MS-100Q&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.geekcert.com/ms-100.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.

Your network contains an Active Directory domain.

You deploy a Microsoft Azure Active Directory (Azure AD) tenant.

Another administrator configures the domain to synchronize to Azure AD.

You discover that 10 user accounts in an organizational unit (OU) are NOT synchronized to Azure AD. All the other user accounts synchronized successfully.

You review Azure AD Connect Health and discover that all the user account synchronizations completed successfully.

You need to ensure that the 10 user accounts are synchronized to Azure AD.

Solution: From Azure AD Connect, you modify the filtering settings.

Does this meet the goal?

A. Yes

B. No

Correct Answer: A

The question states that "all the user account synchronizations completed successfully". Therefore, we know that Azure AD Connect is working and configured correctly. The only thing that would prevent the 10 user accounts from being synchronized is that they are being excluded from the synchronization cycle by a filtering rule.

Reference: https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-configure-filtering

QUESTION 2

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 company has a Microsoft 365 tenant.

You suspect that several Office 365 features were recently updated.

You need to view a list of the features that were recently updated in the tenant.

Solution: You use Reports from the Microsoft Purview compliance portal.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

QUESTION 3

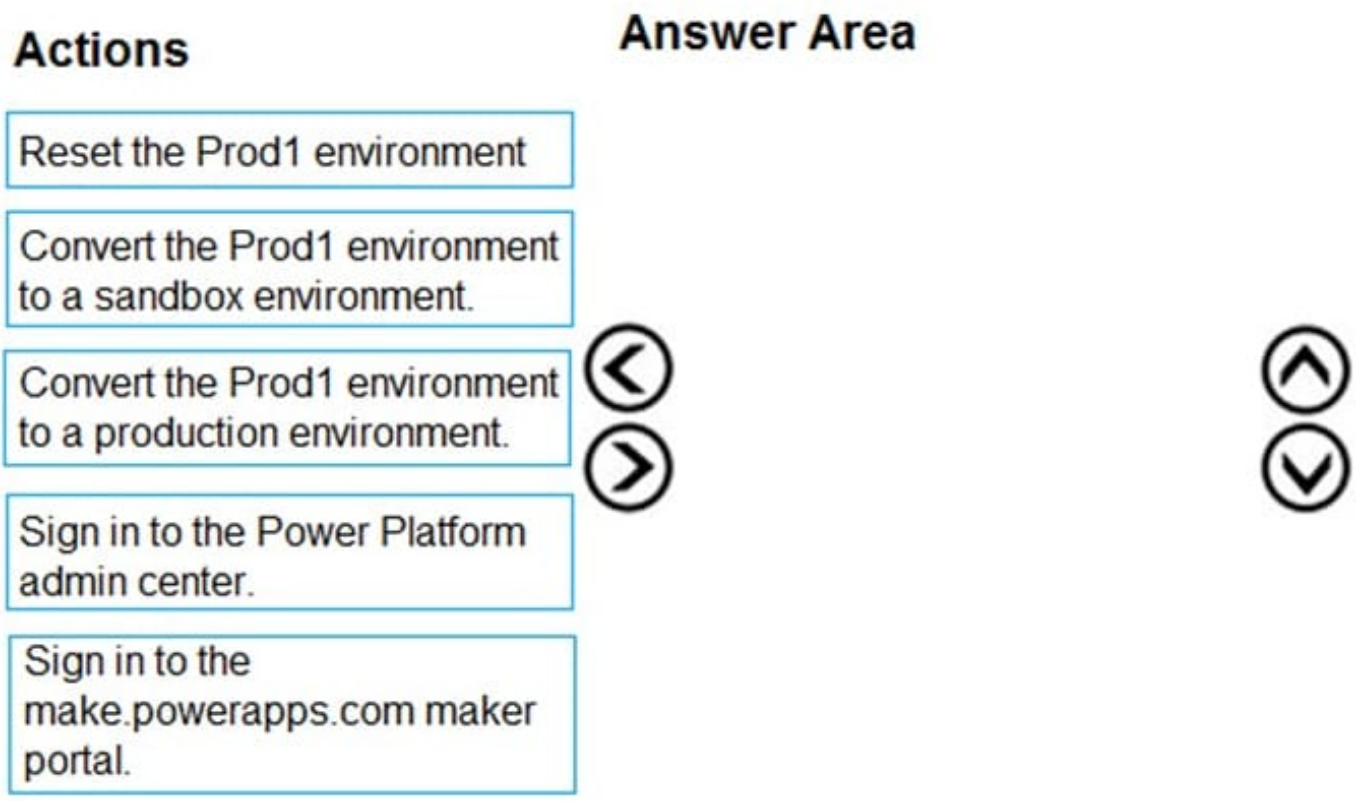
DRAG DROP

You have a pilot app named App1 deployed to a Microsoft Power Platform production environment named Prod1.

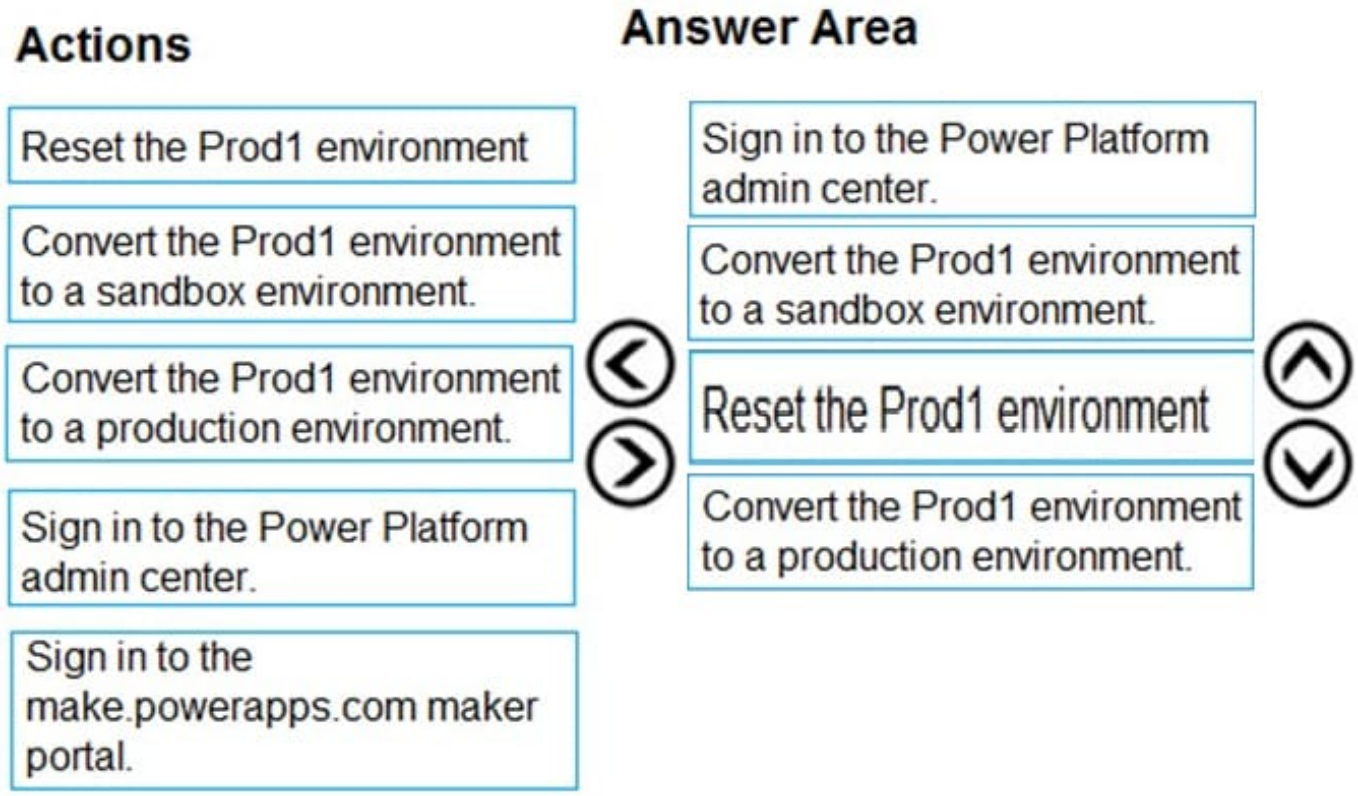
You need to reset the Prod1 environment in preparation for the production deployment of App1.

Which four 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.

Select and Place:



Correct Answer:



Reference: https://docs.microsoft.com/en-us/power-platform/admin/switch-environment

https://docs.microsoft.com/en-us/power-platform/admin/reset-environment

QUESTION 4

HOTSPOT

You have a Microsoft 365 subscription that uses a default domain named contoso.com. The domain contains the users shown in the following table.

Name	Member of
User1	Compliant
User2	Group1, Group2

The domain contains the devices shown in the following table.

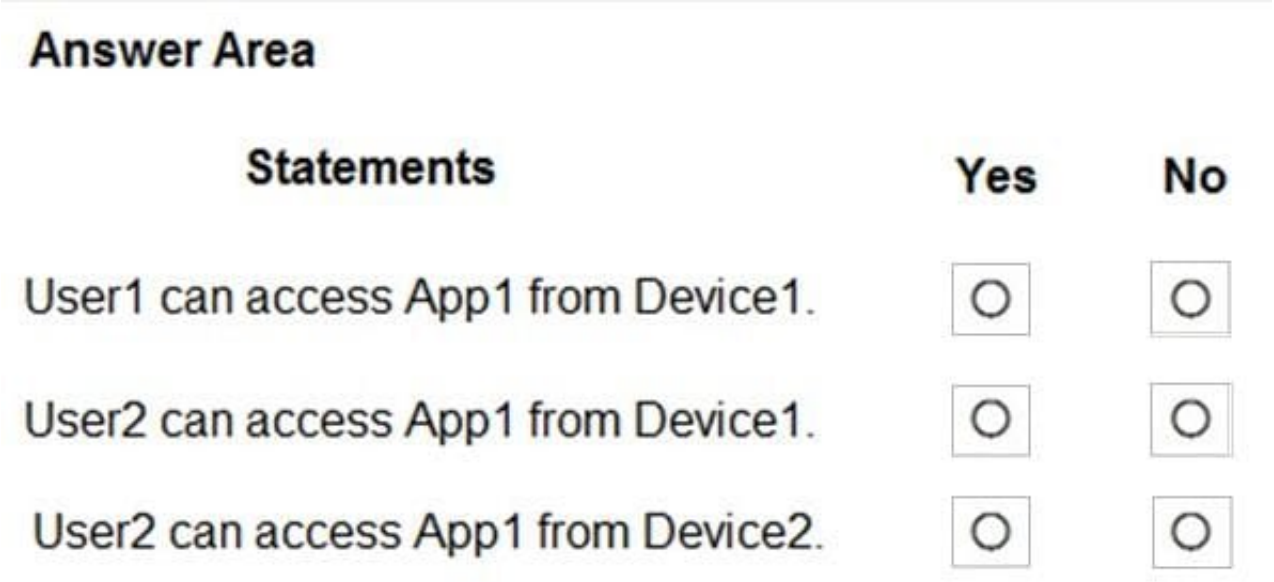
Name	Compliance status
Device1	Compliant
Device2	Noncompliant

The domain contains conditional access policies that control access to a cloud app named App1. The policies are configured as shown in the following table.

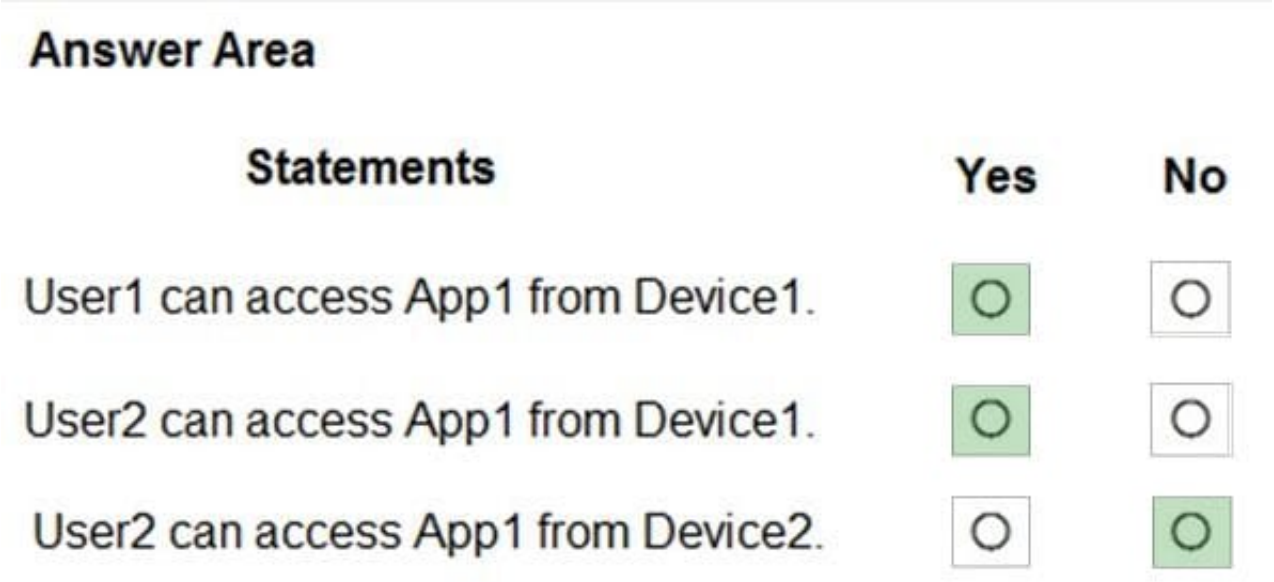
Name	Includes	Excludes	Device state includes	Device state excludes	Grant
Policy1	Group1	*None*	All device states	Devices marked as compliant	Block access
Policy2	Group1	Group2	*None*	*None*	Block Access
Policy3	Group1	*None*	All device states	*None*	Grant access

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:



Correct Answer:



Box 1: Yes.

User1 is in a group named Compliant. All the conditional access policies apply to Group1 so they don\\'t apply to User1.

As there is no conditional access policy blocking access for the group named Compliant, User1 is able to access App1 using any device.

Box 2: Yes.

User2 is in Group1 so Policy1 applies first. Policy1 excludes compliant devices and Device1 is compliant. Therefore, Policy1 does not apply so we move on to Policy2.

User2 is also in Group2. Policy2 excludes Group2. Therefore, Policy2 does not apply so we move on to Policy3.

Policy3 applies to Group1 so Policy3 applies to User2. Policy3 applies to 'All device states' so Policy3 applies to Device1. Policy3 grants access. Therefore, User2 can access App1 using Device1.

Box 3: No.

User2 is in Group1 so Policy1 applies. Policy1 excludes compliant devices but Devices is non-compliant. Therefore, User2 cannot access App1 from Device2.

References:

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/plan-conditional-access

QUESTION 5

HOTSPOT

You have a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com that includes a user named User1.

You enable multi-factor authentication for contoso.com and configure the following two fraud alert settings:

1.

Set Allow users to submit fraud alerts: On

2.

Automatically block users who report fraud: On

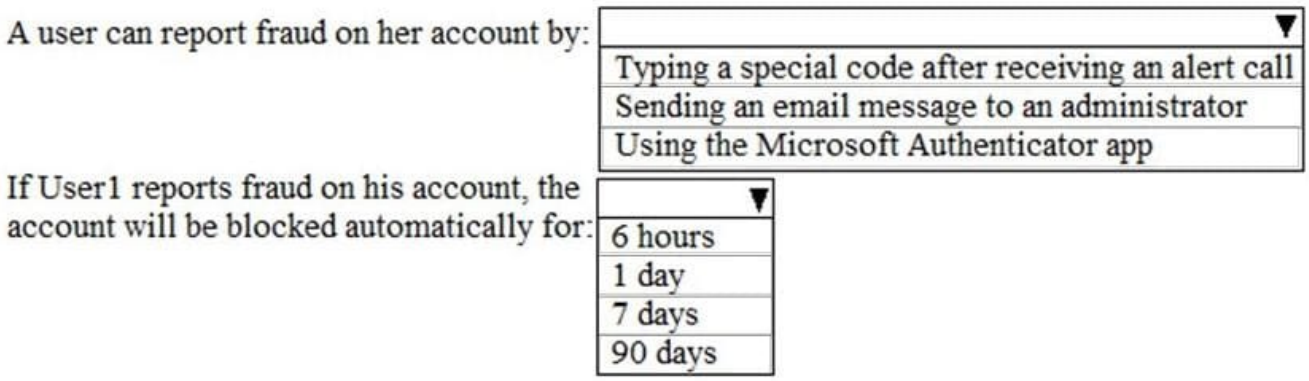
You need to instruct the users in your organization to use the fraud reporting features correctly.

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

NOTE: Each correct selection is worth one point.

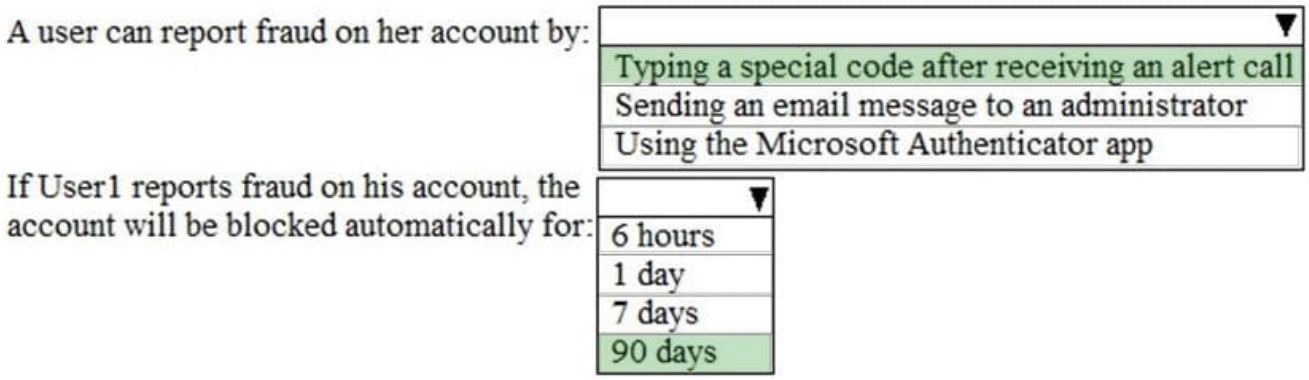
Hot Area:

Answer Area



Correct Answer:

Answer Area



Code to report fraud during initial greeting: When users receive a phone call to perform two-step verification, they normally press # to confirm their sign-in. To report fraud, the user enters a code before pressing #. This code is 0 by default,

but you can customize it.

Block user when fraud is reported: If a user reports fraud, their account is blocked for 90 days or until an administrator unblocks their account. An administrator can review sign-ins by using the sign-in report, and take appropriate action to

prevent future fraud. An administrator can then unblock the user\\'s account.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings#fraud-alert

You have a Microsoft 365 subscription that contains a guest user named User1. User1 is assigned the User administrator role.

You have a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com. Contoso.com is configured as shown in the following exhibit.