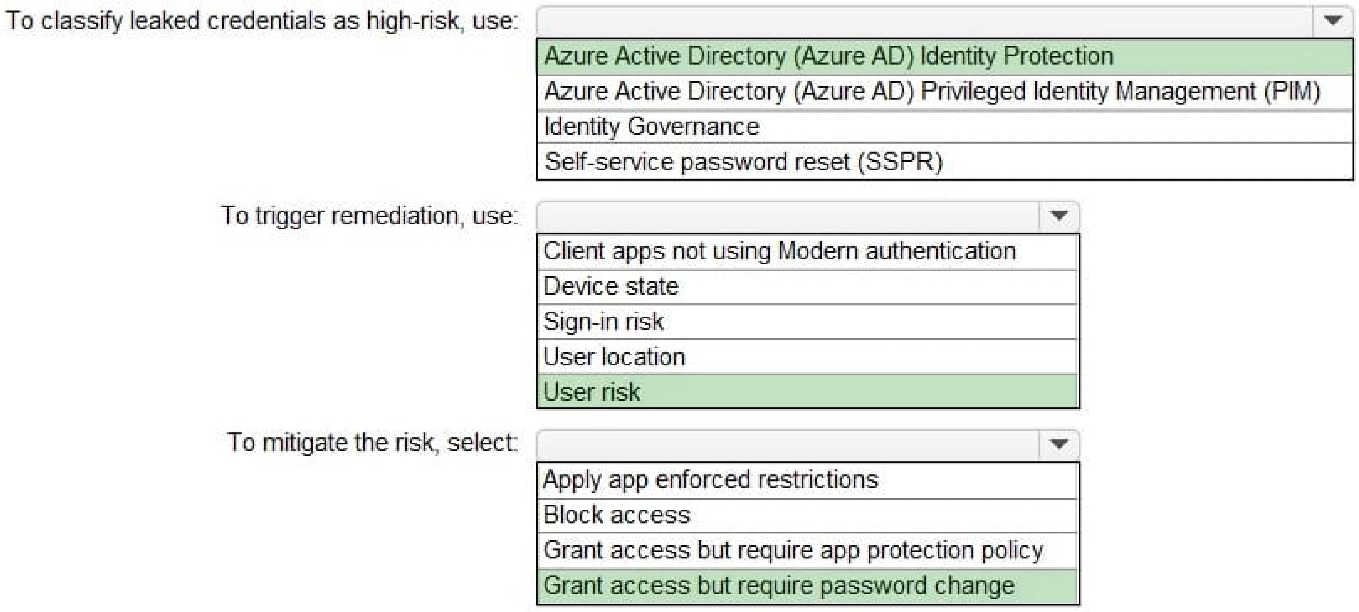
To trigger remediation, use:

- Client apps not using Modern authentication
- Device state
- Sign-in risk
- User location
- User risk

To mitigate the risk, select:

- Apply app enforced restrictions
- Block access
- Grant access but require app protection policy
- Grant access but require password change

Correct Answer:



To classify leaked credentials as high-risk, use:

- [✓ Azure Active Directory (Azure AD) Identity Protection]
- Azure Active Directory (Azure AD) Privileged Identity Management (PIM)
- Identity Governance
- Self-service password reset (SSPR)

To trigger remediation, use:

- Client apps not using Modern authentication
- Device state
- Sign-in risk
- User location
- [✓ User risk]

To mitigate the risk, select:

- Apply app enforced restrictions
- Block access
- Grant access but require app protection policy
- [✓ Grant access but require password change]

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

QUESTION 14

You configure a new Microsoft 36S 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 (Ml A) registration policy1.

D. Configure password protection for Windows Server Active Directory.

Correct Answer: B

QUESTION 15

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