MS-100$^{Q\&As}$

Microsoft 365 Identity and Services

Pass Microsoft MS-100 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/ms-100.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Microsoft Official Exam Center

QUESTION 1

HOTSPOT

You have a Microsoft 365 E5 subscription.

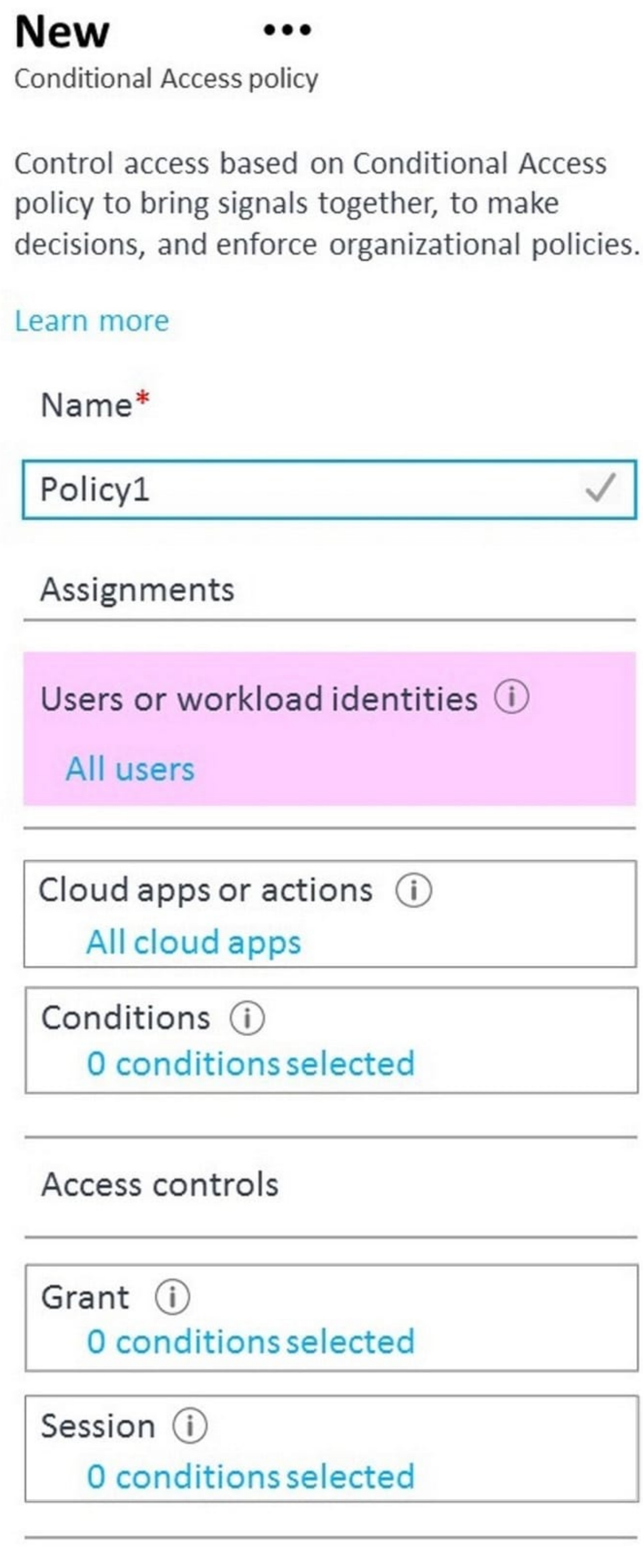
You create a Conditional Access policy named Policy1 and assign Policy1 to all users.

You need to configure Policy 1 to enforce multi-factor authentication (MFA) if the user risk level is high.

Which two settings should you configure in Policy1? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



New •••

Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies.

Learn more

Name*

Policy1 ✓

Assignments

Users or workload identities ⓘ
All users

Cloud apps or actions ⓘ
All cloud apps

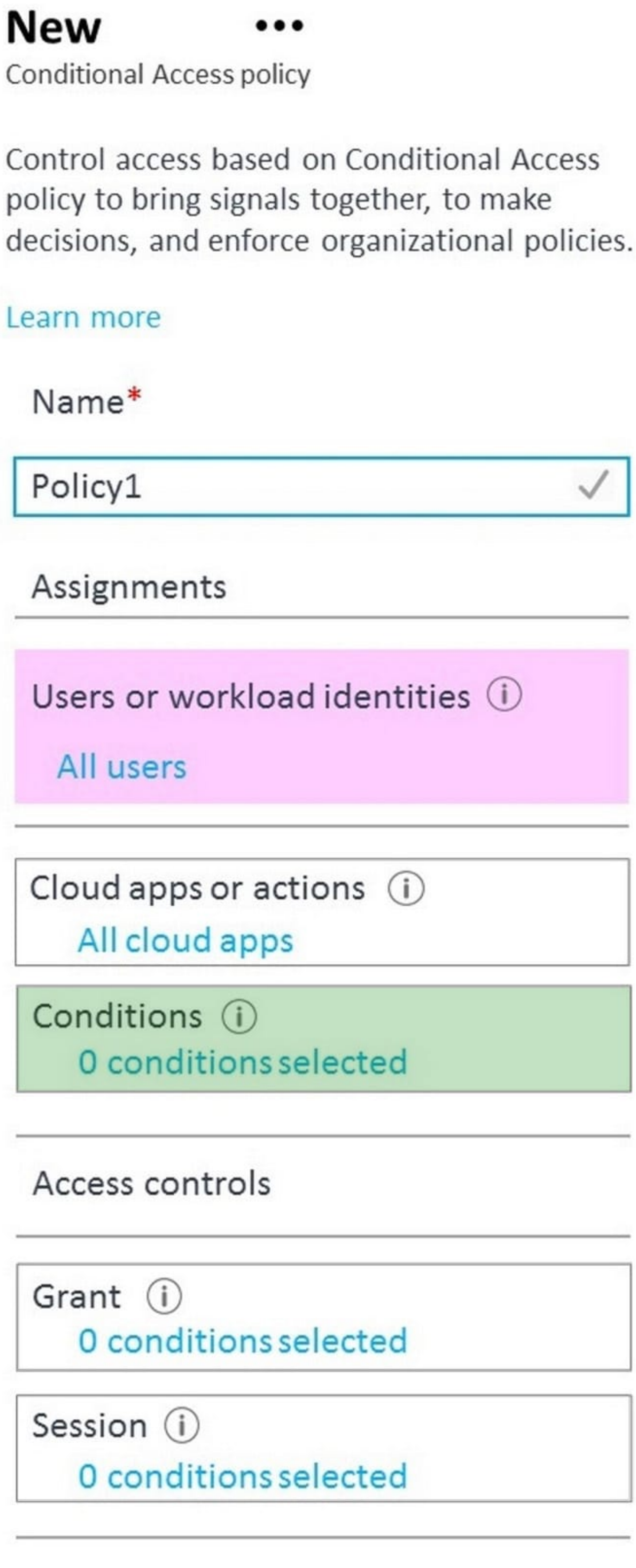
Conditions ⓘ
0 conditions selected

Access controls

Grant ⓘ
0 conditions selected

Session ⓘ
0 conditions selected

Correct Answer:



New •••

Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies.

Learn more

Name*

Policy1 ✓

Assignments

Users or workload identities ⓘ
All users

Cloud apps or actions ⓘ
All cloud apps

Conditions ⓘ
0 conditions selected

Access controls

Grant ⓘ
0 conditions selected

Session ⓘ
0 conditions selected

Box 1: Conditions

Sign-in risk policy in Conditional Access (see steps 7 and 8 below).

1.

Sign in to the Azure portal as a Conditional Access Administrator, Security Administrator, or Global Administrator.

2.

Browse to Azure Active Directory > Security > Conditional Access.

3.

Select New policy.

4.

Give your policy a name. We recommend that organizations create a meaningful standard for the names of their policies.

5.

Under Assignments, select Users or workload identities.

a.

Under Include, select All users.

b.

Under Exclude, select Users and groups and choose your organization\\'s emergency access or break-glass accounts.

c.

Select Done.

6.

Under Cloud apps or actions > Include, select All cloud apps.

7.

Under Conditions > Sign-in risk, set Configure to Yes. Under Select the sign-in risk level this policy will apply to. (This guidance is based on Microsoft recommendations and may be different for each organization)

a.Select High and Medium.

b.Select Done.

8.

Under Access controls > Grant.

a.

Select Grant access, Require multifactor authentication.

b.

Select Select.

9. Under Session.

a.

Select Sign-in frequency.

b.

Ensure Every time is selected.

c.

Select Select.

10.

Confirm your settings and set Enable policy to Report-only.

11.

Select Create to create to enable your policy.

Reference: https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure-risk-policies

QUESTION 2

You are developing a new Microsoft Teams app that will contain the following functionality:

1.

Start a new chat

2.

Prompt users to install an app.

3.

Make a Microsoft Graph API call.

4.

Trigger a search-based command.

Which two functionalities can be implemented by using a deep link? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point

A. Prompt users to install an app.

B. Trigger a search-based command.

C. Start a new chat

D. Make a Microsoft Graph API call.

Correct Answer: AC

QUESTION 3

Your company has an Enterprise E5 subscription of Microsoft 365.

You have been tasked with making sure that sales department users are compelled to make use of multi-factor authentication for all cloud-based applications.

Which of the following actions should you take?

A. You should create an DLP.

B. You should create a new app registration.

C. You should create a session policy.

D. You should create a sign-in risk policy.

Correct Answer: D

References: https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-sign-in-risk-policy

QUESTION 4

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.

Your network contains an on-premises Active Directory forest named contoso.com. The forest contains the following domains:

Contoso.com

East.contoso.com

An Azure AD Connect server is deployed to contoso.com. Azure AD Connect syncs to an Azure Active Directory (Azure AD) tenant.

You deploy a new domain named west.contoso.com to the forest.

You need to ensure that west.contoso.com syncs to the Azure AD tenant.

Solution: You install a new Azure AD Connect server in west.contoso.com and set AD Connect to active mode.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

You can only have one the AD Connect per tenant and one is already located in the root domain. Instead, run the wizard and add the new child domain to sync.

Reference: https://docs.microsoft.com/en-us/azure/active-directory/hybrid/plan-connect-topologies

QUESTION 5

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.

Your network contains an Active Directory forest.

You deploy Microsoft 365.

You plan to implement directory synchronization.

You need to recommend a security solution for the synchronized identities. The solution must meet the following requirements:

1.

Users must be able to authenticate successfully to Microsoft 365 services if Active Directory becomes unavailable.

2.

User passwords must be 10 characters or more.

Solution: Implement pass-through authentication and modify the password settings from the Default Domain Policy in Active Directory.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

This solution does not meet the following requirement:

Users must be able to authenticate successfully to Microsoft 365 services if Active Directory becomes unavailable.

This is because with pass-through authentication, the authentication is performed by the on-premise Active Directory.

This solution does meet the following requirement:

User passwords must be 10 characters or more.

Configuring the Default Domain Policy in the on-premise Active Directory meets the requirement.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-password-hash-synchronization