A user can report fraud on her account by:

▼
Typing a special code after receiving an alert call
Sending an email message to an administrator
Using the Microsoft Authenticator app

If User1 reports fraud on his account, the account will be blocked automatically for:

▼
6 hours
1 day
7 days
90 days

QUESTION 54

From the Microsoft Azure Active Directory (Azure AD) Identity Protection dashboard, you view the risk events shown in the exhibit. (Click the Exhibit tab.)
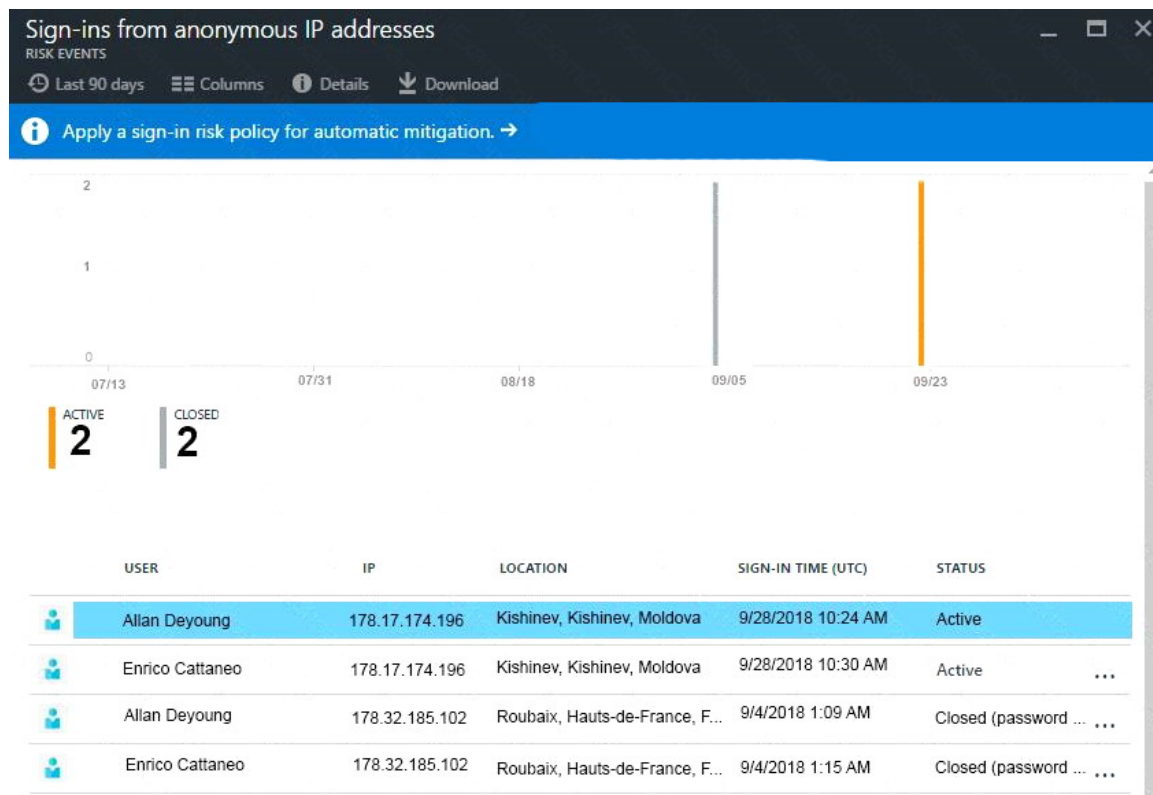
You need to reduce the likelihood that the sign-ins are identified as risky.

What should you do?

A. From the Security & Compliance admin center, add the users to the Security Readers role group.
B. From the Conditional access blade in the Azure Active Directory admin center, create named locations.
C. From the Azure Active Directory admin center, configure the trusted IPs for multi-factor authentication.
D. From the Security & Compliance admin center, create a classification label.

Correct Answer: B
Explanation:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition

QUESTION 55
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 named contoso.com that is synced to Microsoft Azure Active Directory (Azure AD).

You manage Windows 10 devices by using Microsoft System Center Configuration Manager (Current Branch).

You configure a pilot for co-management.

You add a new device named Device1 to the domain. You install the Configuration Manager client on Device1.

You need to ensure that you can manage Device1 by using Microsoft Intune and Configuration Manager.

Solution: You add Device1 to an Active Directory group.

Does this meet the goal?

A. Yes
B. No

Correct Answer: A
Explanation:
https://www.scconfigmgr.com/2017/11/30/how-to-setup-co-management-part-6/

QUESTION 56
Your company has a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com.

You sign up for Microsoft Store for Business.

The tenant contains the users shown in the following table.

Name	Microsoft Store for Business role	Azure AD role
User1	Purchaser	*None*
User2	Basic Purchaser	*None*
User3	*None*	Application administrator
User4	*None*	Cloud application administrator
User5	*None*	*None*

Microsoft Store for Business has the following Shopping behavior settings:
▪ Allow users to shop is set to On.
▪ Make everyone a Basic Purchaser is set to Off.

You need to identify which users can install apps from the Microsoft for Business private store.

Which users should you identify?

A. A.user1, User2, User3, User4, and User5
B. User1 only
C. User1 and User2 only
D. User3 and User4 only
E. User1, User2, User3, and User4 only

Correct Answer: C
Explanation:
Allow users to shop controls the shopping experience in Microsoft Store for Education. When this setting is on, Purchasers and Basic Purchasers can purchase products and services from Microsoft Store for Education.

References:
https://docs.microsoft.com/en-us/microsoft-store/acquire-apps-microsoft-store-for-business

QUESTION 57
HOTSPOT
You have three devices enrolled in Microsoft Intune as shown in the following table.

Name	Microsoft Store for Business role	Azure AD role
User1	Purchaser	*None*
User2	Basic Purchaser	*None*
User3	*None*	Application administrator
User4	*None*	Cloud application administrator
User5	*None*	*None*

The device compliance policies in Intune are configured as shown in the following table.

Name	Platform	Require BitLocker	Assigned
Policy1	Windows 10 and later	Require	Yes
Policy2	Windows 10 and later	Not configured	Yes
Policy3	Windows 10 and later	Require	No

The device compliance policies have the assignment shown in the following table.

Name	Assigned to
Policy1	Group3
Policy2	Group2

For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

Statements	Yes	No
Device1 is compliant.	○	○
Device2 is compliant.	○	○
Device3 is compliant.	○	○

Correct Answer:

Statements	Yes	No
Device1 is compliant.	○	**○**
Device2 is compliant.	○	**○**
Device3 is compliant.	**○**	○

QUESTION 58
HOTSPOT
You have a Microsoft 365 subscription.

You have a group named Support. Users in the Support group frequently send email messages to external users.

The manager of the Support group wants to randomly review messages that contain attachments.

You need to provide the manager with the ability to review messages that contain attachments sent from the Support group users to external users. The manager must have access to only 10 percent of the messages.

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

NOTE: Each correct selection is worth one point.

To meet the goal for the manager, create:

A label policy
A retention policy
A supervisor policy
An alert policy
MyAnalytics

To review the messages, the manager must use:

A message trace
An eDiscovery case
MyAnalytics
Outlook Web App

Correct Answer:

To meet the goal for the manager, create:

A label policy
A retention policy
A supervisor policy
An alert policy
MyAnalytics

To review the messages, the manager must use:

A message trace
An eDiscovery case
MyAnalytics
Outlook Web App

QUESTION 59
HOTSPOT
You have a Microsoft 365 Enterprise subscription.

You create a password policy as shown in the following exhibit.