Microsoft.VCEup.com.MS-101.2022-July-04.214q

Number: MS-101
Passing Score: 800
Time Limit: 120 min

MS-101

Microsoft 365 Mobility and Security

Question Set 1

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.

You are deploying Microsoft Intune.

You successfully enroll Windows 10 devices in Intune.

When you try to enroll an iOS device in Intune, you get an error.

You need to ensure that you can enroll the iOS device in Intune.

Solution: You add your user account as a device enrollment manager.

Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:

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.

You are deploying Microsoft Intune.

You successfully enroll Windows 10 devices in Intune.

When you try to enroll an iOS device in Intune, you get an error. You

need to ensure that you can enroll the iOS device in Intune.

Solution: You configure the Apple MDM Push certificate.

Does this meet the goal?

A. Yes
B. No

Correct Answer: A
Section: [none]
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/intune/apple-mdm-push-certificate-get

QUESTION 3

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 are deploying Microsoft Intune.

You successfully enroll Windows 10 devices in Intune.

When you try to enroll an iOS device in Intune, you get an error. You

need to ensure that you can enroll the iOS device in Intune.

Solution: You create an Apple Configurator enrollment profile.

Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:

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 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 pilot 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 create a device configuration profile from the Device Management admin center.

Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:

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 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 pilot 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
Section: [none]
Explanation

Explanation/Reference:
References: https://www.scconfigmgr.com/2017/11/30/how-to-setup-co-management-part-6/

QUESTION 6
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 pilot 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 unjoin Device1 from the Active Directory domain.

Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section: [none]
Explanation

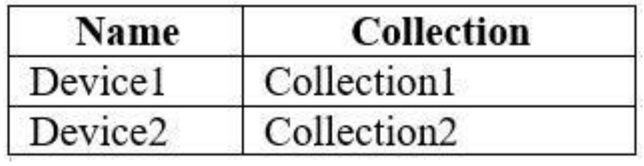
Explanation/Reference:

QUESTION 7 HOTSPOT

Your network contains an Active Directory forest named contoso.com that is synced to Microsoft Azure Active Directory (Azure AD).

You use Microsoft Endpoint Configuration Manager for device management.

You have the Windows 10 devices shown in the following table.

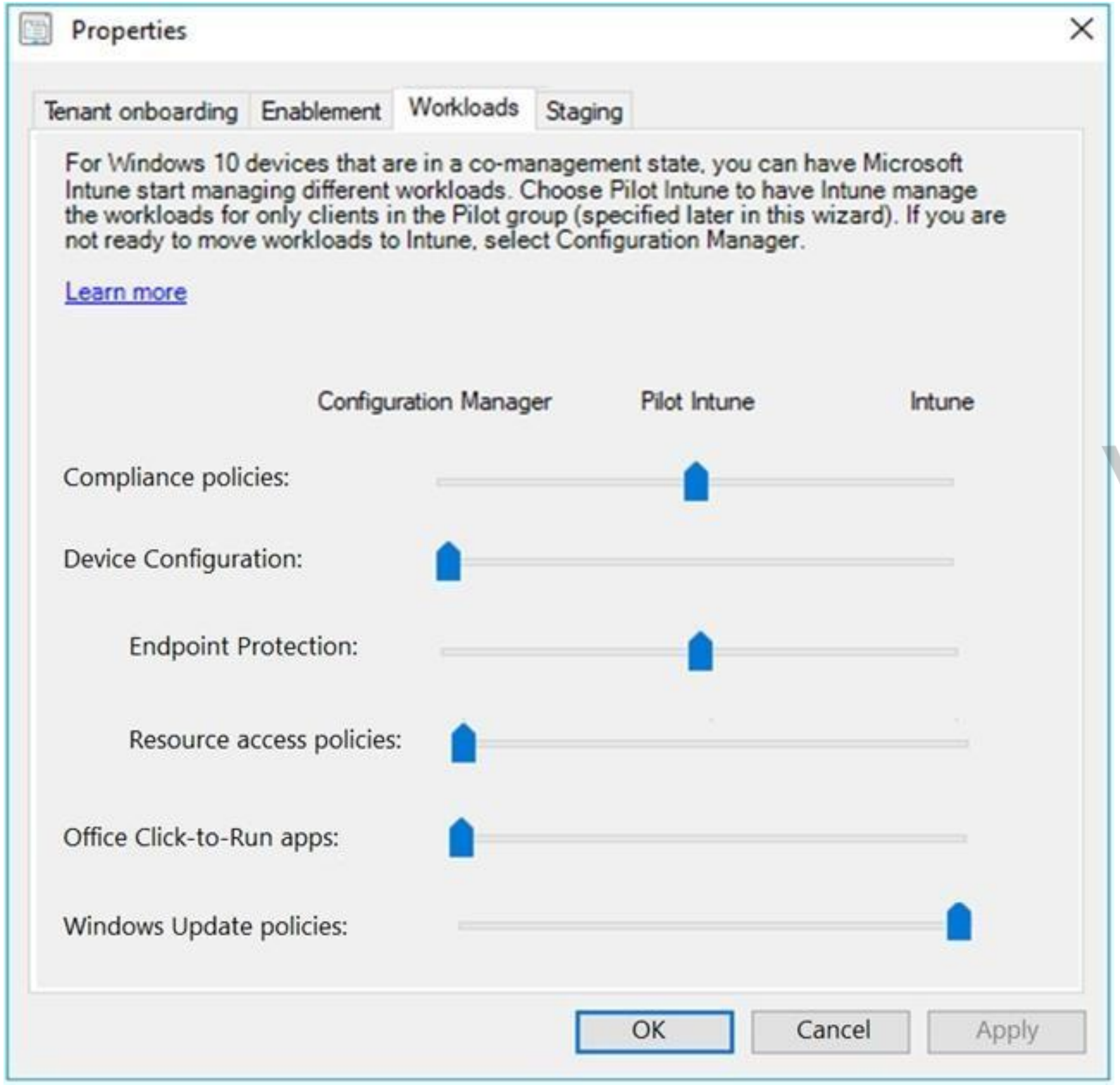


Name	Collection
Device1	Collection1
Device2	Collection2

You configure Endpoint Configuration Manager co-management as follows:

- Automatic enrollment in Intune: Pilot
- Pilot collection for all workloads: Collection2

You configure co-management workloads as shown in the following exhibit.



For Windows 10 devices that are in a co-management state, you can have Microsoft Intune start managing different workloads. Choose Pilot Intune to have Intune manage the workloads for only clients in the Pilot group (specified later in this wizard). If you are not ready to move workloads to Intune, select Configuration Manager.

Learn more

	Configuration Manager	Pilot Intune	Intune
Compliance policies:		●	
Device Configuration:	●		
Endpoint Protection:		●	
Resource access policies:	●		
Office Click-to-Run apps:	●		
Windows Update policies:			●

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:

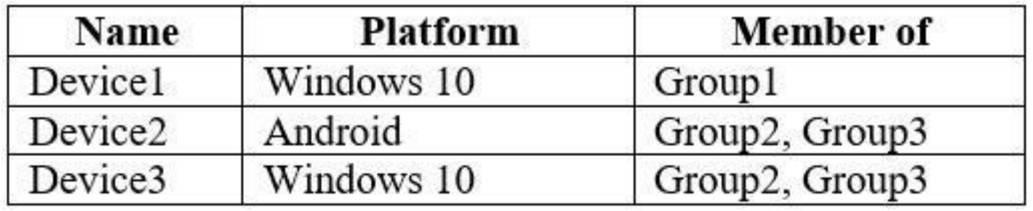
Correct Answer:

Section: [none]
Explanation

Explanation/Reference:

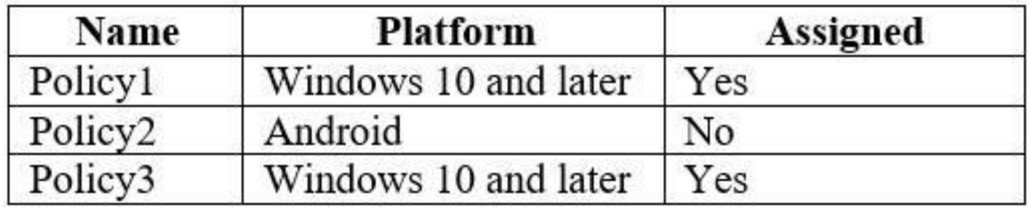
QUESTION 8 HOTSPOT

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



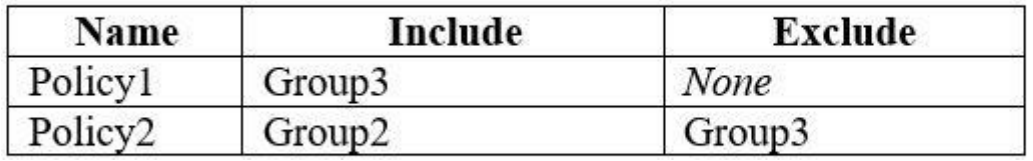
Name	Platform	Member of
Device1	Windows 10	Group1
Device2	Android	Group2, Group3
Device3	Windows 10	Group2, Group3

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



Name	Platform	Assigned
Policy1	Windows 10 and later	Yes
Policy2	Android	No
Policy3	Windows 10 and later	Yes

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



Name	Include	Exclude
Policy1	Group3	*None*
Policy2	Group2	Group3

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:

Section: [none]
Explanation

Explanation/Reference:

QUESTION 9 You have Windows 10 Pro devices that are joined to an Active Directory domain.

You plan to create a Microsoft 365 tenant and to upgrade the devices to Windows 10 Enterprise.

You are evaluating whether to deploy Windows Hello for Business.

What are two prerequisites of the deployment? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. Microsoft Intune enrollment
B. Microsoft Azure Active Directory (Azure AD)
C. smartcards

D. TPM-enabled devices

Correct Answer: AB
Section: [none]
Explanation

Explanation/Reference:
Reference: https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-hybrid-aadj-sso-base

QUESTION 10 You have a Microsoft 365 tenant.

All users are assigned the Enterprise Mobility + Security license.

You need to ensure that when users join their device to Microsoft Azure Active Directory (Azure AD), the device is enrolled in Microsoft Intune automatically.

What should you configure?

A. Enrollment restrictions from the Device Management admin center
B. device enrollment managers from the Device Management admin center
C. MAM User scope from the Azure Active Directory admin center
D. MDM User scope from the Azure Active Directory admin center

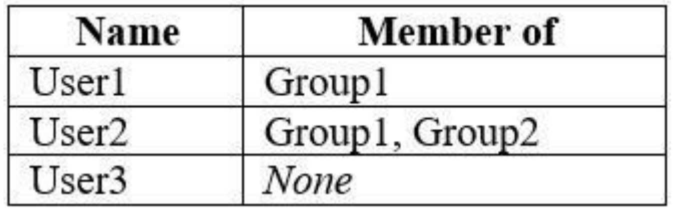
Correct Answer: D
Section: [none]
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/intune/windows-enroll

QUESTION 11
HOTSPOT

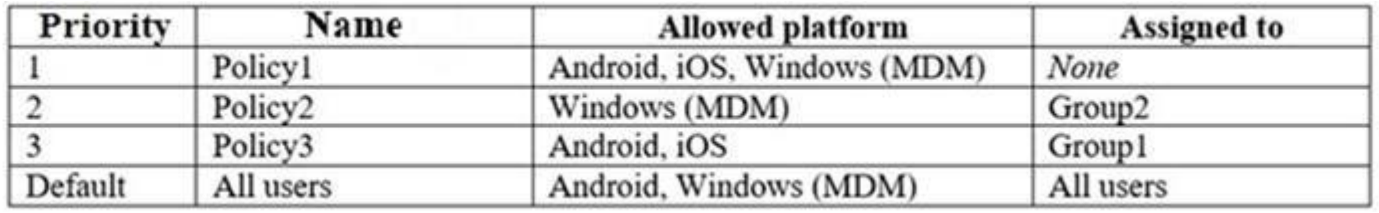
You have several devices enrolled in Microsoft Endpoint Manager.

You have a Microsoft Azure Active Directory (Azure AD) tenant that includes the users shown in the following table.



Name	Member of
User1	Group1
User2	Group1, Group2
User3	*None*

The device type restrictions in Endpoint Manager are configured as shown in the following table.



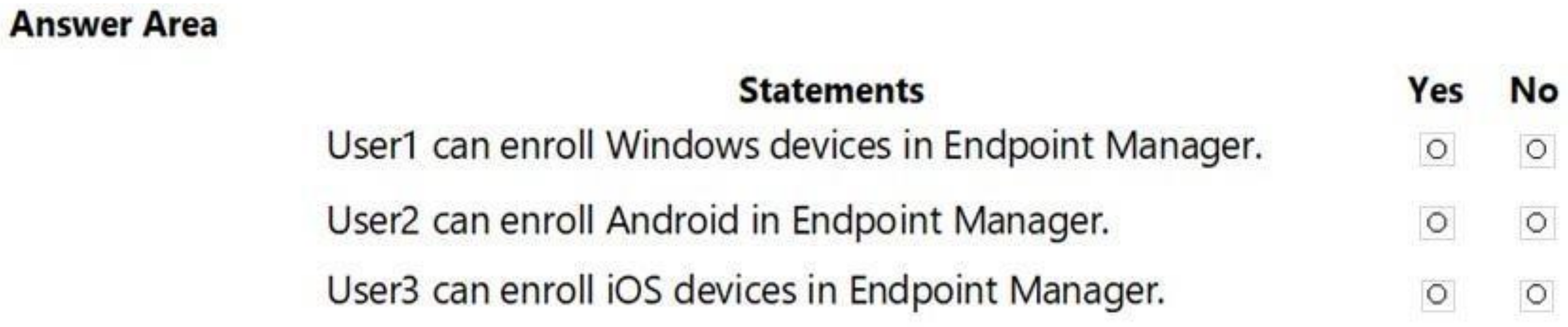
Priority	Name	Allowed platform	Assigned to
1	Policy1	Android, iOS, Windows (MDM)	*None*
2	Policy2	Windows (MDM)	Group2
3	Policy3	Android, iOS	Group1
Default	All users	Android, Windows (MDM)	All users

You add User3 as a device enrollment manager in Endpoint Manager.

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

NOTE: Each correct selection is worth one point.

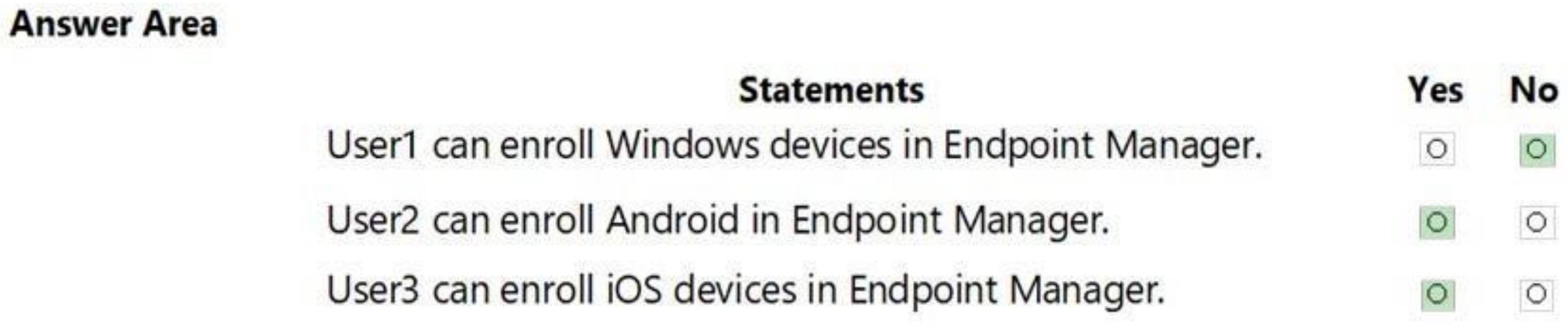
Hot Area:



Answer Area

Statements	Yes	No
User1 can enroll Windows devices in Endpoint Manager.	○	○
User2 can enroll Android in Endpoint Manager.	○	○
User3 can enroll iOS devices in Endpoint Manager.	○	○

Correct Answer:



Answer Area

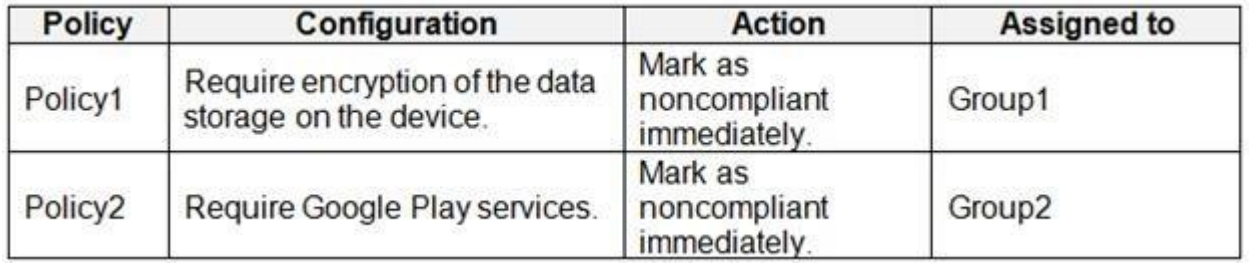
Statements	Yes	No
User1 can enroll Windows devices in Endpoint Manager.	○	[✓ ○]
User2 can enroll Android in Endpoint Manager.	[✓ ○]	○
User3 can enroll iOS devices in Endpoint Manager.	[✓ ○]	○

Section: [none]
Explanation

Explanation/Reference:

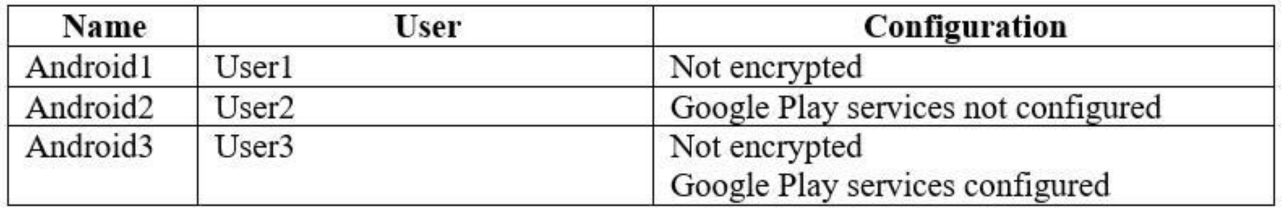
QUESTION 12
HOTSPOT

You create two device compliance policies for Android devices as shown in the following table.



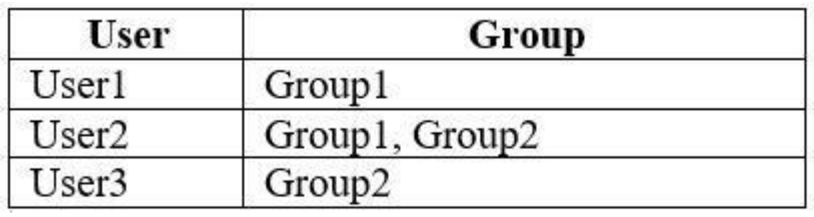
Policy	Configuration	Action	Assigned to
Policy1	Require encryption of the data storage on the device.	Mark as noncompliant immediately.	Group1
Policy2	Require Google Play services.	Mark as noncompliant immediately.	Group2

You have the Android devices shown in the following table.



Name	User	Configuration
Android1	User1	Not encrypted
Android2	User2	Google Play services not configured
Android3	User3	Not encrypted Google Play services configured

The users belong to the groups shown in the following table.



User	Group
User1	Group1
User2	Group1, Group2
User3	Group2

The users enroll their device in Microsoft Intune.

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:

Section: [none]
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/intune-user-help/enroll-your-device-in-intune-android

QUESTION 13
HOTSPOT

Your network contains an Active Directory domain named contoso.com. All client devices run Windows 10 and are joined to the domain.

You update the Windows 10 devices by using Windows Update for Business.

What is the maximum amount of time you can defer Windows 10 updates? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Correct Answer:

Section: [none]
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/windows/deployment/update/waas-manage-updates-wufb

QUESTION 14
Your company uses Microsoft Endpoint Configuration Manager and Microsoft Endpoint Manager to co-manage devices.

Which two actions can be performed only from Endpoint Manager? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. Deploy applications to Windows 10 devices.
B. Deploy VPN profiles to iOS devices.
C. Deploy VPN profiles to Windows 10 devices.
D. Publish applications to Android devices.

Correct Answer: BD

Section: [none]
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/sccm/comanage/overview
https://docs.microsoft.com/en-us/sccm/mdm/deploy-use/create-vpn-profiles

QUESTION 15
HOTSPOT

Your network contains an Active Directory domain named contoso.com that uses Microsoft System Center Configuration Manager (Current Branch).

You have Windows 10 and Windows 8.1 devices.

You need to ensure that you can analyze the upgrade readiness of all the Windows 8.1 devices and analyze the update compliance of all the Windows 10 devices.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Correct Answer:

Section: [none]
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/windows/deployment/upgrade/upgrade-readiness-get-started https://docs.microsoft.com/en-us/windows/deployment/update/update-compliance-get-started

QUESTION 16 You have a Microsoft Azure Active Directory (Azure AD) tenant named contoso.onmicrosoft.com.

You have a Microsoft 365 subscription.

You need to ensure that administrators can manage the configuration settings for all the Windows 10 devices in your organization.

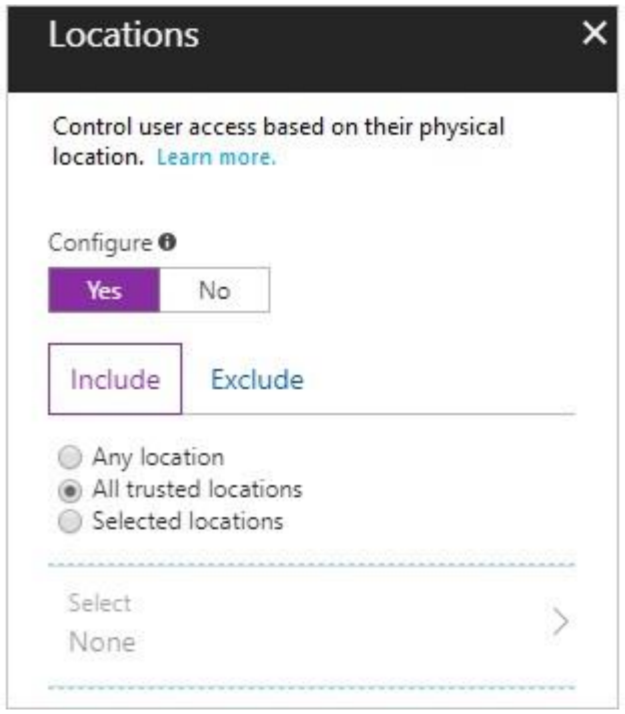
What should you configure?

A. the Enrollment restrictions
B. the mobile device management (MDM) authority
C. the Exchange on-premises access settings
D. the Windows enrollment settings

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/intune/mdm-authority-set

QUESTION 17
You configure a conditional access policy. The locations settings are configured as shown in the Locations exhibit. (Click the **Locations** tab.)



Locations

Control user access based on their physical location. Learn more.

Configure

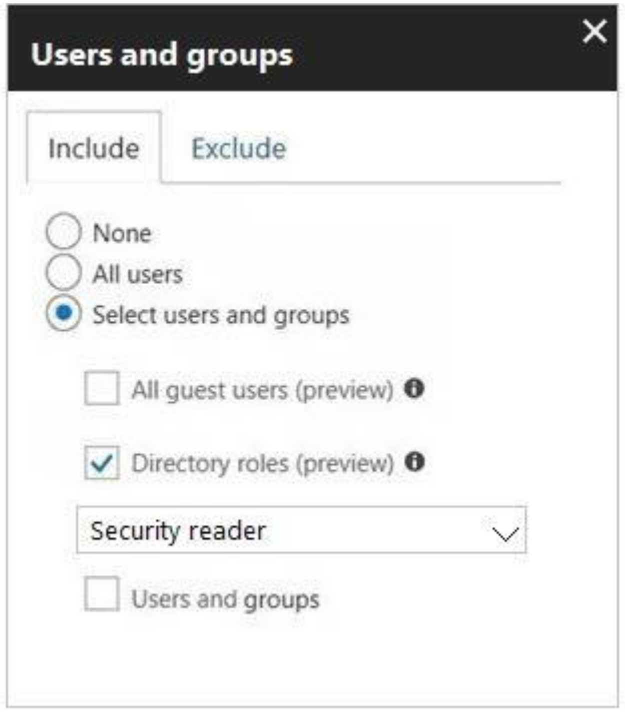
Yes | No

Include | Exclude

○ Any location
● All trusted locations
○ Selected locations

Select
None

The users and groups settings are configured as shown in the Users and Groups exhibit. (Click **Users and Groups** tab.)



Users and groups

Include | Exclude

○ None
○ All users
● Select users and groups

□ All guest users (preview)

☑ Directory roles (preview)

Security reader

□ Users and groups

Members of the Security reader group report that they cannot sign in to Microsoft Active Directory (Azure AD) on their device while they are in the office.

You need to ensure that the members of the Security reader group can sign in in to Azure AD on their device while they are in the office. The solution must use the principle of least privilege.

What should you do?

A. From the conditional access policy, configure the device state.
B. From the Azure Active Directory admin center, create a custom control.
C. From the Device Management admin center, create a device compliance policy.
D. From the Azure Active Directory admin center, create a named location.

Correct Answer: D

Section: [none]
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition

QUESTION 18 You have computers that run Windows 10 Enterprise and are joined to the domain.

You plan to delay the installation of new Windows builds so that the IT department can test application compatibility.

You need to prevent Windows from being updated for the next 30 days.

Which two Group Policy settings should you configure? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

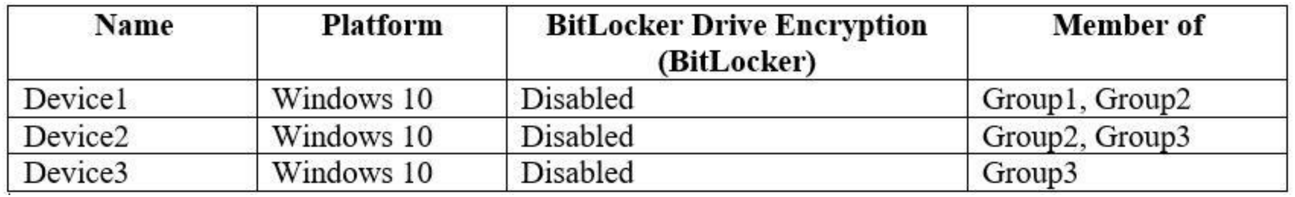
A. Select when Quality Updates are received
B. Select when Preview Builds and Feature Updates are received
C. Turn off auto-restart for updates during active hours
D. Manage preview builds
E. Automatic updates detection frequency

Correct Answer: BD
Section: [none]
Explanation

Explanation/Reference:
References: https://insider.windows.com/en-us/for-business-organization-admin/

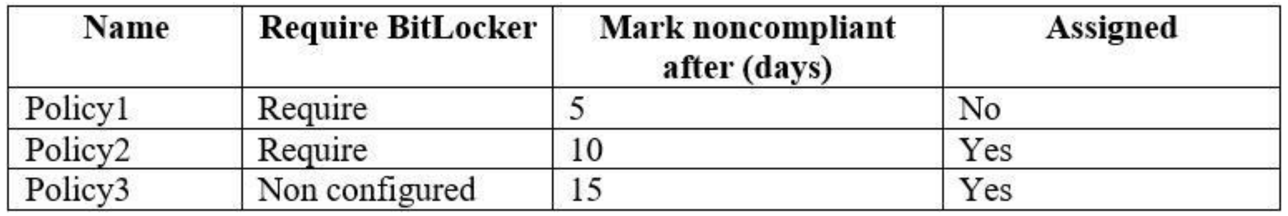
QUESTION 19
HOTSPOT

You have three devices enrolled in Microsoft Endpoint Manager as shown in the following table.



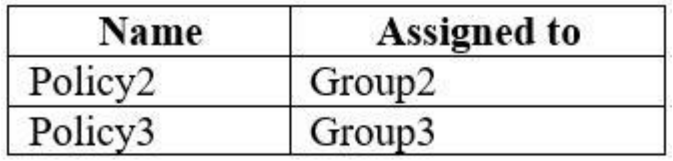
Name	Platform	BitLocker Drive Encryption (BitLocker)	Member of
Device1	Windows 10	Disabled	Group1, Group2
Device2	Windows 10	Disabled	Group2, Group3
Device3	Windows 10	Disabled	Group3

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



Name	Require BitLocker	Mark noncompliant after (days)	Assigned
Policy1	Require	5	No
Policy2	Require	10	Yes
Policy3	Non configured	15	Yes

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



Name	Assigned to
Policy2	Group2
Policy3	Group3

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:

Section: [none]
Explanation

Explanation/Reference:

QUESTION 20 You have a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com.

You need to provide a user with the ability to sign up for Microsoft Store for Business for contoso.com. The solution must use the principle of least privilege.

Which role should you assign to the user?

A. Cloud application administrator
B. Application administrator
C. Global administrator
D. Service administrator

Correct Answer: C
Section: [none]
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/microsoft-store/roles-and-permissions-microsoft-store-for-business

QUESTION 21
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 are deploying Microsoft Intune.

You successfully enroll Windows 10 devices in Intune.

When you try to enroll an iOS device in Intune, you get an error.

You need to ensure that you can enroll the iOS device in Intune.

Solution: You create the Mobility (MDM and MAM) settings.

Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:

QUESTION 22

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 pilot 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 a Configuration Manager device collection.

Does this meet the goal?

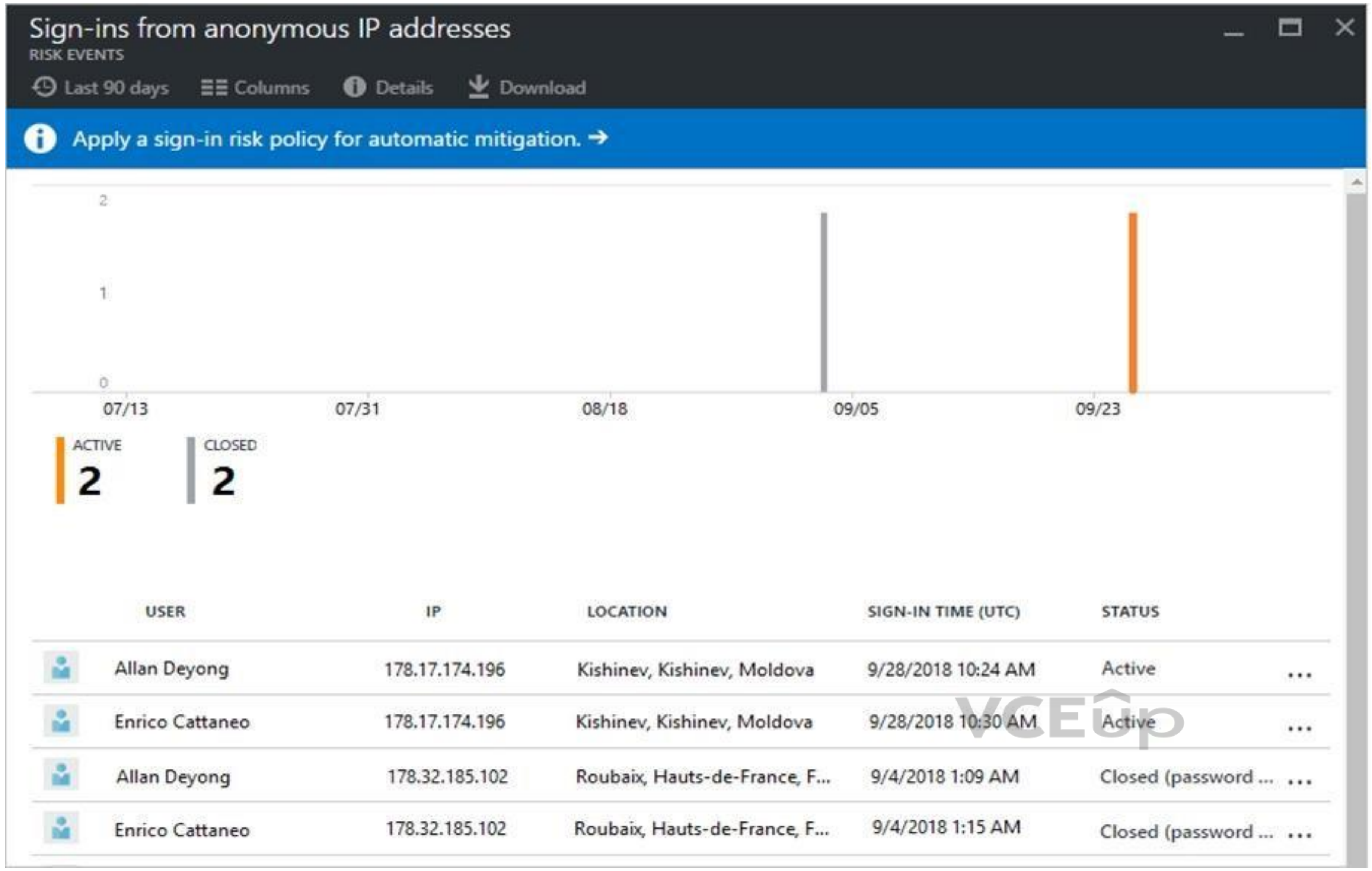
A. Yes
B. No

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:

QUESTION 23

From the Microsoft Azure Active Directory (Azure AD) Identity Protection dashboard, you view the risk events shown in the exhibit. (Click the **Exhibit** tab.)


Sign-ins from anonymous IP addresses
RISK EVENTS
Last 90 days
Columns
Details
Download
Apply a sign-in risk policy for automatic mitigation. →
2
1
0
07/13
07/31
08/18
09/05
09/23
ACTIVE
2
CLOSED
2

	USER	IP	LOCATION	SIGN-IN TIME (UTC)	STATUS	
	Allan Deyong	178.17.174.196	Kishinev, Kishinev, Moldova	9/28/2018 10:24 AM	Active	...
	Enrico Cattaneo	178.17.174.196	Kishinev, Kishinev, Moldova	9/28/2018 10:30 AM	Active	...
	Allan Deyong	178.32.185.102	Roubaix, Hauts-de-France, F...	9/4/2018 1:09 AM	Closed (password ...	...
	Enrico Cattaneo	178.32.185.102	Roubaix, Hauts-de-France, F...	9/4/2018 1:15 AM	Closed (password ...	...

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

Correct Answer: D
Section: [none]
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition

QUESTION 24 Your company has a Microsoft 365 E5 subscription.

Users in the research department work with sensitive data.

You need to prevent the research department users from accessing potentially unsafe websites by using hyperlinks embedded in email messages and documents. Users in other departments must not be restricted.

What should you do from the Security & Compliance admin center?

A. Create a data loss prevention (DLP) policy that has a Content is shared condition.
B. Modify the default safe links policy.
C. Create a data loss prevention (DLP) policy that has a Content contains condition.
D. Create a new safe links policy.

Correct Answer: D
Section: [none]
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/office365/securitycompliance/set-up-atp-safe-links-policies#policies-that-apply-to-specific-email-recipients

QUESTION 25 You have a Microsoft 365 tenant.

You have a line-of-business application named App1 that users access by using the My Apps portal.

After some recent security breaches, you implement a conditional access policy for App1 that uses Conditional Access App Control.

You need to be alerted by email if impossible travel is detected for a user of App1. The solution must ensure that alerts are generated for App1 only.

What should you do?

A. From Microsoft Cloud App Security, create a Cloud Discovery anomaly detection policy.
B. From Microsoft Cloud App Security, modify the impossible travel alert policy.
C. From Microsoft Cloud App Security, create an app discovery policy.
D. From the Azure Active Directory admin center, modify the conditional access policy.

Correct Answer: A
Section: [none]
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/cloud-app-security/cloud-discovery-anomaly-detection-policy

QUESTION 26 A user receives the following message when attempting to sign in to https://myapps.microsoft.com:

“Your sign-in was blocked. We’ve detected something unusual about this sign-in. For example, you might be signing in from a new location, device, or app. Before you can continue, we need to verify your identity. Please contact your admin.”

Which configuration prevents the users from signing in?

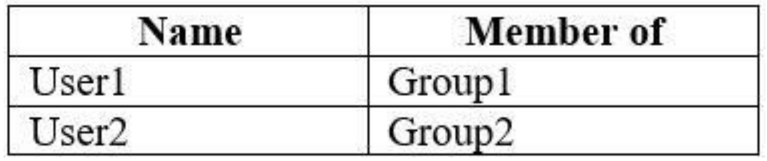
A. Microsoft Azure Active Directory (Azure AD) Identity Protection policies
B. Microsoft Azure Active Directory (Azure AD) conditional access policies
C. Security & Compliance supervision policies
D. Security & Compliance data loss prevention (DLP) policies

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview

QUESTION 27
HOTSPOT

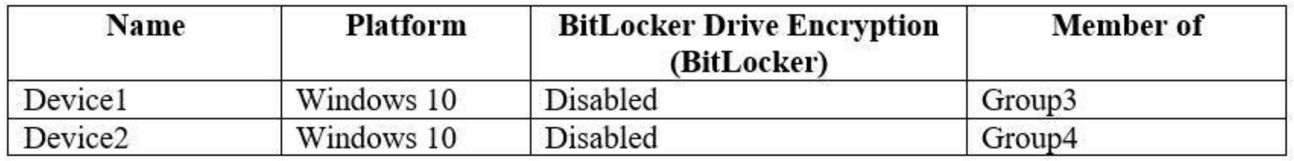
You have the Microsoft Azure Active Directory (Azure AD) users shown in the following table.



Name	Member of
User1	Group1
User2	Group2

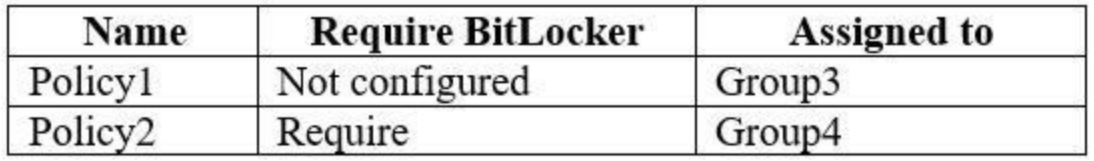
Your company uses Microsoft Intune.

Several devices are enrolled in Intune as shown in the following table.



Name	Platform	BitLocker Drive Encryption (BitLocker)	Member of
Device1	Windows 10	Disabled	Group3
Device2	Windows 10	Disabled	Group4

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



Name	Require BitLocker	Assigned to
Policy1	Not configured	Group3
Policy2	Require	Group4

You create a conditional access policy that has the following settings:

▪ The Assignments settings are configured as follows:
1. Users and groups: Group1
2. Cloud apps: Microsoft Office 365 Exchange Online
3. Conditions: Include All device state, exclude Device marked as compliant ▪ Access controls is set to Block 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:

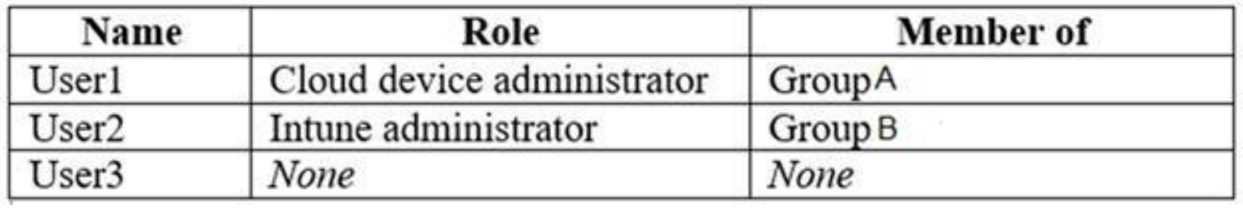
Section: [none]
Explanation

Explanation/Reference:

QUESTION 28
HOTSPOT

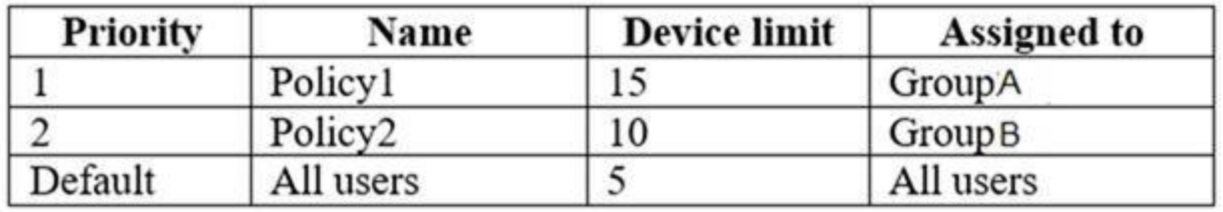
You have several devices enrolled in Microsoft Intune.

You have a Microsoft Azure Active Directory (Azure AD) tenant that includes the users shown in the following table.



Name	Role	Member of
User1	Cloud device administrator	GroupA
User2	Intune administrator	GroupB
User3	*None*	*None*

The device limit restrictions in Intune are configured as shown in the following table.



Priority	Name	Device limit	Assigned to
1	Policy1	15	GroupA
2	Policy2	10	GroupB
Default	All users	5	All users

You add User3 as a device enrollment manager in Intune.

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:

Section: [none]
Explanation

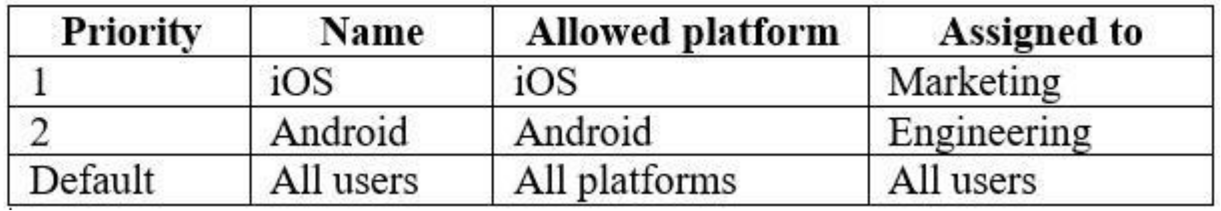
Explanation/Reference:
Reference: https://docs.microsoft.com/en-us/intune/device-enrollment-manager-enroll

QUESTION 29
HOTSPOT

Your company has a Microsoft 365 tenant.

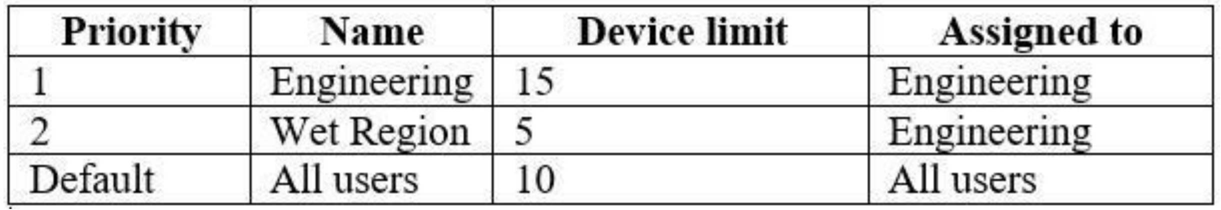
You plan to allow users from the engineering department to enroll their mobile device in mobile device management (MDM).

The device type restrictions are configured as shown in the following table.



Priority	Name	Allowed platform	Assigned to
1	iOS	iOS	Marketing
2	Android	Android	Engineering
Default	All users	All platforms	All users

The device limit restrictions are configured as shown in the following table.

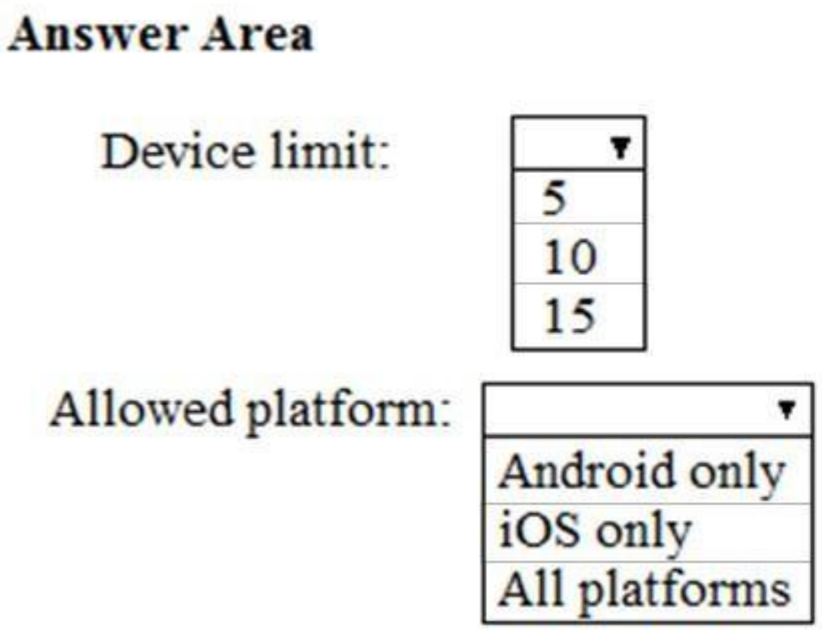


Priority	Name	Device limit	Assigned to
1	Engineering	15	Engineering
2	Wet Region	5	Engineering
Default	All users	10	All users

What is the effective configuration for the members of the Engineering group? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

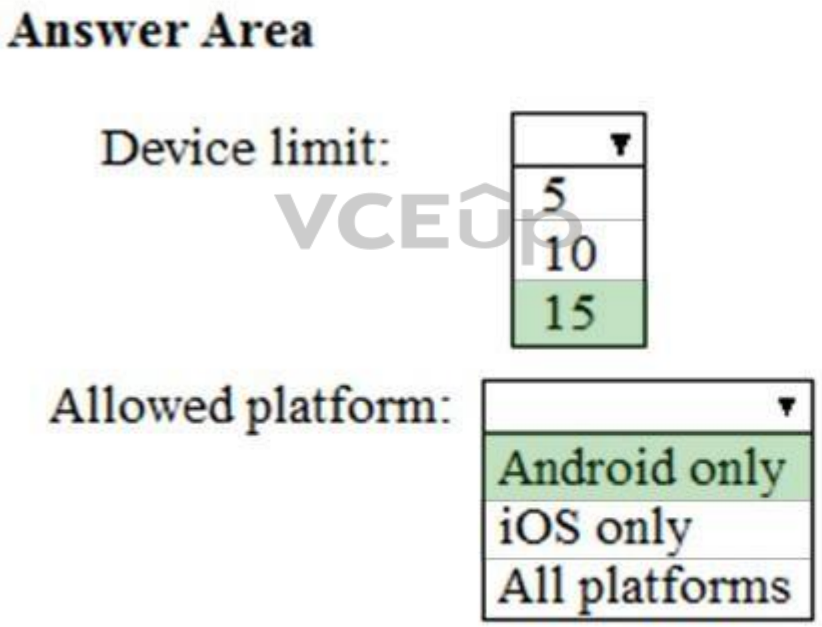


Answer Area

Device limit: ▾
- 5
- 10
- 15

Allowed platform: ▾
- Android only
- iOS only
- All platforms

Correct Answer:



Answer Area

Device limit: ▾
- 5
- 10
- [✓ 15]

Allowed platform: ▾
- [✓ Android only]
- iOS only
- All platforms

Section: [none]
Explanation

Explanation/Reference:

QUESTION 30 Your network contains an Active Directory domain named contoso.com. The domain contains 100 Windows 8.1 devices.

You plan to deploy a custom Windows 10 Enterprise image to the Windows 8.1 devices.

You need to recommend a Windows 10 deployment method.

What should you recommend?

A. a provisioning package

B. an in-place upgrade
C. wipe and load refresh
D. Windows Autopilot

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/microsoft-365/enterprise/windows10-infrastructure

QUESTION 31 You use Microsoft System Center Configuration Manager (Current Branch) to manage devices.

Your company uses the following types of devices:
▪ Windows 10
▪ Windows 8.1
▪ Android ▪
iOS

Which devices can be managed by using co-management?

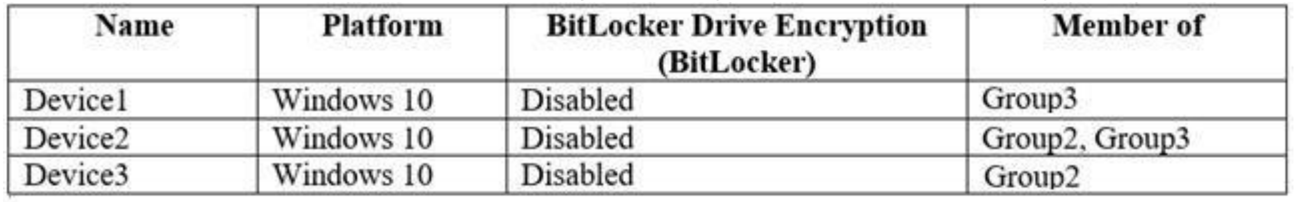
A. Windows 10 and Windows 8.1 only
B. Windows 10, Android, and iOS only
C. Windows 10 only
D. Windows 10, Windows 8.1, Android, and iOS

Correct Answer: D
Section: [none]
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/sccm/core/plan-design/choose-a-device-management-solution#bkmk_intune

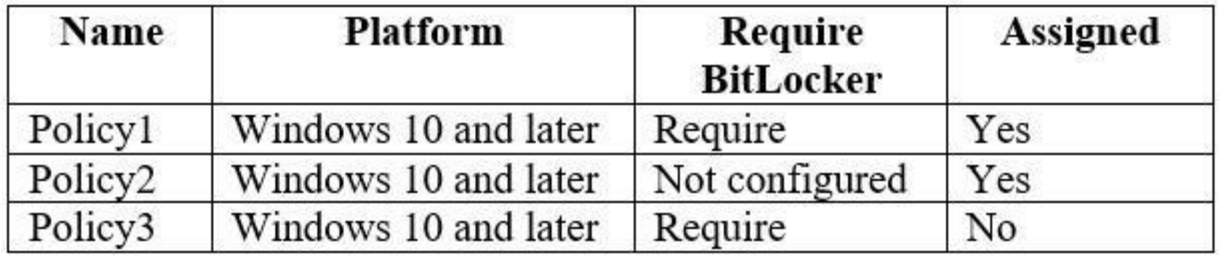
QUESTION 32
HOTSPOT

You have three devices enrolled in Microsoft Endpoint Manager as shown in the following table.



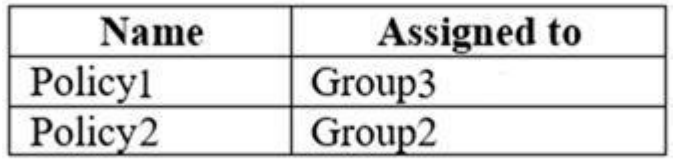
Name	Platform	BitLocker Drive Encryption (BitLocker)	Member of
Device1	Windows 10	Disabled	Group3
Device2	Windows 10	Disabled	Group2, Group3
Device3	Windows 10	Disabled	Group2

The device compliance policies in Endpoint Manager 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 assignments 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.

Hot Area:

Correct Answer:

Section: [none]
Explanation

Explanation/Reference:

QUESTION 33 Your company has a Microsoft 365
E3 subscription.

All devices run Windows 10 Pro and are joined to Microsoft Azure Active Directory (Azure AD).

You need to change the edition of Windows 10 to Enterprise the next time users sign in to their computer. The solution must minimize downtime for the users.

What should you use?

A. Windows Autopilot
B. Windows Update
C. Subscription Activation
D. an in-place upgrade

Correct Answer: A
Section: [none]
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/windows/deployment/windows-autopilot/windows-autopilot

QUESTION 34
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 pilot 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: Define a Configuration Manager device collection as the pilot collection. Add Device1 to the collection.

Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:

QUESTION 35
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 are deploying Microsoft Intune.

You successfully enroll Windows 10 devices in Intune.

When you try to enroll an iOS device in Intune, you get an error. You

need to ensure that you can enroll the iOS device in Intune.

Solution: You configure the Mobility (MDM and MAM) settings.

Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:

QUESTION 36 Your company
has 10 offices.

The network contains an Active Directory domain named contoso.com. The domain contains 500 client computers. Each office is configured as a separate subnet.

You discover that one of the offices has the following:

- Computers that have several preinstalled applications
- Computers that use nonstandard computer names
- Computers that have Windows 10 preinstalled
- Computers that are in a workgroup

You must configure the computers to meet the following corporate requirements:

- All the computers in the office must be joined to the domain.
- All the computers in the office must have computer names that use a prefix of CONTOSO. ▪ All
the computers in the office must only have approved corporate applications installed.

You need to recommend a solution to redeploy the computers. The solution must minimize the deployment time.

Which deployment method should you recommend?

A. a provisioning package

B. wipe and load refresh
C. Windows Autopilot
D. an in-place upgrade

Correct Answer: A
Section: [none]
Explanation

Explanation/Reference:
Explanation:
By using a Provisioning, IT administrators can create a self-contained package that contains all of the configuration, settings, and apps that need to be applied to a device.

Incorrect Answers:
C: With Windows Autopilot the user can set up pre-configure devices without the need consult their IT administrator. D:
Use the In-Place Upgrade option when you want to keep all (or at least most) existing applications.

References: https://docs.microsoft.com/en-us/windows/deployment/windows-10-deployment-scenarios https://docs.microsoft.com/en-us/windows/deployment/windows-autopilot/windows-autopilot

QUESTION 37
Your company has a Microsoft 365 subscription. The subscription contains 500 devices that run Windows 10 and 100 devices that run iOS.

You need to create Microsoft Intune device configuration profiles to meet the following requirements:

▪ Configure Wi-Fi connectivity to a secured network named ContosoNet. ▪ Require passwords of at least six characters to lock the devices.

What is the minimum number of device configuration profiles that you should create?

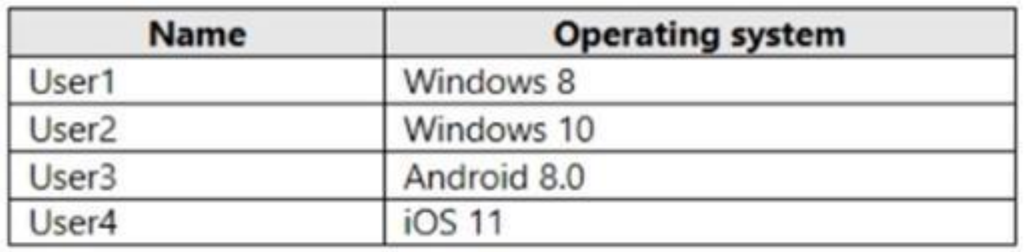
A. 4 B.
2
C. 1

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:

QUESTION 38 Your company has a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com and a Microsoft 365 subscription.

The company recently hired four new users who have the devices shown in the following table.



Name	Operating system
User1	Windows 8
User2	Windows 10
User3	Android 8.0
User4	iOS 11

You configure the Microsoft 365 subscription to ensure that the new devices enroll in Microsoft Intune automatically.

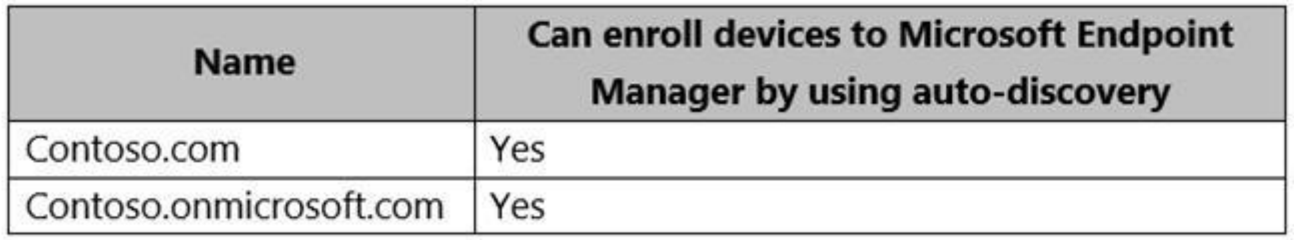
Which users have a device that can enroll in Microsoft Intune automatically?

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

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:

QUESTION 39
Your company has a Microsoft 365 subscription that contains the domains shown in the following table.



Name	Can enroll devices to Microsoft Endpoint Manager by using auto-discovery
Contoso.com	Yes
Contoso.onmicrosoft.com	Yes

The company plans to add a custom domain named fabrikam.com to the subscription, and then to enable enrollment of devices to Endpoint Manager by using auto-discovery for fabrikam.com.

You need to add a DNS record to the fabrikam.com domain to enable device enrollment by using auto-discovery.

Which record type should you use for the new record?

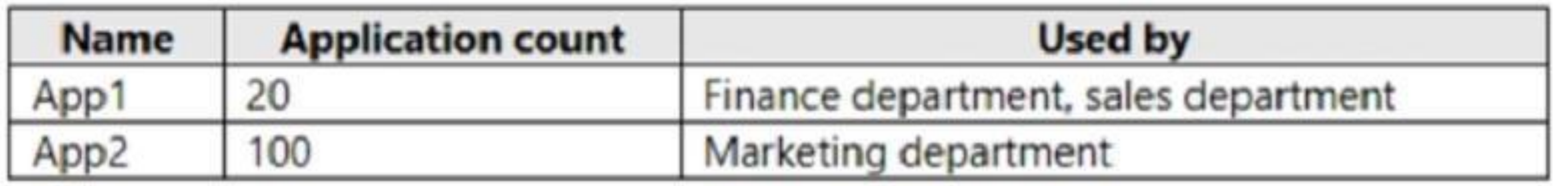
A. PTR
B. SRV
C. CNAME
D. TXT

Correct Answer: C
Section: [none]
Explanation

Explanation/Reference:
Reference:
https://docs.microsoft.com/en-us/mem/intune/enrollment/windows-enroll#simplify-windows-enrollment-without-azure-ad-premium

QUESTION 40
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 domain. The domain contains 2,000 computers that run Windows 8.1 and have applications installed as shown in the following table.



Name	Application count	Used by
App1	20	Finance department, sales department
App2	100	Marketing department

You enroll all the computers in Upgrade Readiness.

You need to ensure that App1 and App2 have an UpgradeDecision status of Ready to upgrade.

Solution: You set the ReadyForWindows status of App2 to Highly adopted.

Does this meet the goal?

A. Yes
B. No

Correct Answer: A
Section: [none]
Explanation

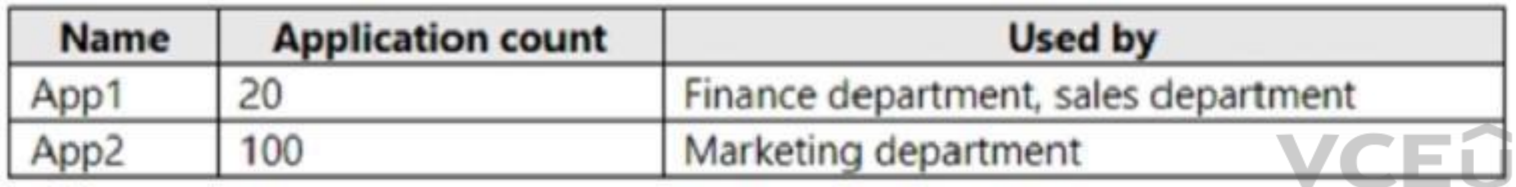
Explanation/Reference:
Explanation:
App1 has a “low install count” (2% or less) so will be Ready to upgrade. We just need to change the setting for App2.

References: https://docs.microsoft.com/en-us/windows/deployment/upgrade/upgrade-readiness-identify-apps

QUESTION 41
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 domain. The domain contains 2,000 computers that run Windows 8.1 and have applications installed as shown in the following table.



Name	Application count	Used by
App1	20	Finance department, sales department
App2	100	Marketing department

You enroll all the computers in Upgrade Readiness.

You need to ensure that App1 and App2 have an UpgradeDecision status of Ready to upgrade.

Solution: You set the Importance status of App1 to Business critical.

Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section: [none]
Explanation

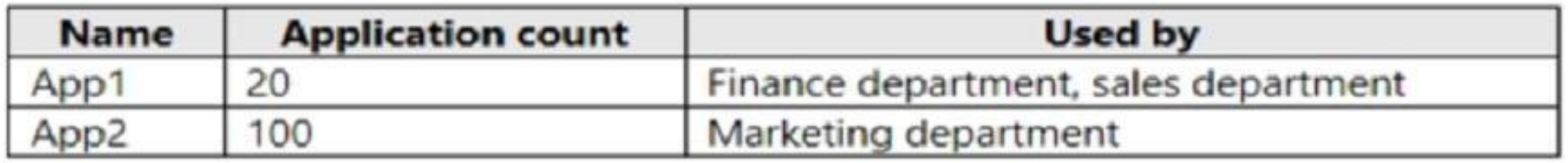
Explanation/Reference:
Explanation:
Business Critical will prevent the app having a status of Ready to upgrade.

References: https://docs.microsoft.com/en-us/windows/deployment/upgrade/upgrade-readiness-identify-apps

QUESTION 42
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 domain. The domain contains 2,000 computers that run Windows 8.1 and have applications installed as shown in the following table.



Name	Application count	Used by
App1	20	Finance department, sales department
App2	100	Marketing department

You enroll all the computers in Upgrade Readiness.

You need to ensure that App1 and App2 have an UpgradeDecision status of Ready to upgrade.

Solution: You set the ReadyForWindows status of App1 to Highly adopted.

Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section: [none]
Explanation

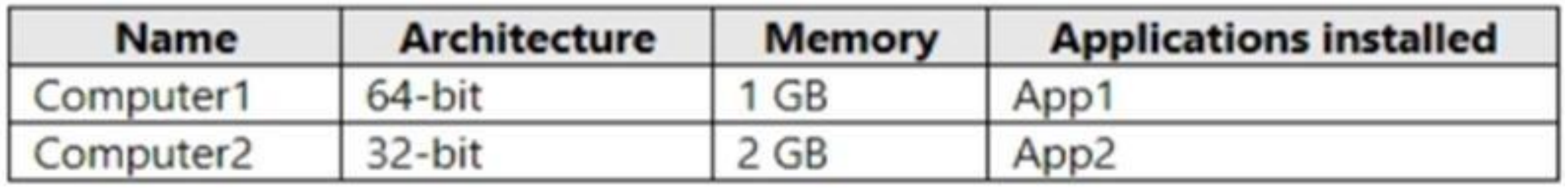
Explanation/Reference:
Explanation:
App1 has a “low install count” (2% or less) so will be Ready to upgrade. We need to change the setting for App2.

References: https://docs.microsoft.com/en-us/windows/deployment/upgrade/upgrade-readiness-identify-apps

QUESTION 43
HOTSPOT

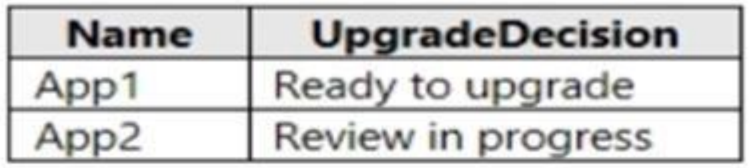
You have 100 computers that run Windows 8.1 and are enrolled in Upgrade Readiness.

Two of the computers are configured as shown in the following table.



Name	Architecture	Memory	Applications installed
Computer1	64-bit	1 GB	App1
Computer2	32-bit	2 GB	App2

From Upgrade Readiness, you view the applications shown in the following table.



Name	UpgradeDecision
App1	Ready to upgrade
App2	Review in progress

You enroll a computer named Computer3 in Upgrade Readiness. Computer3 has the following configurations:

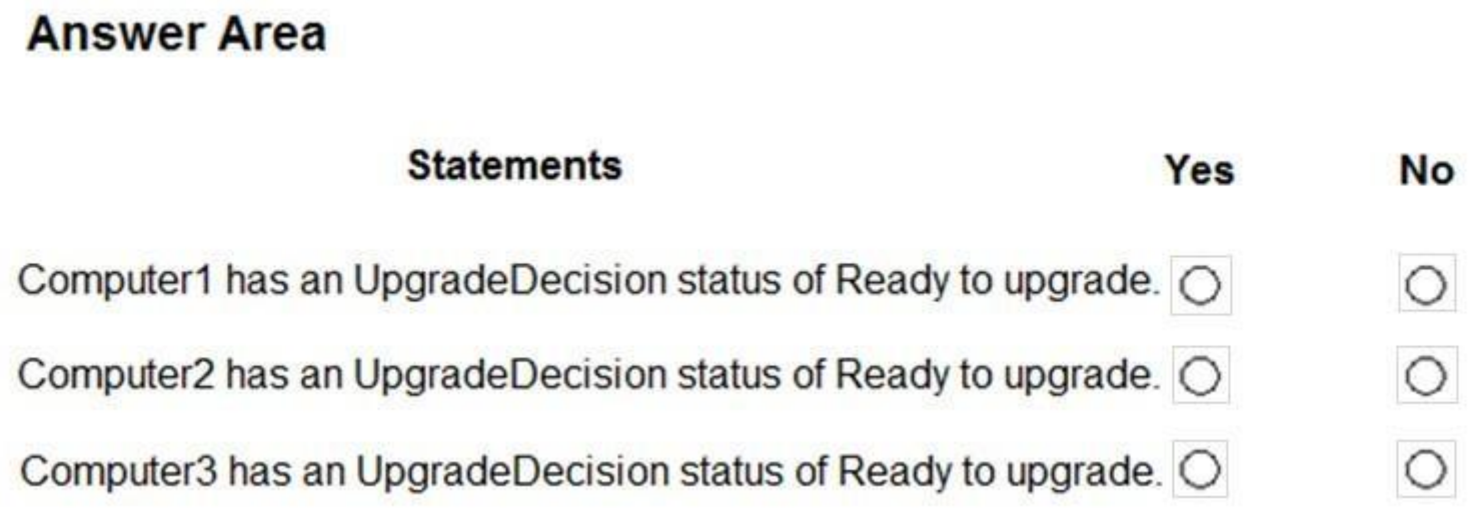
- 8 GB of memory
- 64-bit architecture
- An application named App3 installed

App3 is installed on Computer3 only.

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

NOTE: Each correct selection is worth one point.

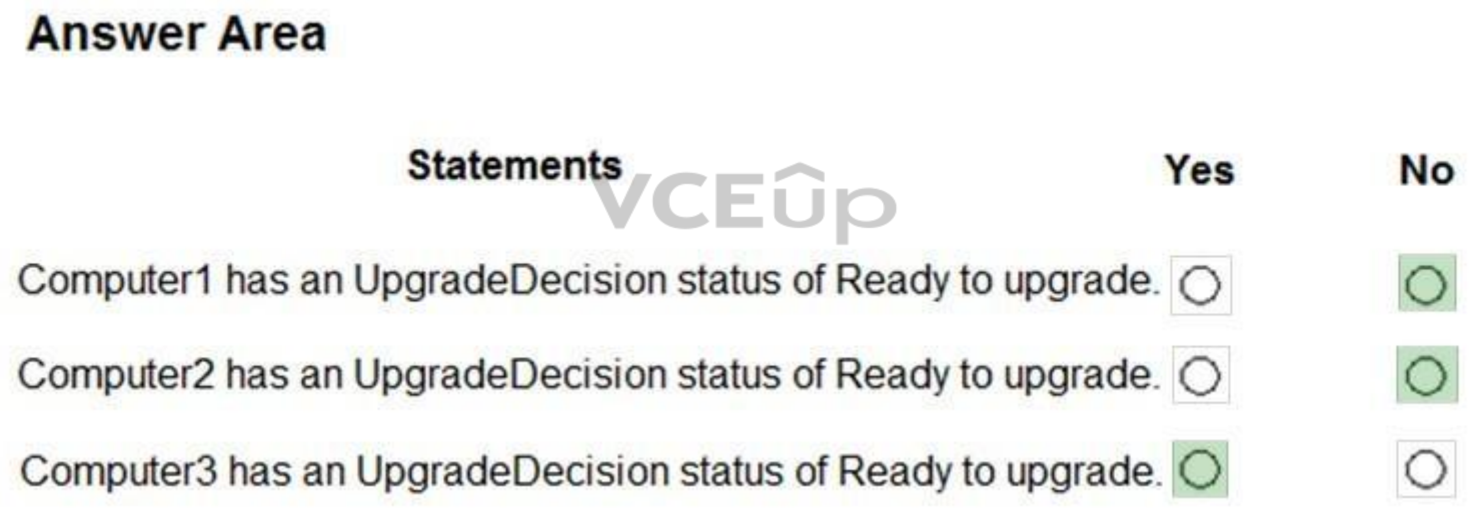
Hot Area:



Answer Area

Statements	Yes	No
Computer1 has an UpgradeDecision status of Ready to upgrade.	○	○
Computer2 has an UpgradeDecision status of Ready to upgrade.	○	○
Computer3 has an UpgradeDecision status of Ready to upgrade.	○	○

Correct Answer:



Answer Area

Statements	Yes	No
Computer1 has an UpgradeDecision status of Ready to upgrade.	○	[✓ ○]
Computer2 has an UpgradeDecision status of Ready to upgrade.	○	[✓ ○]
Computer3 has an UpgradeDecision status of Ready to upgrade.	[✓ ○]	○

Section: [none]
Explanation

Explanation/Reference:
QUESTION 44 Your network contains an on-premises Active Directory domain that syncs to Azure Active Directory (Azure AD).

The domain contains two servers named Server1 and Server2 that run Windows Server 2016. Server1 has the File Server Resource Manager role service installed.

You need to configure Server1 to use the Azure Rights Management (Azure RMS) connector.

You install the Microsoft Management connector on Server1.

What should you do next on Server1?

A. Run the `GenConnectorConfig.ps1` script.
B. Configure the URL of the AIPMigrated group.
C. Enable BitLocker Drive Encryption (BitLocker).

D. Install a certification authority (CA).

Correct Answer: A
Section: [none]
Explanation

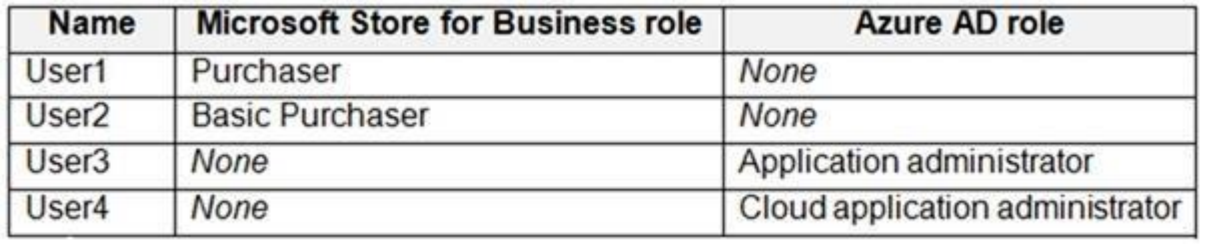
Explanation/Reference:
Explanation:
If you want to use the server configuration tool for the RMS connector, to automate the configuration of registry settings on your on-premises servers, download and run the GenConnectorConfig.ps1 script.

References: https://docs.microsoft.com/en-us/azure/information-protection/install-configure-rms-connector#installing-the-rms-connector

QUESTION 45 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

Microsoft Store for Business has the following Shopping behavior settings:

▪ Make everyone a Basic Purchaser is set to **Off**. ▪ Allow
app requests is set to **On**.

You need to identify which users can add apps to the Microsoft Store for Business private store.

Which users should you identify?

A. User1 and User2 only
B. User3 onlyC. User1 only
D. User3 and User4 only

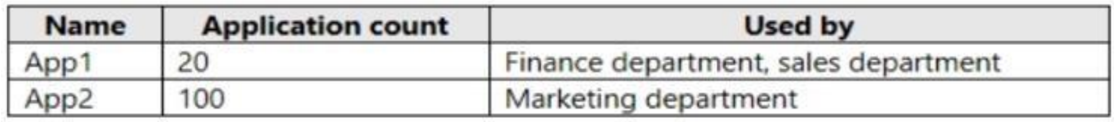
Correct Answer: A
Section: [none]
Explanation

Explanation/Reference:

QUESTION 46
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 domain. The domain contains 2,000 computers that run Windows 8.1 and have applications installed as shown in the following table.



Name	Application count	Used by
App1	20	Finance department, sales department
App2	100	Marketing department

You enroll all the computers in Upgrade Readiness.

You need to ensure that App1 and App2 have an UpgradeDecision status of Ready to upgrade.

Solution: You set the importance status of App2 to Low install count.

Does this meet the goal?

A. Yes
B. No

Correct Answer: A
Section: [none]
Explanation

Explanation/Reference:
Explanation:
If an app is installed on less than 2% of the targeted devices, it's marked Low install count. Two percent is the default value. You can adjust the threshold in the readiness settings from 0% to 10%. Desktop Analytics automatically marks these apps as Ready to upgrade.

Reference:
https://docs.microsoft.com/en-us/configmgr/desktop-analytics/about-deployment-plans

QUESTION 47 You have two conditional access policies named Policy1 and Policy2.

Policy1 has the following settings:

▪ Assignments:
- Users and groups: User1
- Cloud apps or actions: Office 365 Exchange Online
- Conditions: 0 conditions selected ▪ Access controls:
- Grant: Grant access
- Session: 0 controls selected ▪ Enable policy: On

Policy2 has the following settings:

▪ Assignments:
- Users and groups: User1
- Cloud apps or actions: Office 365 Exchange Online
- Conditions: 0 conditions selected ▪ Access controls:
- Grant: Block access
- Session: 0 controls selected ▪ Enable policy: On

You need to ensure that User1 can access Microsoft Exchange Online only from devices that are marked as compliant.

What should you do?

A. Modify the Grant settings of Policy2.
B. Disable Policy2.
C. Modify the Conditions settings of Policy2.
D. Modify the Grant settings of Policy1.

Correct Answer: C
Section: [none]
Explanation

Explanation/Reference:

QUESTION 48

You have a Microsoft 365 E5 subscription that uses an Azure Active Directory (Azure AD) tenant named contoso.com.

You need to ensure that users can enroll devices in Microsoft Endpoint Manager without manually entering the address of Microsoft Endpoint Manager.

Which two DNS records should you create? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. a CNAME record for AutoDiscover.contoso.com
B. a CNAME record for EnterpriseEnrollment.contoso.com
C. a TXT record for EnterpriseRegistration.contoso.com
D. an SRV record for _SIP._TLS.contoso.com
E. an SRV record for _SIPfederationTLS.contoso.com
F. a CNAME record for EnterpriseRegistration.contoso.com
G. a TXT record for EnterpriseEnrollment.contoso.com

Correct Answer: BF
Section: [none]
Explanation

Explanation/Reference:
Reference:
https://docs.microsoft.com/en-us/mem/intune/enrollment/windows-enroll#simplify-windows-enrollment-without-azure-ad-premium

QUESTION 49
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 domain. The domain contains domain controllers that run Windows Server 2019. The functional level of the forest and the domain is Windows Server 2012 R2.

The domain contains 100 computers that run Windows 10 and a member server named Server1 that runs Windows Server 2012 R2.

You plan to use Server1 to manage the domain and to configure Windows 10 Group Policy settings.

You install the Group Policy Management Console (GPMC) on Server1.

You need to configure the Windows Update for Business Group Policy settings on Server1.

Solution: You raise the forest functional level to Windows Server 2016. You copy the Group Policy Administrative Templates from a Windows 10 computer to the Netlogon share on all the domain controllers.

Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:

QUESTION 50
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 domain. The domain contains domain controllers that run Windows Server 2019. The functional level of the forest and the domain is Windows Server 2012 R2.

The domain contains 100 computers that run Windows 10 and a member server named Server1 that runs Windows Server 2012 R2.

You plan to use Server1 to manage the domain and to configure Windows 10 Group Policy settings.

You install the Group Policy Management Console (GPMC) on Server1.

You need to configure the Windows Update for Business Group Policy settings on Server1.

Solution: You copy the Group Policy Administrative Templates from a Windows 10 computer to Server1.

Does this meet the goal?

A. Yes
B. No

Correct Answer: A
Section: [none]
Explanation

Explanation/Reference:

QUESTION 51
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 domain. The domain contains domain controllers that run Windows Server 2019. The functional level of the forest and the domain is Windows Server 2012 R2.

The domain contains 100 computers that run Windows 10 and a member server named Server1 that runs Windows Server 2012 R2.

You plan to use Server1 to manage the domain and to configure Windows 10 Group Policy settings.

You install the Group Policy Management Console (GPMC) on Server1.

You need to configure the Windows Update for Business Group Policy settings on Server1.

Solution: You upgrade Server1 to Windows Server 2019.

Does this meet the goal?

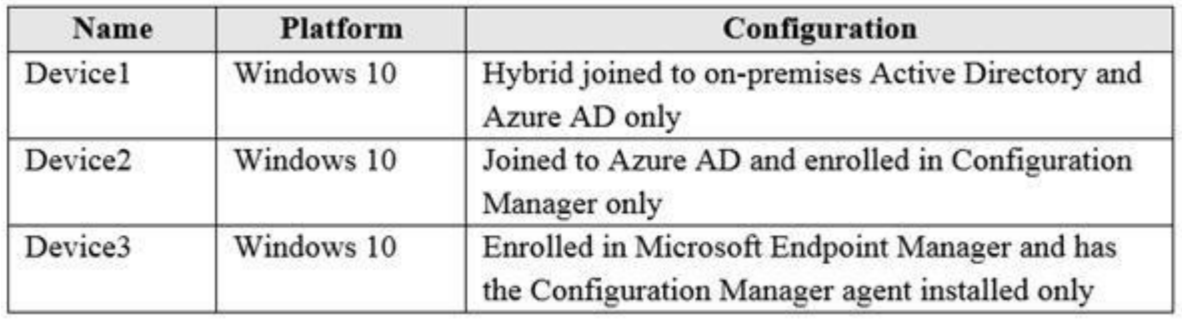
A. Yes
B. No

Correct Answer: A
Section: [none]
Explanation

Explanation/Reference:

QUESTION 52 You have a hybrid Azure Active Directory (Azure AD) tenant and a Microsoft Endpoint Configuration Manager deployment.

You have the devices shown in the following table.



Name	Platform	Configuration
Device1	Windows 10	Hybrid joined to on-premises Active Directory and Azure AD only
Device2	Windows 10	Joined to Azure AD and enrolled in Configuration Manager only
Device3	Windows 10	Enrolled in Microsoft Endpoint Manager and has the Configuration Manager agent installed only

You plan to enable co-management.

You need to identify which devices support co-management without requiring the installation of additional software.

Which devices should you identify?

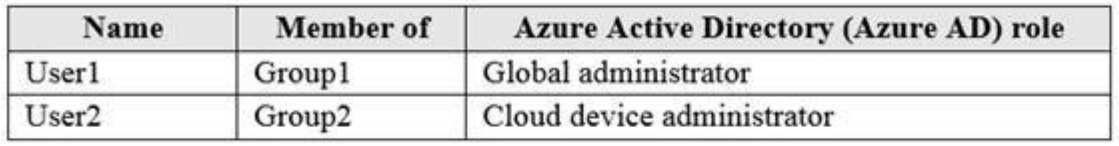
A. Device1 only B.
Device2 only
C. Device3 only
D. Device2 and Device3 only
E. Device1, Device2, and Device3

Correct Answer: D
Section: [none]
Explanation

Explanation/Reference:

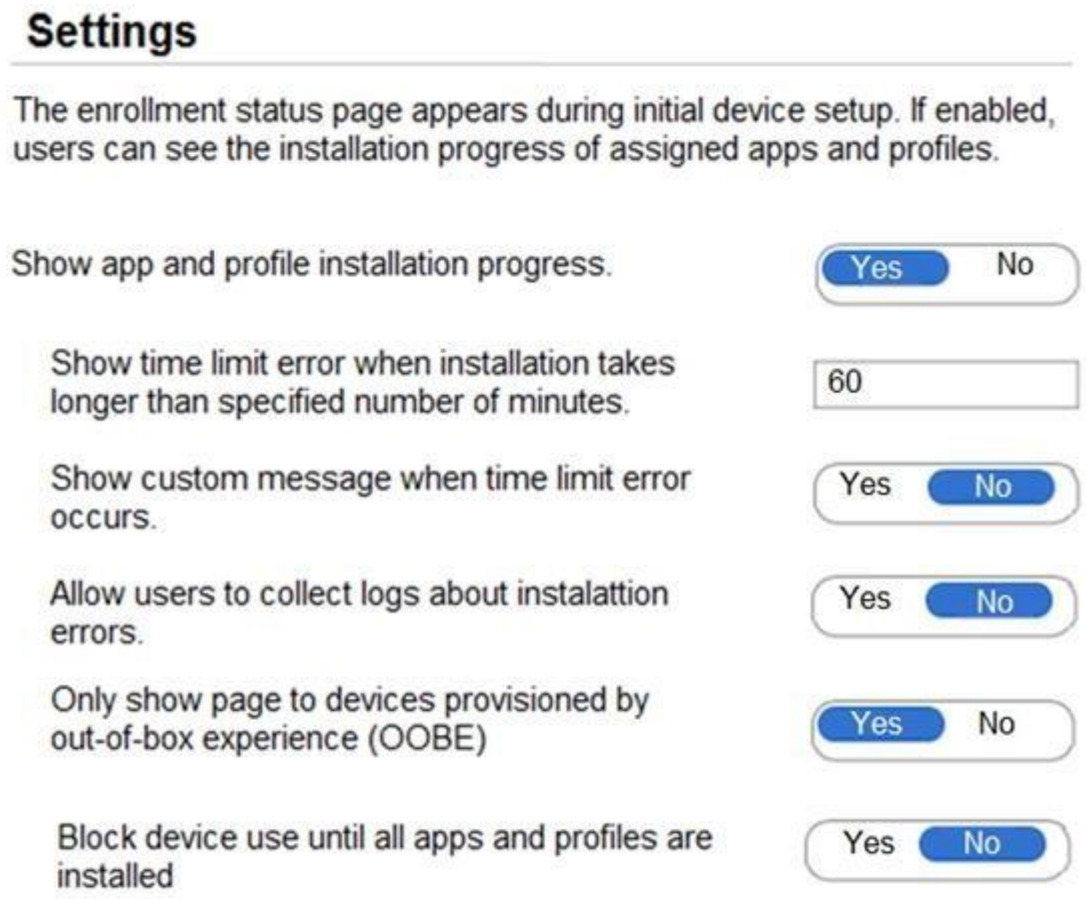
QUESTION 53
HOTSPOT

You have a Microsoft 365 subscription that contains the users shown in the following table.



Name	Member of	Azure Active Directory (Azure AD) role
User1	Group1	Global administrator
User2	Group2	Cloud device administrator

You configure an Enrollment Status Page profile as shown in the following exhibit.



Settings

The enrollment status page appears during initial device setup. If enabled, users can see the installation progress of assigned apps and profiles.

Show app and profile installation progress. [✓ Yes] No

Show time limit error when installation takes longer than specified number of minutes. 60

Show custom message when time limit error occurs. Yes [✓ No]

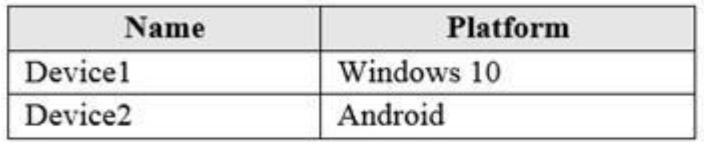
Allow users to collect logs about instalattion errors. Yes [✓ No]

Only show page to devices provisioned by out-of-box experience (OOBE) [✓ Yes] No

Block device use until all apps and profiles are installed Yes [✓ No]

You assign the policy to Group1.

You purchase the devices shown in the following table.



Name	Platform
Device1	Windows 10
Device2	Android

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:

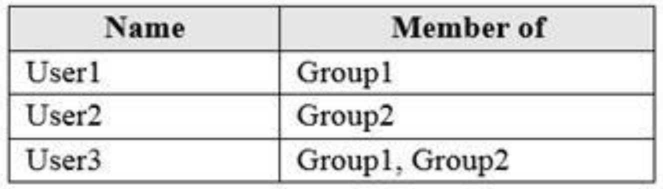
Correct Answer:

Section: [none]
Explanation

Explanation/Reference:
Reference: https://docs.microsoft.com/en-us/mem/intune/enrollment/windows-enrollment-status

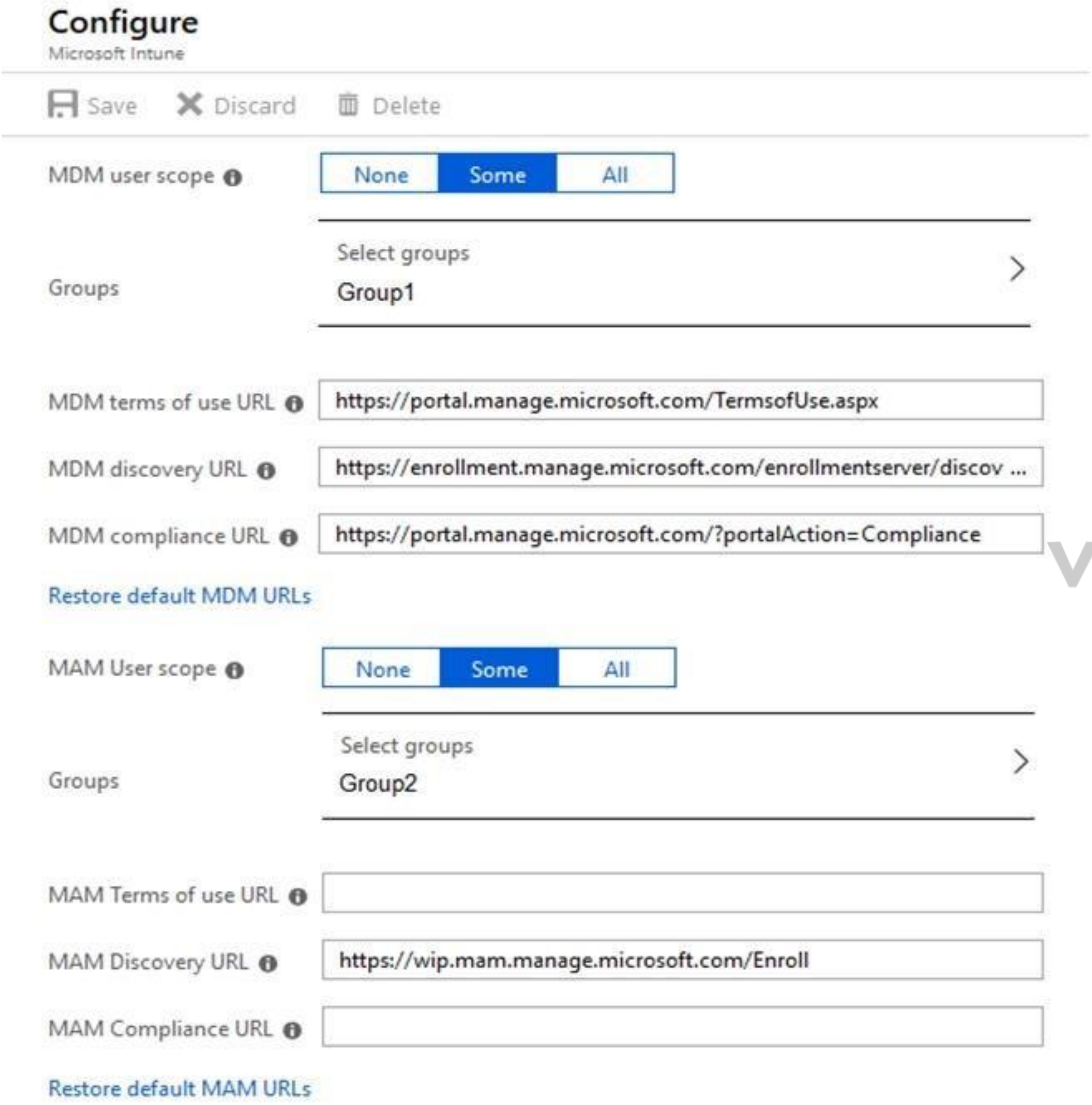
QUESTION 54
HOTSPOT

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



Name	Member of
User1	Group1
User2	Group2
User3	Group1, Group2

You integrate Microsoft Intune and contoso.com as shown in the following exhibit.



Configure

Microsoft Intune

MDM user scope: None [✓ Some] All

Groups: Select groups Group1

MDM terms of use URL: https://portal.manage.microsoft.com/TermsofUse.aspx

MDM discovery URL: https://enrollment.manage.microsoft.com/enrollmentserver/discov ...

MDM compliance URL: https://portal.manage.microsoft.com/?portalAction=Compliance

MAM User scope: None [✓ Some] All

Groups: Select groups Group2

MAM Terms of use URL:

MAM Discovery URL: https://wip.mam.manage.microsoft.com/Enroll

MAM Compliance URL:

You purchase a Windows 10 device named Device1.

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:

Section: [none]
Explanation

Explanation/Reference:
Reference: https://docs.microsoft.com/en-us/mem/intune/enrollment/windows-enroll

QUESTION 55
HOTSPOT

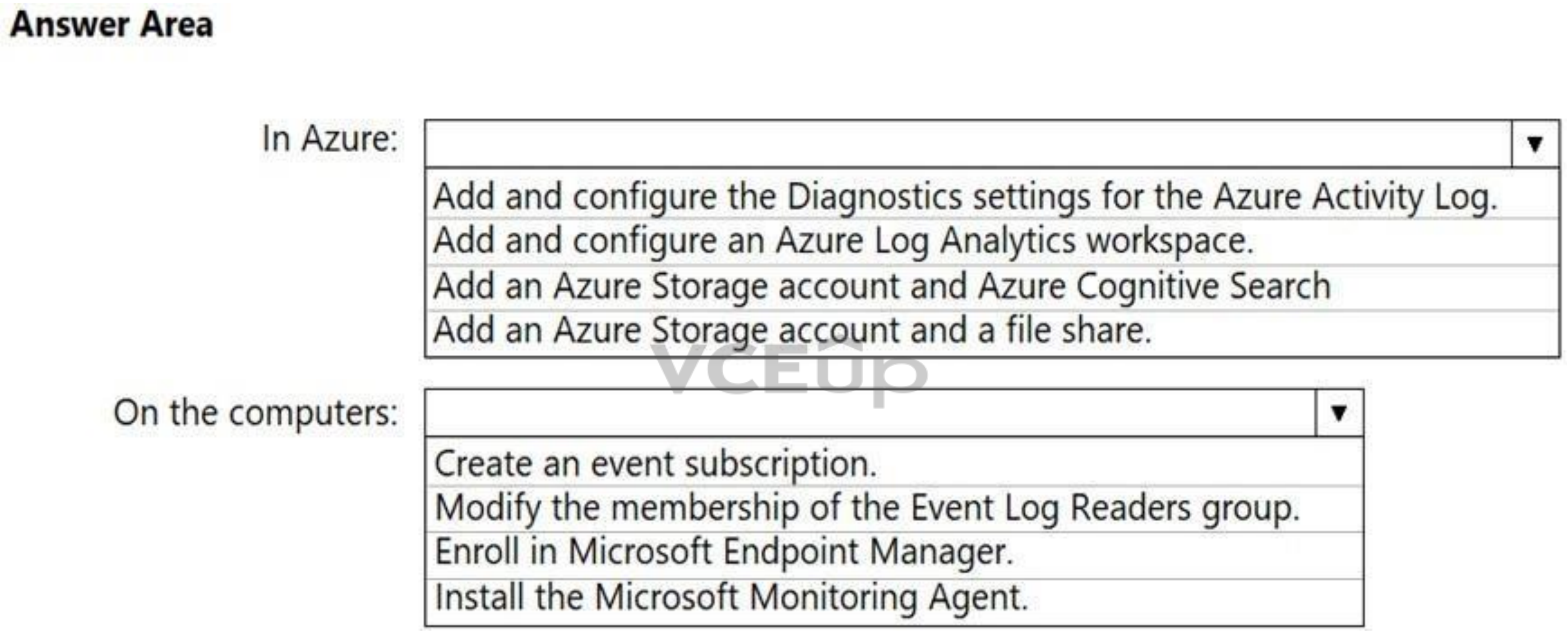
You have an Azure subscription and an on-premises Active Directory domain. The domain contains 50 computers that run Windows 10.

You need to centrally monitor System log events from the computers.

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

NOTE: Each correct selection is worth one point.

Hot Area:

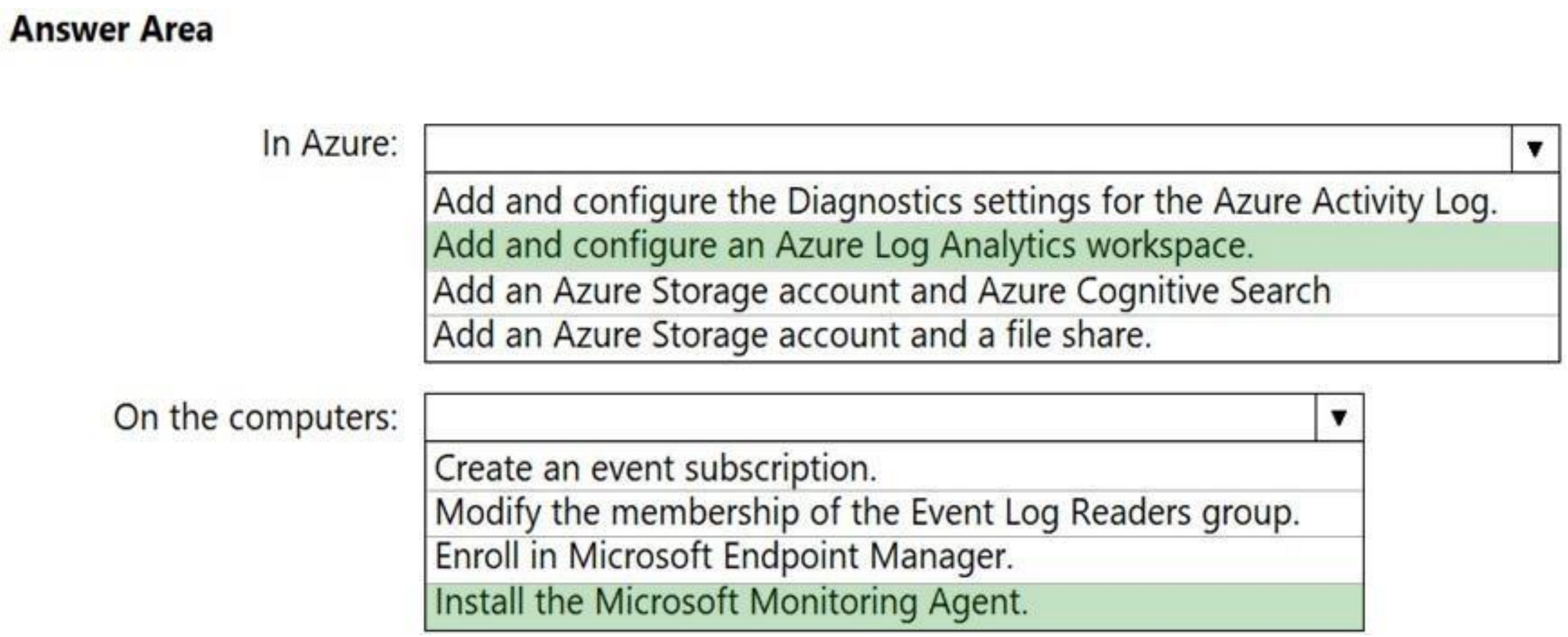


Answer Area

In Azure: ▼
- Add and configure the Diagnostics settings for the Azure Activity Log.
- Add and configure an Azure Log Analytics workspace.
- Add an Azure Storage account and Azure Cognitive Search
- Add an Azure Storage account and a file share.

On the computers: ▼
- Create an event subscription.
- Modify the membership of the Event Log Readers group.
- Enroll in Microsoft Endpoint Manager.
- Install the Microsoft Monitoring Agent.

Correct Answer:



Answer Area

In Azure: ▼
- Add and configure the Diagnostics settings for the Azure Activity Log.
- [✓ Add and configure an Azure Log Analytics workspace.]
- Add an Azure Storage account and Azure Cognitive Search
- Add an Azure Storage account and a file share.

On the computers: ▼
- Create an event subscription.
- Modify the membership of the Event Log Readers group.
- Enroll in Microsoft Endpoint Manager.
- [✓ Install the Microsoft Monitoring Agent.]

Section: [none]
Explanation

Explanation/Reference:
Reference: https://docs.microsoft.com/en-us/azure/azure-monitor/learn/quick-collect-windows-computer

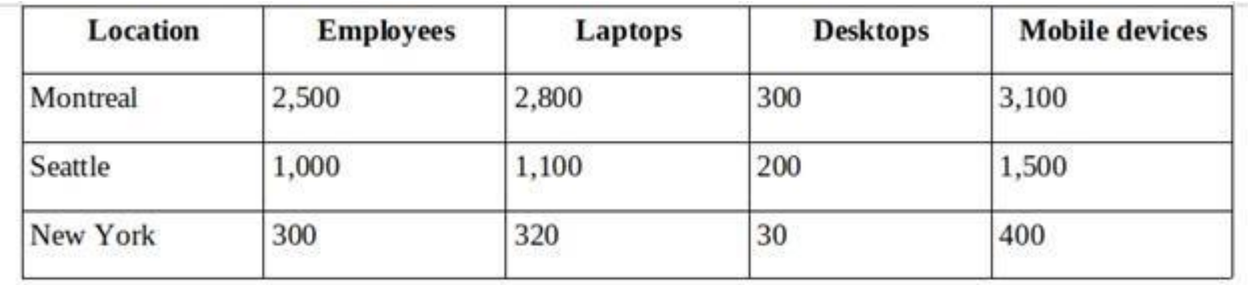
Testlet 2

Case Study

Overview

Contoso, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.

The company has the employees and devices shown in the following table.

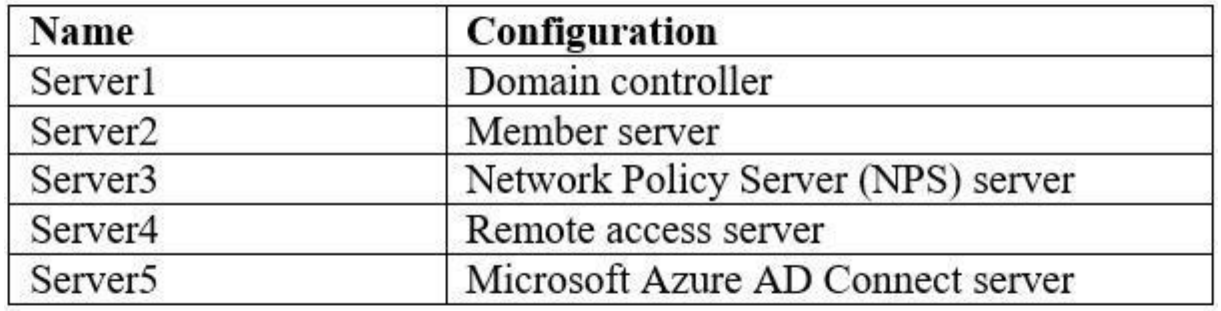


Location	Employees	Laptops	Desktops	Mobile devices
Montreal	2,500	2,800	300	3,100
Seattle	1,000	1,100	200	1,500
New York	300	320	30	400

Contoso recently purchased a Microsoft 365 E5 subscription.

Existing Environment

The network contains an on-premises Active Directory forest named contoso.com. The forest contains the servers shown in the following table.

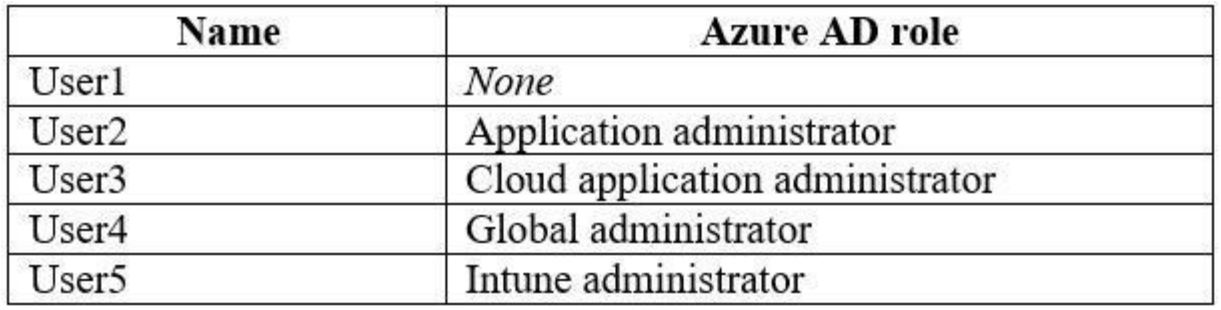


Name	Configuration
Server1	Domain controller
Server2	Member server
Server3	Network Policy Server (NPS) server
Server4	Remote access server
Server5	Microsoft Azure AD Connect server

All servers run Windows Server 2016. All desktops and laptops run Windows 10 Enterprise and are joined to the domain.

The mobile devices of the users in the Montreal and Seattle offices run Android. The mobile devices of the users in the New York office run iOS.

The domain is synced to Azure Active Directory (Azure AD) and includes the users shown in the following table.



Name	Azure AD role
User1	*None*
User2	Application administrator
User3	Cloud application administrator
User4	Global administrator
User5	Intune administrator

The domain also includes a group named Group1.

Requirements

Planned Changes
Contoso plans to implement the following changes:

- Implement Microsoft 365.

- Manage devices by using Microsoft Intune.
- Implement Azure Advanced Threat Protection (ATP).
- Every September, apply the latest feature updates to all Windows computers. Every March, apply the latest feature updates to the computers in the New York office only.

Technical Requirements

Contoso identifies the following technical requirements:

- When a Windows 10 device is joined to Azure AD, the device must enroll in Intune automatically.
- Dedicated support technicians must enroll all the Montreal office mobile devices in Intune.
- User1 must be able to enroll all the New York office mobile devices in Intune.
- Azure ATP sensors must be installed and must **NOT** use port mirroring.
- Whenever possible, the principle of least privilege must be used. ▪ A Microsoft Store for Business must be created.

Compliance Requirements

Contoso identifies the following compliance requirements:

- Ensure that the users in Group1 can only access Microsoft Exchange Online from devices that are enrolled in Intune and configured in accordance with the corporate policy. ▪ Configure Windows Information Protection (WIP) for the Windows 10 devices.

QUESTION 1 You need to ensure that the support technicians can meet the technical requirement for the Montreal office mobile devices.

What is the minimum of dedicated support technicians required?

A. 1
B. 4
C. 7
D. 31

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/sccm/mdm/deploy-use/enroll-devices-with-device-enrollment-manager

QUESTION 2 You need to create the Microsoft Store for Business.

Which user can create the store?

A. User2
B. User3
C. User4
D. User5

Correct Answer: C
Section: [none]
Explanation

Explanation/Reference:
References:
https://docs.microsoft.com/en-us/microsoft-store/roles-and-

permissions-microsoft-store-for-business

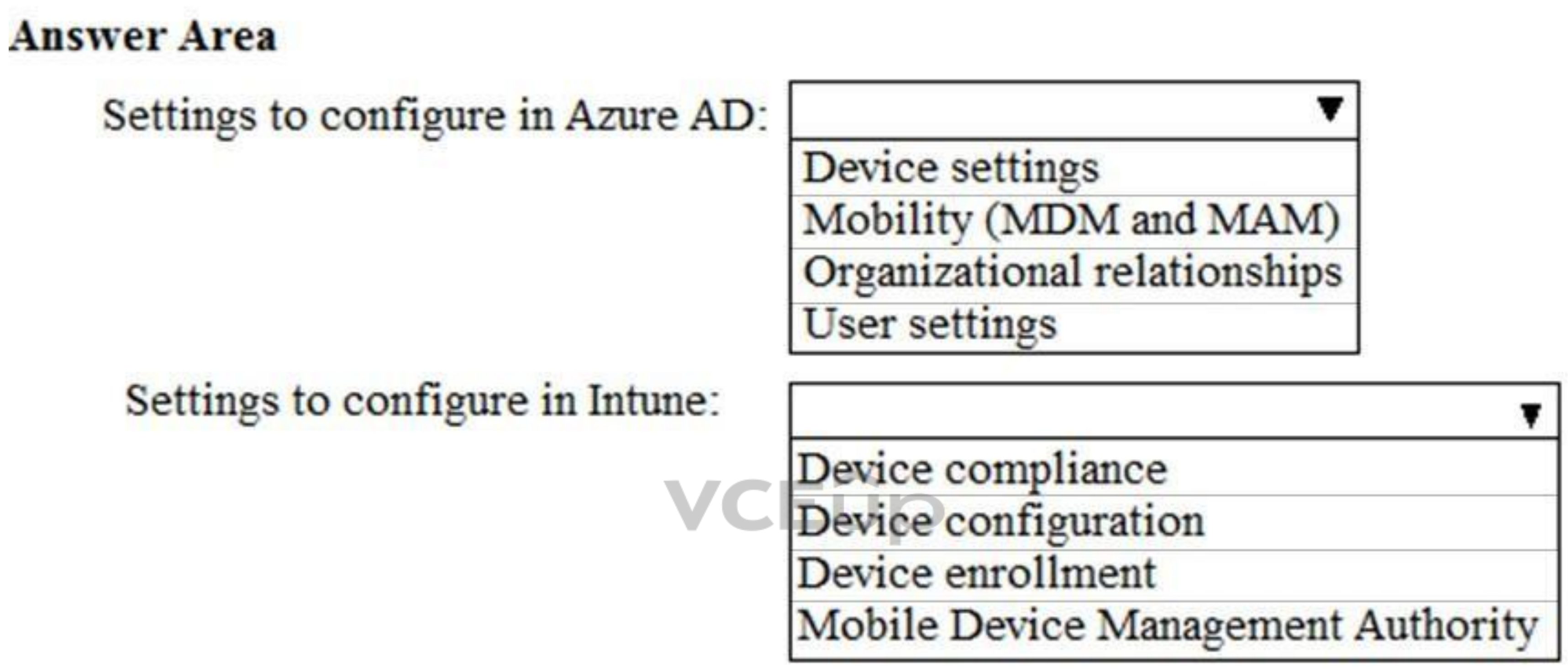
QUESTION 3 HOTSPOT

You need to meet the Intune requirements for the Windows 10 devices.

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

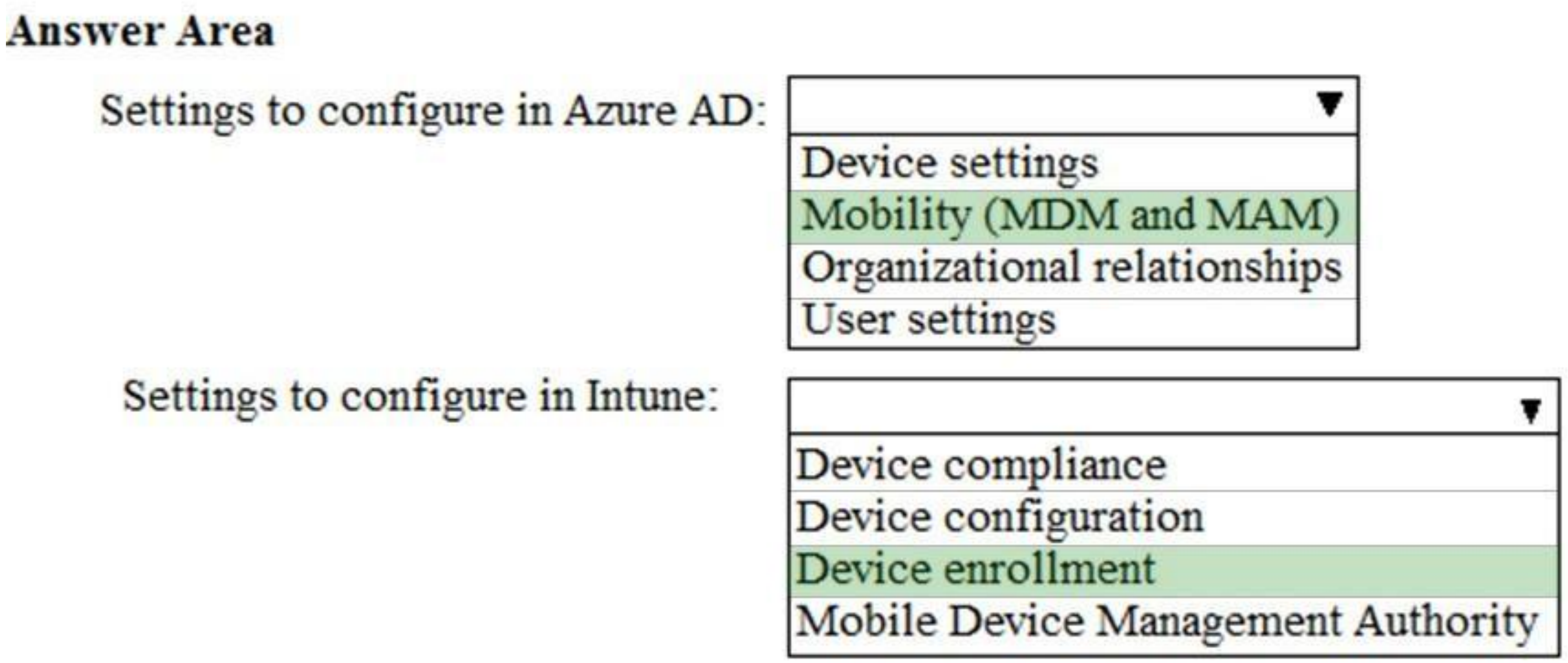
Settings to configure in Azure AD: ▼

- Device settings
- Mobility (MDM and MAM)
- Organizational relationships
- User settings

Settings to configure in Intune: ▼

- Device compliance
- Device configuration
- Device enrollment
- Mobile Device Management Authority

Correct Answer:



Answer Area

Settings to configure in Azure AD: ▼

- Device settings
- [✓ Mobility (MDM and MAM)]
- Organizational relationships
- User settings

Settings to configure in Intune: ▼

- Device compliance
- Device configuration
- [✓ Device enrollment]
- Mobile Device Management Authority

Section: [none]
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/intune/windows-enroll

QUESTION 4 HOTSPOT

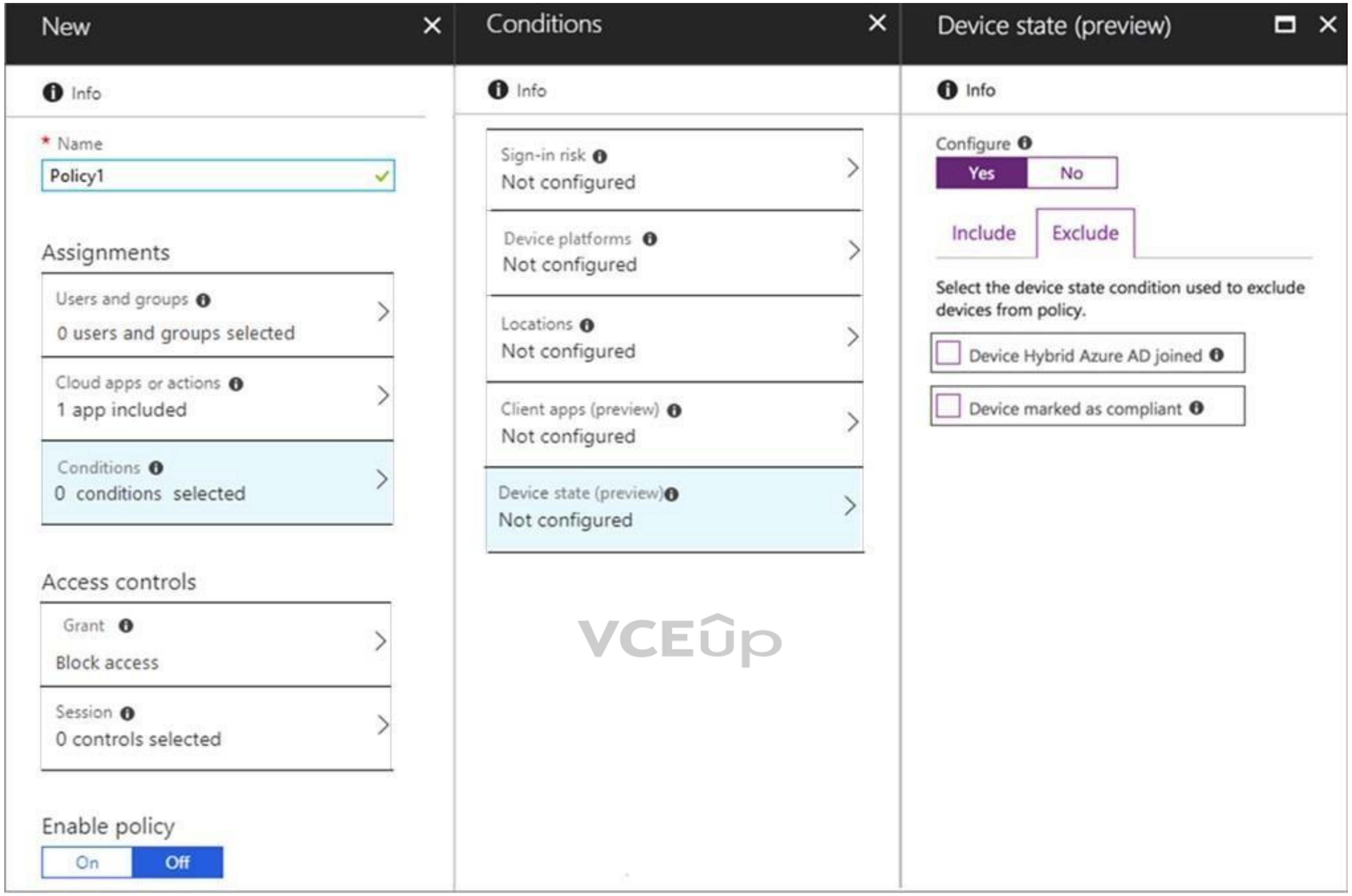
You need to configure a conditional access policy to meet the compliance requirements.

You add Exchange Online as a cloud app.

Which two additional 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

Info

* Name

Policy1

Assignments

Users and groups
0 users and groups selected

Cloud apps or actions
1 app included

Conditions
0 conditions selected

Access controls

Grant
Block access

Session
0 controls selected

Enable policy

On [✓ Off]

Conditions

Info

Sign-in risk
Not configured

Device platforms
Not configured

Locations
Not configured

Client apps (preview)
Not configured

Device state (preview)
Not configured

Device state (preview)

Info

Configure

[✓ Yes] No

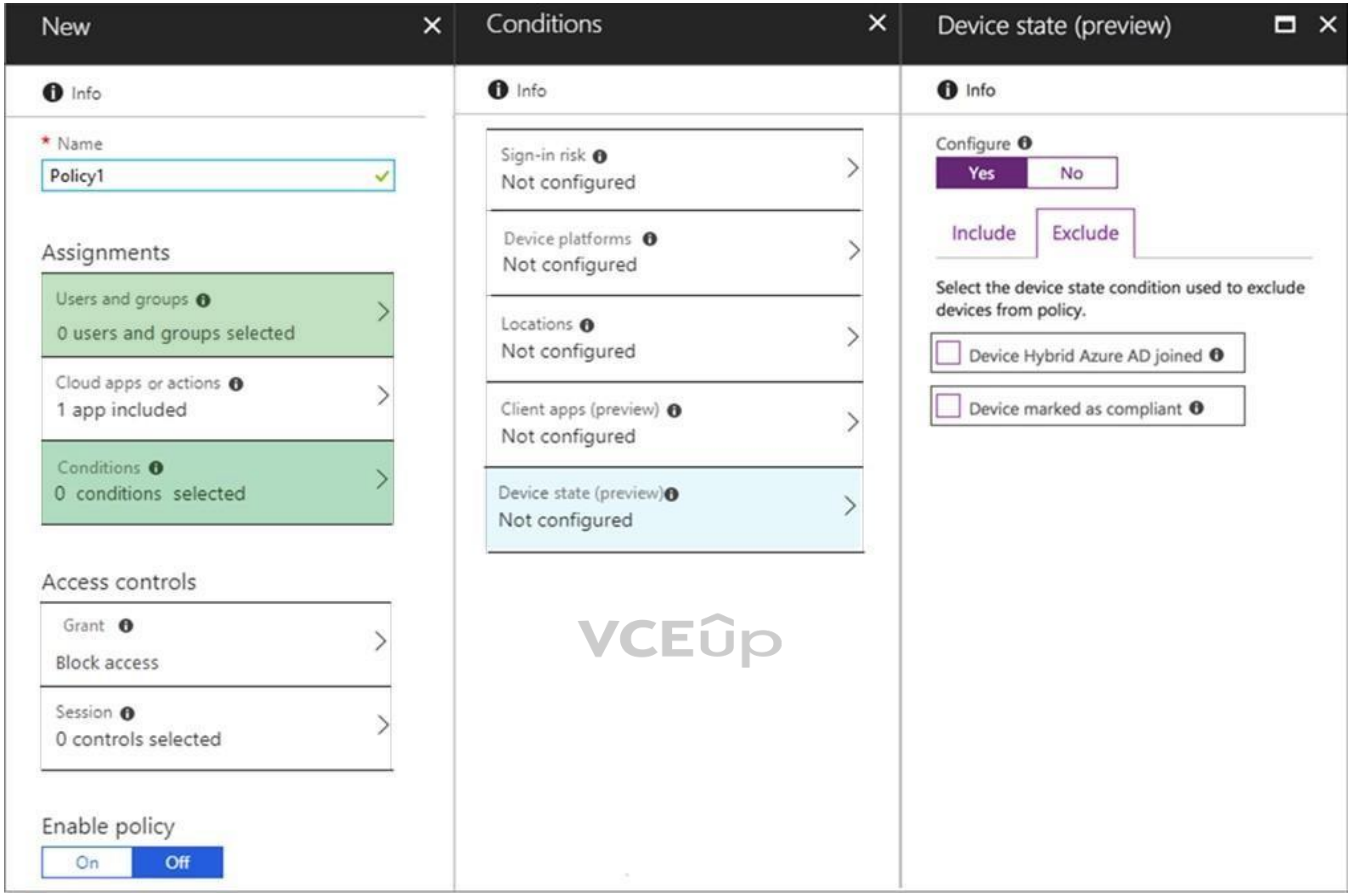
Include [✓ Exclude]

Select the device state condition used to exclude devices from policy.

□ Device Hybrid Azure AD joined

□ Device marked as compliant

Correct Answer:



New

Info

* Name

Policy1

Assignments

Users and groups

0 users and groups selected

Cloud apps or actions

1 app included

Conditions

0 conditions selected

Access controls

Grant

Block access

Session

0 controls selected

Enable policy

On | Off

Conditions

Info

Sign-in risk

Not configured

Device platforms

Not configured

Locations

Not configured

Client apps (preview)

Not configured

Device state (preview)

Not configured

Device state (preview)

Info

Configure

Yes | No

Include | Exclude

Select the device state condition used to exclude devices from policy.

□ Device Hybrid Azure AD joined

□ Device marked as compliant

Section: [none]
Explanation

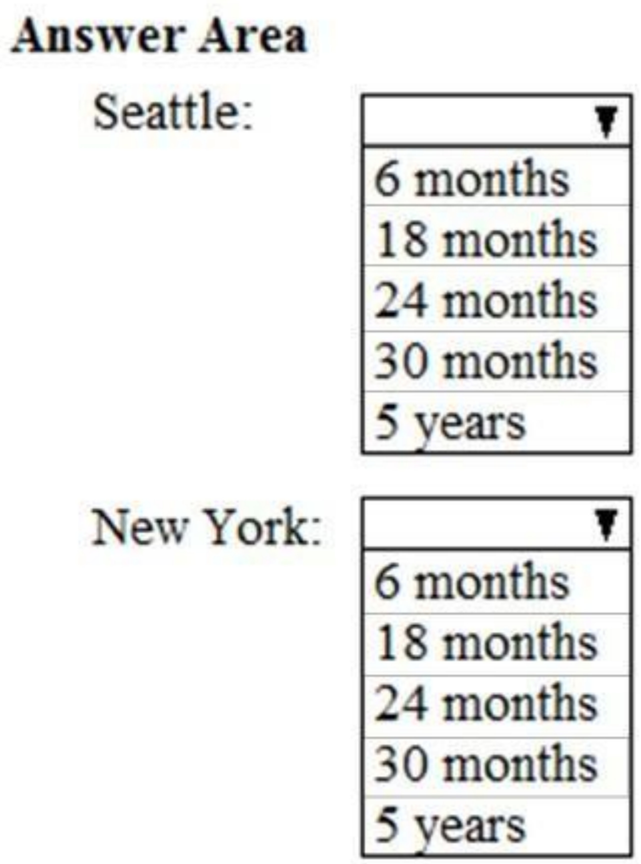
Explanation/Reference:
References: https://docs.microsoft.com/en-us/intune/create-conditional-access-intune

QUESTION 5 HOTSPOT

As of March, how long will the computers in each office remain supported by Microsoft? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

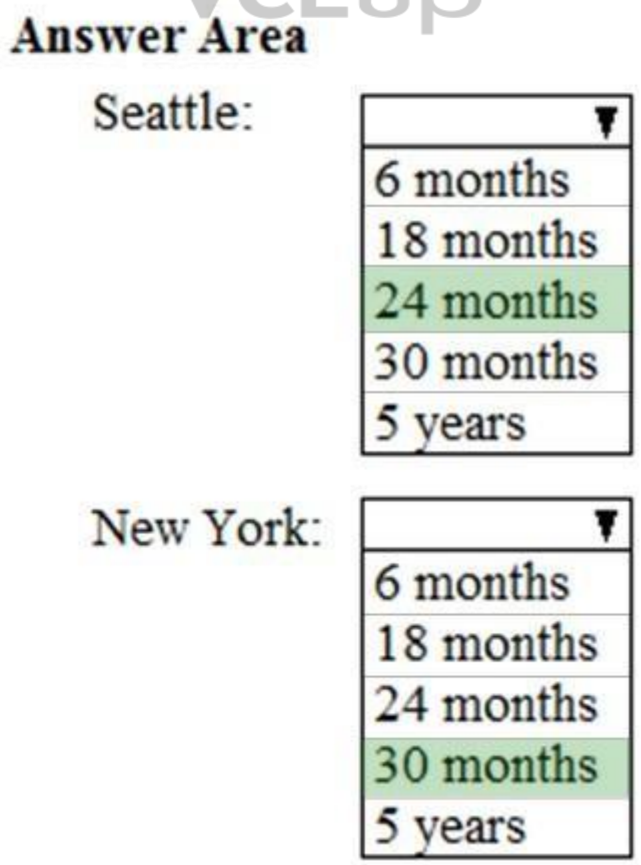
Seattle:

▼
6 months
18 months
24 months
30 months
5 years

New York:

▼
6 months
18 months
24 months
30 months
5 years

Correct Answer:



Answer Area

Seattle:

▼
6 months
18 months
[✓ 24 months]
30 months
5 years

New York:

▼
6 months
18 months
24 months
[✓ 30 months]
5 years

Section: [none]
Explanation

Explanation/Reference:
References: https://www.windowscentral.com/whats-difference-between-quality-updates-and-feature-updates-windows-10

QUESTION 6 You need to ensure that User1 can enroll the devices to meet the technical requirements.

What should you do?

A. From the Azure Active Directory admin center, assign User1 the Cloud device administrator role.
B. From the Azure Active Directory admin center, configure the Maximum number of devices per user setting.
C. From the Endpoint Management admin center, add User1 as a device enrollment manager.
D. From the Endpoint Management admin center, configure the Enrollment restrictions.

Correct Answer: C
Section: [none]
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/sccm/mdm/deploy-use/enroll-devices-with-device-enrollment-manager

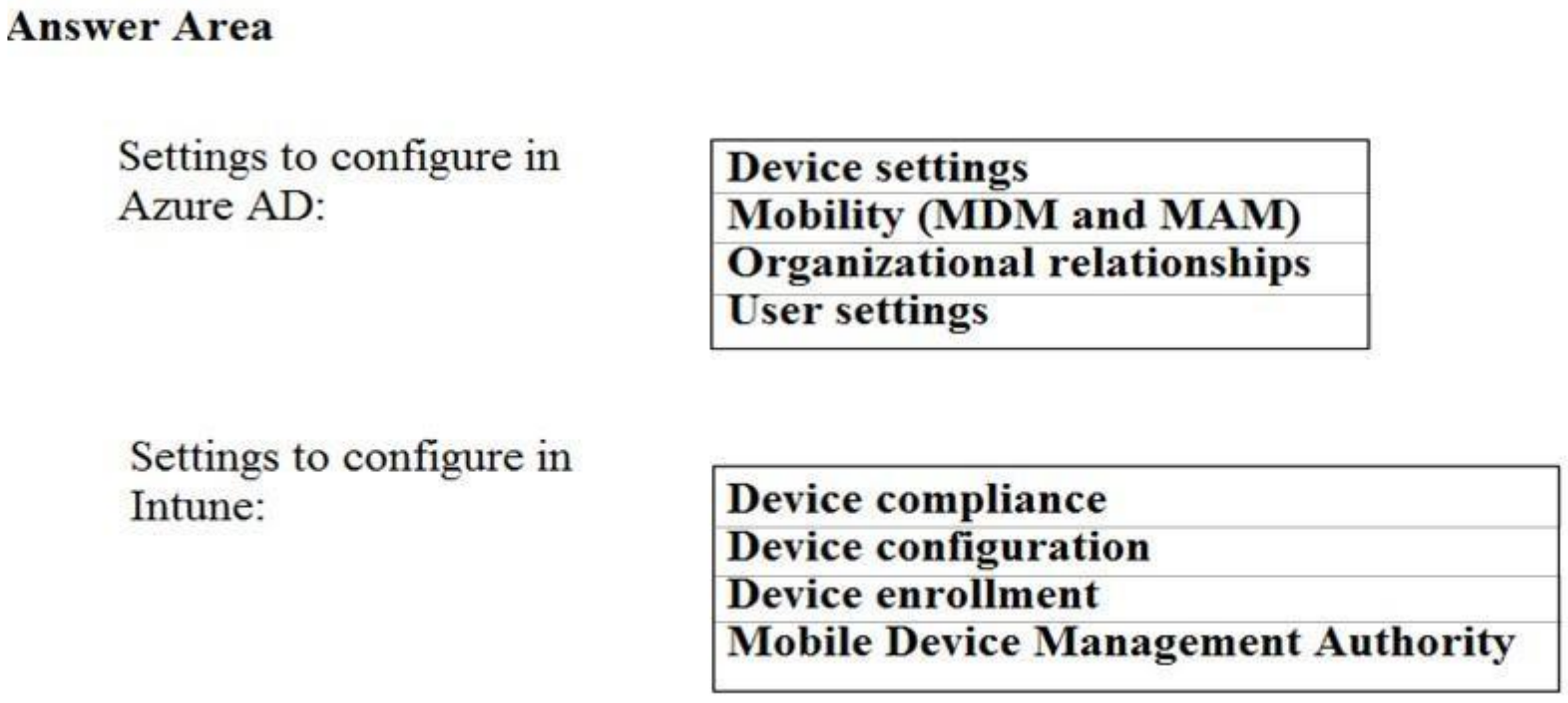
QUESTION 7 HOTSPOT

You need to meet the technical requirements and planned changes for Intune.

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

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

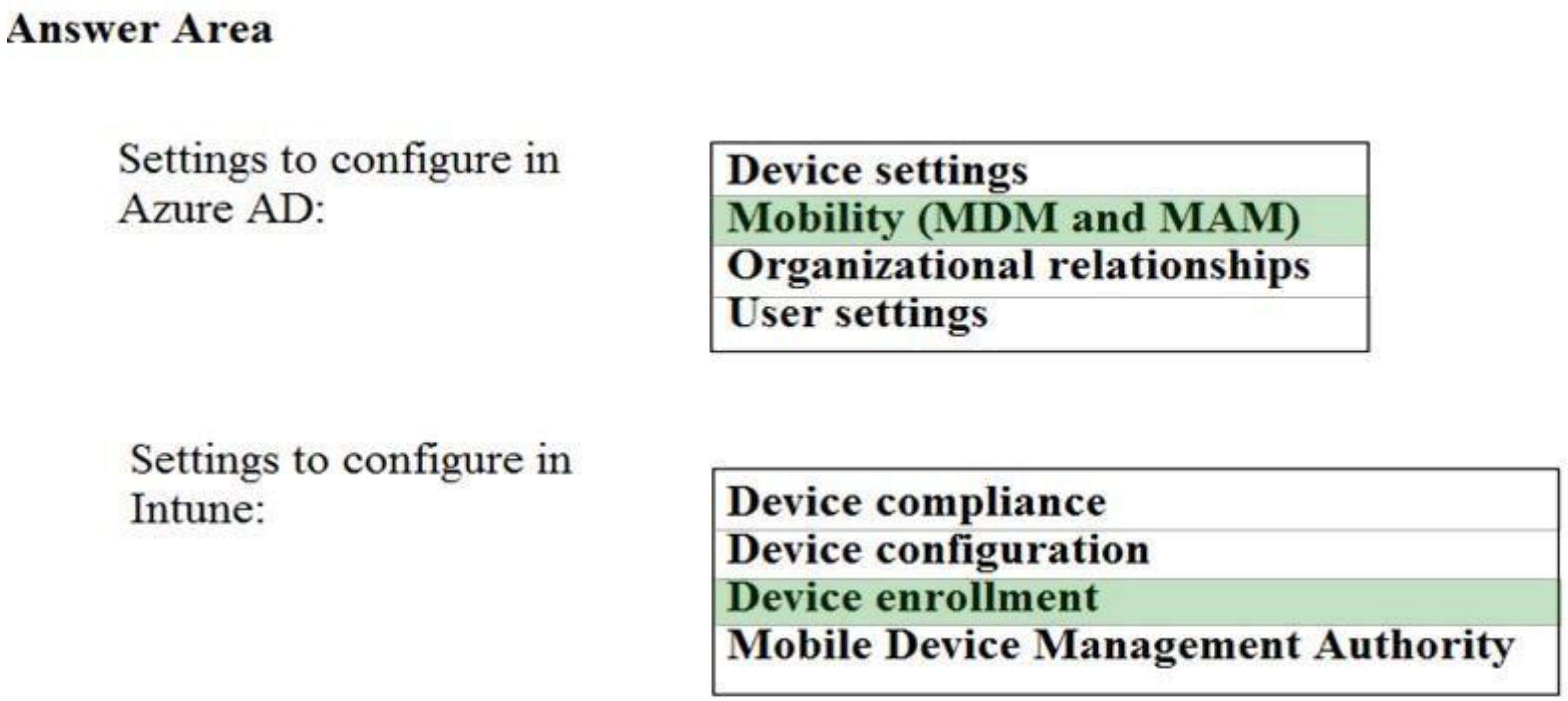
Settings to configure in Azure AD:

- Device settings
- Mobility (MDM and MAM)
- Organizational relationships
- User settings

Settings to configure in Intune:

- Device compliance
- Device configuration
- Device enrollment
- Mobile Device Management Authority

Correct Answer:



Answer Area

Settings to configure in Azure AD:

- Device settings
- [✓ Mobility (MDM and MAM)]
- Organizational relationships
- User settings

Settings to configure in Intune:

- Device compliance
- Device configuration
- [✓ Device enrollment]
- Mobile Device Management Authority

Section: [none]
Explanation

Explanation/Reference:
Reference:
https://docs.microsoft.com/en-us/intune/windows-enroll

Testlet 3

Case Study

Overview

ADatum Corporation is an international financial services company that has 5,000 employees.

ADatum has six offices: a main office in New York and five branch offices in Germany, the United Kingdom, France, Spain, and Italy.

All the offices are connected to each other by using a WAN link. Each office connects directly to the Internet.

Existing Environment

Current Infrastructure

ADatum recently purchased a Microsoft 365 subscription.

All user files are migrated to Microsoft 365.

All mailboxes are hosted in Microsoft 365. The users in each office have email suffixes that include the country of the user, for example, user1@us.adatum.com or user2@uk.adatum.com.

Each office has a security information and event management (SIEM) appliance. The appliance comes from three different vendors.

ADatum uses and processes Personally Identifiable Information (PII).

Problem Statements

ADatum entered into litigation. The legal department must place a hold on all the documents of a user named User1 that are in Microsoft 365.

Requirements

Business Goals

ADatum wants to be fully compliant with all the relevant data privacy laws in the regions where is operates.

ADatum wants to minimize the cost of hardware and software whenever possible. **Technical**

Requirements

ADatum identifies the following technical requirements:

- Centrally perform log analysis for all offices.
- Aggregate all data from the SIEM appliances to a central cloud repository for later analysis.
- Ensure that a SharePoint administrator can identify who accessed a specific file stored in a document library.
- Provide the users in the finance department with access to Service assurance information in Microsoft Office 365.
- Ensure that documents and email messages containing the PII data of European Union (EU) citizens are preserved for 10 years.
- If a user attempts to download 1,000 or more files from Microsoft SharePoint Online within 30 minutes, notify a security administrator and suspend the user's user account.
- A security administrator requires a report that shown which Microsoft 365 users signed in. Based on the report, the security administrator will create a policy to require multi-factor authentication when a sign-in is high risk.
- Ensure that the users in the New York office can only send email messages that contain sensitive U.S. PII data to other New York office uses. Email messages must be monitored to ensure compliance. Auditors in the New York office must have access to reports that show the sent and received email messages containing sensitive U.S. PII data.

QUESTION 1

You need to recommend a solution for the security administrator. The solution must meet the technical requirements.

What should you include in the recommendation?

A. Microsoft Azure Active Directory (Azure AD) Privileged Identity Management

B. Microsoft Azure Active Directory (Azure AD) Identity Protection

C. Microsoft Azure Active Directory (Azure AD) conditional access policies
D. Microsoft Azure Active Directory (Azure AD) authentication methods

Correct Answer: C
Section: [none]
Explanation

Explanation/Reference:
References:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/untrusted-networks

Question Set 1

QUESTION 1

Your network contains an on-premises Active Directory domain.

Your company has a security policy that prevents additional software from being installed on domain controllers.

You need to monitor a domain controller by using Microsoft Azure Advanced Threat Protection (ATP).

What should you do? More than one answer choice may achieve the goal. Select the **BEST** answer.

A. Deploy an Azure ATP sensor, and then configure port mirroring.
B. Deploy an Azure ATP sensor, and then configure detections.
C. Deploy an Azure ATP standalone sensor, and then configure detections.
D. Deploy an Azure ATP standalone sensor, and then configure port mirroring.

Correct Answer: D
Section: [none]
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/azure-advanced-threat-protection/install-atp-step5

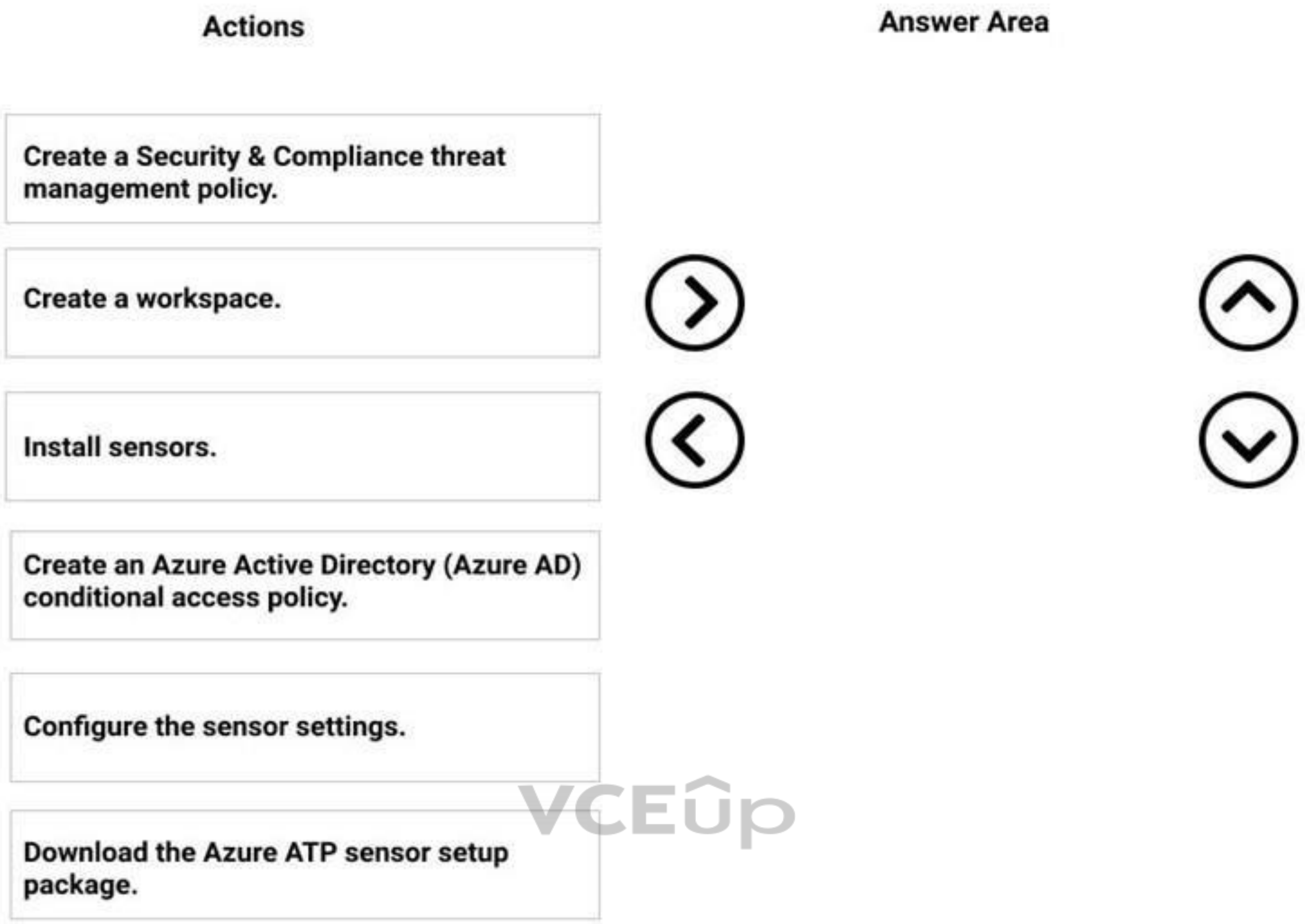
QUESTION 2
DRAG DROP

You create a Microsoft 365 subscription.

You need to create a deployment plan for Microsoft Azure Advanced Threat Protection (ATP).

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:

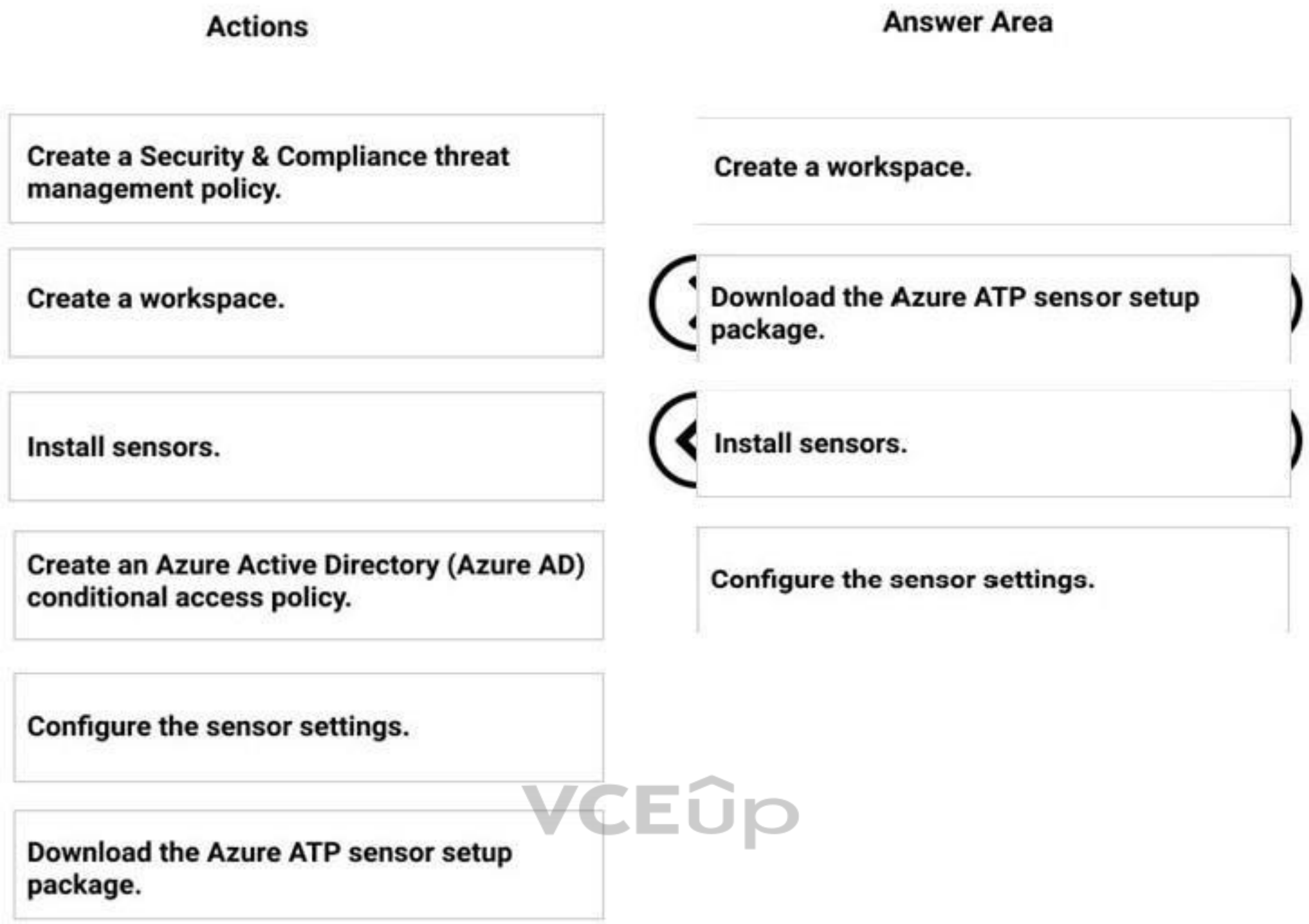


Actions

Answer Area

- Create a Security & Compliance threat management policy.
- Create a workspace.
- Install sensors.
- Create an Azure Active Directory (Azure AD) conditional access policy.
- Configure the sensor settings.
- Download the Azure ATP sensor setup package.

Correct Answer:



Actions

Create a Security & Compliance threat management policy.

Create a workspace.

Install sensors.

Create an Azure Active Directory (Azure AD) conditional access policy.

Configure the sensor settings.

Download the Azure ATP sensor setup package.

Answer Area

Create a workspace.

Download the Azure ATP sensor setup package.

Install sensors.

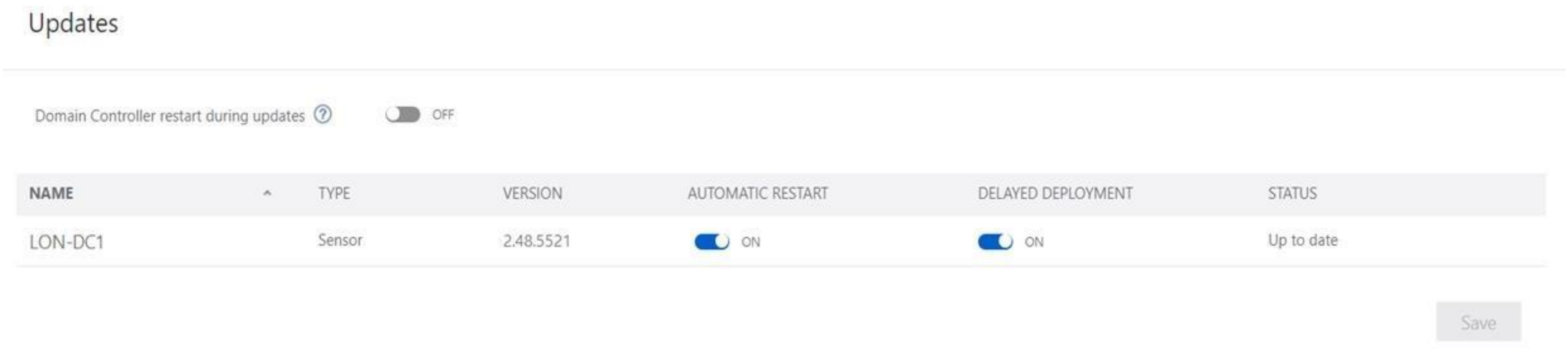
Configure the sensor settings.

Section: [none]
Explanation

Explanation/Reference:
References: https://blog.ahasayen.com/azure-advanced-threat-protection-deployment/

QUESTION 3 You implement Microsoft Azure Advanced Threat Protection (Azure ATP).

You have an Azure ATP sensor configured as shown in the following exhibit.



Updates

Domain Controller restart during updates ⓘ OFF

NAME	TYPE	VERSION	AUTOMATIC RESTART	DELAYED DEPLOYMENT	STATUS
LON-DC1	Sensor	2.48.5521	ON	ON	Up to date

How long after the Azure ATP cloud service is updated will the sensor update?

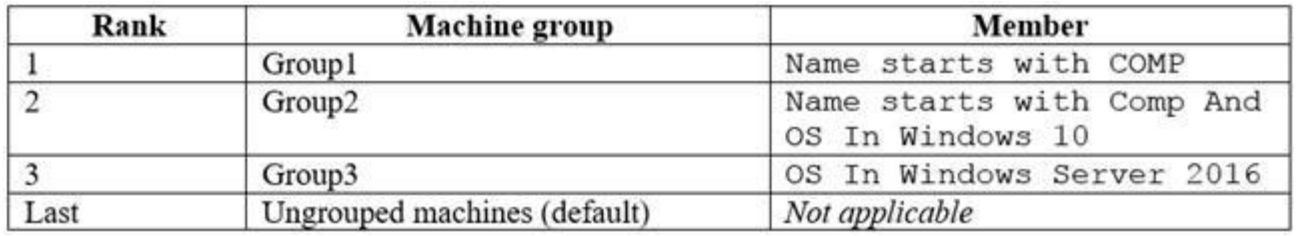
A. 72 hours B.
12 hours
C. 48 hours
D. 7 days
E. 24 hours

Correct Answer: E
Section: [none]
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/azure-advanced-threat-protection/atp-whats-new

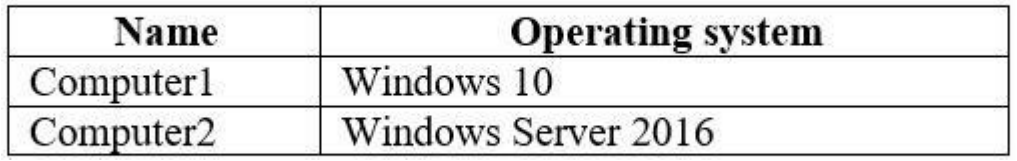
QUESTION 4 HOTSPOT

Your company uses Microsoft Defender Advanced Threat Protection (ATP). Microsoft Defender ATP contains the device groups shown in the following table.



Rank	Machine group	Member
1	Group1	Name starts with COMP
2	Group2	Name starts with Comp And OS In Windows 10
3	Group3	OS In Windows Server 2016
Last	Ungrouped machines (default)	*Not applicable*

You onboard computers to Microsoft Defender ATP as shown in the following table.

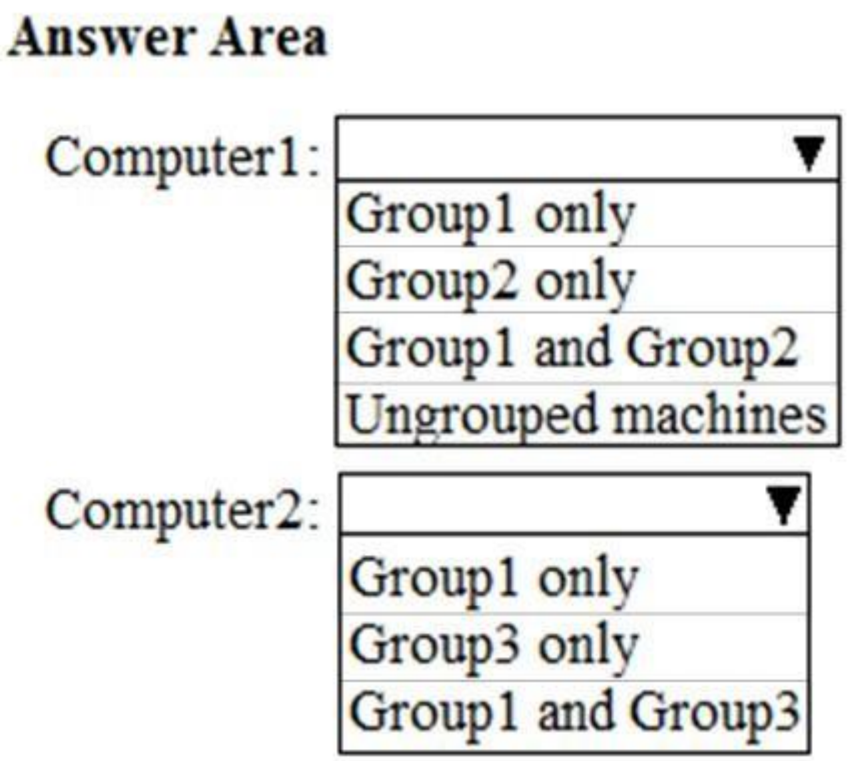


Name	Operating system
Computer1	Windows 10
Computer2	Windows Server 2016

Of which groups are Computer1 and Computer2 members? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

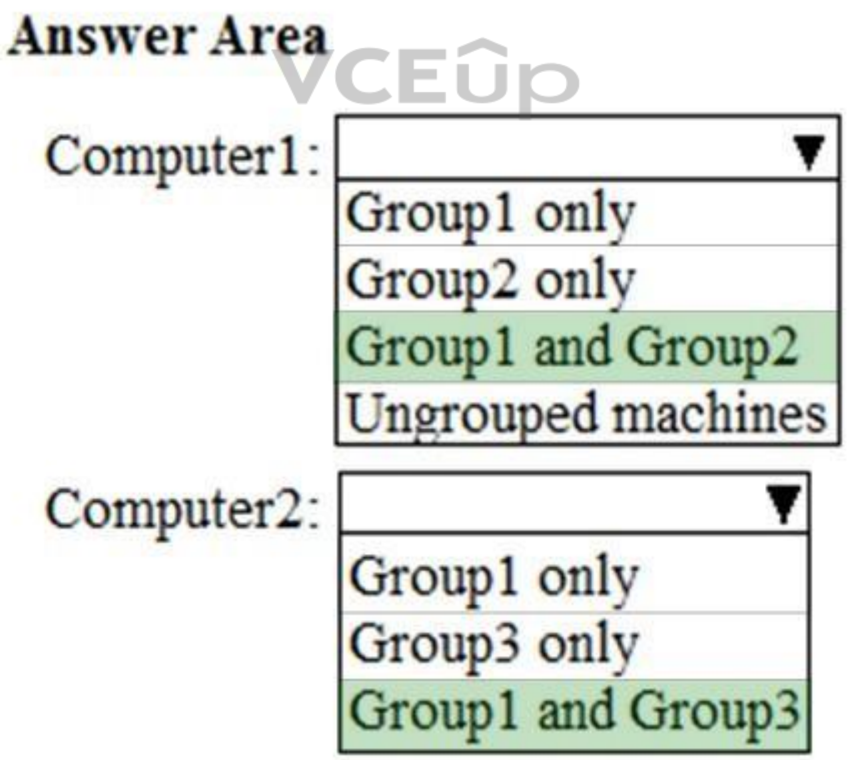
Computer1: ▼

- Group1 only
- Group2 only
- Group1 and Group2
- Ungrouped machines

Computer2: ▼

- Group1 only
- Group3 only
- Group1 and Group3

Correct Answer:



Answer Area

Computer1: ▼

- Group1 only
- Group2 only
- [✓ Group1 and Group2]
- Ungrouped machines

Computer2: ▼

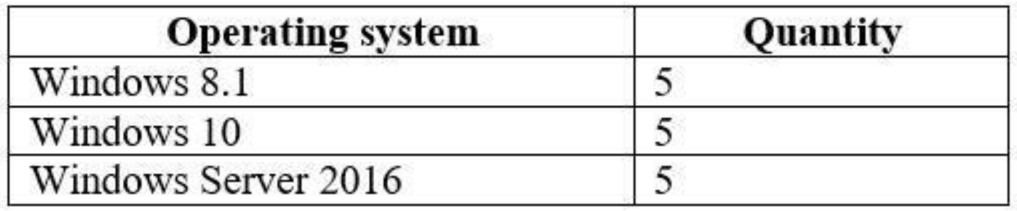
- Group1 only
- Group3 only
- [✓ Group1 and Group3]

Section: [none]
Explanation

Explanation/Reference:
QUESTION 5
DRAG DROP

You have a Microsoft 365 subscription.

You have the devices shown in the following table.



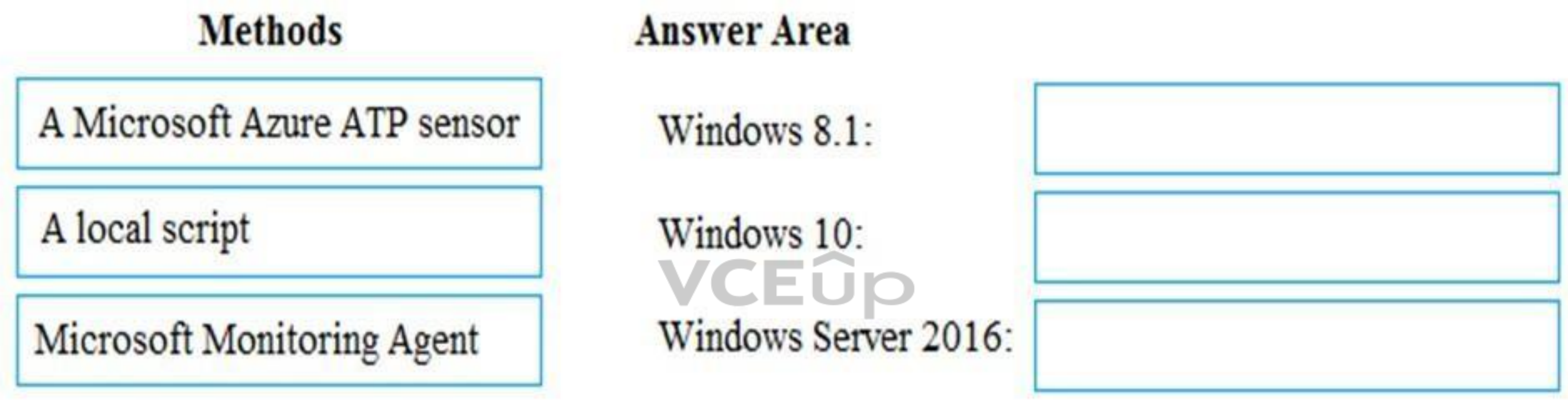
Operating system	Quantity
Windows 8.1	5
Windows 10	5
Windows Server 2016	5

You need to onboard the devices to Microsoft Defender Advanced Threat Protection (ATP). The solution must avoid installing software on the devices whenever possible.

Which onboarding method should you use for each operating system? To answer, drag the appropriate methods to the correct operating systems. Each method may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:



Methods

- A Microsoft Azure ATP sensor
- A local script
- Microsoft Monitoring Agent

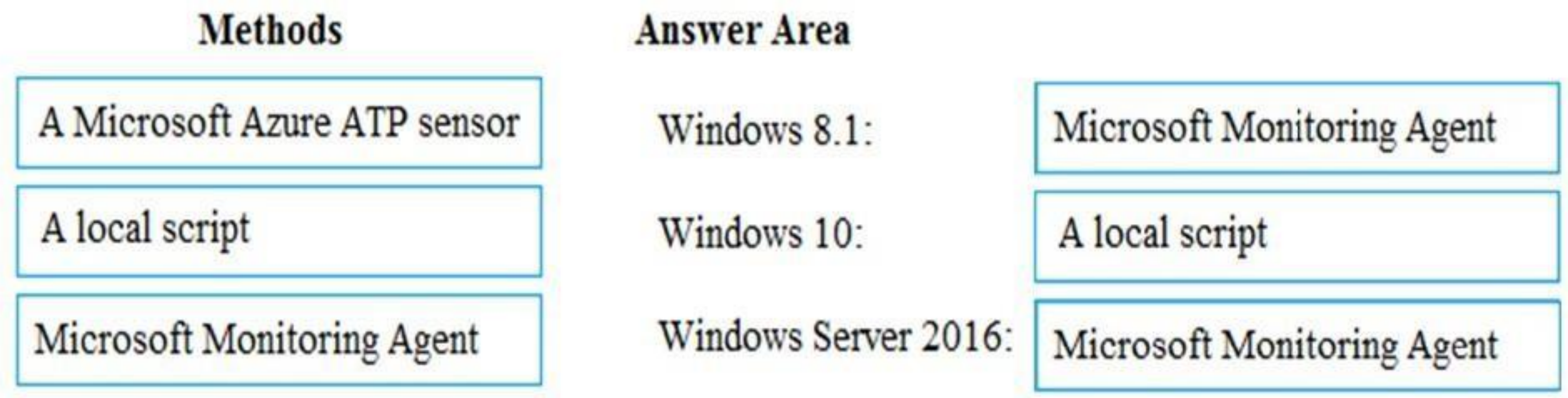
Answer Area

Windows 8.1:

Windows 10:

Windows Server 2016:

Correct Answer:



Methods

- A Microsoft Azure ATP sensor
- A local script
- Microsoft Monitoring Agent

Answer Area

Windows 8.1: Microsoft Monitoring Agent

Windows 10: A local script

Windows Server 2016: Microsoft Monitoring Agent

Section: [none]
Explanation

Explanation/Reference:

References: https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-atp/onboard-downlevel-windows-defender-advanced-threat-protection https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-atp/configure-endpoints-windows-defender-advanced-threat-protection https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-atp/configure-server-endpoints-windows-defender-advanced-threat-protection

QUESTION 6

The users at your company use Dropbox Business to store documents. The users access Dropbox Business by using the MyApps portal.

You need to ensure that user access to Dropbox Business is authenticated by using a Microsoft 365 identity. The documents must be protected if the data is downloaded to a device that is not trusted.

What should you do?

A. From the Device Management admin center, configure conditional access settings.
B. From the Azure Active Directory admin center, configure the device settings.
C. From the Azure Active Directory admin center, configure application proxy settings.
D. From the Device Management admin center, configure device enrollment settings.

Correct Answer: C
Section: [none]
Explanation

Explanation/Reference:
Explanation:
Azure Active Directory's Application Proxy provides secure remote access to on-premises web applications. After a single sign-on to Azure AD, users can access both cloud and on-premises applications through an external URL or an internal application portal.

Reference: https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/application-proxy

QUESTION 7

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 subscription.

You discover that some external users accessed content on a Microsoft SharePoint site. You modify the SharePoint sharing policy to prevent sharing outside your organization.

You need to be notified if the SharePoint sharing policy is modified in the future.

Solution: From the SharePoint admin center, you modify the sharing settings.

Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:

QUESTION 8

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 subscription.

You need to prevent users from accessing your Microsoft SharePoint Online sites unless the users are connected to your on-premises network.

Solution: From the Device Management admin center, you create a trusted location and a compliance policy Does

this meet the goal?

A. Yes
B. No

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:
Explanation:
Conditional Access in SharePoint Online can be configured to use an IP Address white list to allow access.

References: https://techcommunity.microsoft.com/t5/Microsoft-SharePoint-Blog/Conditional-Access-in-SharePoint-Online-and-OneDrive-for/ba-p/46678

QUESTION 9
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 subscription.

You need to prevent users from accessing your Microsoft SharePoint Online sites unless the users are connected to your on-premises network.

Solution: From the Microsoft 365 admin center, you configure the Organization profile settings.

Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:
Explanation:
Conditional Access in SharePoint Online can be configured to use an IP Address white list to allow access.

References: https://techcommunity.microsoft.com/t5/Microsoft-SharePoint-Blog/Conditional-Access-in-SharePoint-Online-and-OneDrive-for/ba-p/46678A

QUESTION 10
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 subscription.

You need to prevent users from accessing your Microsoft SharePoint Online sites unless the users are connected to your on-premises network.

Solution: From the Azure Active Directory admin center, you create a trusted location and a conditional access policy.

Does this meet the goal?

A. Yes

B. No

Correct Answer: A
Section: [none]
Explanation

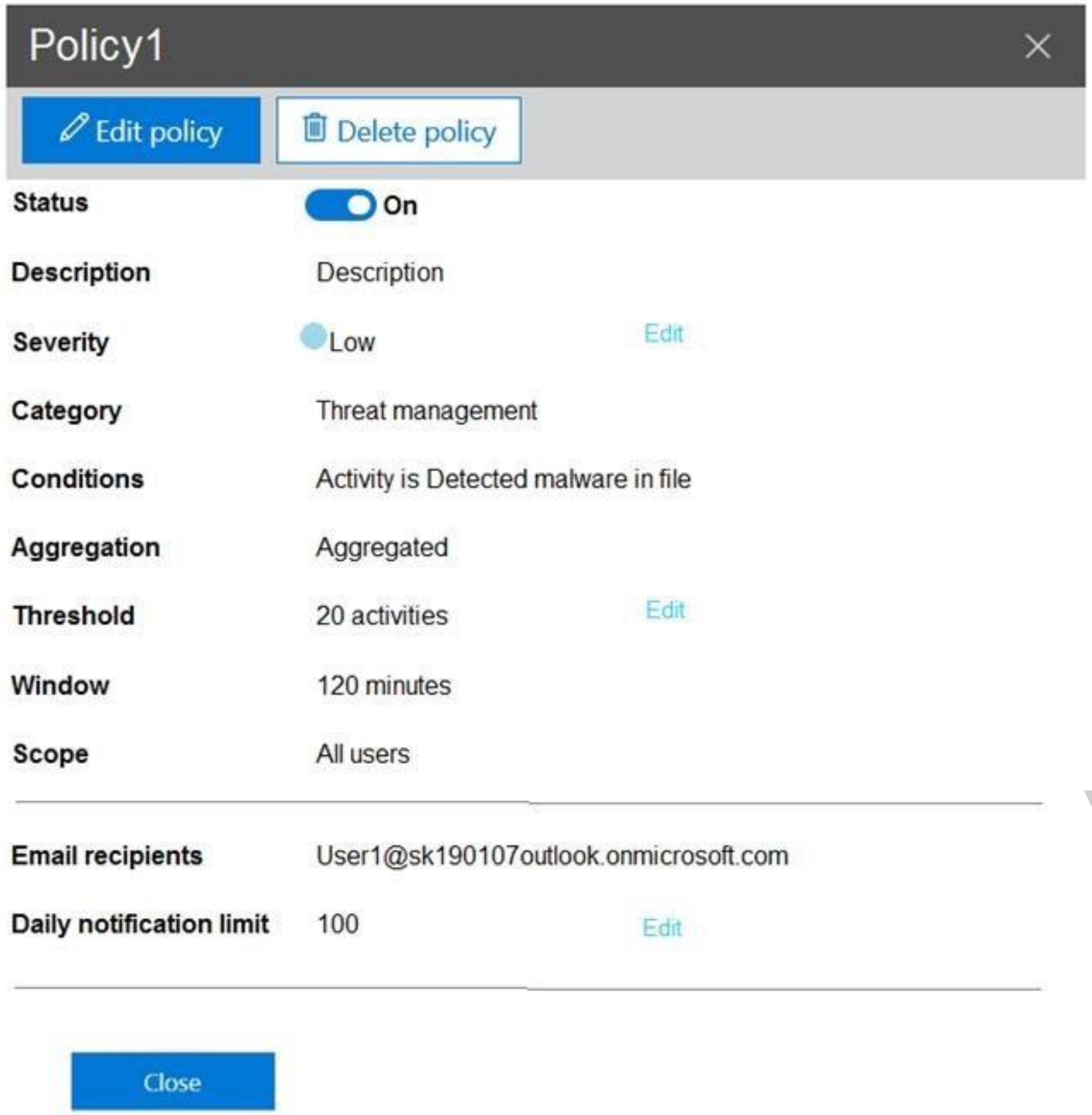
Explanation/Reference:
Explanation:
Conditional Access in SharePoint Online can be configured to use an IP Address white list to allow access.

References: https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition
https://techcommunity.microsoft.com/t5/Microsoft-SharePoint-Blog/Conditional-Access-in-SharePoint-Online-and-OneDrive-for/ba-p/46678

QUESTION 11
HOTSPOT

You have Microsoft 365 subscription.

You create an alert policy as shown in the following exhibit.



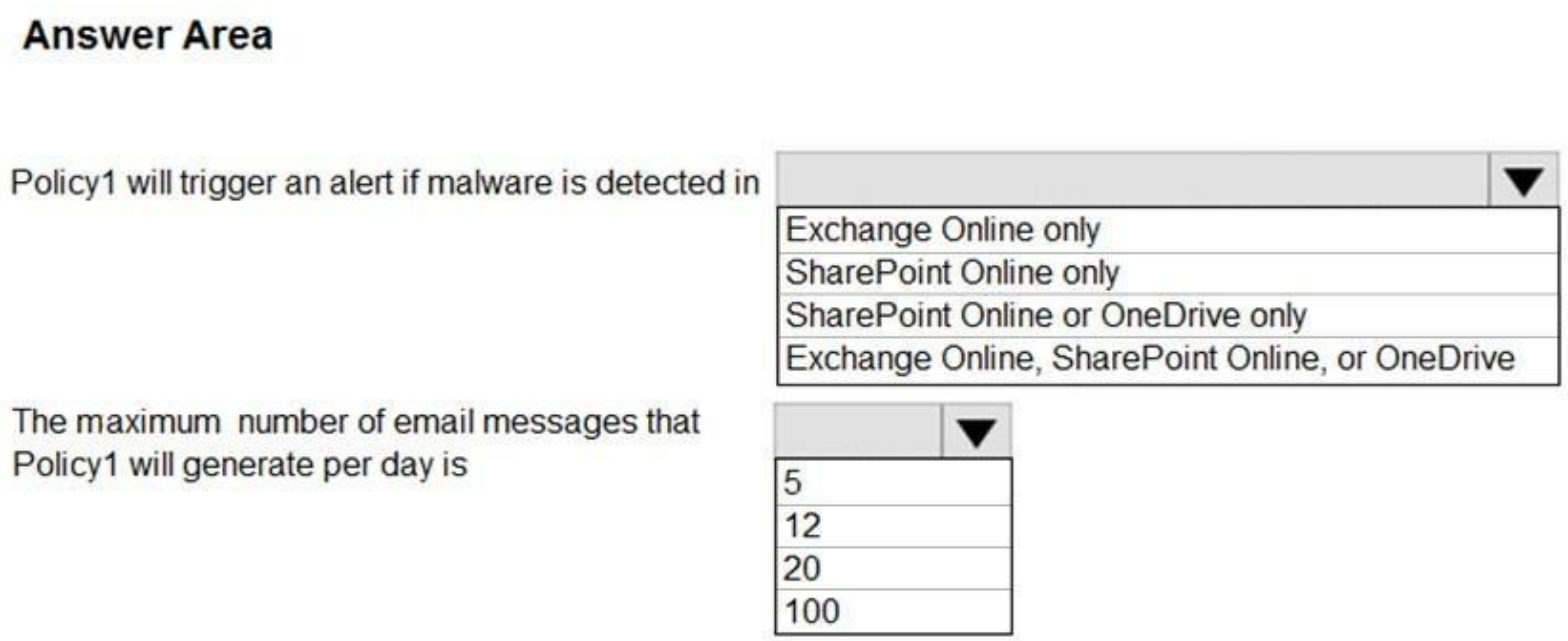
Policy1

Status	On
Description	Description
Severity	Low
Category	Threat management
Conditions	Activity is Detected malware in file
Aggregation	Aggregated
Threshold	20 activities
Window	120 minutes
Scope	All users
Email recipients	User1@sk190107outlook.onmicrosoft.com
Daily notification limit	100

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:



Answer Area

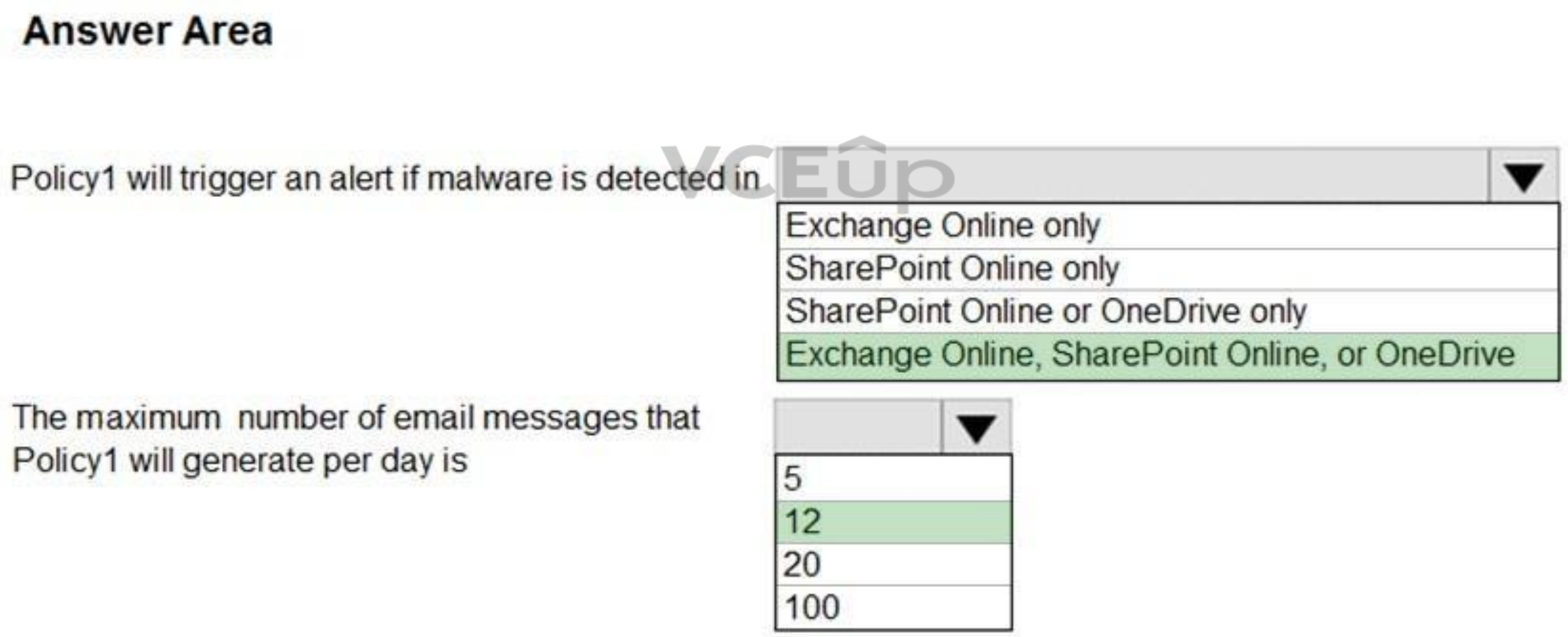
Policy1 will trigger an alert if malware is detected in

- Exchange Online only
- SharePoint Online only
- SharePoint Online or OneDrive only
- Exchange Online, SharePoint Online, or OneDrive

The maximum number of email messages that Policy1 will generate per day is

- 5
- 12
- 20
- 100

Correct Answer:



Answer Area

Policy1 will trigger an alert if malware is detected in

- Exchange Online only
- SharePoint Online only
- SharePoint Online or OneDrive only
- [✓ Exchange Online, SharePoint Online, or OneDrive]

The maximum number of email messages that Policy1 will generate per day is

- 5
- [✓ 12]
- 20
- 100

Section: [none]
Explanation

Explanation/Reference:
Explanation:
Note: The Aggregation settings has a 120 minute window

QUESTION 12 You have a Microsoft 365 subscription.

All users have their email stored in Microsoft Exchange Online.

In the mailbox of a user named User1, you need to preserve a copy of all the email messages that contain the word ProjectX.

What should you do?

A. From the Security & Compliance admin center, create a label and a label policy.
B. From the Exchange admin center, create a mail flow rule.
C. From the Security & Compliance admin center, start a message trace.
D. From Exchange admin center, start a mail flow message trace.

Correct Answer: A
Section: [none]
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/azure/information-protection/configure-policy-classification

QUESTION 13
HOTSPOT

You have a new Microsoft 365 subscription.

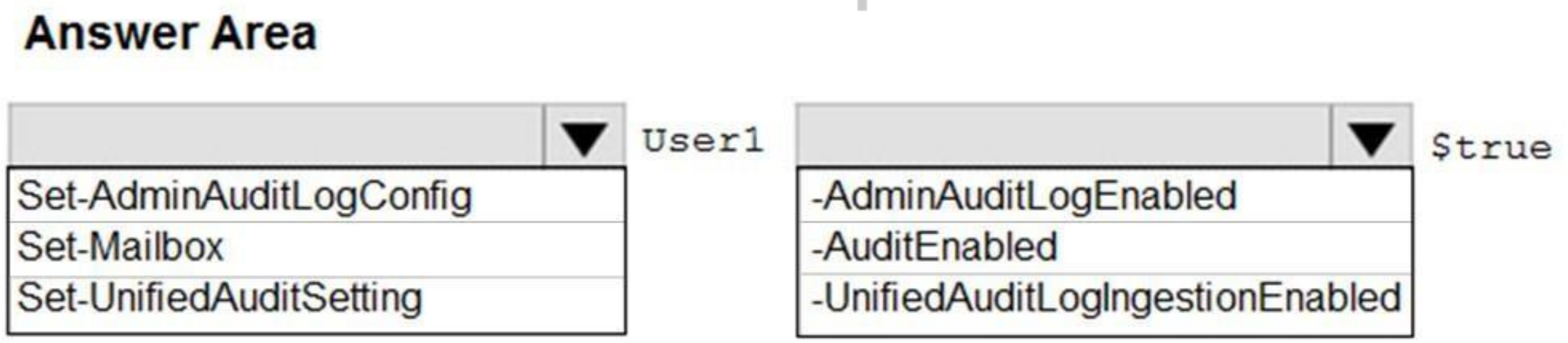
A user named User1 has a mailbox in Microsoft Exchange Online.

You need to log any changes to the mailbox folder permissions of User1.

Which command should you run? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



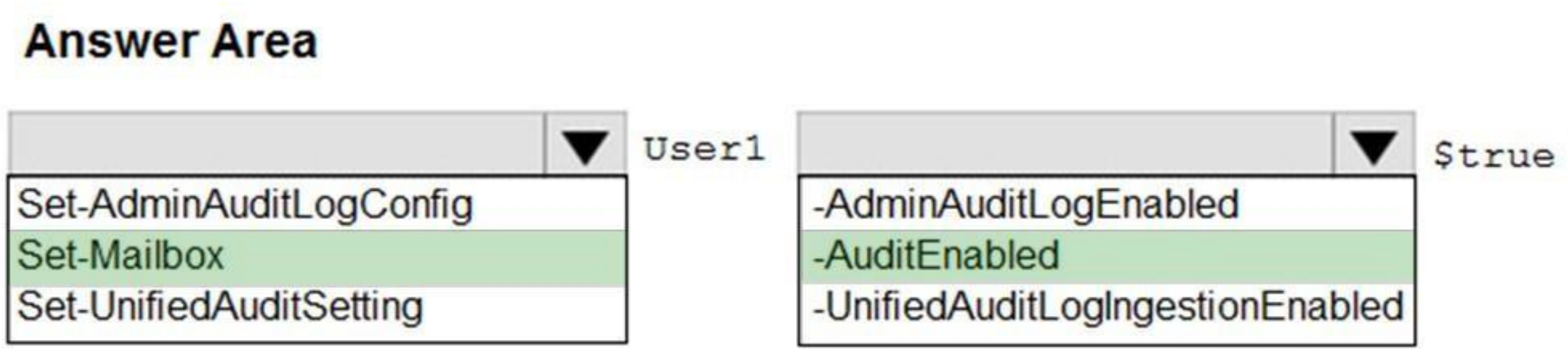
Answer Area

▼ User1 ▼ $true

Set-AdminAuditLogConfig
Set-Mailbox
Set-UnifiedAuditSetting

-AdminAuditLogEnabled
-AuditEnabled
-UnifiedAuditLogIngestionEnabled

Correct Answer:



Answer Area

Set-AdminAuditLogConfig Set-Mailbox Set-UnifiedAuditSetting	User1	-AdminAuditLogEnabled -AuditEnabled -UnifiedAuditLogIngestionEnabled	$true

Section: [none]
Explanation

Explanation/Reference:
Explanation:

To enable auditing for a single mailbox (in this example, belonging to Holly Sharp), use this PowerShell command: Set-Mailbox username -AuditEnabled $true

References: https://support.microsoft.com/en-us/help/4026501/office-auditing-in-office-365-for-admins
https://docs.microsoft.com/en-us/powershell/module/exchange/mailboxes/set-mailbox?view=exchange-ps

QUESTION 14 You have a Microsoft 365 subscription.

You recently configured a Microsoft SharePoint Online tenant in the subscription.

You plan to create an alert policy.

You need to ensure that an alert is generated only when malware is detected in more than five documents stored in SharePoint Online during a period of 10 minutes.

What should you do first?

A. Enable Microsoft Office 365 Cloud App Security.
B. Deploy Microsoft Defender Advanced Threat Protection (Microsoft Defender ATP)
C. Enable Microsoft Office 365 Analytics.

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:

QUESTION 15
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 subscription.

You discover that some external users accessed content on a Microsoft SharePoint site. You modify the SharePoint sharing policy to prevent sharing outside your organization.

You need to be notified if the SharePoint sharing policy is modified in the future.

Solution: From the Security & Compliance admin center, you create a threat management policy.

Does this meet the goal?

A. Yes
B. No

Correct Answer: A
Section: [none]
Explanation

Explanation/Reference:

QUESTION 16 You have a Microsoft 365 subscription.

You need to be notified if users receive email containing a file that has a virus.

What should you do?

A. From the Exchange admin center, create an in-place eDiscovery & hold.
B. From the Security & Compliance admin center, create a safe attachments policy.
C. From the Security & Compliance admin center, create a data loss prevention (DLP) policy.
D. From the Security & Compliance admin center, create an alert policy.

Correct Answer: D
Section: [none]
Explanation

Explanation/Reference:
Reference:
https://docs.microsoft.com/en-us/office365/securitycompliance/alert-policies

QUESTION 17 You have a Microsoft Azure Active Directory (Azure AD) tenant.

The organization needs to sign up for Microsoft Store for Business. The solution must use the principle of least privilege.

Which role should you assign to the user?

A. Global administrator
B. Cloud application administrator
C. Application administrator
D. Service administrator

Correct Answer: A
Section: [none]
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/microsoft-store/sign-up-microsoft-store-for-business

QUESTION 18
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 subscription.

You discover that some external users accessed content on a Microsoft SharePoint site. You modify the SharePoint sharing policy to prevent sharing outside your organization.

You need to be notified if the SharePoint sharing policy is modified in the future.

Solution: From the SharePoint site, you create an alert.

Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:

QUESTION 19
You have a Microsoft 365 subscription and an on-premises Active Directory domain named contoso.com. All client computers run Windows 10 Enterprise and are joined to the domain.

You need to enable Microsoft Defender Credential Guard on all the computers.

What should you do?

A. From the Security & Compliance admin center, configure the DKIM signatures for the domain.
B. From a domain controller, create a Group Policy object (GPO) that enables the Restrict delegation of credentials to remote servers setting.
C. From the Security & Compliance admin center, create a device security policy.
D. From a domain controller, create a Group Policy object (GPO) that enabled the Turn On Virtualization Based Security setting.

Correct Answer: D
Section: [none]
Explanation

Explanation/Reference:
Reference: https://docs.microsoft.com/en-us/windows/security/identity-protection/credential-guard/credential-guard-manage

QUESTION 20 Your company has a Microsoft 365 subscription that uses an Azure Active Directory (Azure AD) tenant named contoso.com.

The company purchases a cloud app named App1 that supports Microsoft Cloud App Security monitoring.

You configure App1 to be available from the My Apps portal.

You need to ensure that you can monitor App1 from Cloud App Security.

What should you do?

A. From the Azure Active Directory admin center, create a conditional access policy.
B. From the Azure Active Directory admin center, create an app registration.
C. From the Endpoint Management admin center, create an app protection policy.
D. From the Endpoint Management admin center, create an app configuration policy.

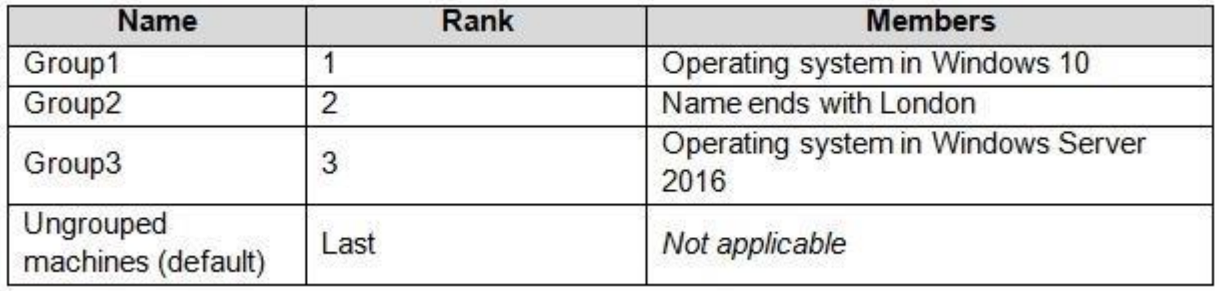
Correct Answer: A
Section: [none]
Explanation

Explanation/Reference:

QUESTION 21
HOTSPOT

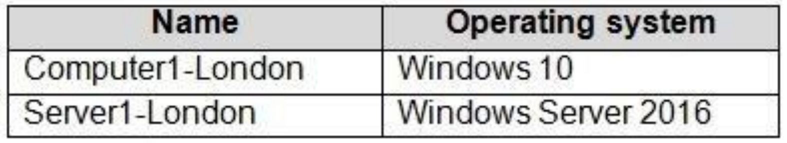
You use Microsoft Defender Advanced Threat Protection (Microsoft Defender ATP).

You have the Microsoft Defender ATP machine groups shown in the following table.



Name	Rank	Members
Group1	1	Operating system in Windows 10
Group2	2	Name ends with London
Group3	3	Operating system in Windows Server 2016
Ungrouped machines (default)	Last	*Not applicable*

You plan to onboard computers to Microsoft Defender ATP as shown in the following table.

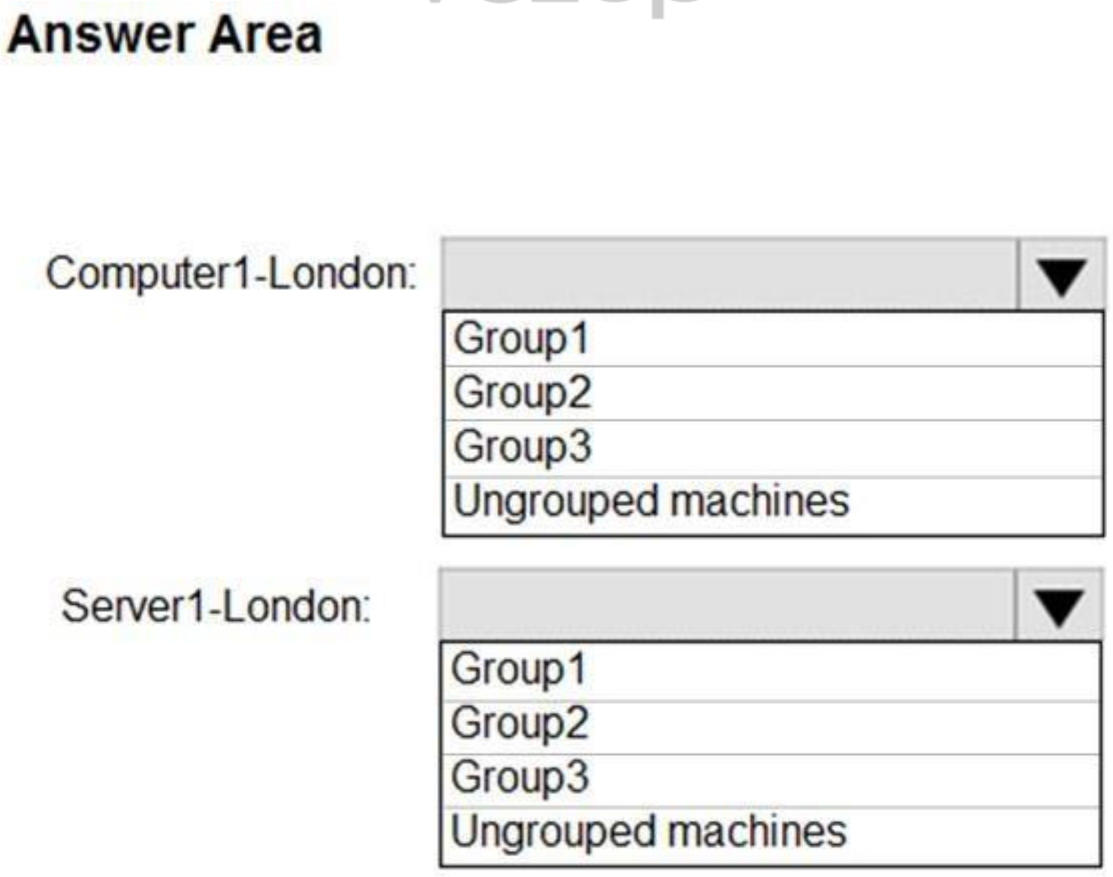


Name	Operating system
Computer1-London	Windows 10
Server1-London	Windows Server 2016

To which machine group will each computer be added? To answer, select the appropriate options in the answer are.

NOTE: Each correct selection is worth one point.

Hot Area:

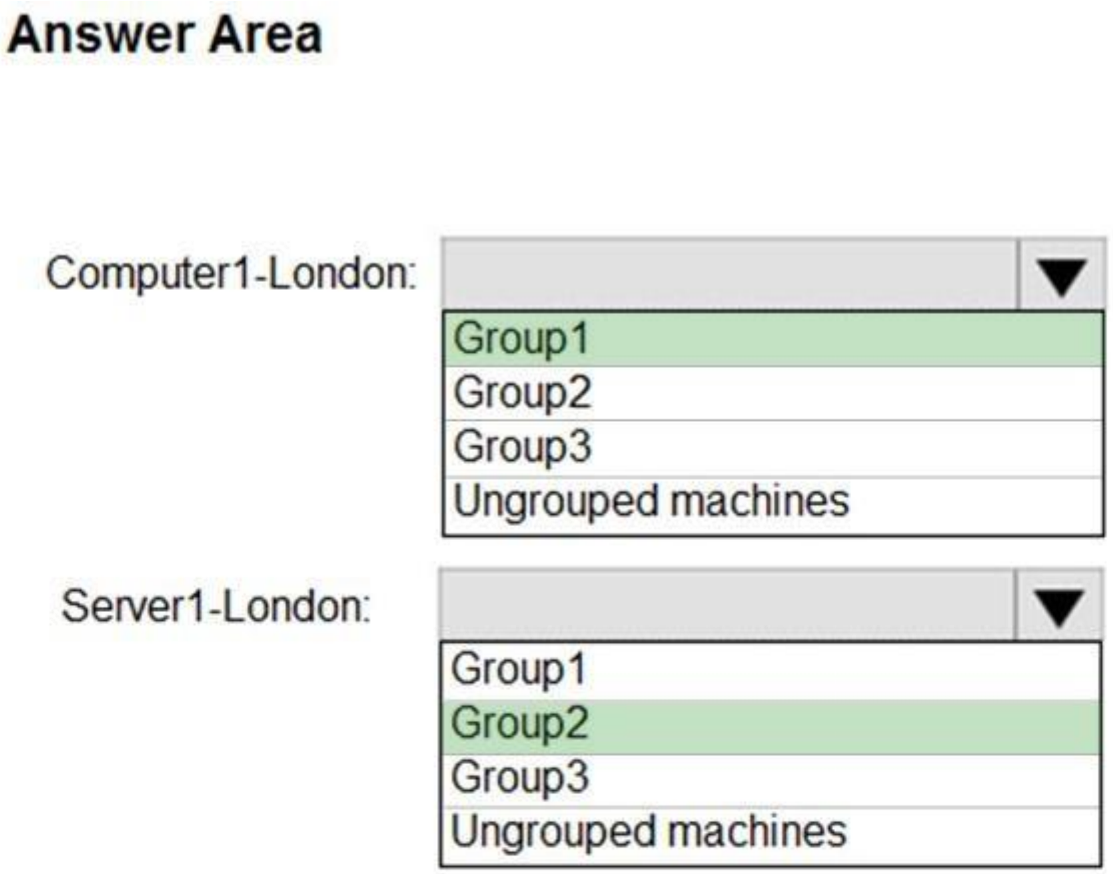


Answer Area

Computer1-London:
- Group1
- Group2
- Group3
- Ungrouped machines

Server1-London:
- Group1
- Group2
- Group3
- Ungrouped machines

Correct Answer:



Answer Area

Computer1-London:

[✓ Group1]
Group2
Group3
Ungrouped machines

Server1-London:

Group1
[✓ Group2]
Group3
Ungrouped machines

Section: [none]
Explanation
Explanation/Reference:

QUESTION 22
Your company has 5,000 Windows 10 devices. All the devices are protected by using Microsoft Defender Advanced Threat Protection (ATP).

You need to create a filtered view that displays which Microsoft Defender ATP alert events have a high severity and occurred during the last seven days.

What should you use in Microsoft Defender ATP?

A. the threat intelligence API
B. Automated investigations
C. Threat analytics
D. Advanced hunting

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-atp/investigate-alerts-windows-defender-advanced-threat-protection https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-atp/automated-investigations-windows-defender-advanced-threat-protection

QUESTION 23
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 subscription.

You need to prevent users from accessing your Microsoft SharePoint Online sites unless the users are connected to your on-premises network.

Solution: From the Device Management admin center, you create a device configuration profile.

Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:

QUESTION 24
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 an Azure Active Directory (Azure AD) tenant that contains a user named User1.

Your company purchases a Microsoft 365 subscription.

You need to ensure that User1 is assigned the required role to create file policies and manage alerts in the Cloud App Security admin center.

Solution: From the Security & Compliance admin center, you assign the Security Administrator role to User1.

Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/cloud-app-security/manage-admins

QUESTION 25
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 an Azure Active Directory (Azure AD) tenant that contains a user named User1.

Your company purchases a Microsoft 365 subscription.

You need to ensure that User1 is assigned the required role to create file policies and manage alerts in the Cloud App Security admin center.

Solution: From the Azure Active Directory admin center, you assign the Security administrator role to User1.

Does this meet the goal?

A. Yes
B. No

Correct Answer: A
Section: [none]
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/cloud-app-security/manage-admins

QUESTION 26
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 an Azure Active Directory (Azure AD) tenant that contains a user named User1.

Your company purchases a Microsoft 365 subscription.

You need to ensure that User1 is assigned the required role to create file policies and manage alerts in the Cloud App Security admin center.

Solution: From the Azure Active Directory admin center, you assign the Compliance administrator role to User1.

Does this meet the goal?

A. Yes
B. No

Correct Answer: A
Section: [none]
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/cloud-app-security/manage-admins

QUESTION 27
HOTSPOT

Your company purchases a cloud app named App1.

You plan to publish App1 by using a conditional access policy named Policy1.

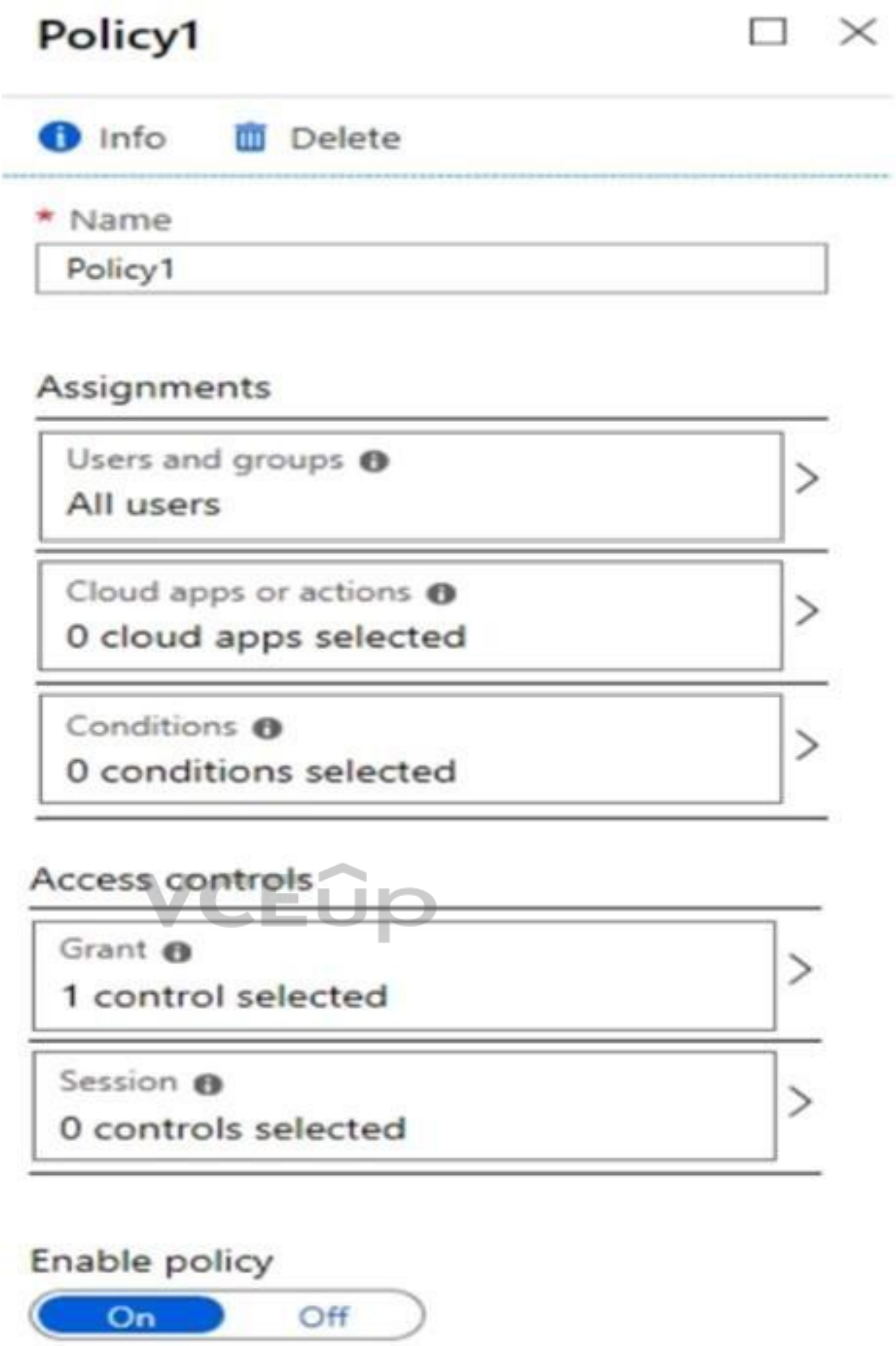
You need to ensure that you can control access to App1 by using a Microsoft Cloud App Security session policy.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area



Policy1

* Name

Policy1

Assignments

Users and groups: All users

Cloud apps or actions: 0 cloud apps selected

Conditions: 0 conditions selected

Access controls

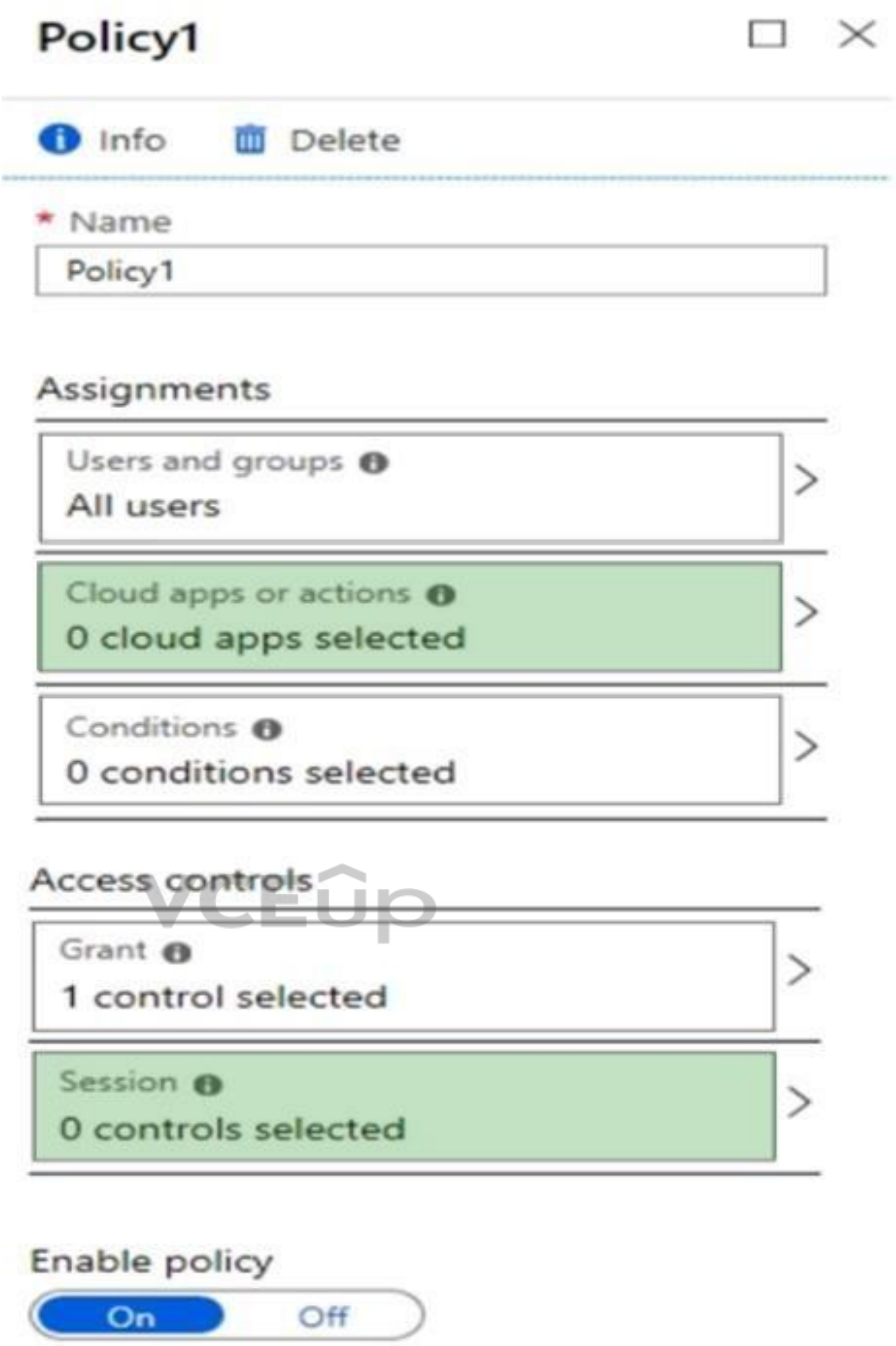
Grant: 1 control selected

Session: 0 controls selected

Enable policy

Correct Answer:

Answer Area



Policy1

* Name

Policy1

Assignments

Users and groups
All users

Cloud apps or actions
0 cloud apps selected

Conditions
0 conditions selected

Access controls

Grant
1 control selected

Session
0 controls selected

Enable policy

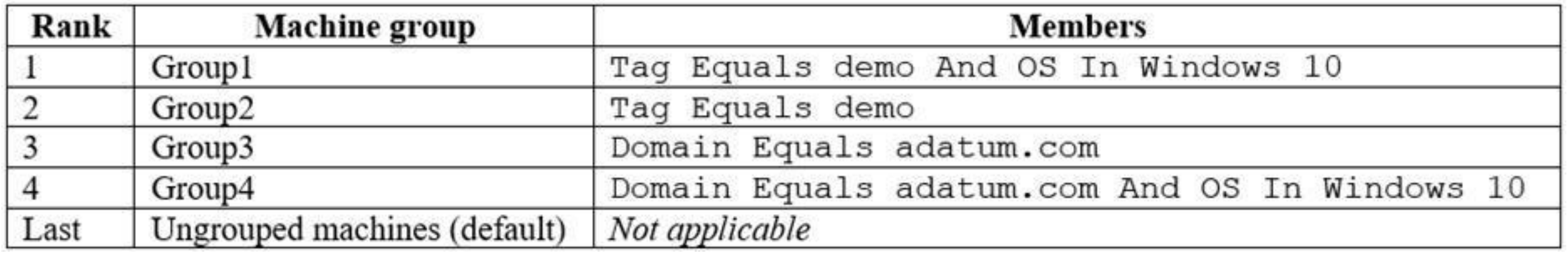
On Off

Section: [none]
Explanation

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

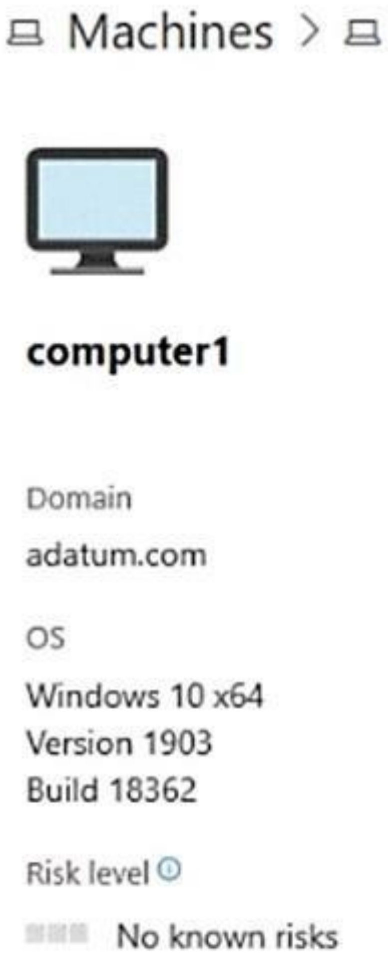
QUESTION 28
HOTSPOT

Your company uses Microsoft Defender Advanced Threat Protection (ATP). Microsoft Defender ATP includes the machine groups shown in the following table.



Rank	Machine group	Members
1	Group1	Tag Equals demo And OS In Windows 10
2	Group2	Tag Equals demo
3	Group3	Domain Equals adatum.com
4	Group4	Domain Equals adatum.com And OS In Windows 10
Last	Ungrouped machines (default)	*Not applicable*

You onboard a computer named computer1 to Microsoft Defender ATP as shown in the following exhibit.



Machines > computer1

computer1

Domain

adatum.com

OS

Windows 10 x64
Version 1903
Build 18362

Risk level

No known risks

Use the drop-down menus to select the answer choice that completes each statement.

NOTE: Each correct selection is worth one point.

Hot Area:

Correct Answer:

Section: [none]
Explanation

Explanation/Reference:

QUESTION 29
HOTSPOT

You have a Microsoft 365 subscription.

You are planning a threat management solution for your organization.

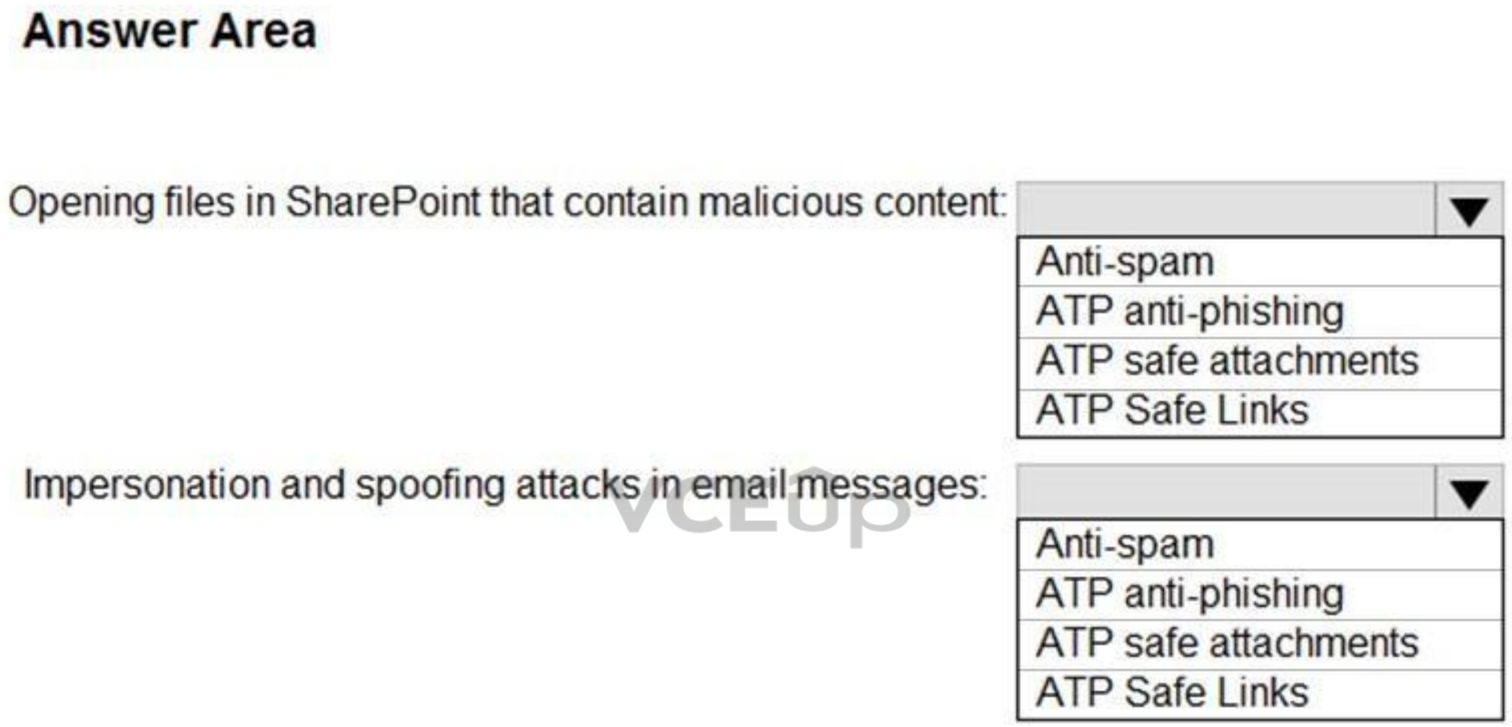
You need to minimize the likelihood that users will be affected by the following threats:

▪ Opening files in Microsoft SharePoint that contain malicious content ▪ Impersonation and spoofing attacks in email messages

Which policies should you create in the Security & Compliance admin center? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

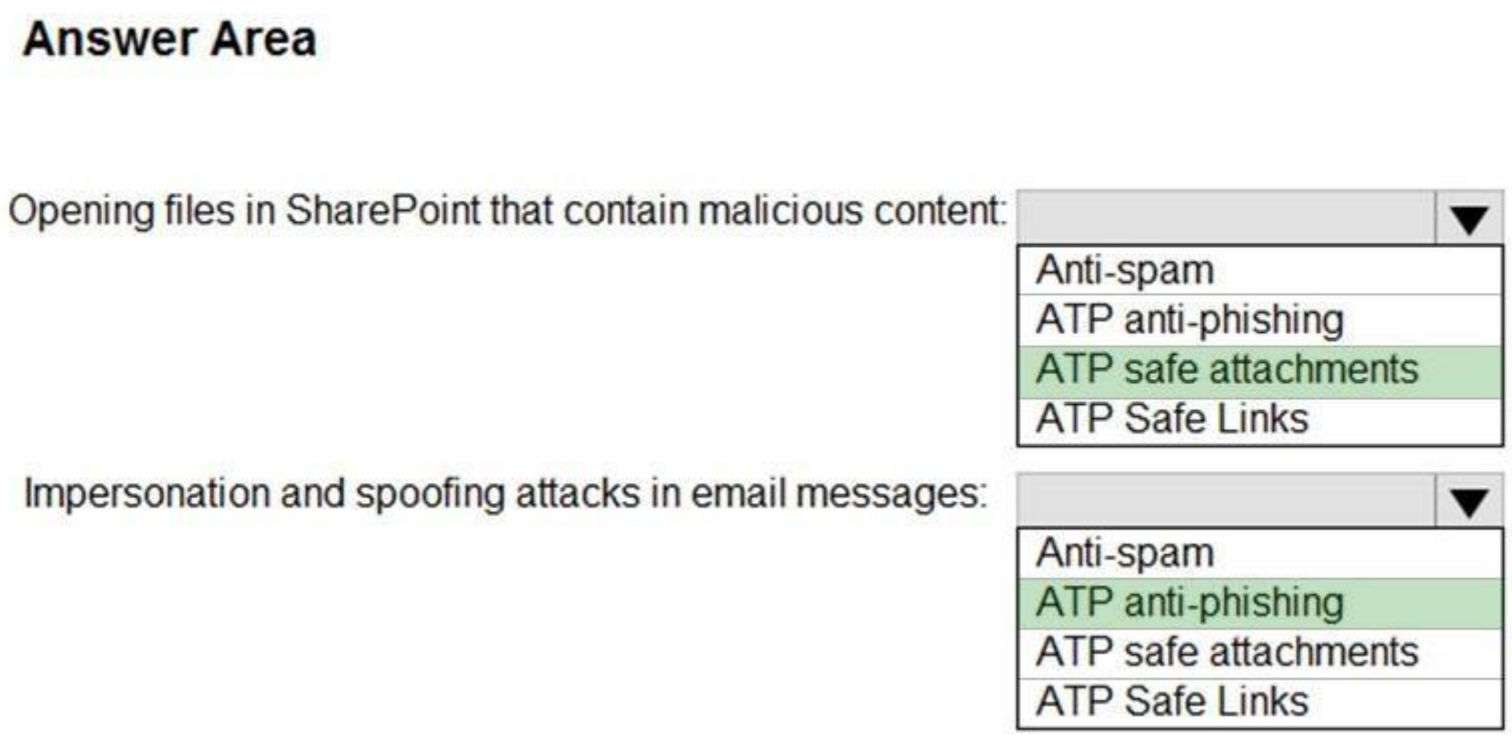


Answer Area

Opening files in SharePoint that contain malicious content: ▼
- Anti-spam
- ATP anti-phishing
- ATP safe attachments
- ATP Safe Links

Impersonation and spoofing attacks in email messages: ▼
- Anti-spam
- ATP anti-phishing
- ATP safe attachments
- ATP Safe Links

Correct Answer:



Answer Area

Opening files in SharePoint that contain malicious content:
- Anti-spam
- ATP anti-phishing
- [✓ ATP safe attachments]
- ATP Safe Links

Impersonation and spoofing attacks in email messages:
- Anti-spam
- [✓ ATP anti-phishing]
- ATP safe attachments
- ATP Safe Links

Section: [none]
Explanation

Explanation/Reference:
Explanation:

Box 1: ATP Safe Attachments
ATP Safe Attachments provides zero-day protection to safeguard your messaging system, by checking email attachments for malicious content. It routes all messages and attachments that do not have a virus/malware signature to a special environment, and then uses machine learning and analysis techniques to detect malicious intent. If no suspicious activity is found, the message is forwarded to the mailbox.

Box 2: ATP anti-phishing
ATP anti-phishing protection detects attempts to impersonate your users and custom domains. It applies machine learning models and advanced impersonation-detection algorithms to avert phishing attacks.

ATP Safe Links provides time-of-click verification of URLs, for example, in emails messages and Office files. Protection is ongoing and applies across your messaging and Office environment. Links are scanned for each click: safe links remain accessible and malicious links are dynamically blocked.

References: https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/office-365-atp#configure-atp-policies

QUESTION 30 You have a Microsoft 365 subscription.

All users have their email stored in Microsoft Exchange Online.

In the mailbox of a user named User1, you need to preserve a copy of all the email messages that contain the word ProjectX.

What should you do first?

A. From Microsoft Cloud App Security, create an access policy.
B. From the Security & Compliance admin center, create an eDiscovery case.
C. From Microsoft Cloud App Security, create an activity policy.
D. From the Security & Compliance admin center, create a data loss prevention (DLP) policy.

Correct Answer: D
Section: [none]
Explanation

Explanation/Reference:
Explanation:
A DLP policy contains a few basic things:
Where to protect the content: locations such as Exchange Online, SharePoint Online, and OneDrive for Business sites, as well as Microsoft Teams chat and channel messages.
When and how to protect the content by enforcing rules comprised of:
Conditions the content must match before the rule is enforced. For example, a rule might be configured to look only for content containing Social Security numbers that's been shared with people outside your organization.
Actions that you want the rule to take automatically when content matching the conditions is found. For example, a rule might be configured to block access to a document and send both the user and compliance officer an email notification.

References: https://docs.microsoft.com/en-us/microsoft-365/compliance/data-loss-prevention-policies

QUESTION 31 You have a Microsoft 365 subscription.

From the subscription, you perform an audit log search, and you download all the results.

You plan to review the audit log data by using Microsoft Excel.

You need to ensure that each audited property appears in a separate Excel column.

What should you do first?

A. From Power Query Editor, transform the JSON data.
B. Format the Operations column by using conditional formatting.
C. Format the AuditData column by using conditional formatting.
D. From Power Query Editor, transform the XML data.

Correct Answer: A
Section: [none]
Explanation

Explanation/Reference:
Explanation:
After you search the Office 365 audit log and download the search results to a CSV file, the file contains a column named AuditData, which contains additional information about each event. The data in this column is formatted as a JSON object, which contains multiple properties that are configured as property:value pairs separated by commas. You can use the JSON transform feature in the Power Query Editor in Excel to split each property in the JSON object in the AuditData column into multiple columns so that each property has its own column. This lets you sort and filter on one or more of these properties

References: https://docs.microsoft.com/en-us/microsoft-365/compliance/export-view-audit-log-records

QUESTION 32 You have a Microsoft 365 subscription.

You need to be notified if users receive email containing a file that has a virus.

What should you do?

A. From the Exchange admin center, create a spam filter policy.
B. From the Security & Compliance admin center, create a data governance event.
C. From the Security & Compliance admin center, create an alert policy.
D. From the Exchange admin center, create a mail flow rule.

Correct Answer: C
Section: [none]
Explanation

Explanation/Reference:
Explanation:

You can create alert policies to track malware activity and data loss incidents. We've also included several default alert policies that help you monitor activities such as assigning admin privileges in Exchange Online, malware attacks, phishing campaigns, and unusual levels of file deletions and external sharing.

The **Email messages containing malware removed after delivery** default alert generates an alert when any messages containing malware are delivered to mailboxes in your organization.

Incorrect answers:
A: A spam filter policy includes selecting the action to take on messages that are identified as spam. Spam filter policy settings are applied to inbound messages.

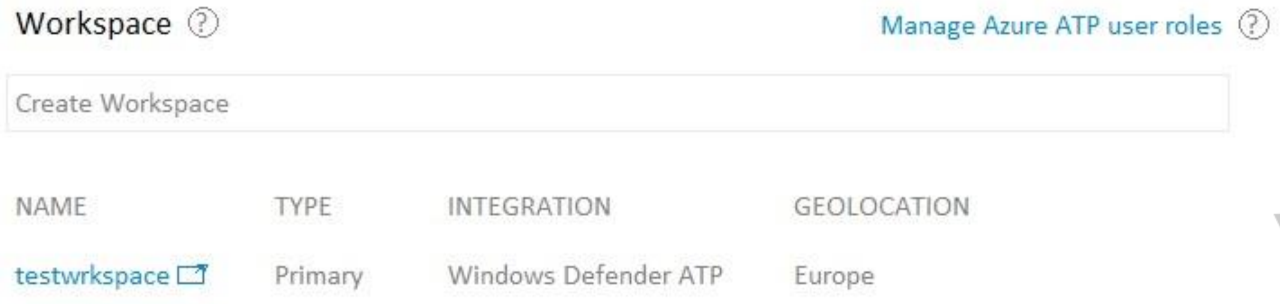
B: A data governance event commences when an administrator creates it, following which background processes look for content relating to the event and take the retention action defined in the label. The retention action can be to keep or remove items, or to mark them for manual disposition.

D: You can inspect email attachments in your Exchange Online organization by setting up mail flow rules. Exchange Online offers mail flow rules that provide the ability to examine email attachments as a part of your messaging security and compliance needs. However, mail flow rules are not used to detect malware in emails.

Reference:
https://docs.microsoft.com/en-us/office365/securitycompliance/alert-policies

QUESTION 33
DRAG DROP

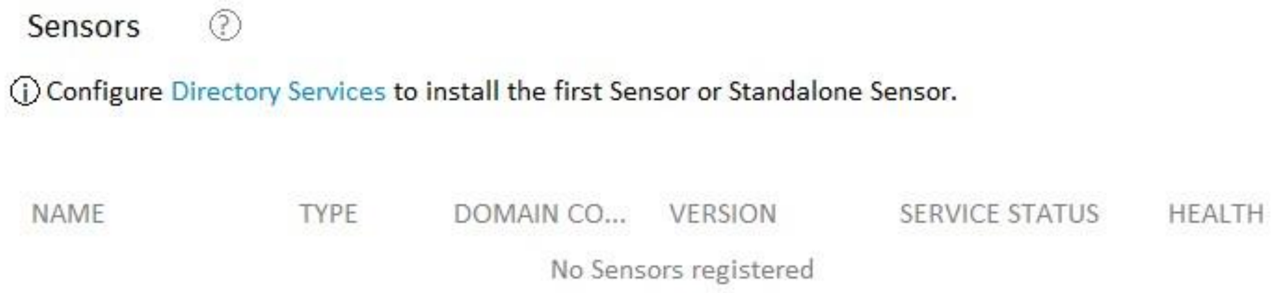
You have the Microsoft Azure Advanced Threat Protection (ATP) workspace shown in the Workspace exhibit. (Click the **Workspace** tab.)



Workspace ⓘ Manage Azure ATP user roles ⓘ

NAME	TYPE	INTEGRATION	GEOLOCATION
testwrkspace	Primary	Windows Defender ATP	Europe

The sensors settings for the workspace are configured as shown in the Sensors exhibit. (Click the **Sensors** tab.)



Sensors ⓘ

ⓘ Configure Directory Services to install the first Sensor or Standalone Sensor.

NAME	TYPE	DOMAIN CO...	VERSION	SERVICE STATUS	HEALTH
		No Sensors registered			

You need to ensure that Azure ATP stores data in Asia.

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.

Select and Place:

Correct Answer:

Section: [none]
Explanation

Explanation/Reference:

QUESTION 34

Your company has five security information and event management (SIEM) appliances. The traffic logs from each appliance are saved to a file share named Logs.

You need to analyze the traffic logs.

What should you do from Microsoft Cloud App Security?

A. Click **Investigate**, and then click **Activity log**.
B. Click **Control**, and then click **Policies**. Create a file policy.
C. Click **Discover**, and then click **Create snapshot report**.
D. Click **Investigate**, and then click **Files**.

Correct Answer: A
Section: [none]
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/office365/securitycompliance/investigate-an-activity-in-office-365-cas

QUESTION 35
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 an Azure Active Directory (Azure AD) tenant that contains a user named User1.

Your company purchases a Microsoft 365 subscription.

You need to ensure that User1 is assigned the required role to create file policies and manage alerts in the Cloud App Security admin center.

Solution: From the Cloud App Security admin center, you assign the App/instance admin role for all Microsoft Online Services to User1.

Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:
Explanation:
App/instance admin: Has full or read-only permissions to all of the data in Microsoft Cloud App Security that deals exclusively with the specific app or instance of an app selected.

Reference: https://docs.microsoft.com/en-us/cloud-app-security/manage-admins

QUESTION 36
Your company has a Microsoft 365 subscription that uses an Azure Active Directory (Azure AD) tenant named contoso.com.

The tenant is configured to use Azure AD Identity Protection.

You plan to use an application named App1 that creates reports of Azure AD Identity Protection usage.

You register App1 in the tenant.

You need to ensure that App1 can read the risk event information of contoso.com.

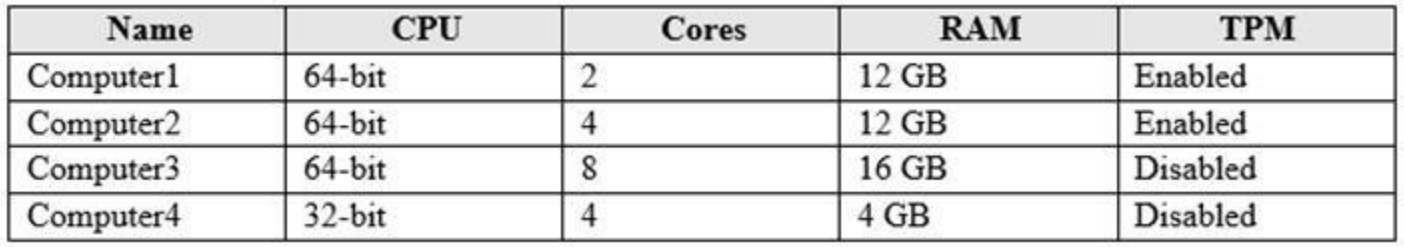
To which API should you delegate permissions?

A. Windows Azure Service Management API
B. Windows Azure Active Directory
C. Microsoft Graph
D. Office 365 Management

Correct Answer: C
Section: [none]
Explanation

Explanation/Reference:
Reference:
https://docs.microsoft.com/en-us/graph/api/resources/identityprotection-root?view=graph-rest-beta

QUESTION 37
Your company has a Microsoft 365 subscription that uses an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant contains computers that run Windows 10 Enterprise and are managed by using Microsoft Intune. The computers are configured as shown in the following table.



Name	CPU	Cores	RAM	TPM
Computer1	64-bit	2	12 GB	Enabled
Computer2	64-bit	4	12 GB	Enabled
Computer3	64-bit	8	16 GB	Disabled
Computer4	32-bit	4	4 GB	Disabled

You plan to implement Windows Defender Application Guard for contoso.com.

You need to identify on which two Windows 10 computers Windows Defender Application Guard can be installed.

Which two computers should you identify? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Computer1
B. Computer3
C. Computer2
D. Computer4

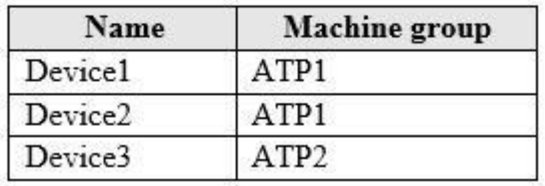
Correct Answer: BC
Section: [none]
Explanation

Explanation/Reference:
Reference:
https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-guard/reqs-wd-app-guard

QUESTION 38
HOTSPOT

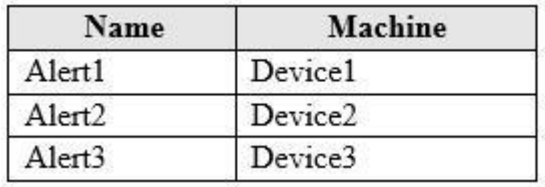
Your company uses Microsoft Defender Advanced Threat Protection (Microsoft Defender ATP).

The devices onboarded to Microsoft Defender ATP are shown in the following table.



Name	Machine group
Device1	ATP1
Device2	ATP1
Device3	ATP2

The alerts visible in the Microsoft Defender ATP alerts queue are shown in the following table.



Name	Machine
Alert1	Device1
Alert2	Device2
Alert3	Device3

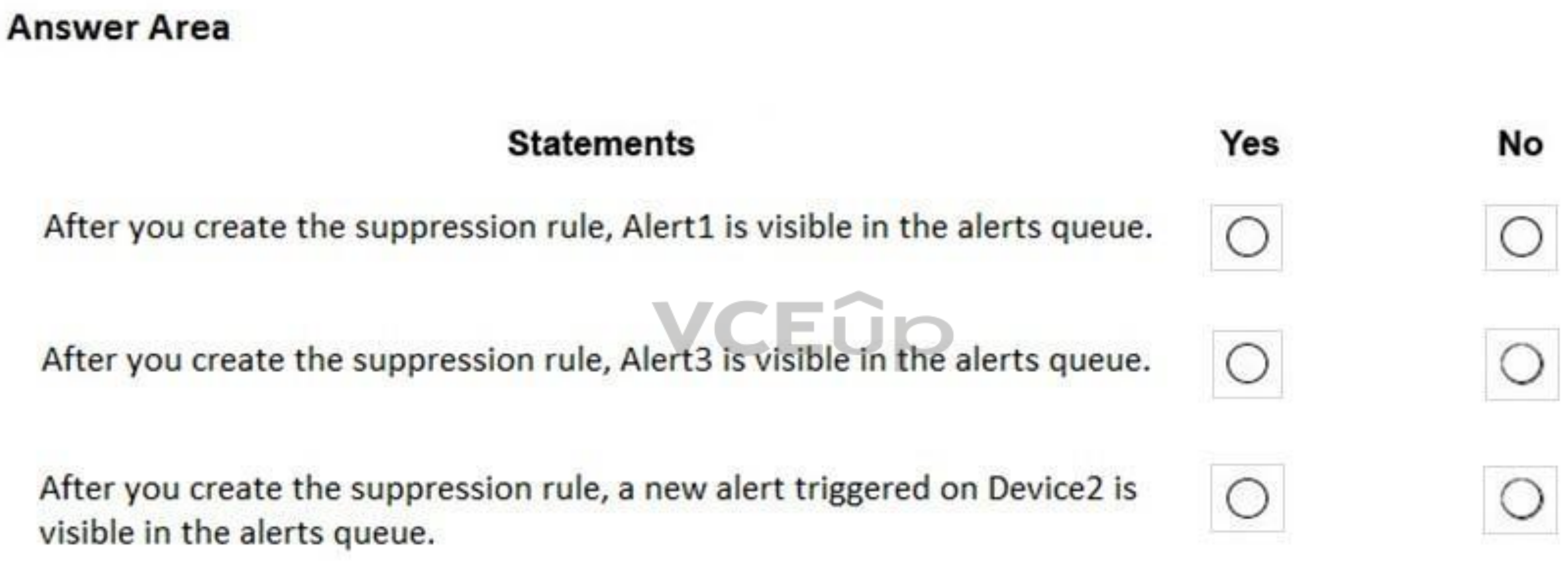
You create a suppression rule that has the following settings:

- Triggering IOC: Any IOC
- Action: Hide alert
- Suppression scope: Alerts on ATP1 machine group

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

NOTE: Each correct selection is worth one point.

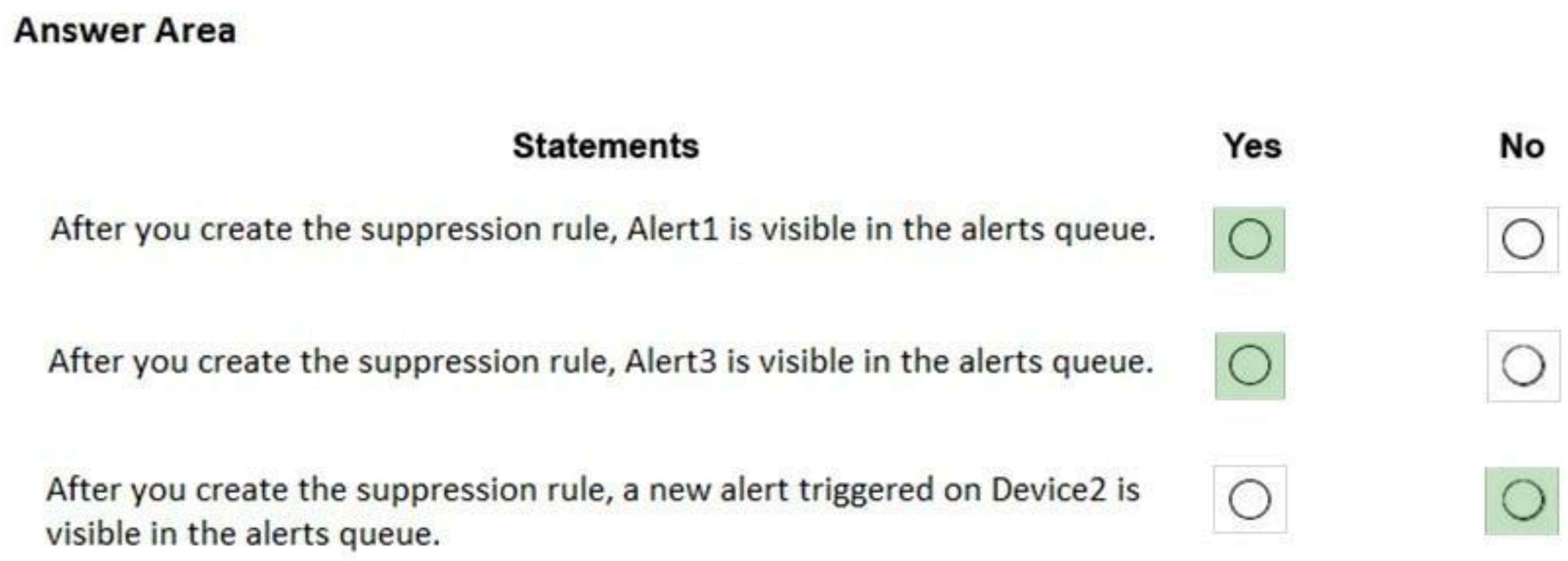
Hot Area:



Answer Area

Statements	Yes	No
After you create the suppression rule, Alert1 is visible in the alerts queue.	○	○
After you create the suppression rule, Alert3 is visible in the alerts queue.	○	○
After you create the suppression rule, a new alert triggered on Device2 is visible in the alerts queue.	○	○

Correct Answer:



Answer Area

Statements	Yes	No
After you create the suppression rule, Alert1 is visible in the alerts queue.	[✓ ○]	○
After you create the suppression rule, Alert3 is visible in the alerts queue.	[✓ ○]	○
After you create the suppression rule, a new alert triggered on Device2 is visible in the alerts queue.	○	[✓ ○]

Section: [none]
Explanation

Explanation/Reference:
Explanation:

A suppression rule will not affect alerts that are already in the alerts queue. Only new alerts will be suppressed.

QUESTION 39
HOTSPOT

Your company has a Microsoft 365 subscription.

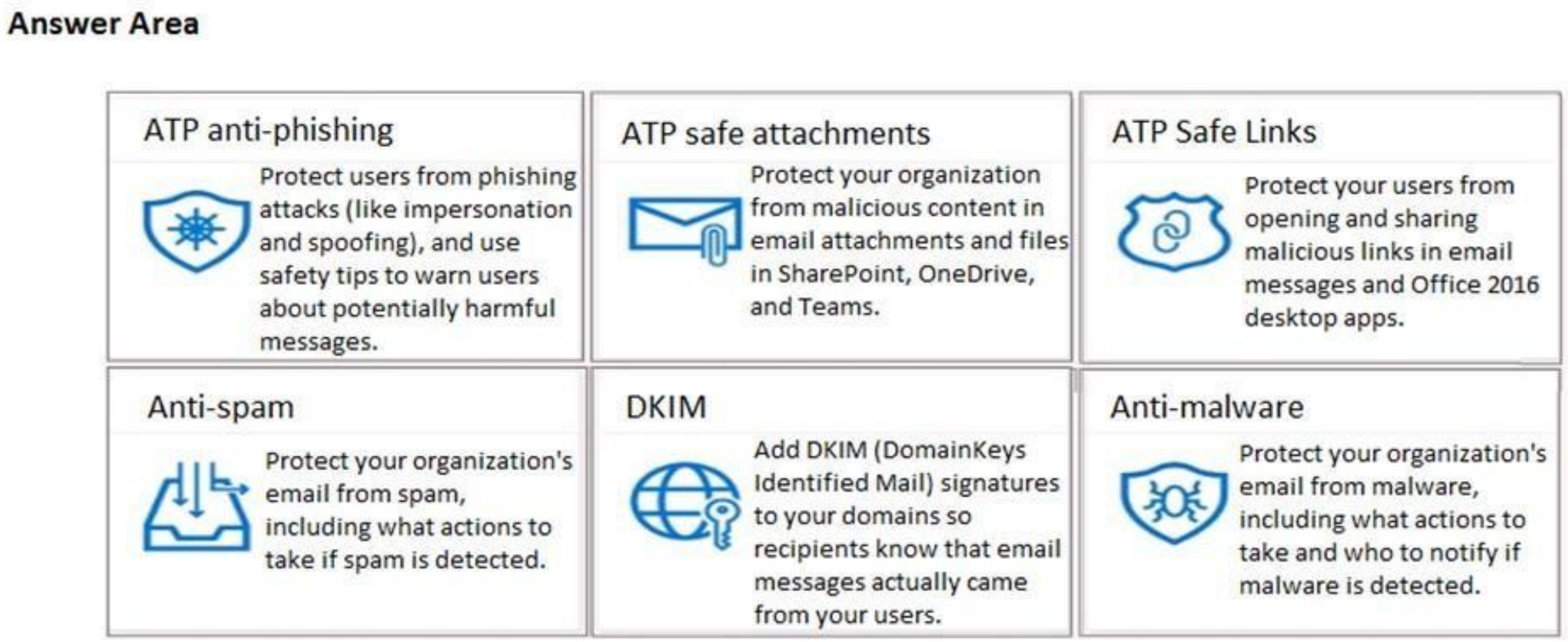
You need to configure Microsoft 365 to meet the following requirements:

▪ Malware found in email attachments must be quarantined for 20 days. ▪ The
email address of senders to your company must be verified.

Which two options should you configure in the Security & Compliance admin center? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

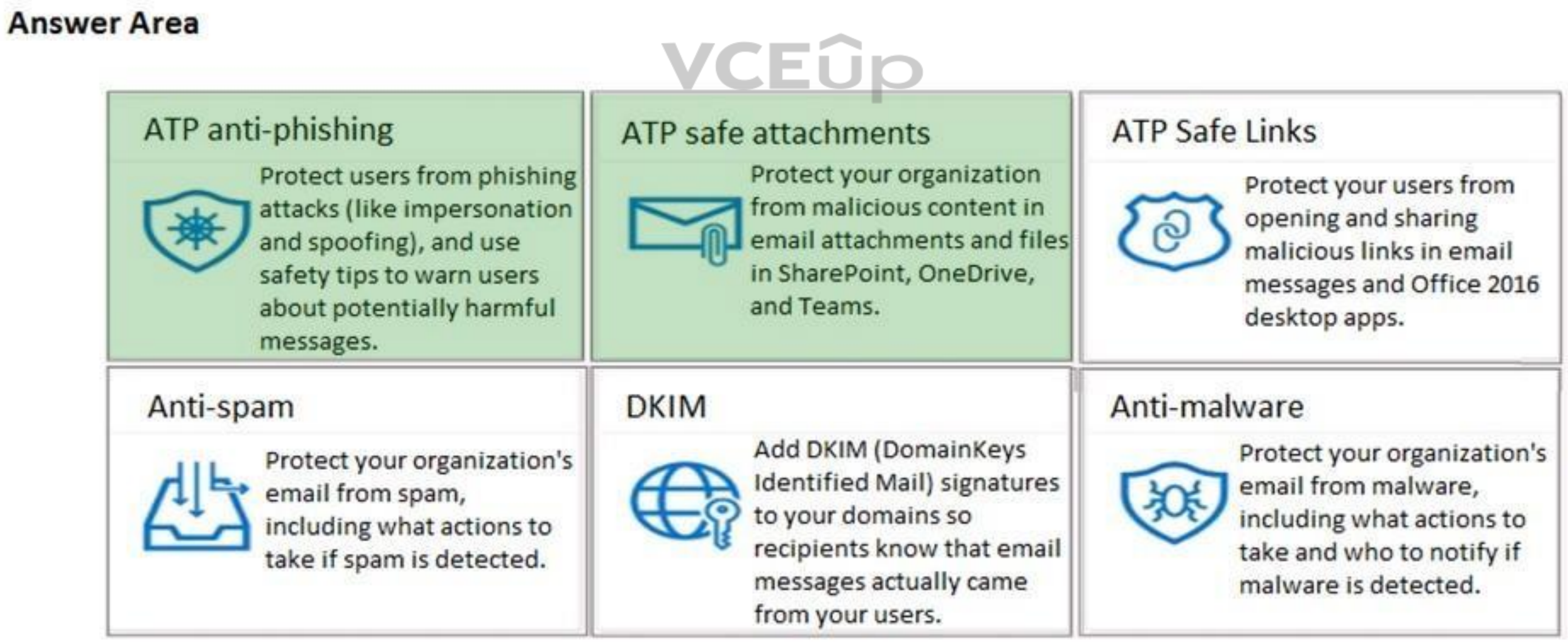
Hot Area:



Answer Area

ATP anti-phishing Protect users from phishing attacks (like impersonation and spoofing), and use safety tips to warn users about potentially harmful messages.	ATP safe attachments Protect your organization from malicious content in email attachments and files in SharePoint, OneDrive, and Teams.	ATP Safe Links Protect your users from opening and sharing malicious links in email messages and Office 2016 desktop apps.
Anti-spam Protect your organization's email from spam, including what actions to take if spam is detected.	DKIM Add DKIM (DomainKeys Identified Mail) signatures to your domains so recipients know that email messages actually came from your users.	Anti-malware Protect your organization's email from malware, including what actions to take and who to notify if malware is detected.

Correct Answer:



Answer Area

🟩 ATP anti-phishing Protect users from phishing attacks (like impersonation and spoofing), and use safety tips to warn users about potentially harmful messages.	🟩 ATP safe attachments Protect your organization from malicious content in email attachments and files in SharePoint, OneDrive, and Teams.	ATP Safe Links Protect your users from opening and sharing malicious links in email messages and Office 2016 desktop apps.
Anti-spam Protect your organization's email from spam, including what actions to take if spam is detected.	DKIM Add DKIM (DomainKeys Identified Mail) signatures to your domains so recipients know that email messages actually came from your users.	Anti-malware Protect your organization's email from malware, including what actions to take and who to notify if malware is detected.

Section: [none]
Explanation

Explanation/Reference:

QUESTION 40

You have a Microsoft 365 subscription that uses Microsoft Defender Advanced Threat Protection (Microsoft Defender ATP).

All the devices in your organization are onboarded to Microsoft Defender ATP.

You need to ensure that an alert is generated if malicious activity was detected on a device during the last 24 hours.

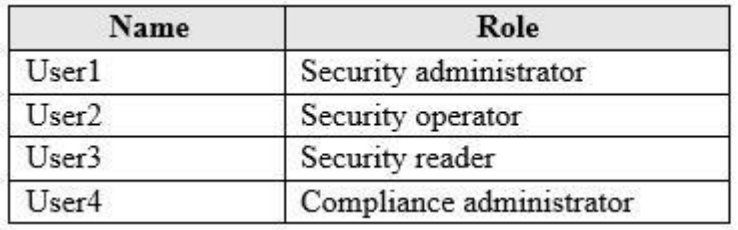
What should you do?

A. From Alerts queue, create a suppression rule and assign an alert
B. From the Security & Compliance admin center, create an audit log search
C. From Advanced hunting, create a query and a detection rule
D. From the Security & Compliance admin center, create a data loss prevention (DLP) policy

Correct Answer: C
Section: [none]
Explanation

Explanation/Reference:
Reference:
https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/custom-detection-rules

QUESTION 41
You have an Azure Active Directory (Azure AD) tenant and a Microsoft 365 E5 subscription. The tenant contains the users shown in the following table.



Name	Role
User1	Security administrator
User2	Security operator
User3	Security reader
User4	Compliance administrator

You plan to implement Microsoft Defender Advanced Threat Protection (Microsoft Defender ATP).

You verify that role-based access control (RBAC) is turned on in Microsoft Defender ATP.

You need to identify which user can view security incidents from the Microsoft Defender Security Center.

Which user should you identify?

A. User1
B. User2
C. User3
D. User4

Correct Answer: A
Section: [none]
Explanation

Explanation/Reference:

QUESTION 42
Your network contains an on-premises Active Directory domain named contoso.com. The domain contains 1,000 Windows 10 devices.

You perform a proof of concept (PoC) deployment of Microsoft Defender Advanced Threat Protection (ATP) for 10 test devices. During the onboarding process, you configure Microsoft Defender ATP-related data to be stored in the United States.

You plan to onboard all the devices to Microsoft Defender ATP.

You need to store the Microsoft Defender ATP data in Europe.

What should you do first?

A. Create a workspace.
B. Onboard a new device.
C. Delete the workspace.
D. Offboard the test devices.

Correct Answer: D
Section: [none]
Explanation

Explanation/Reference:

QUESTION 43 You have a Microsoft 365 subscription.

You need to be notified if users receive email containing a file that has a virus.

What should you do?

A. From the Exchange admin center, create an in-place eDiscovery & hold.
B. From the Security & Compliance admin center, create a data governance event.
C. From the Exchange admin center, create an anti-malware policy.
D. From the Exchange admin center, create a mail flow rule.

Correct Answer: C
Section: [none]
Explanation

Explanation/Reference:
Reference: https://docs.microsoft.com/en-us/office365/servicedescriptions/exchange-online-service-description/anti-spam-and-anti-malware-protection

QUESTION 44 You have a Microsoft 365 subscription that contains 500 users.

You have several hundred computers that run the 64-bit version of Windows 10 Enterprise and have the following configurations:

- Two volumes that contain data
- A CPU that has two cores
- TPM disabled
- 4 GB of RAM

All the computers are managed by using Microsoft Endpoint Manager.

You need to ensure that you can turn on Windows Defender Application Guard on the computers.

What should you do first?

A. Modify the edition of Windows 10.
B. Create an additional volume.
C. Replace the CPU and enable TPM.
D. Replace the CPU and increase the RAM.

Correct Answer: D
Section: [none]
Explanation

Explanation/Reference:
Explanation:
The computers need 4 CPU cores and 8GB of RAM.

Reference: https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-guard/reqs-wd-app-guard

QUESTION 45 You have a Microsoft 365 E5 subscription that uses Microsoft Defender Advanced Threat Protection (Microsoft Defender ATP).

From Microsoft Defender ATP, you turn on the Allow or block file advanced feature.

You need to block users from downloading a file named File1.exe.

What should you use?

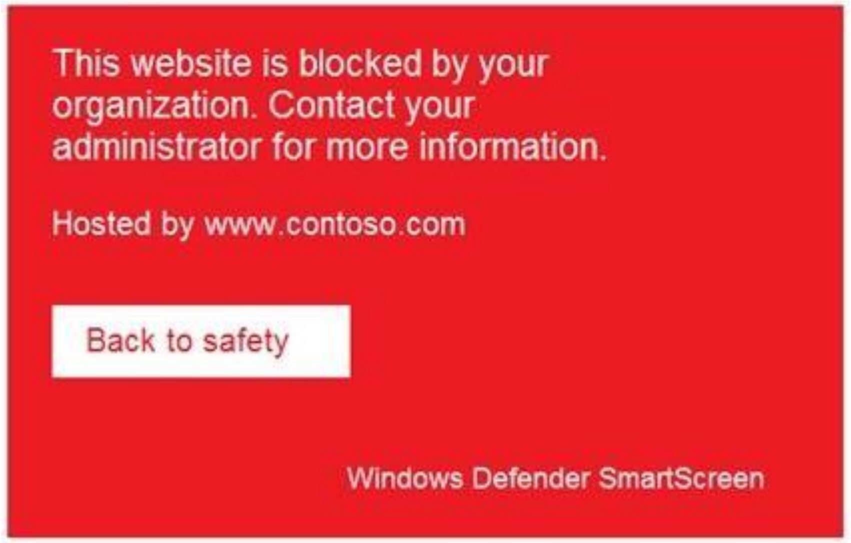
A. a suppression rule
B. an indicator
C. a device configuration profile

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:
Reference: https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/respond-file-alerts#allow-or-block-file

QUESTION 46 You have a Microsoft 365 E5 subscription that uses Microsoft Defender Advanced Threat Protection (Microsoft Defender ATP).

When users attempt to access the portal of a partner company, they receive the message shown in the following exhibit.



This website is blocked by your organization. Contact your administrator for more information.

Hosted by www.contoso.com

Back to safety

Windows Defender SmartScreen

You need to enable user access to the partner company's portal.

Which Microsoft Defender ATP setting should you modify?

A. Custom detections
B. Advanced hunting
C. Alert notifications

D. Indicators
E. Alert suppression

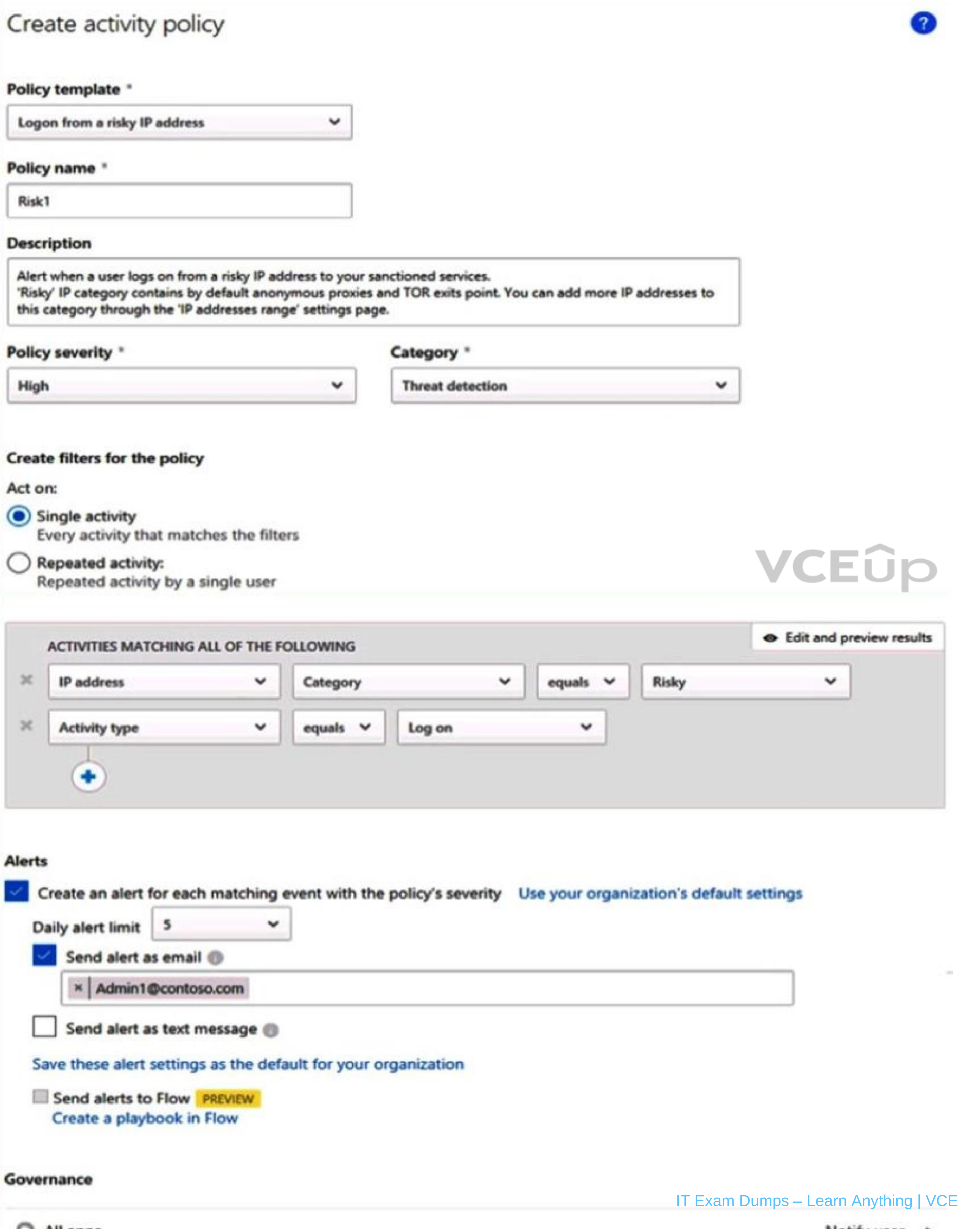
Correct Answer: D
Section: [none]
Explanation

Explanation/Reference:
Reference: https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/manage-indicators

QUESTION 47
HOTSPOT

You have a Microsoft 365 subscription.

You create a Microsoft Cloud App Security policy named Risk1 based on the Logon from a risky IP address template as shown in the following exhibit.



Create activity policy

Policy template *

Logon from a risky IP address

Policy name *

Risk1

Description

Alert when a user logs on from a risky IP address to your sanctioned services.
'Risky' IP category contains by default anonymous proxies and TOR exits point. You can add more IP addresses to this category through the 'IP addresses range' settings page.

Policy severity *

High

Category *

Threat detection

Create filters for the policy

Act on:

● Single activity
Every activity that matches the filters

○ Repeated activity:
Repeated activity by a single user

ACTIVITIES MATCHING ALL OF THE FOLLOWING

IP address | Category | equals | Risky

Activity type | equals | Log on

Alerts

☑ Create an alert for each matching event with the policy's severity Use your organization's default settings

Daily alert limit 5

☑ Send alert as email

Admin1@contoso.com

□ Send alert as text message

Save these alert settings as the default for your organization

□ Send alerts to Flow PREVIEW
Create a playbook in Flow

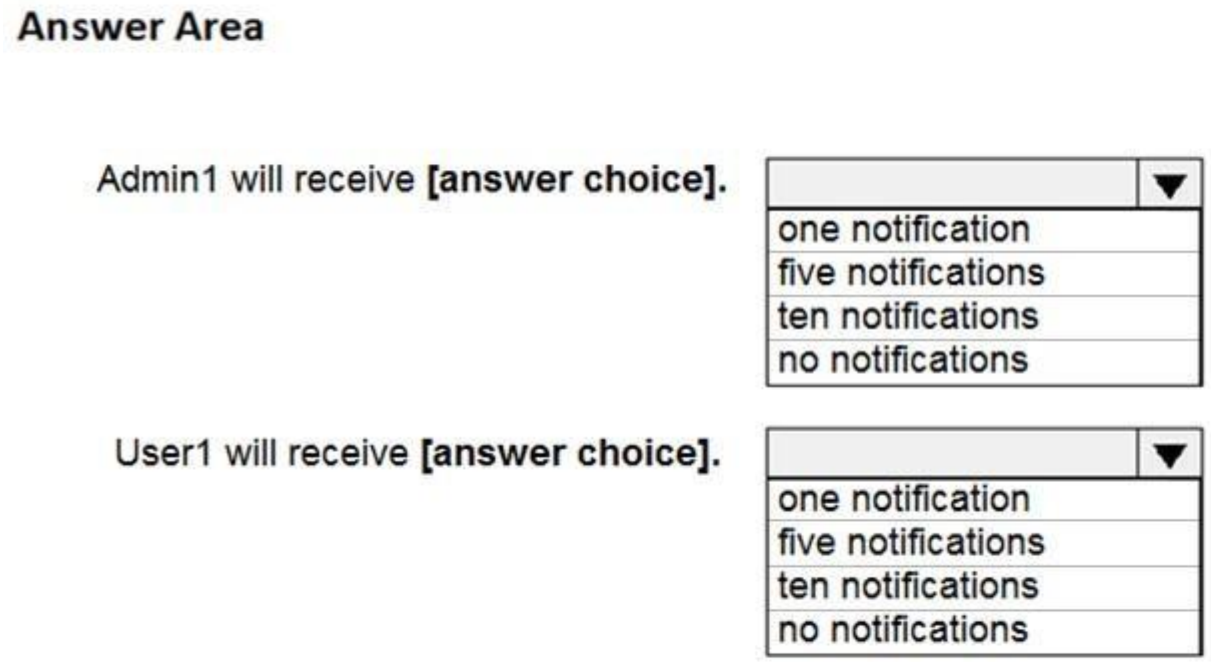
Governance

You have two users named User1 and User2. Each user signs in to Microsoft SharePoint Online from a risky IP address 10 times within 24 hours.

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:



Answer Area

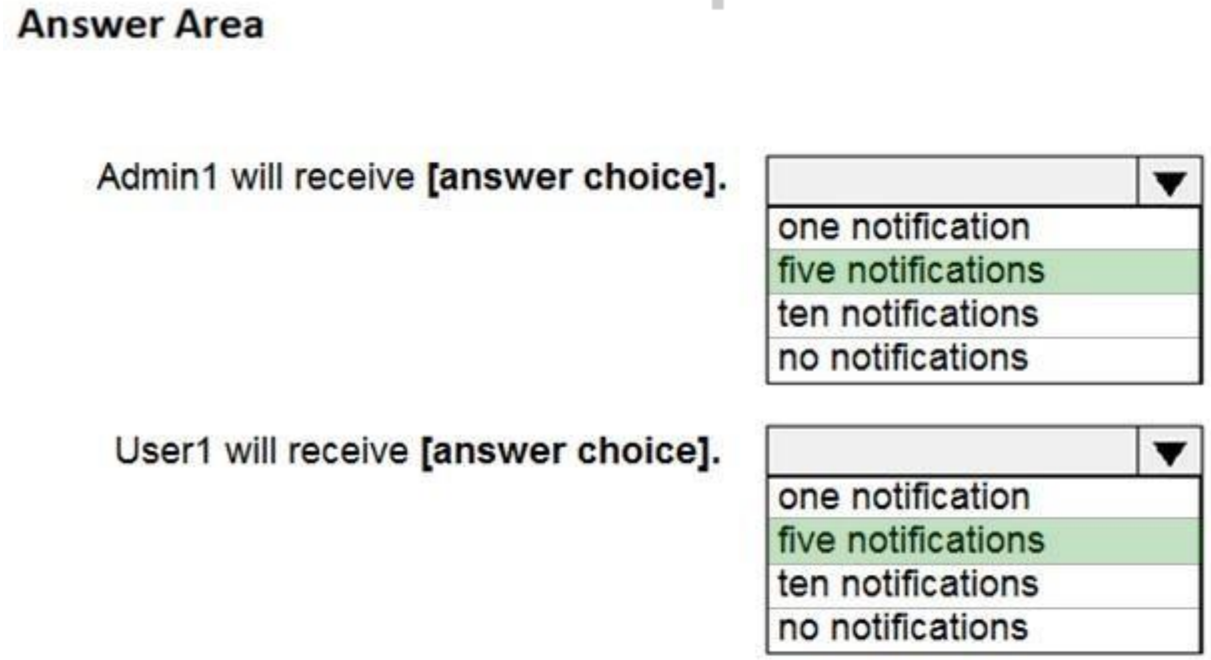
Admin1 will receive **[answer choice].**

- one notification
- five notifications
- ten notifications
- no notifications

User1 will receive **[answer choice].**

- one notification
- five notifications
- ten notifications
- no notifications

Correct Answer:



Answer Area

Admin1 will receive **[answer choice].**

- one notification
- [✓ five notifications]
- ten notifications
- no notifications

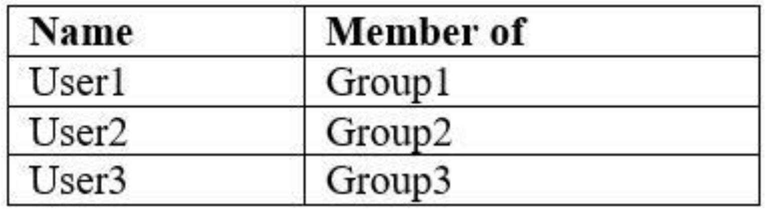
User1 will receive **[answer choice].**

- one notification
- [✓ five notifications]
- ten notifications
- no notifications

Section: [none]
Explanation

Explanation/Reference:
QUESTION 48
HOTSPOT

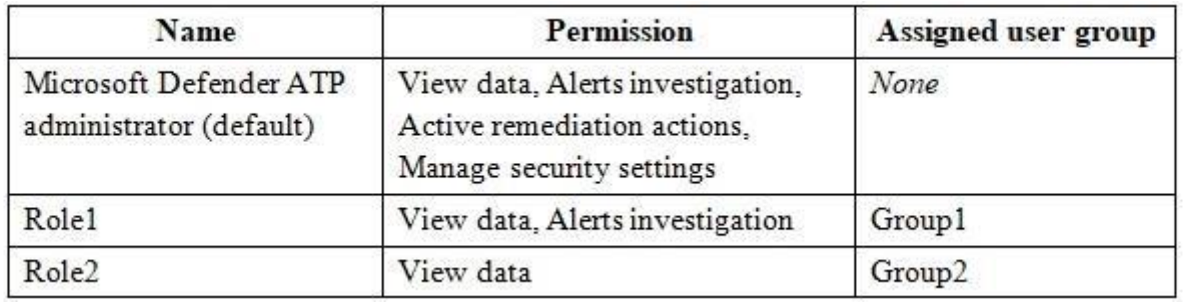
You have a Microsoft Azure Activity Directory (Azure AD) tenant contains the users shown in the following table.



Name	Member of
User1	Group1
User2	Group2
User3	Group3

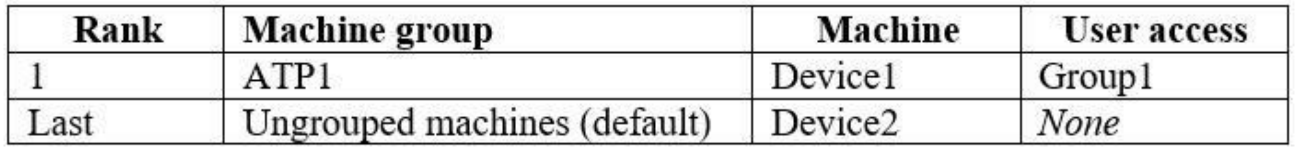
Group3 is a member of Group1.

Your company uses Microsoft Defender Advanced Threat Protection (ATP). Microsoft Defender ATP contains the roles shown in the following table.



Name	Permission	Assigned user group
Microsoft Defender ATP administrator (default)	View data, Alerts investigation, Active remediation actions, Manage security settings	*None*
Role1	View data, Alerts investigation	Group1
Role2	View data	Group2

Microsoft Defender ATP contains the device groups shown in the following table.



Rank	Machine group	Machine	User access
1	ATP1	Device1	Group1
Last	Ungrouped machines (default)	Device2	*None*

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:

Section: [none]
Explanation

Explanation/Reference:

QUESTION 49
HOTSPOT

Your company uses Microsoft Cloud App Security.

You plan to integrate Cloud App Security and security information and event management (SIEM).

You need to deploy a SIEM agent on a server that runs Windows Server 2016.

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

NOTE: Each correct selection is worth one point.

Hot Area:

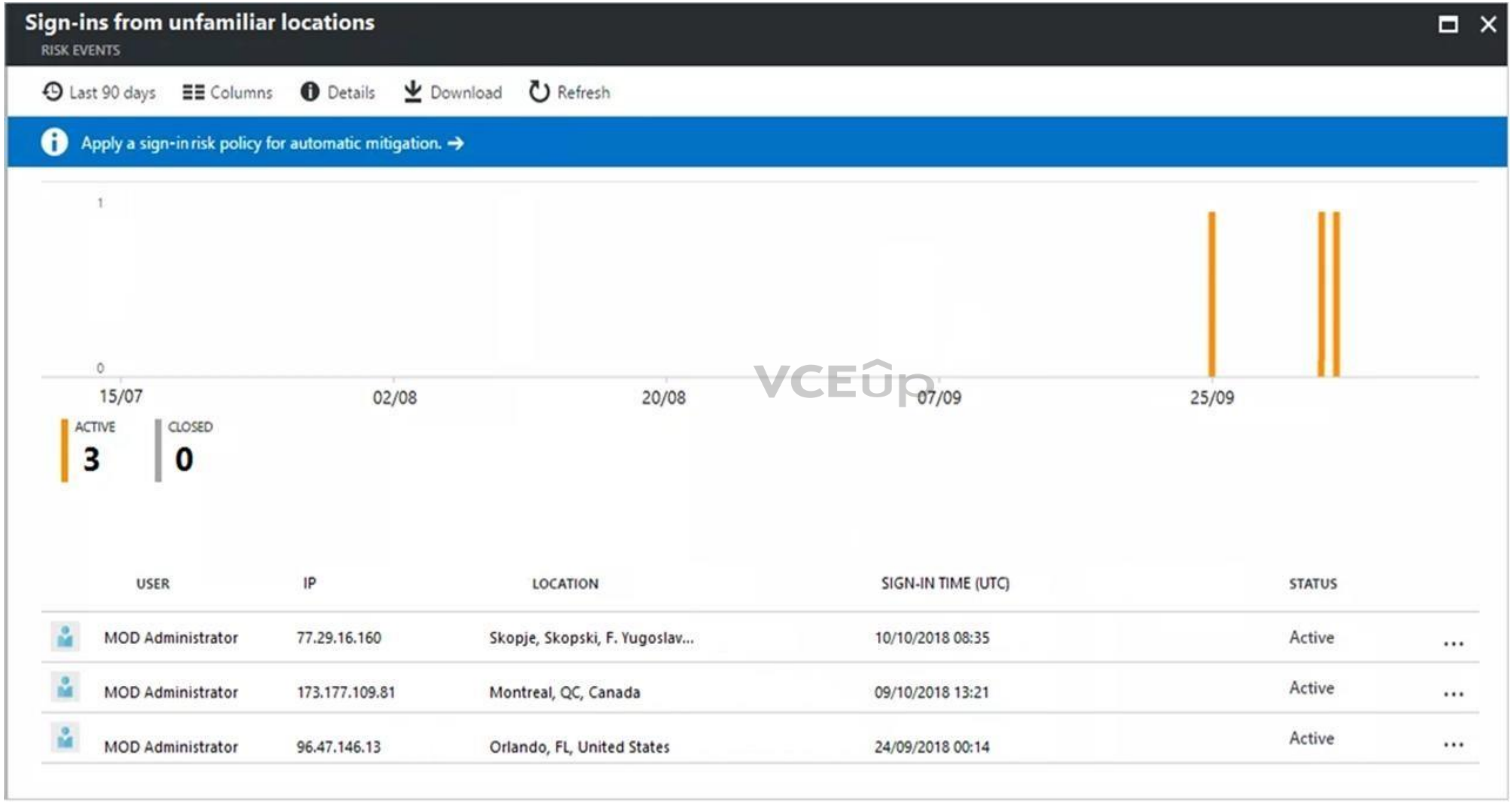
Correct Answer:

Section: [none]
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/office365/securitycompliance/integrate-your-siem-server-with-office-365-cas

QUESTION 50
HOTSPOT

From the Microsoft Azure Active Directory (Azure AD) Identity Protection dashboard, you view the risk events shown in the following exhibit.



Sign-ins from unfamiliar locations

RISK EVENTS

USER	IP	LOCATION	SIGN-IN TIME (UTC)	STATUS
MOD Administrator	77.29.16.160	Skopje, Skopski, F. Yugoslav...	10/10/2018 08:35	Active
MOD Administrator	173.177.109.81	Montreal, QC, Canada	09/10/2018 13:21	Active
MOD Administrator	96.47.146.13	Orlando, FL, United States	24/09/2018 00:14	Active

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:

Correct Answer:

Section: [none]
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-getstarted

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

https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/quickstart-configure-named-locations

QUESTION 51 Your company uses Microsoft Azure Advanced Threat Protection (ATP) and Microsoft Defender ATP.

You need to integrate Microsoft Defender ATP and Azure ATP.

What should you do?

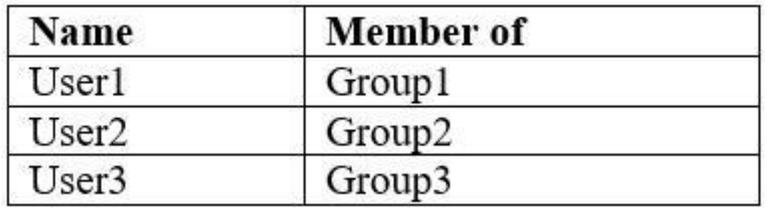
A. From Azure ATP, configure the notifications and reports.
B. From Azure ATP, configure the data sources.
C. From Microsoft Defender Security Center, configure the Machine management settings.
D. From Microsoft Defender Security Center, configure the General settings.

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/azure-advanced-threat-protection/integrate-wd-atp

QUESTION 52
HOTSPOT

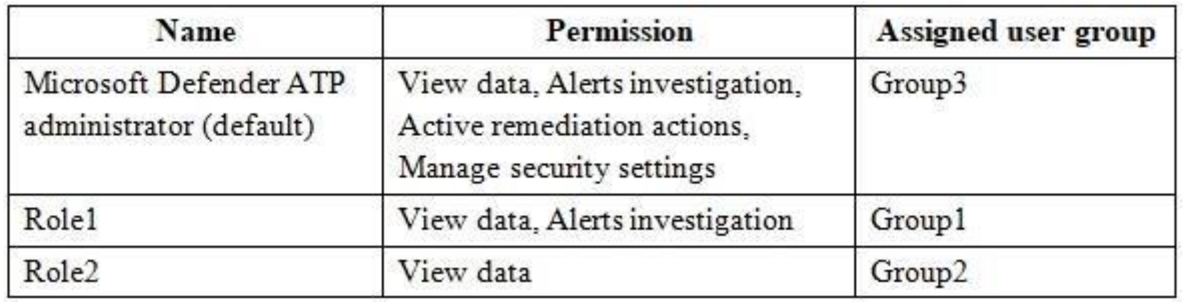
You have a Microsoft Azure Activity Directory (Azure AD) tenant contains the users shown in the following table.



Name	Member of
User1	Group1
User2	Group2
User3	Group3

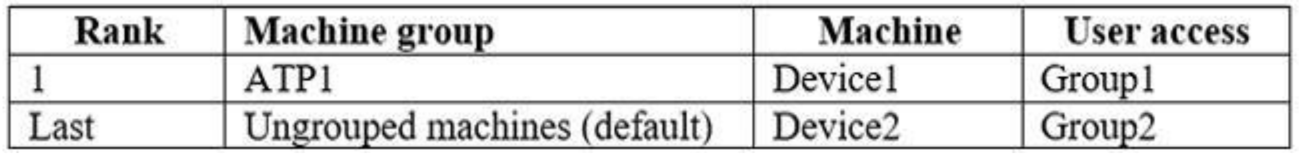
Group3 is a member of Group1.

Your company uses Microsoft Defender Advanced Threat Protection (ATP). Microsoft Defender ATP contains the roles shown in the following table.



Name	Permission	Assigned user group
Microsoft Defender ATP administrator (default)	View data, Alerts investigation, Active remediation actions, Manage security settings	Group3
Role1	View data, Alerts investigation	Group1
Role2	View data	Group2

Microsoft Defender ATP contains the device groups shown in the following table.



Rank	Machine group	Machine	User access
1	ATP1	Device1	Group1
Last	Ungrouped machines (default)	Device2	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.

Hot Area:

Correct Answer:

Section: [none]
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-atp/user-roles-windows-defender-advanced-threat-protection

QUESTION 53
HOTSPOT

You have a Microsoft 365 subscription. All client devices are managed by Microsoft Endpoint Manager.

You need to implement Microsoft Defender Advanced Threat Protection (ATP) for all the supported devices enrolled in mobile device management (MDM).

What should you include in the device configuration profile? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Correct Answer:

Section: [none]
Explanation

Explanation/Reference:
Reference:
https://docs.microsoft.com/en-us/intune/advanced-threat-protection

QUESTION 54 You have a Microsoft
365 subscription.

Your company purchases a new financial application named App1.

From Cloud Discovery in Microsoft Cloud App Security, you view the Discovered apps page and discover that many applications have a low score because they are missing information about domain registration and consumer popularity.

You need to prevent the missing information from affecting the App1 score.

What should you configure from the Cloud Discover settings?

A. Organization details
B. Default behavior
C. Score metrics
D. App tags

Correct Answer: D

Section: [none]
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/cloud-app-security/discovered-app-queries

QUESTION 55 You have a Microsoft 365 E5 subscription.

You need to be notified if users receive email containing a file that has a virus.

What should you do?

A. From the Exchange admin center, create an in-place eDiscovery & hold.
B. From the Exchange admin center, create a spam filter policy.
C. From the Exchange admin center, create an anti-malware policy.
D. From the Exchange admin center, create a mail flow rule.

Correct Answer: C
Section: [none]
Explanation

Explanation/Reference:
Reference: https://docs.microsoft.com/en-us/office365/servicedescriptions/exchange-online-service-description/anti-spam-and-anti-malware-protection

QUESTION 56
HOTSPOT

You have a Microsoft 365 subscription that links to an Azure Active Directory (Azure AD) tenant named contoso.onmicrosoft.com.

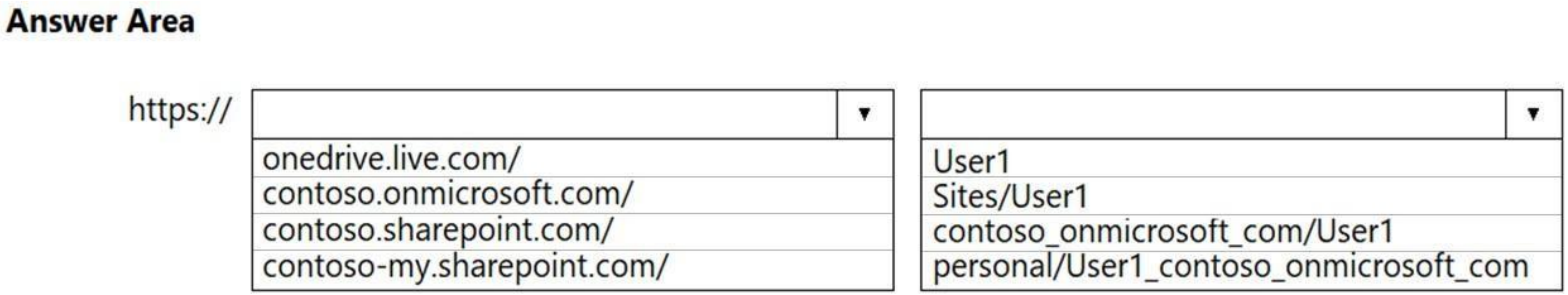
A user named User1 stores documents in Microsoft OneDrive.

You need to place the contents of User1's OneDrive account on an eDiscovery hold.

Which URL should you use for the eDiscovery hold? To answer, select the appropriate options in the answer area.

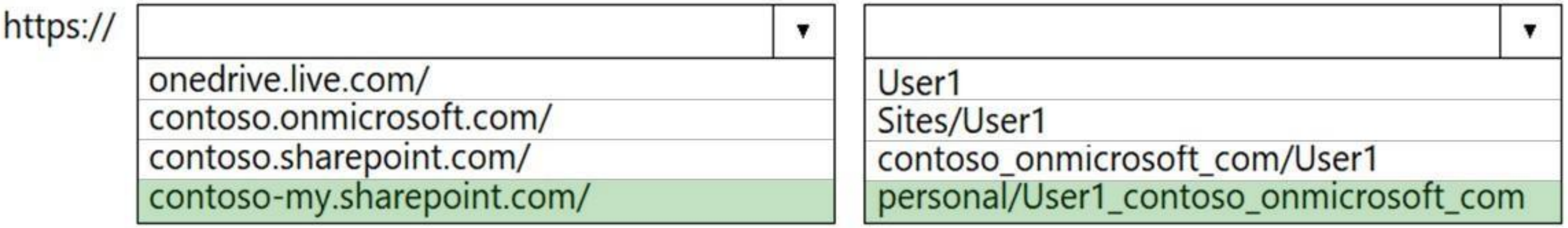
NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:

Answer Area



https://

- onedrive.live.com/
- contoso.onmicrosoft.com/
- contoso.sharepoint.com/
- [✓ contoso-my.sharepoint.com/]

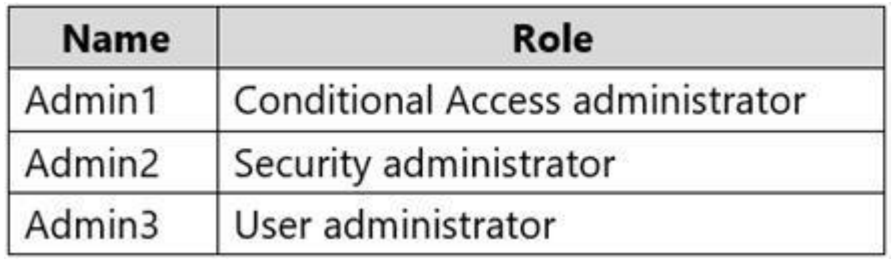
- User1
- Sites/User1
- contoso_onmicrosoft_com/User1
- [✓ personal/User1_contoso_onmicrosoft_com]

Section: [none]
Explanation

Explanation/Reference:
Reference: https://docs.microsoft.com/en-us/microsoft-365/compliance/create-ediscovery-holds

QUESTION 57
HOTSPOT

You have a Microsoft 365 E5 subscription linked to an Azure Active Directory (Azure AD) tenant. The tenant contains a group named Group1 and the users shown in the following table:



Name	Role
Admin1	Conditional Access administrator
Admin2	Security administrator
Admin3	User administrator

The tenant has a conditional access policy that has the following configurations:

▪ Name: Policy1 ▪
Assignments:
- Users and groups: Group1
- Cloud aps or actions: All cloud apps ▪ Access controls:

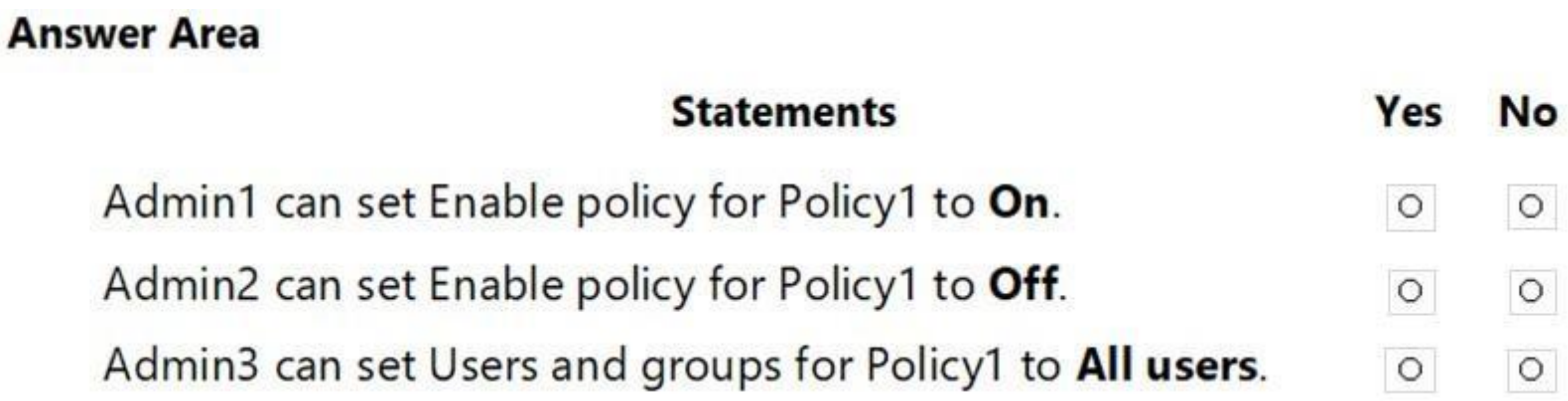
▪ Grant, require multi-factor authentication ▪
Enable policy: Report-only

You set **Enabled Security defaults** to **Yes** for the tenant.

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

NOTE: Each correct selection is worth one point.

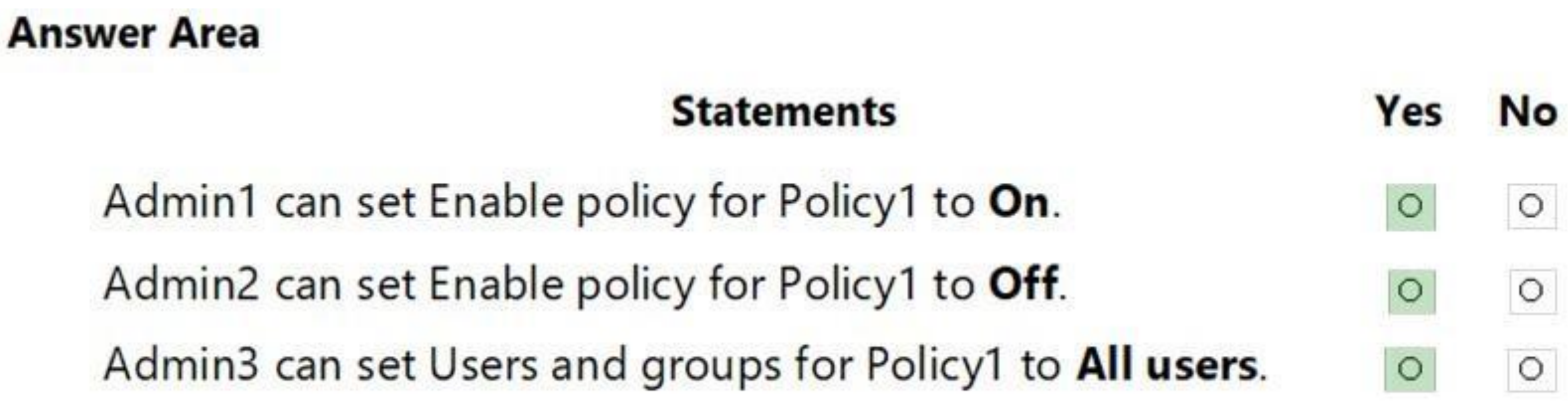
Hot Area:



Answer Area

Statements	Yes	No
Admin1 can set Enable policy for Policy1 to **On**.	○	○
Admin2 can set Enable policy for Policy1 to **Off**.	○	○
Admin3 can set Users and groups for Policy1 to **All users**.	○	○

Correct Answer:



Answer Area

Statements	Yes	No
Admin1 can set Enable policy for Policy1 to **On**.	[✓ ○]	○
Admin2 can set Enable policy for Policy1 to **Off**.	[✓ ○]	○
Admin3 can set Users and groups for Policy1 to **All users**.	[✓ ○]	○

Section: [none]
Explanation

Explanation/Reference:
Explanation:

Report-only mode is a new Conditional Access policy state that allows administrators to evaluate the impact of Conditional Access policies before enabling them in their environment. With the release of report-only mode: ▪ Conditional Access policies can be enabled in report-only mode.

- ▪ During sign-in, policies in report-only mode are evaluated but not enforced.
- ▪ Results are logged in the Conditional Access and Report-only tabs of the Sign-in log details.
- ▪ Customers with an Azure Monitor subscription can monitor the impact of their Conditional Access policies using the Conditional Access insights workbook.

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-report-only

Testlet 2

Case Study

Overview

Contoso, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.

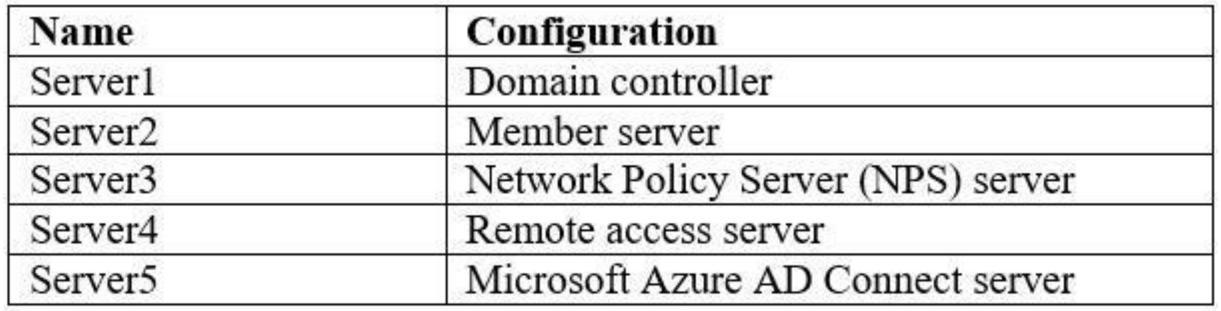
The company has the employees and devices shown in the following table.

Location	Employees	Laptops	Desktops	Mobile devices
Montreal	2,500	2,800	300	3,100
Seattle	1,000	1,100	200	1,500
New York	300	320	30	400

Contoso recently purchased a Microsoft 365 E5 subscription.

Existing Environment

The network contains an on-premises Active Directory forest named contoso.com. The forest contains the servers shown in the following table.

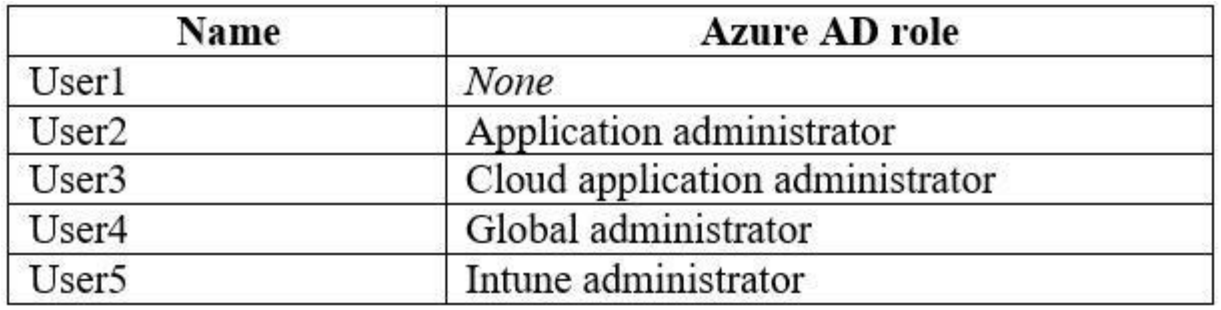


Name	Configuration
Server1	Domain controller
Server2	Member server
Server3	Network Policy Server (NPS) server
Server4	Remote access server
Server5	Microsoft Azure AD Connect server

All servers run Windows Server 2016. All desktops and laptops run Windows 10 Enterprise and are joined to the domain.

The mobile devices of the users in the Montreal and Seattle offices run Android. The mobile devices of the users in the New York office run iOS.

The domain is synced to Azure Active Directory (Azure AD) and includes the users shown in the following table.



Name	Azure AD role
User1	*None*
User2	Application administrator
User3	Cloud application administrator
User4	Global administrator
User5	Intune administrator

The domain also includes a group named Group1.

Requirements

Planned Changes
Contoso plans to implement the following changes:

- Implement Microsoft 365.
- Manage devices by using Microsoft Intune.
- Implement Azure Advanced Threat Protection (ATP).
- Every September, apply the latest feature updates to all Windows computers. Every March, apply the latest feature updates to the computers in the New York office only.

Technical Requirements

Contoso identifies the following technical requirements:

- When a Windows 10 device is joined to Azure AD, the device must enroll in Intune automatically.
- Dedicated support technicians must enroll all the Montreal office mobile devices in Intune.
- User1 must be able to enroll all the New York office mobile devices in Intune.
- Azure ATP sensors must be installed and must **NOT** use port mirroring.
- Whenever possible, the principle of least privilege must be used. ▪ A
Microsoft Store for Business must be created.

Compliance Requirements

Contoso identifies the following compliance requirements:

▪ Ensure that the users in Group1 can only access Microsoft Exchange Online from devices that are enrolled in Intune and configured in accordance with the corporate policy. ▪ Configure Windows Information Protection (WIP) for the Windows 10 devices.

QUESTION 1 On which server should you install the Azure ATP sensor?

A. Server1
B. Server2C. Server3
D. Server4 E.
Server5

Correct Answer: A
Section: [none]
Explanation

Explanation/Reference:
References:
https://docs.microsoft.com/en-us/azure-advanced-threat-protection/atp-capacity-planning

Testlet 3

Case Study

Overview

ADatum Corporation is an international financial services company that has 5,000 employees.

ADatum has six offices: a main office in New York and five branch offices in Germany, the United Kingdom, France, Spain, and Italy.

All the offices are connected to each other by using a WAN link. Each office connects directly to the Internet.

Existing Environment

Current Infrastructure

ADatum recently purchased a Microsoft 365 subscription.

All user files are migrated to Microsoft 365.

All mailboxes are hosted in Microsoft 365. The users in each office have email suffixes that include the country of the user, for example, user1@us.adatum.com or user2@uk.adatum.com.

Each office has a security information and event management (SIEM) appliance. The appliance comes from three different vendors.

ADatum uses and processes Personally Identifiable Information (PII).

Problem Statements

ADatum entered into litigation. The legal department must place a hold on all the documents of a user named User1 that are in Microsoft 365.

Requirements

Business Goals

ADatum wants to be fully compliant with all the relevant data privacy laws in the regions where is operates.

ADatum wants to minimize the cost of hardware and software whenever possible. **Technical**

Requirements

ADatum identifies the following technical requirements:

- Centrally perform log analysis for all offices.
- Aggregate all data from the SIEM appliances to a central cloud repository for later analysis.
- Ensure that a SharePoint administrator can identify who accessed a specific file stored in a document library.
- Provide the users in the finance department with access to Service assurance information in Microsoft Office 365.
- Ensure that documents and email messages containing the PII data of European Union (EU) citizens are preserved for 10 years.
- If a user attempts to download 1,000 or more files from Microsoft SharePoint Online within 30 minutes, notify a security administrator and suspend the user's user account.
- A security administrator requires a report that shown which Microsoft 365 users signed in. Based on the report, the security administrator will create a policy to require multi-factor authentication when a sign-in is high risk.
- Ensure that the users in the New York office can only send email messages that contain sensitive U.S. PII data to other New York office uses. Email messages must be monitored to ensure compliance. Auditors in the New York office must have access to reports that show the sent and received email messages containing sensitive U.S. PII data.

QUESTION 1 You need to meet the technical requirement for large-volume document retrieval.

What should you create?

A. an activity policy from Microsoft Cloud App Security
B. a data loss prevention (DLP) policy from the Security & Compliance admin center

C. a file policy from Microsoft Cloud App Security
D. an alert policy from the Security & Compliance admin center

Correct Answer: A
Section: [none]
Explanation

Explanation/Reference:
Reference:
https://docs.microsoft.com/en-us/office365/securitycompliance/activity-policies-and-alerts

Question Set 1

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.

You have a Microsoft 365 subscription.

From the Security & Compliance admin center, you create a role group named US eDiscovery Managers by copying the eDiscovery Manager role group.

You need to ensure that the users in the new role group can only perform content searches of mailbox content for users in the United States.

Solution: From Windows PowerShell, you run the `New-AzureRmRoleAssignment` cmdlet with the appropriate parameters.

Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/powershell/module/azurerm.resources/new-azurermroleassignment?view=azurermps-6.13.0

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.

You have a Microsoft 365 subscription.

From the Security & Compliance admin center, you create a role group named US eDiscovery Managers by copying the eDiscovery Manager role group.

You need to ensure that the users in the new role group can only perform content searches of mailbox content for users in the United States.

Solution: From the Security & Compliance admin center, you modify the roles of the US eDiscovery Managers role group.

Does this meet the goal?

A. Yes
B. No

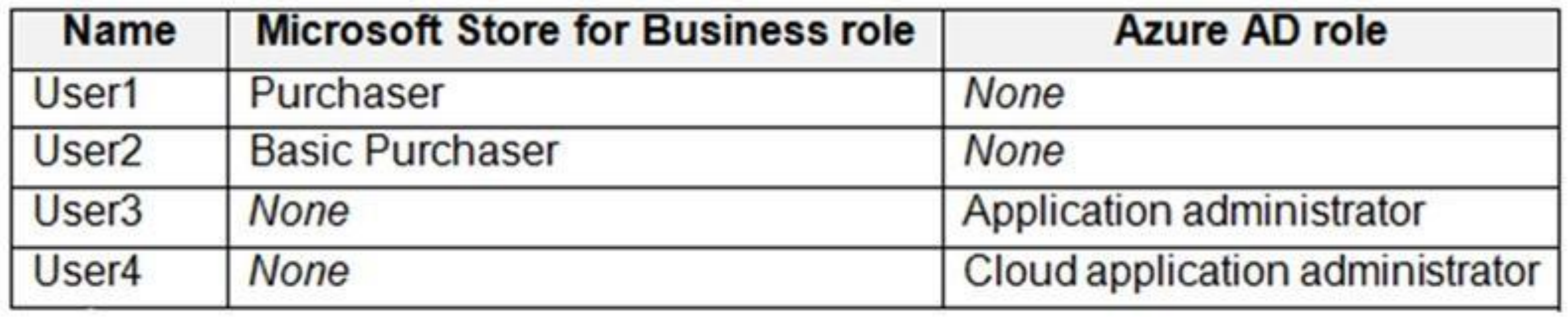
Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:

QUESTION 3 Your company has a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com.

You sign 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

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. User3 only
B. User1 only
C. User1 and User2 only
D. User3 and User4 only

Correct Answer: C
Section: [none]
Explanation

Explanation/Reference:
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 4
You have a Microsoft 365 subscription that contains a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com.

In the tenant, you create a user named User1.

You need to ensure that User1 can publish retention labels from the Security & Compliance admin center. The solution must use the principle of least privilege.

To which role group should you add User1?

A. Security Administrator
B. Records Management
C. Compliance Administrator
D. eDiscovery Manager

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:
References:
https://docs.microsoft.com/en-us/office365/securitycompliance/file-plan-manager

QUESTION 5 You plan to use the Security & Compliance admin center to import several PST files into Microsoft 365 mailboxes.

Which three actions should you perform before you import the data? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. From the Exchange admin center, create a public folder.
B. Copy the PST files by using AzCopy.
C. From the Exchange admin center, assign admin roles.
D. From the Microsoft Azure portal, create a storage account that has a blob container.
E. From the Microsoft 365 admin center, deploy an add-in.
F. Create a mapping file that uses the CSV file format.

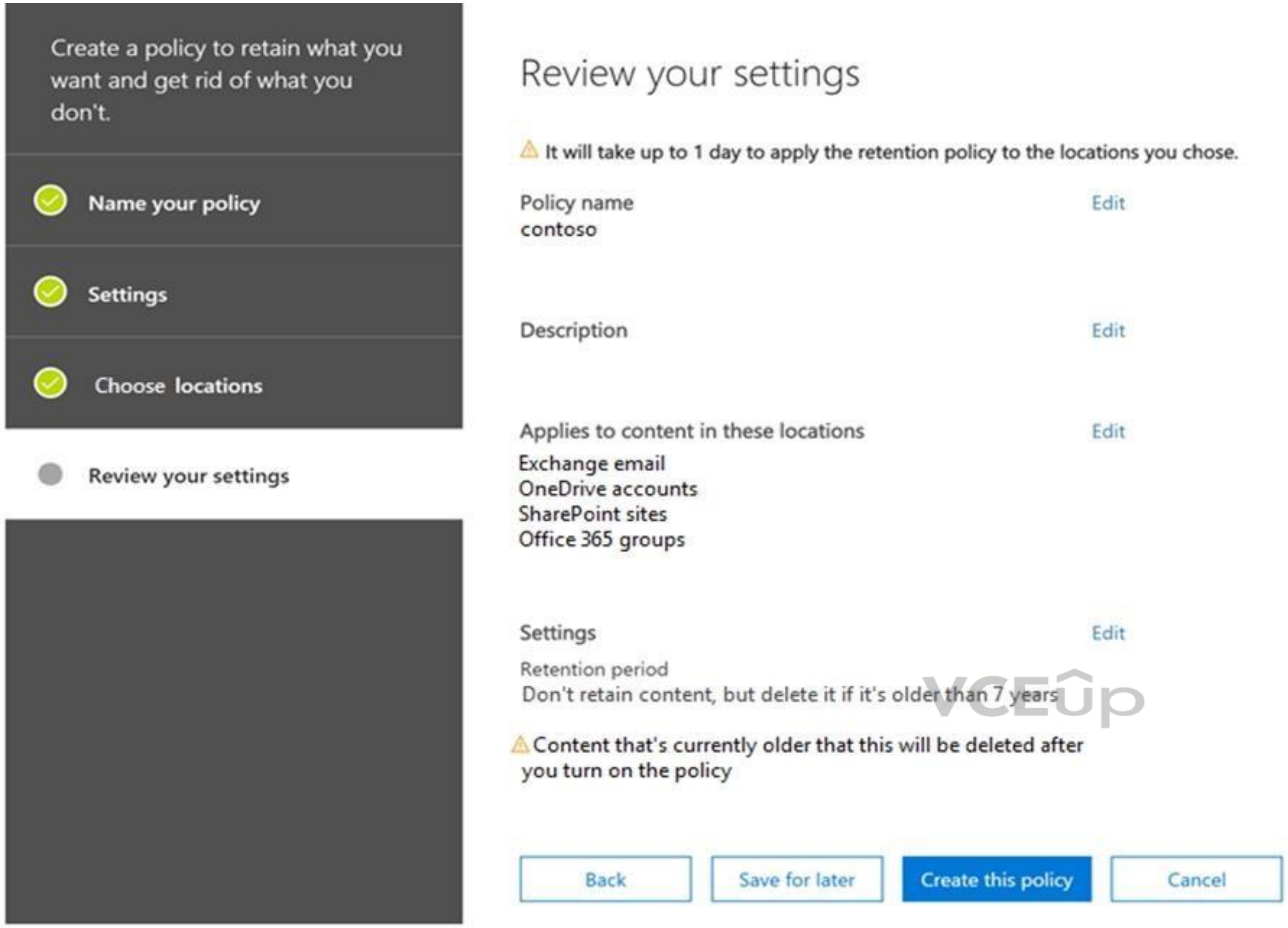
Correct Answer: BCF
Section: [none]
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/office365/securitycompliance/use-network-upload-to-import-pst-files

QUESTION 6 HOTSPOT

You have a Microsoft 365 tenant.

You plan to create a retention policy as shown in the following exhibit.



Create a policy to retain what you want and get rid of what you don't.
Name your policy
Settings
Choose locations
Review your settings

Review your settings

⚠ It will take up to 1 day to apply the retention policy to the locations you chose.

Policy name
contoso

Description

Applies to content in these locations
Exchange email
OneDrive accounts
SharePoint sites
Office 365 groups

Settings
Retention period
Don't retain content, but delete it if it's older than 7 years

⚠ Content that's currently older that this will be deleted after you turn on the policy

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:

Correct Answer:

Section: [none]
Explanation

Explanation/Reference:

QUESTION 7 You deploy Microsoft Azure Information Protection.

You need to ensure that a security administrator named SecAdmin1 can always read and inspect data protected by Azure Rights Management (Azure RMS).

What should you do?

A. From the Security & Compliance admin center, add SecAdmin1 to the eDiscovery Manager role group.
B. From the Azure Active Directory admin center, add SecAdmin1 to the Security Reader role group.
C. From the Security & Compliance admin center, add SecAdmin1 to the Compliance Administrator role group.
D. From Windows PowerShell, enable the super user feature and assign the role to SecAdmin1.

Correct Answer: D
Section: [none]
Explanation

Explanation/Reference:
Explanation:
The super user feature of the Azure Rights Management service from Azure Information Protection ensures that authorized people and services can always read and inspect the data that Azure Rights Management protects for your organization. However, the super user feature is not enabled by default. The PowerShell cmdlet Enable-AadrmSuperUserFeature is used to manually enable the super user feature.

References: https://docs.microsoft.com/en-us/azure/information-protection/configure-super-users

QUESTION 8
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 new Microsoft 365 subscription.

You need to prevent users from sending email messages that contain Personally Identifiable Information (PII).

Solution: From the Cloud App Security admin center, you create an access policy.

Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:

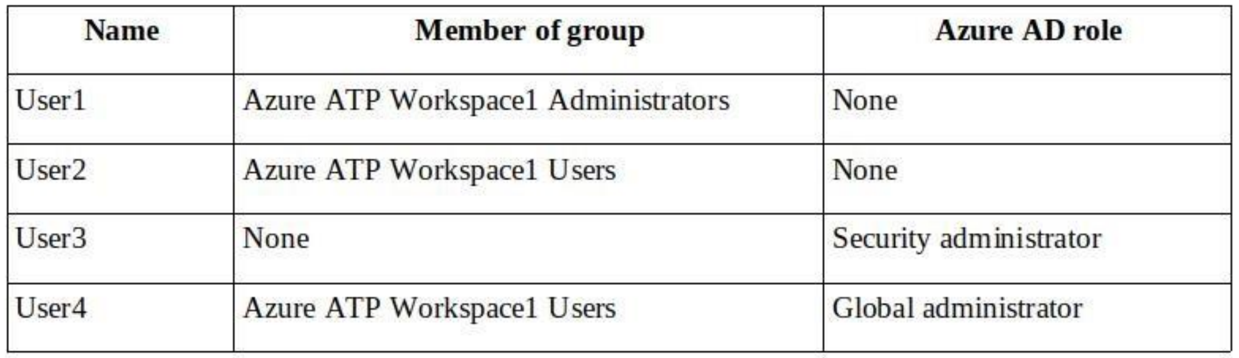
QUESTION 9
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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 Azure Active Directory (Azure AD) tenant named contoso.com.

You create an Azure Advanced Threat Protection (ATP) workspace named Workspace1.

The tenant contains the users shown in the following table.



Name	Member of group	Azure AD role
User1	Azure ATP Workspace1 Administrators	None
User2	Azure ATP Workspace1 Users	None
User3	None	Security administrator
User4	Azure ATP Workspace1 Users	Global administrator

You need to modify the configuration of the Azure ATP sensors.

Solution: You instruct User4 to modify the Azure ATP sensor configuration.

Does this meet the goal?

A. Yes
B. No

Correct Answer: A
Section: [none]
Explanation

Explanation/Reference:
Explanation:
Only Azure ATP administrators can modify the sensors.

Any global administrator or security administrator on the tenant's Azure Active Directory is automatically an Azure ATP administrator.

References: https://docs.microsoft.com/en-us/azure-advanced-threat-protection/atp-role-groups

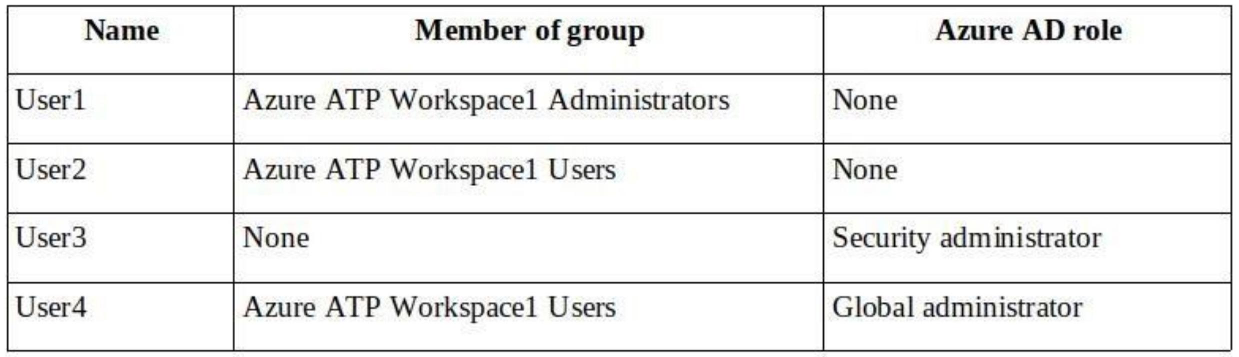
QUESTION 10
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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 Azure Active Directory (Azure AD) tenant named contoso.com.

You create an Azure Advanced Threat Protection (ATP) workspace named Workspace1.

The tenant contains the users shown in the following table.



Name	Member of group	Azure AD role
User1	Azure ATP Workspace1 Administrators	None
User2	Azure ATP Workspace1 Users	None
User3	None	Security administrator
User4	Azure ATP Workspace1 Users	Global administrator

You need to modify the configuration of the Azure ATP sensors.

Solution: You instruct User3 to modify the Azure ATP sensor configuration.

Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section: [none]
Explanation

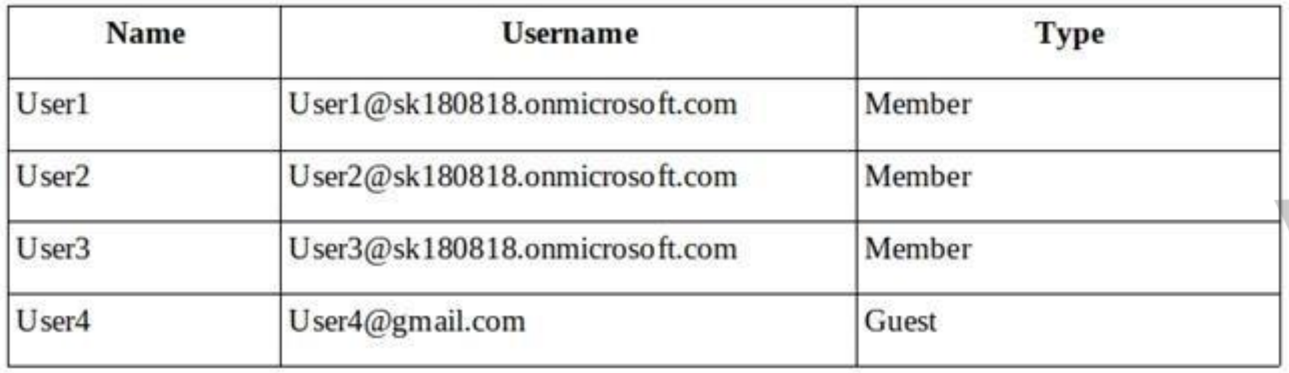
Explanation/Reference:
Explanation:
Only Azure ATP administrators can modify the sensors.

Any global administrator or security administrator on the tenant's Azure Active Directory is automatically an Azure ATP administrator.

Reference: https://docs.microsoft.com/en-us/azure-advanced-threat-protection/atp-role-groups

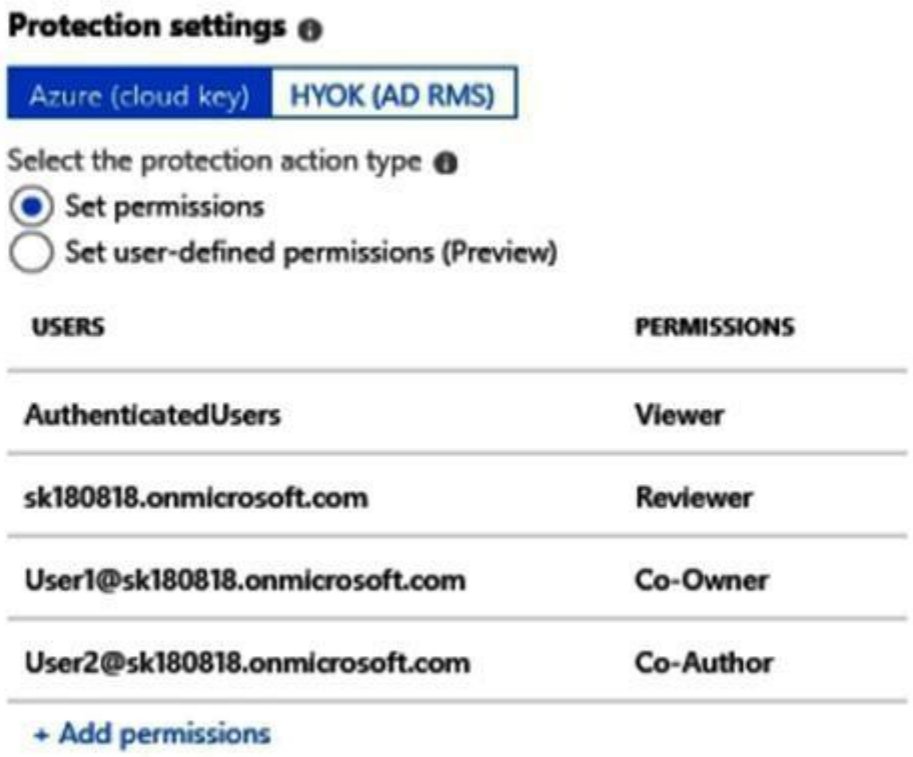
QUESTION 11
HOTSPOT

You have a Microsoft Azure Active Directory (Azure AD) tenant named sk180818.onmicrosoft.com. The tenant contains the users shown in the following table.



Name	Username	Type
User1	User1@sk180818.onmicrosoft.com	Member
User2	User2@sk180818.onmicrosoft.com	Member
User3	User3@sk180818.onmicrosoft.com	Member
User4	User4@gmail.com	Guest

In Azure Information Protection, you create a label named Label1 as shown in the following exhibit.



Protection settings

Azure (cloud key) | HYOK (AD RMS)

Select the protection action type

● Set permissions

○ Set user-defined permissions (Preview)

USERS	PERMISSIONS
AuthenticatedUsers	Viewer
sk180818.onmicrosoft.com	Reviewer
User1@sk180818.onmicrosoft.com	Co-Owner
User2@sk180818.onmicrosoft.com	Co-Author

+ Add permissions

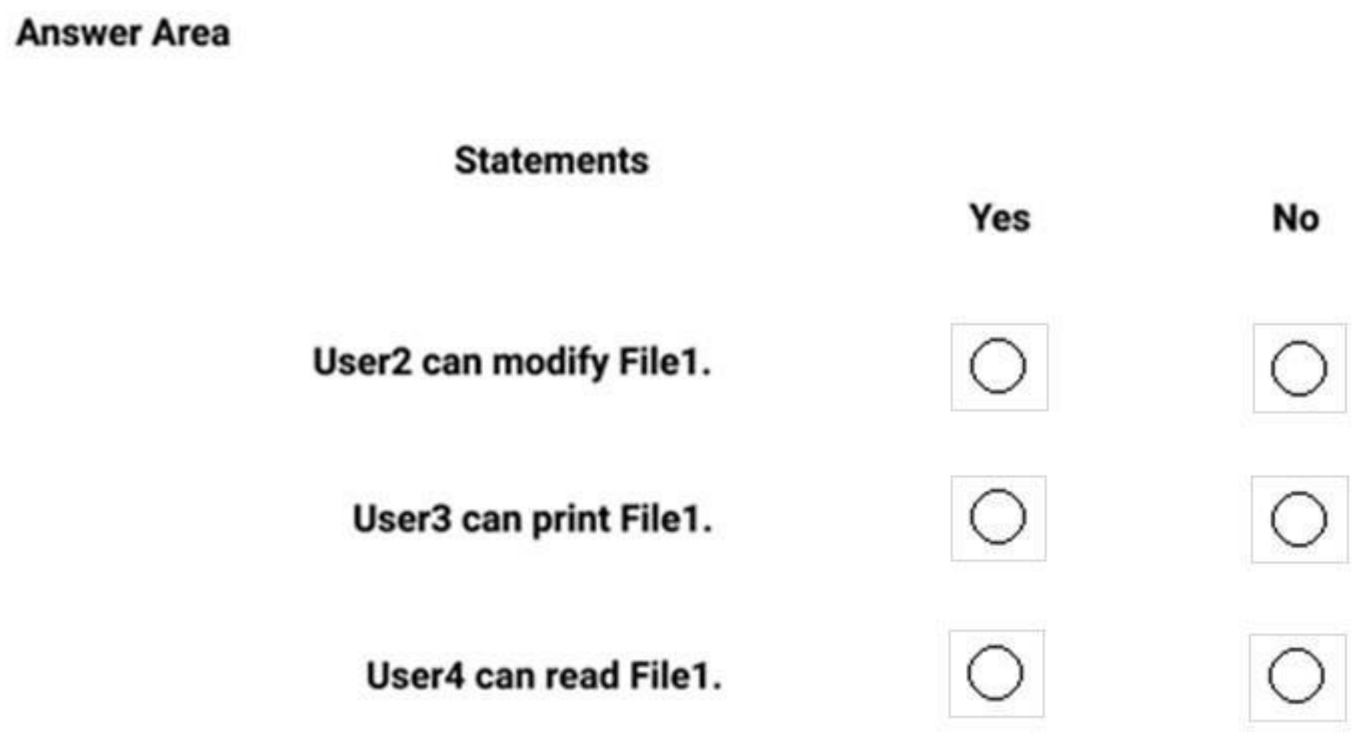
Label1 is applied to a file named File1.

You send File1 as an email attachment to User1, User2, User3, and User4.

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

NOTE: Each correct selection is worth one point.

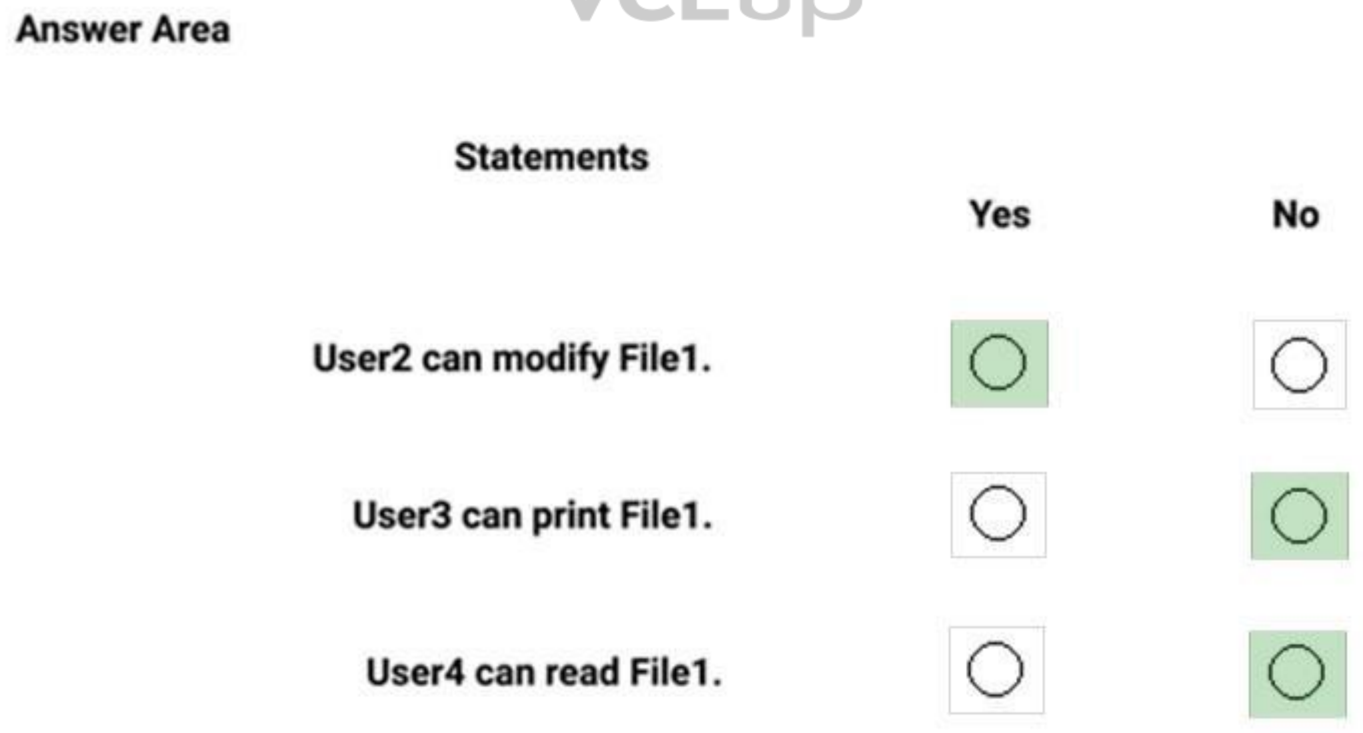
Hot Area:



Answer Area

Statements	Yes	No
User2 can modify File1.	○	○
User3 can print File1.	○	○
User4 can read File1.	○	○

Correct Answer:



Answer Area

Statements	Yes	No
User2 can modify File1.	●	○
User3 can print File1.	○	●
User4 can read File1.	○	●

Section: [none]
Explanation

Explanation/Reference:

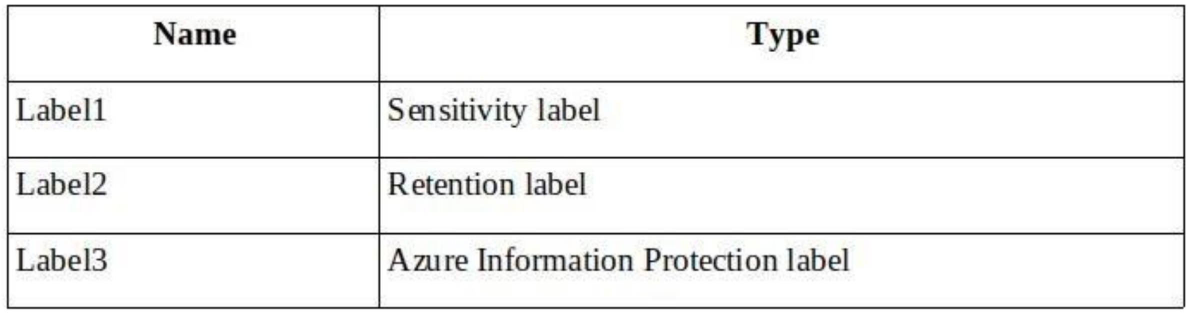
Reference: https://docs.microsoft.com/en-us/azure/information-protection/configure-usage-rights#rights-included-in-permissions-levels

QUESTION 12
HOTSPOT

Your company has a Microsoft 365 subscription that uses an Azure Active Directory (Azure AD) tenant named contoso.com.

The company stores 2 TBs of data in SharePoint Online document libraries.

The tenant has the labels shown in the following table.

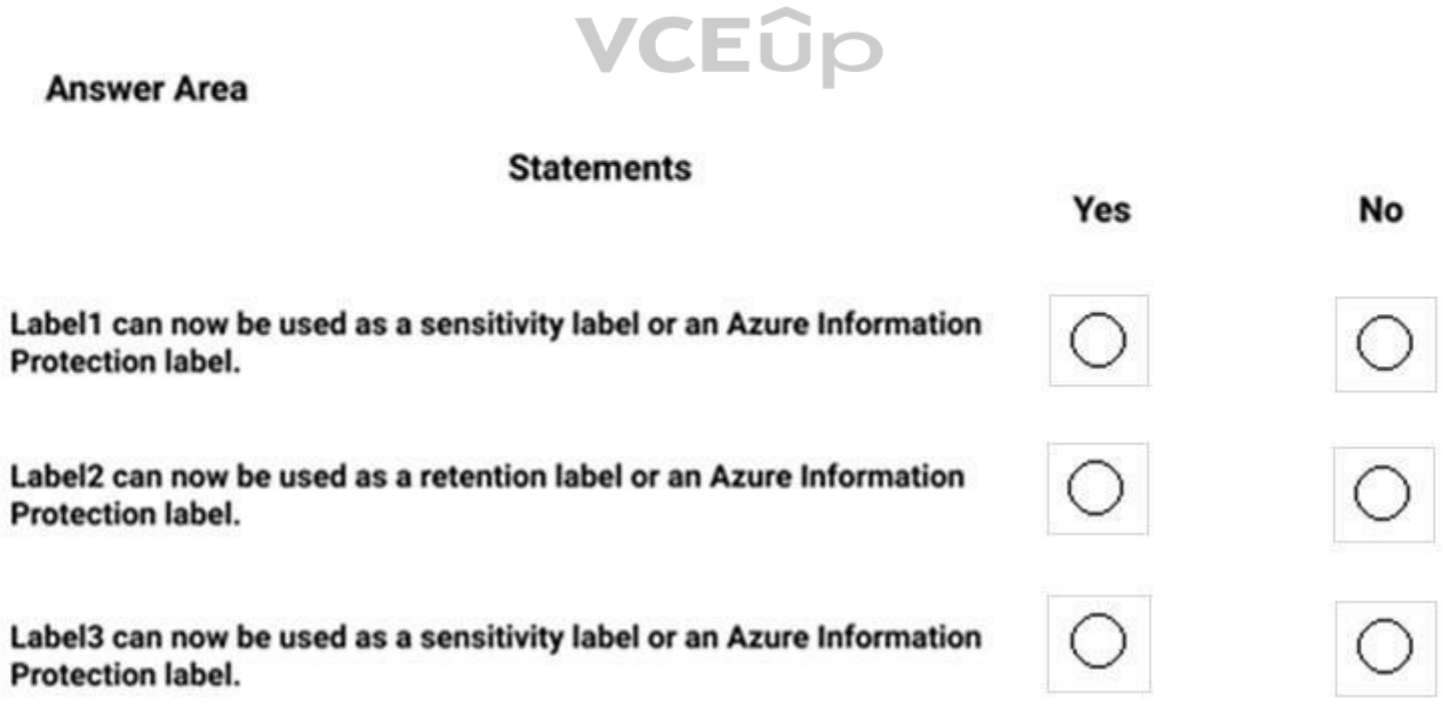


Name	Type
Label1	Sensitivity label
Label2	Retention label
Label3	Azure Information Protection label

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

NOTE: Each correct selection is worth one point.

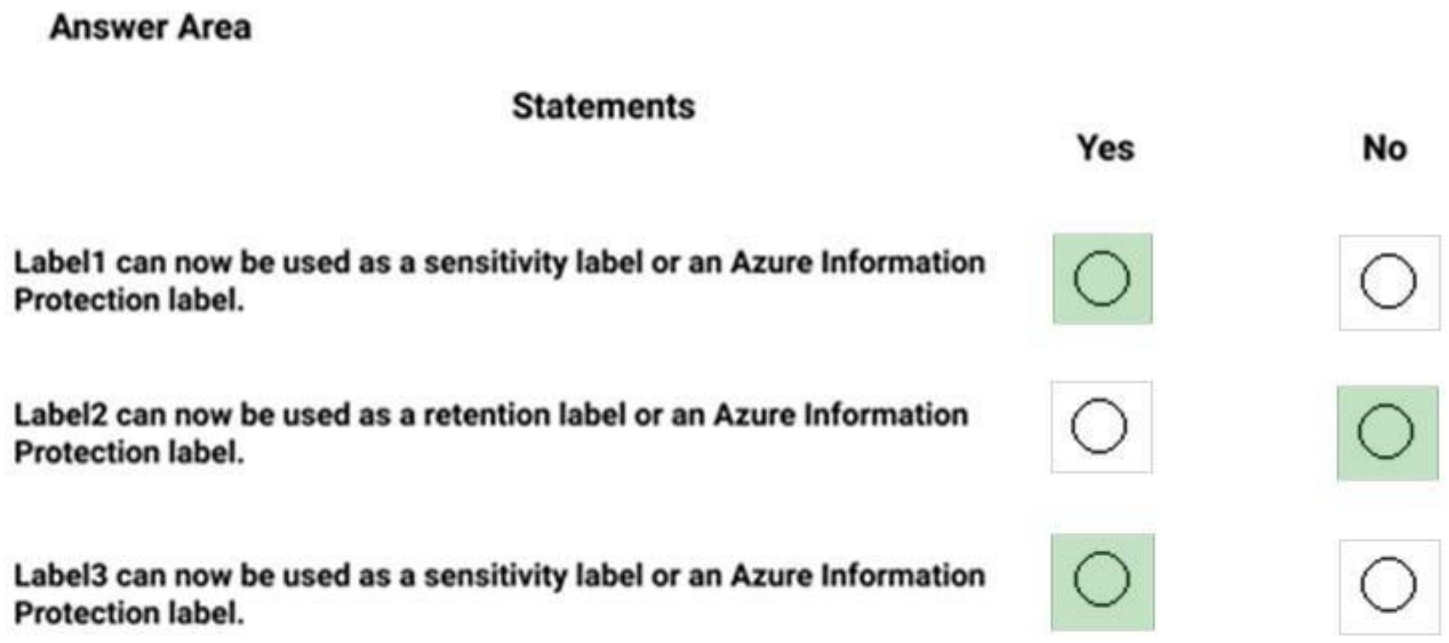
Hot Area:



Answer Area

Statements	Yes	No
Label1 can now be used as a sensitivity label or an Azure Information Protection label.	○	○
Label2 can now be used as a retention label or an Azure Information Protection label.	○	○
Label3 can now be used as a sensitivity label or an Azure Information Protection label.	○	○

Correct Answer:



Answer Area

Statements	Yes	No
Label1 can now be used as a sensitivity label or an Azure Information Protection label.	[✓ ○]	○
Label2 can now be used as a retention label or an Azure Information Protection label.	○	[✓ ○]
Label3 can now be used as a sensitivity label or an Azure Information Protection label.	[✓ ○]	○

Section: [none]
Explanation

Explanation/Reference:

QUESTION 13
HOTSPOT

You create a Microsoft 365 subscription.

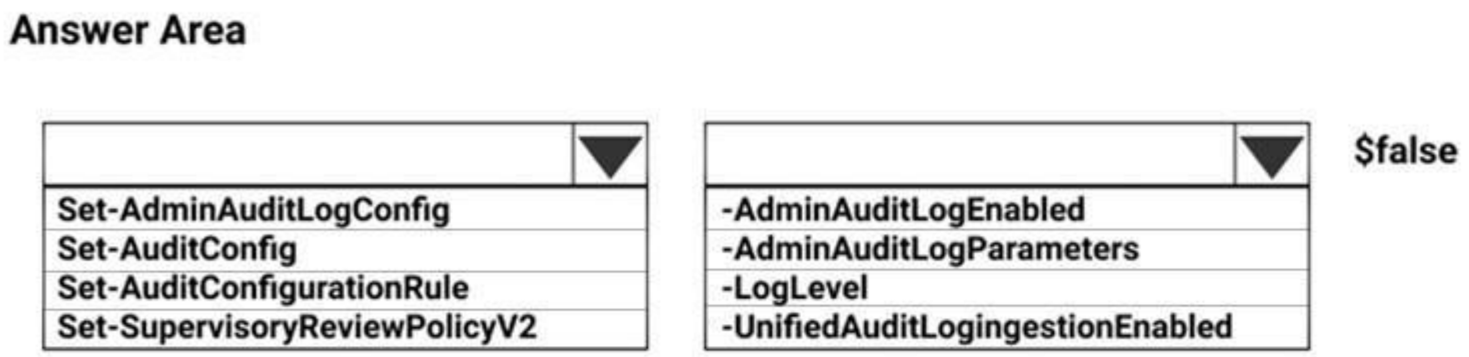
Your company’s privacy policy states that user activities must NOT be audited.

You need to disable audit logging in Microsoft 365.

How should you complete the command? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



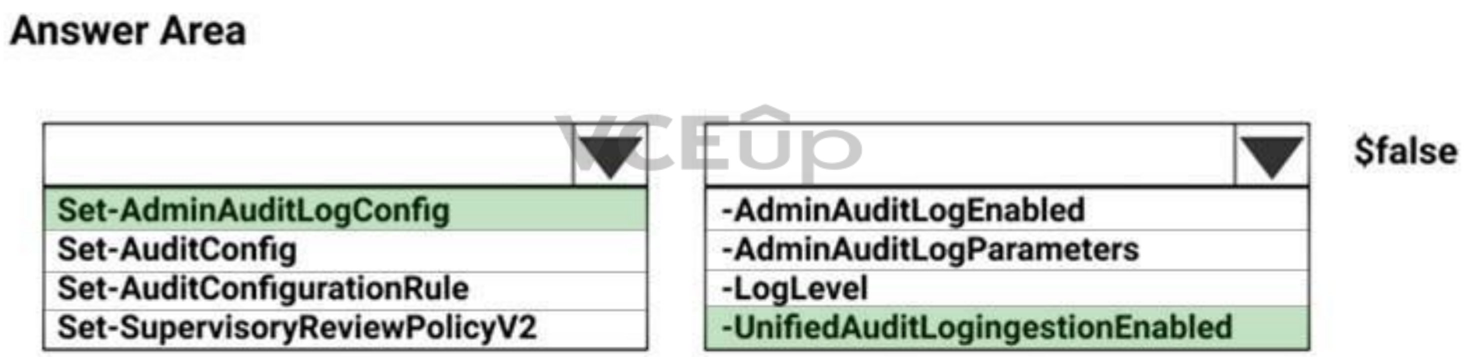
Answer Area

Set-AdminAuditLogConfig
Set-AuditConfig
Set-AuditConfigurationRule
Set-SupervisoryReviewPolicyV2

-AdminAuditLogEnabled
-AdminAuditLogParameters
-LogLevel
-UnifiedAuditLogingestionEnabled

$false

Correct Answer:



Answer Area

[✓ Set-AdminAuditLogConfig]
Set-AuditConfig
Set-AuditConfigurationRule
Set-SupervisoryReviewPolicyV2

-AdminAuditLogEnabled
-AdminAuditLogParameters
-LogLevel
[✓ -UnifiedAuditLogingestionEnabled]

$false

Section: [none]
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/office365/securitycompliance/turn-audit-log-search-on-or-off

QUESTION 14
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 new Microsoft 365 subscription.

You need to prevent users from sending email messages that contain Personally Identifiable Information (PII).

Solution: From the Exchange admin center, you create a data loss prevention (DLP) policy.

Does this meet the goal?

A. Yes
B. No

Correct Answer: A
Section: [none]
Explanation

Explanation/Reference:

QUESTION 15 You have a Microsoft 365 subscription.

Some users have iPads that are managed by your company.

You plan to prevent the iPad users from copying corporate data in Microsoft Word and pasting the data into other applications.

What should you create?

A. A conditional access policy.
B. A compliance policy.
C. An app protection policy.
D. An app configuration policy.

Correct Answer: C
Section: [none]
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/intune/app-protection-policy

QUESTION 16
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 new Microsoft 365 subscription.

You need to prevent users from sending email messages that contain Personally Identifiable Information (PII).

Solution: From the Azure portal, you create a Microsoft Azure Information Protection label and an Azure Information Protection policy.

Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:

QUESTION 17

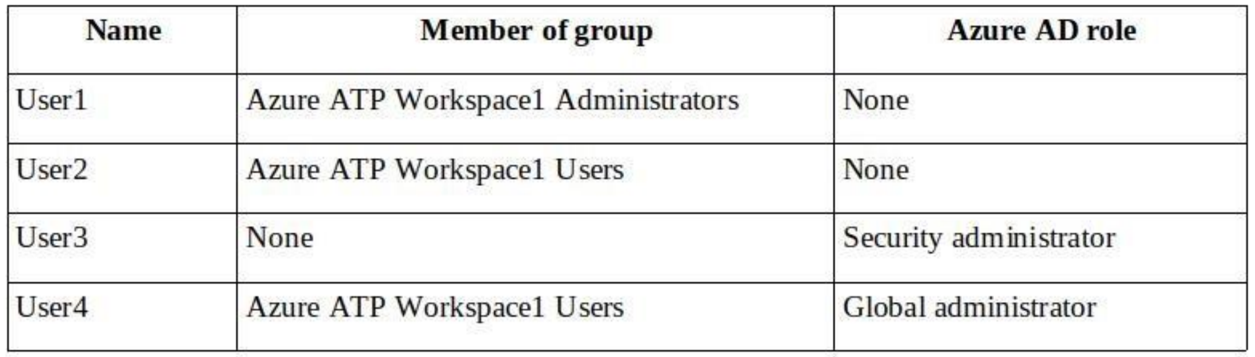
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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 Azure Active Directory (Azure AD) tenant named contoso.com.

You create an Azure Advanced Threat Protection (ATP) workspace named Workspace1.

The tenant contains the users shown in the following table.



Name	Member of group	Azure AD role
User1	Azure ATP Workspace1 Administrators	None
User2	Azure ATP Workspace1 Users	None
User3	None	Security administrator
User4	Azure ATP Workspace1 Users	Global administrator

You need to modify the configuration of the Azure ATP sensors.

Solution: You instruct User1 to modify the Azure ATP sensor configuration.

Does this meet the goal?

A. Yes
B. No

Correct Answer: A
Section: [none]
Explanation

Explanation/Reference:
Explanation:
Only Azure ATP administrators can modify the sensors.

References: https://docs.microsoft.com/en-us/azure-advanced-threat-protection/atp-role-groups

QUESTION 18
HOTSPOT

You have a data loss prevention (DLP) policy.

You need to increase the likelihood that the DLP policy will apply to data that contains medical terms from the International Classification of Diseases (ICD-9-CM). The solution must minimize the number of false positives.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Correct Answer:

Section: [none]
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/office365/securitycompliance/data-loss-prevention-policies https://docs.microsoft.com/en-us/office365/securitycompliance/what-the-sensitive-information-types-look-for#international-classification-of-diseases-icd-9-cm

QUESTION 19
HOTSPOT

From the Security & Compliance admin center, you create a retention policy named Policy1.

You need to prevent all users from disabling the policy or reducing the retention period.

Which command should you run? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Correct Answer:

Section: [none]
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/powershell/module/exchange/policy-and-compliance-retention/set-retentioncompliancepolicy?view=exchange-ps

QUESTION 20 You create a new Microsoft 365 subscription and assign Microsoft 365 E3 licenses to 100 users.

From the Security & Compliance admin center, you enable auditing.

You are planning the auditing strategy.

Which three activities will be audited by default? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. An administrator creates a new Microsoft SharePoint site collection.
B. An administrator creates a new mail flow rule.
C. A user shares a Microsoft SharePoint folder with an external user.
D. A user delegates permissions to their mailbox.
E. A user purges messages from their mailbox.

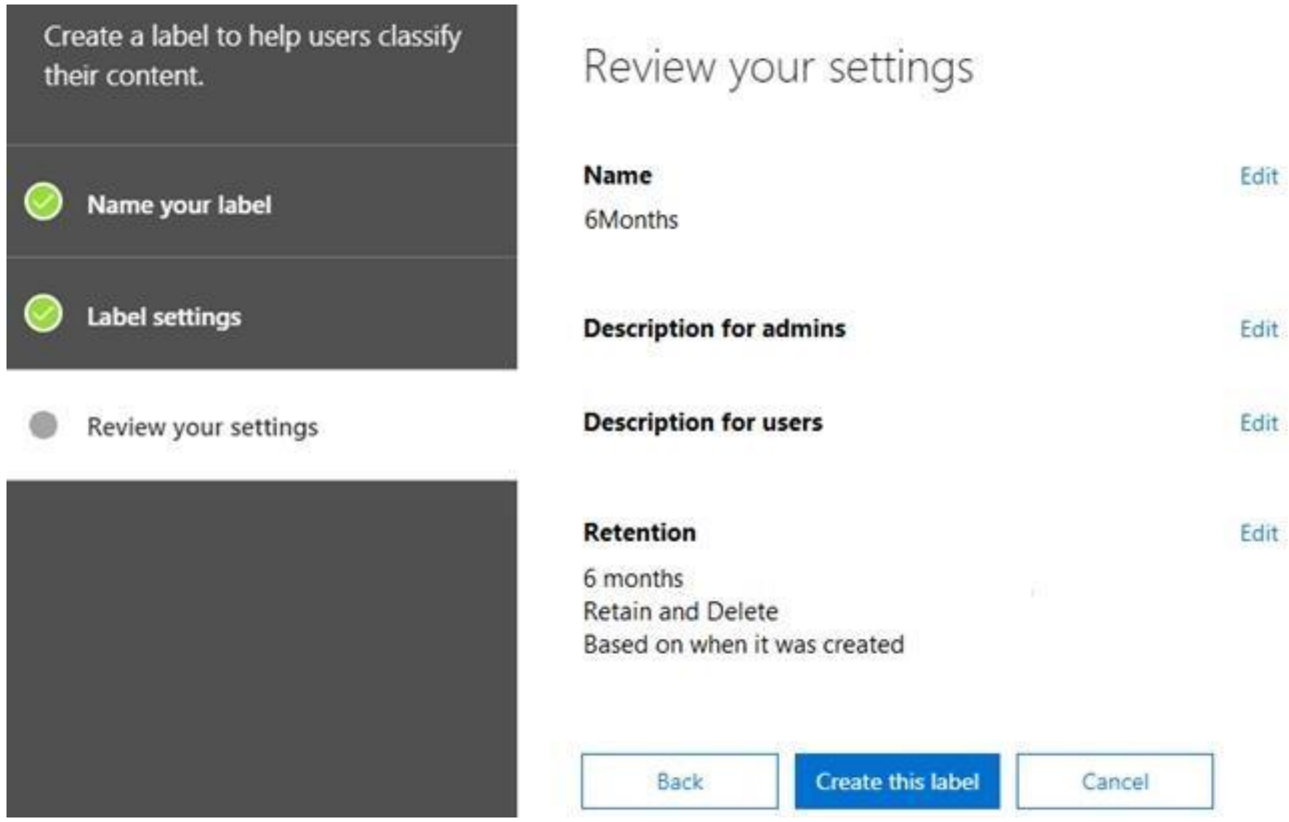
Correct Answer: ABC
Section: [none]
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/office365/securitycompliance/search-the-audit-log-in-security-and-compliance?redirectSourcePath=%252farticle%252f0d4d0f35-390b-4518-800e-0c7ec95e946c

QUESTION 21
HOTSPOT

You have a Microsoft 365 tenant.

You create a retention label as shown in the Retention Label exhibit. (Click the **Retention Label** tab.)



Create a label to help users classify their content.

✓ Name your label

✓ Label settings

● Review your settings

Review your settings

Name Edit

6Months

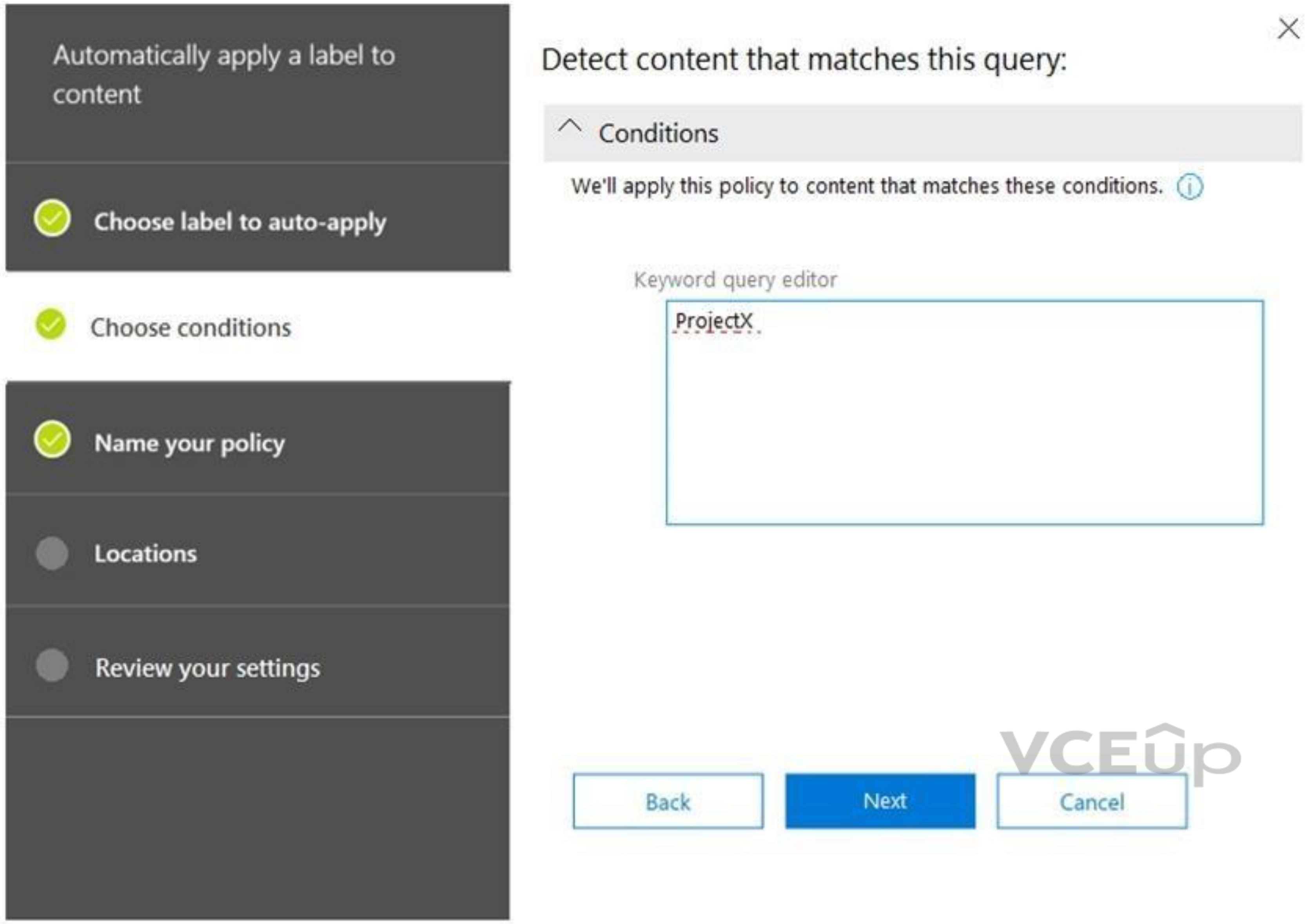
Description for admins Edit

Description for users Edit

Retention Edit

6 months
Retain and Delete
Based on when it was created

You create a label policy as shown in the Label Policy Exhibit. (Click the **Label Policy** tab.)



Automatically apply a label to content
Choose label to auto-apply
Choose conditions
Name your policy
Locations
Review your settings

Detect content that matches this query:

Conditions

We'll apply this policy to content that matches these conditions.

Keyword query editor

ProjectX

The label policy is configured as shown in the following table.

Configuration	Value
Label to auto-apply	6Months
Locations	Exchange email

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:

Section: [none]
Explanation

Explanation/Reference:
References:
https://docs.microsoft.com/en-us/office365/securitycompliance/retention-policies

QUESTION 22

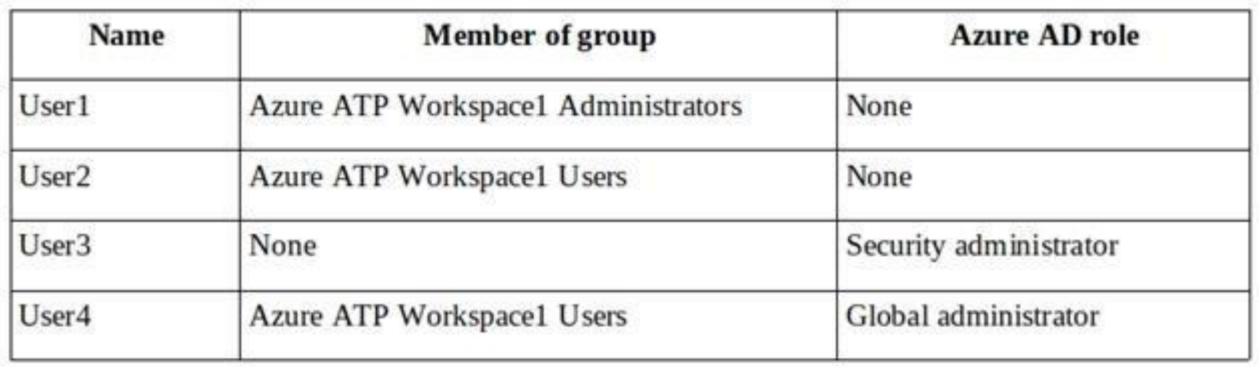
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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 Azure Active Directory (Azure AD) tenant named contoso.com.

You create an Azure Advanced Threat Protection (ATP) workspace named Workspace1.

The tenant contains the users shown in the following table.



Name	Member of group	Azure AD role
User1	Azure ATP Workspace1 Administrators	None
User2	Azure ATP Workspace1 Users	None
User3	None	Security administrator
User4	Azure ATP Workspace1 Users	Global administrator

You need to modify the configuration of the Azure ATP sensors.

Solution: You instruct User2 to modify the Azure ATP sensor configuration.

Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:

QUESTION 23
HOTSPOT

You purchase a new Microsoft 365 subscription.

You create 100 users who are assigned Microsoft 365 E3 licenses.

A manager sends you an email message asking the following questions:

- Question1: Who created a team named Team1 14 days ago?
- Question2: Who signed in to the mailbox of User1 30 days ago?
- Question3: Who modified the list of site collection administrators of a site 60 days ago?

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:

Section: [none]
Explanation

Explanation/Reference:
Reference:
https://docs.microsoft.com/en-us/office365/securitycompliance/search-the-audit-log-in-security-and-compliance?redirectSourcePath=%252farticle%252f0d4d0f35-390b-4518-800e-0c7ec95e946c https://docs.microsoft.com/en-us/office365/securitycompliance/enable-mailbox-auditing

QUESTION 24
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 subscription.

From the Security & Compliance admin center, you create a role group named US eDiscovery Managers by copying the eDiscovery Manager role group.

You need to ensure that the users in the new role group can only perform content searches of mailbox content for users in the United States.

Solution: From the Azure Active Directory admin center, you create a conditional access policy.

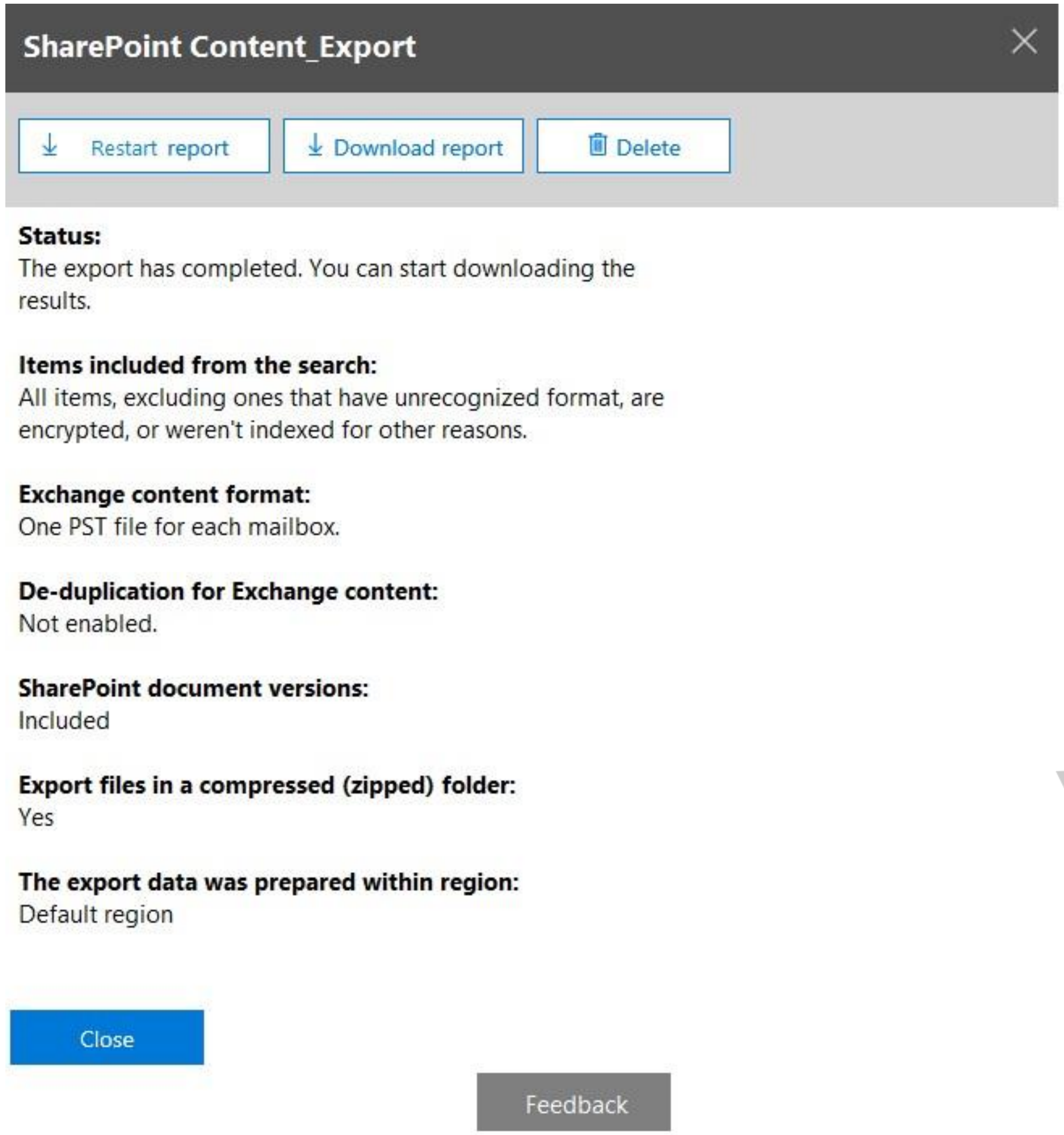
Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:

QUESTION 25
From the Security & Compliance admin center, you create a content export as shown in the exhibit. (Click the **Exhibit** tab.)



Status:
The export has completed. You can start downloading the results.

Items included from the search:
All items, excluding ones that have unrecognized format, are encrypted, or weren't indexed for other reasons.

Exchange content format:
One PST file for each mailbox.

De-duplication for Exchange content:
Not enabled.

SharePoint document versions:
Included

Export files in a compressed (zipped) folder:
Yes

The export data was prepared within region:
Default region

What will be excluded from the export?

A. a 60-MB DOCX file
B. a 12-MB BMP file
C. a 5-KB RTF file
D. an 80-MB PPTX file

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:
Explanation:
Unrecognized file formats are excluded from the search.

Certain types of files, such as Bitmap or MP3 files, don't contain content that can be indexed. As a result, the search indexing servers in Exchange and SharePoint don't perform full-text indexing on these types of files. These types of files are considered to be unsupported file types.

Incorrect Answers:
A: DOCX is a supported Microsoft PowerPoint file format.
C: RTF is a supported Rich Text File format.
D: PPTX is a supported Microsoft PowerPoint file format.

References: https://docs.microsoft.com/en-us/microsoft-365/compliance/partially-indexed-items-in-content-search?view=o365-worldwide
https://docs.microsoft.com/en-us/office365/securitycompliance/export-a-content-search-report

QUESTION 26 You have a Microsoft 365 subscription.

From the Security & Compliance admin center, you create a content search of a mailbox.

You need to view the content of the mail messages found by the search as quickly as possible.

What should you select from the Content search settings?

A. Export report
B. Export results
C. Re-run
D. View results

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:
Explanation:
There is no 'View Results" option. You can preview results but that will only show up to 100 emails. To guarantee you're getting all results, you'll need to export them to a PST file.

References: https://docs.microsoft.com/en-us/microsoft-365/compliance/limits-for-content-search

QUESTION 27
HOTSPOT

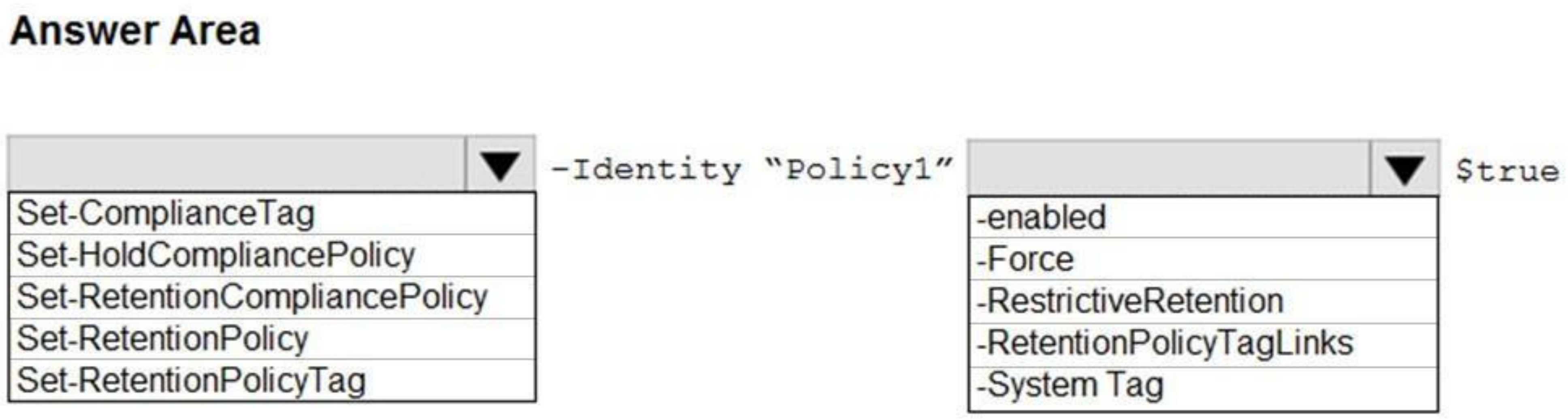
From the Security & Compliance admin center, you create a retention policy named Policy1.

You need to prevent all users from disabling the policy or reducing the retention period.

How should you configure the Azure PowerShell command? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

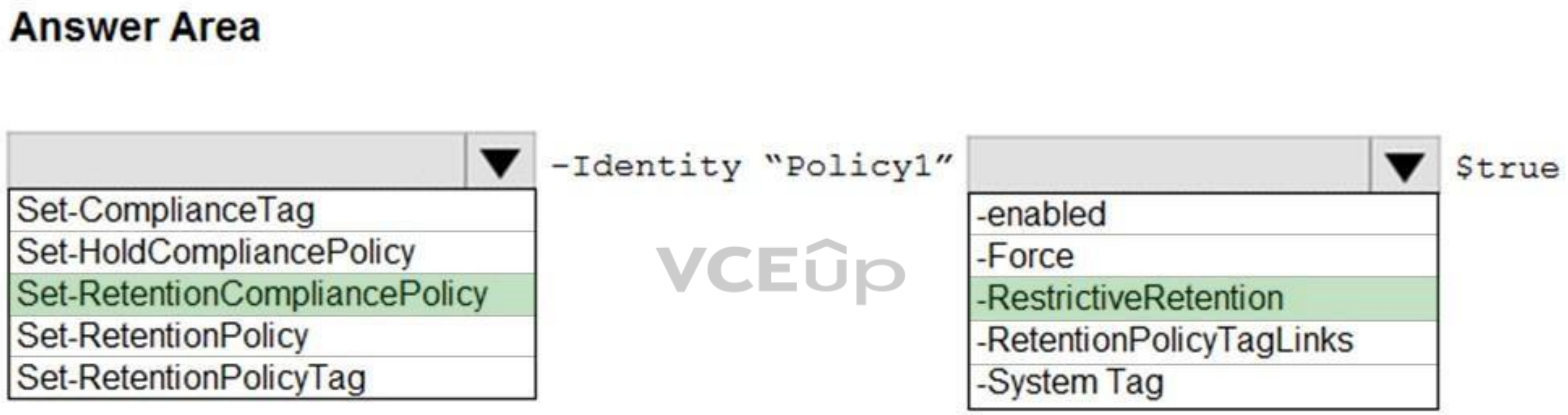
- Set-ComplianceTag
- Set-HoldCompliancePolicy
- Set-RetentionCompliancePolicy
- Set-RetentionPolicy
- Set-RetentionPolicyTag

-Identity "Policy1"

- -enabled
- -Force
- -RestrictiveRetention
- -RetentionPolicyTagLinks
- -System Tag

$true

Correct Answer:



Answer Area

- Set-ComplianceTag
- Set-HoldCompliancePolicy
- [✓ Set-RetentionCompliancePolicy]
- Set-RetentionPolicy
- Set-RetentionPolicyTag

-Identity "Policy1"

- -enabled
- -Force
- [✓ -RestrictiveRetention]
- -RetentionPolicyTagLinks
- -System Tag

$true

Section: [none]
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/powershell/module/exchange/policy-and-compliance-retention/set-retentioncompliancepolicy?view=exchange-ps

QUESTION 28 Your company has a Microsoft 365 subscription that uses an Azure Active Directory (Azure AD) tenant named contoso.com.

A user named User1 is a member of a dynamic group named Group1.

User1 reports that he cannot access documents shared to Group1.

You discover that User1 is no longer a member of Group1.

You suspect that an administrator made a change that caused User1 to be removed from Group1.

You need to identify which administrator made the change.

Which audit log activity should you search in the Security & Compliance admin center?

A. Azure AD group administration activities – Removed member from group

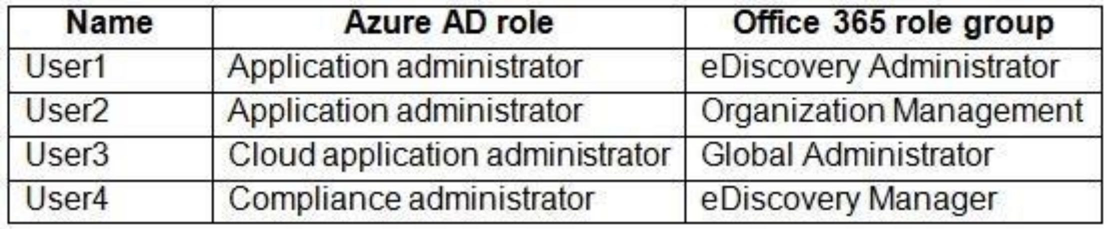
B. User administration activities – Updated user
C. Azure AD group administration activities – Updated group

Correct Answer: C
Section: [none]
Explanation

Explanation/Reference:

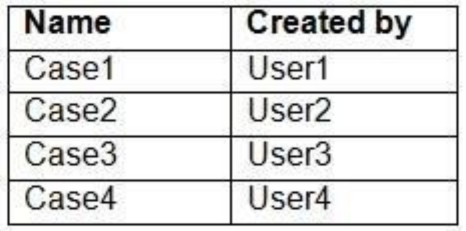
QUESTION 29
HOTSPOT

You have a Microsoft 365 tenant named contoso.com. The tenant contains the users shown in the following table.



Name	Azure AD role	Office 365 role group
User1	Application administrator	eDiscovery Administrator
User2	Application administrator	Organization Management
User3	Cloud application administrator	Global Administrator
User4	Compliance administrator	eDiscovery Manager

You have the eDiscovery cases shown in the following table.

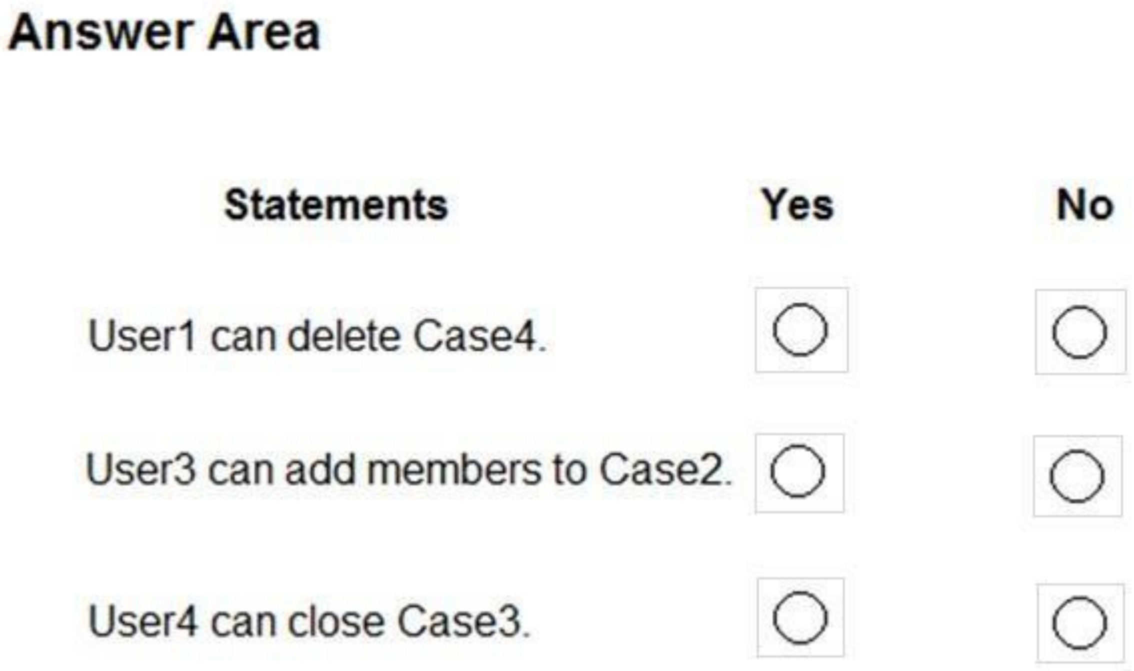


Name	Created by
Case1	User1
Case2	User2
Case3	User3
Case4	User4

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

NOTE: Each correct selection is worth one point.

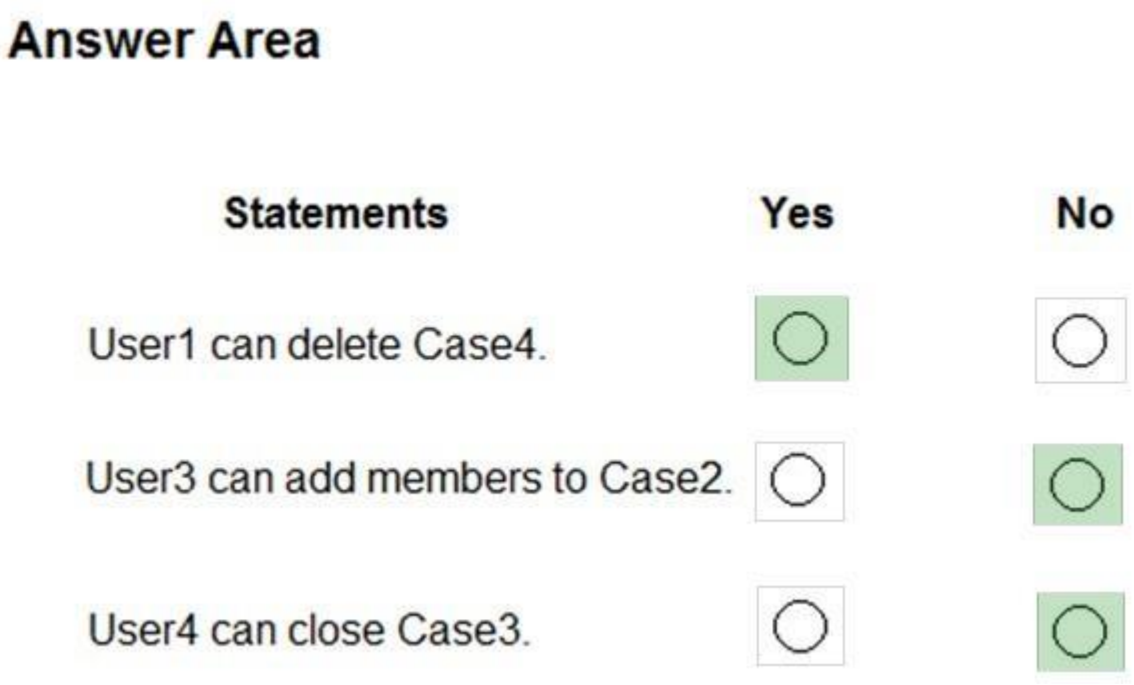
Hot Area:



Answer Area

Statements	Yes	No
User1 can delete Case4.	○	○
User3 can add members to Case2.	○	○
User4 can close Case3.	○	○

Correct Answer:



Answer Area

Statements	Yes	No
User1 can delete Case4.	[✓ ○]	○
User3 can add members to Case2.	○	[✓ ○]
User4 can close Case3.	○	[✓ ○]

Section: [none]
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/microsoft-365/compliance/assign-ediscovery-permissions

QUESTION 30 You have a Microsoft 365 subscription.

All users have their email stored in Microsoft Exchange Online.

In the mailbox of a user named User1, you need to preserve a copy of all the email messages that contain the word ProjectX.

What should you do?

A. From the Security & Compliance admin center, create a data loss prevention (DLP) policy.
B. From the Security & Compliance admin center, create a label and a label policy.
C. From the Security & Compliance admin center, start a message trace.
D. From Microsoft Cloud App Security, create an activity policy.

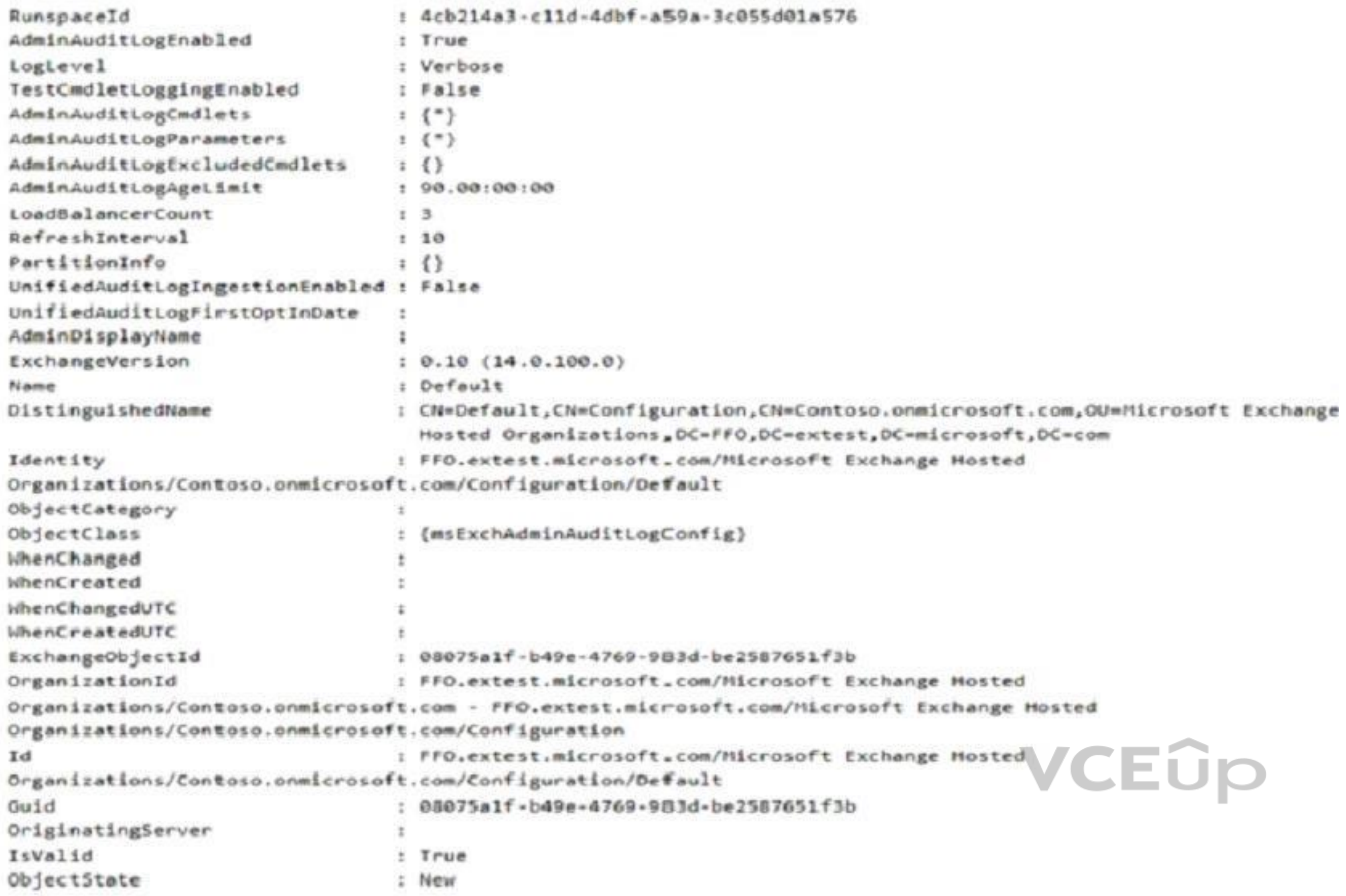
Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:

QUESTION 31 You have a Microsoft 365 tenant.

You discover that administrative tasks are unavailable in the Microsoft Office 365 audit logs of the tenant.

You run the `Get-AdminAuditLogConfig` cmdlet and receive the following output:



```
RunspaceId                      : 4cb214a3-c11d-4dbf-a59a-3c055d01a576
AdminAuditLogEnabled            : True
LogLevel                        : Verbose
TestCmdletLoggingEnabled        : False
AdminAuditLogCmdlets            : {*}
AdminAuditLogParameters         : {*}
AdminAuditLogExcludedCmdlets    : {}
AdminAuditLogAgeLimit           : 90.00:00:00
LoadBalancerCount               : 3
RefreshInterval                 : 10
PartitionInfo                   : {}
UnifiedAuditLogIngestionEnabled : False
UnifiedAuditLogFirstOptInDate   :
AdminDisplayName                :
ExchangeVersion                 : 0.10 (14.0.100.0)
Name                            : Default
DistinguishedName               : CN=Default,CN=Configuration,CN=Contoso.onmicrosoft.com,OU=Microsoft Exchange
                                  Hosted Organizations,DC-FFO,DC-extest,DC-microsoft,DC-com
Identity                        : FFO.extest.microsoft.com/Microsoft Exchange Hosted
Organizations/Contoso.onmicrosoft.com/Configuration/Default
ObjectCategory                  :
ObjectClass                     : {msExchAdminAuditLogConfig}
WhenChanged                     :
WhenCreated                     :
WhenChangedUTC                  :
WhenCreatedUTC                  :
ExchangeObjectId                : 08075a1f-b49e-4769-983d-be2587651f3b
OrganizationId                  : FFO.extest.microsoft.com/Microsoft Exchange Hosted
Organizations/Contoso.onmicrosoft.com - FFO.extest.microsoft.com/Microsoft Exchange Hosted
Organizations/Contoso.onmicrosoft.com/Configuration
Id                              : FFO.extest.microsoft.com/Microsoft Exchange Hosted
Organizations/Contoso.onmicrosoft.com/Configuration/Default
Guid                            : 08075a1f-b49e-4769-983d-be2587651f3b
OriginatingServer               :
IsValid                         : True
ObjectState                     : New
```

You need to ensure that administrative tasks are logged in the Office 365 audit logs.

Which attribute should you modify?

A. `TestCmdletLoggingEnabled`
B. `UnifiedAuditLogIngestionEnabled`
C. `AdminAuditLogEnabled`

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/powershell/module/exchange/policy-and-compliance-audit/set-adminauditlogconfig?view=exchange-ps

QUESTION 32
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 new Microsoft 365 subscription.

You need to prevent users from sending email messages that contain Personally Identifiable Information (PII).

Solution: From the Security & Compliance admin center, you create a data loss prevention (DLP) policy.

Does this meet the goal?

A. Yes
B. No

Correct Answer: A
Section: [none]
Explanation

Explanation/Reference:

QUESTION 33 Your company has a Microsoft 365 tenant.

The company sells products online and processes credit card information.

You need to be notified if a file stored in Microsoft SharePoint Online contains credit card information. The file must be removed automatically from its current location until an administrator can review its contents.

What should you use?

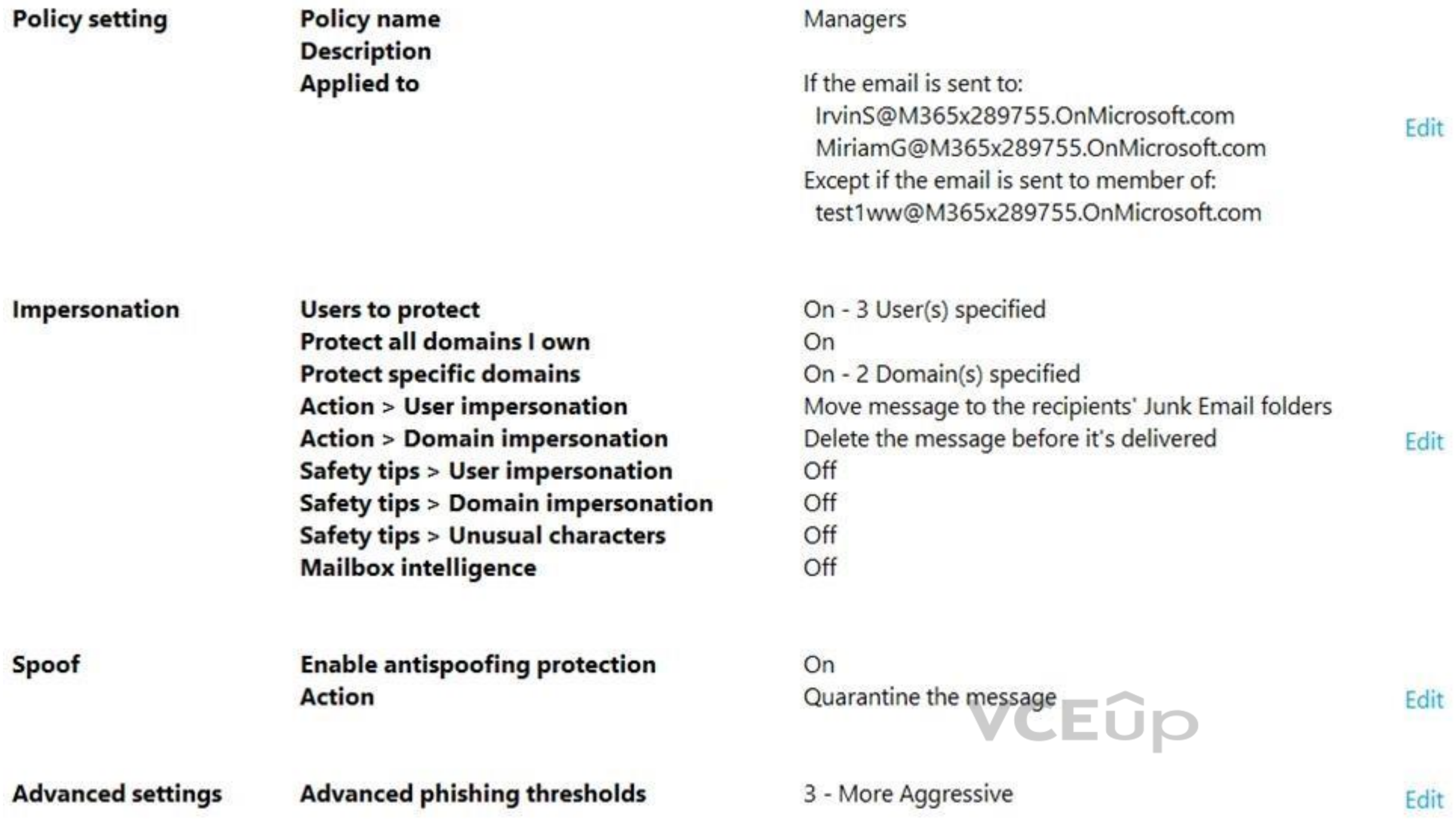
A. a Security & Compliance data loss prevention (DLP) policy
B. a Microsoft Cloud App Security access policy
C. a Security & Compliance retention policy
D. a Microsoft Cloud App Security file policy

Correct Answer: A
Section: [none]
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/office365/securitycompliance/data-loss-prevention-policies

QUESTION 34
HOTSPOT

You configure an anti-phishing policy as shown in the following exhibit.

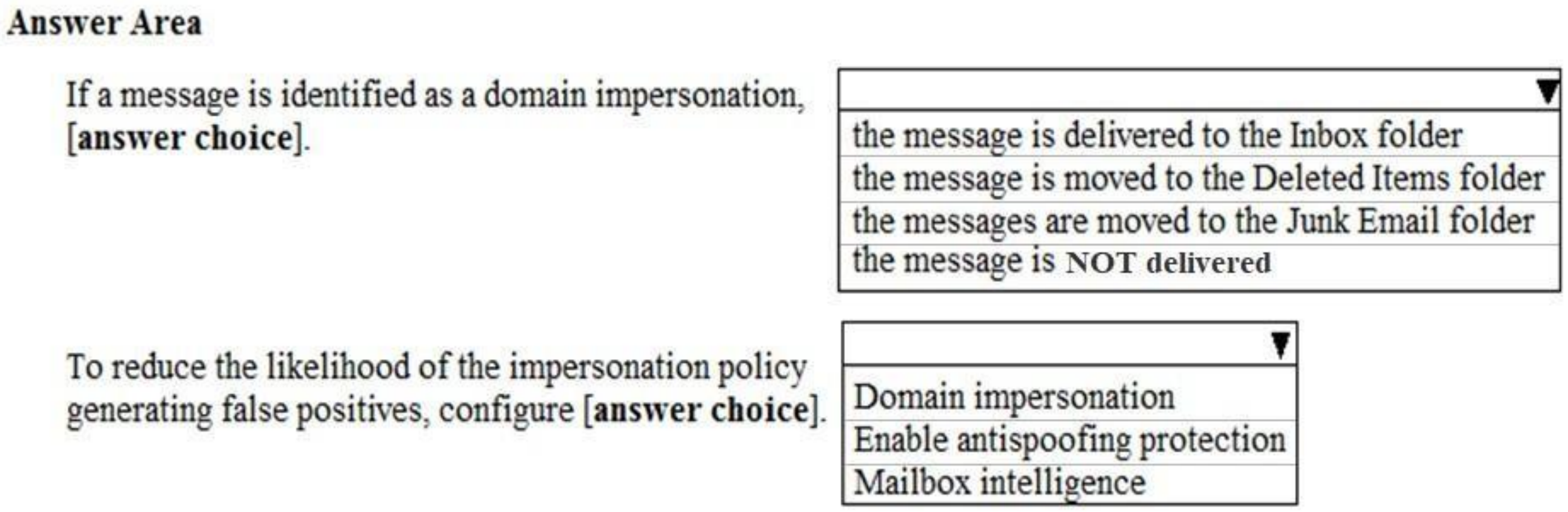


Policy setting	**Policy name** **Description** **Applied to**	Managers If the email is sent to: IrvinS@M365x289755.OnMicrosoft.com MiriamG@M365x289755.OnMicrosoft.com Except if the email is sent to member of: test1ww@M365x289755.OnMicrosoft.com	Edit
Impersonation	**Users to protect** **Protect all domains I own** **Protect specific domains** **Action > User impersonation** **Action > Domain impersonation** **Safety tips > User impersonation** **Safety tips > Domain impersonation** **Safety tips > Unusual characters** **Mailbox intelligence**	On - 3 User(s) specified On On - 2 Domain(s) specified Move message to the recipients' Junk Email folders Delete the message before it's delivered Off Off Off Off	Edit
Spoof	**Enable antispoofing protection** **Action**	On Quarantine the message	Edit
Advanced settings	**Advanced phishing thresholds**	3 - More Aggressive	Edit

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:



Answer Area

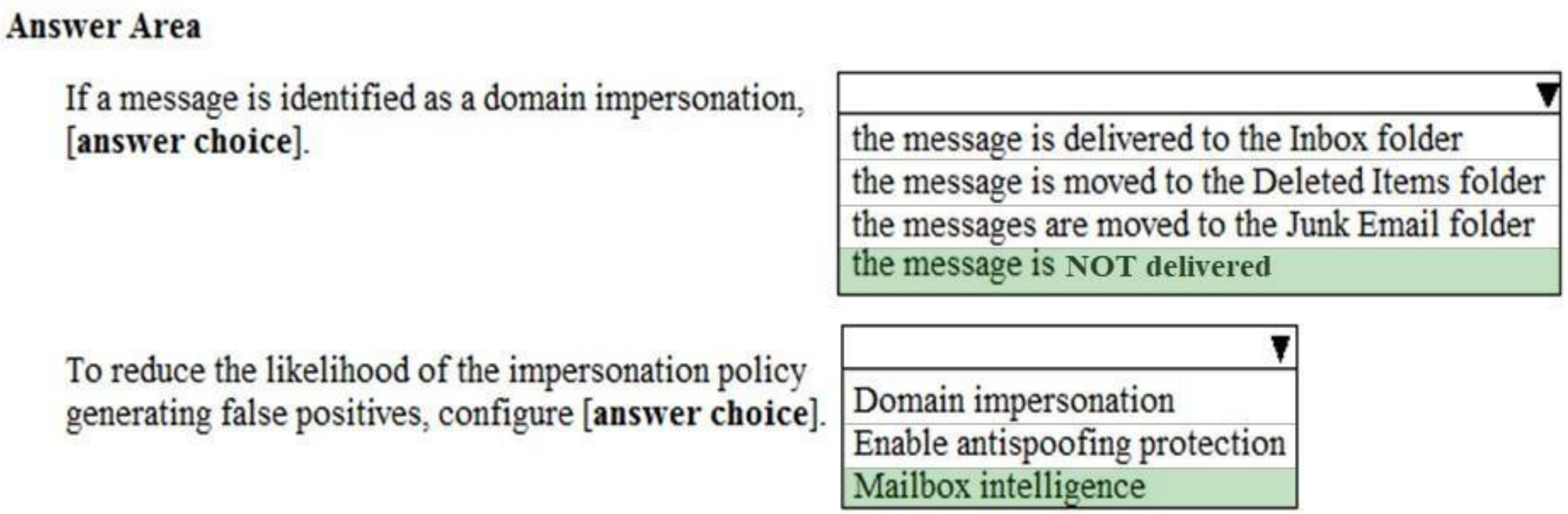
If a message is identified as a domain impersonation, [**answer choice**].

▼
the message is delivered to the Inbox folder
the message is moved to the Deleted Items folder
the messages are moved to the Junk Email folder
the message is **NOT delivered**

To reduce the likelihood of the impersonation policy generating false positives, configure [**answer choice**].

▼
Domain impersonation
Enable antispoofing protection
Mailbox intelligence

Correct Answer:



Answer Area

If a message is identified as a domain impersonation, [answer choice].

- the message is delivered to the Inbox folder
- the message is moved to the Deleted Items folder
- the messages are moved to the Junk Email folder
- [✓ the message is NOT delivered]

To reduce the likelihood of the impersonation policy generating false positives, configure [answer choice].

- Domain impersonation
- Enable antispoofing protection
- [✓ Mailbox intelligence]

Section: [none]
Explanation

Explanation/Reference:
Reference: https://docs.microsoft.com/en-us/office365/securitycompliance/set-up-anti-phishing-policies#learn-about-atp-anti-phishing-policy-options

QUESTION 35
You need to notify the manager of the human resources department when a user in the department shares a file or folder from the department's Microsoft SharePoint Online site.

What should you do?

A. From the Security & Compliance admin center, create an alert policy.
B. From the SharePoint Online site, create an alert.
C. From the SharePoint Online admin center, modify the sharing settings.
D. From the Security & Compliance admin center, create a data loss prevention (DLP) policy.

Correct Answer: A
Section: [none]
Explanation

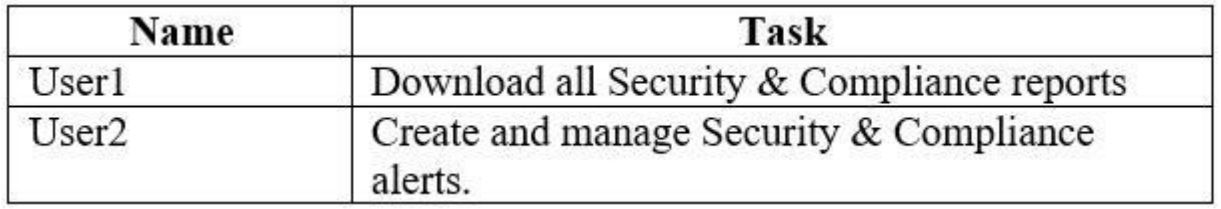
Explanation/Reference:
References: https://docs.microsoft.com/en-us/office365/securitycompliance/create-activity-alerts

QUESTION 36
HOTSPOT

You have a Microsoft 365 subscription.

You are configuring permissions for Security & Compliance.

You need to ensure that the users can perform the tasks shown in the following table.



Name	Task
User1	Download all Security & Compliance reports
User2	Create and manage Security & Compliance alerts.

The solution must use the principle of least privilege.

To which role should you assign each user? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Correct Answer:

Section: [none]
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/office365/securitycompliance/permissions-in-the-security-and-compliance-center#mapping-of-role-groups-to-assigned-roles

QUESTION 37
HOTSPOT

You have a Microsoft Azure Active Directory (Azure AD) tenant named contoso.onmicrosoft.com.

Your company implements Windows Information Protection (WIP).

You need to modify which users and applications are affected by WIP.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Correct Answer:

Section: [none]
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/windows/security/information-protection/windows-information-protection/create-wip-policy-using-intune-azure

QUESTION 38
HOTSPOT

You have a Microsoft 365 subscription.

All users are assigned Microsoft Azure Active Directory Premium licenses.

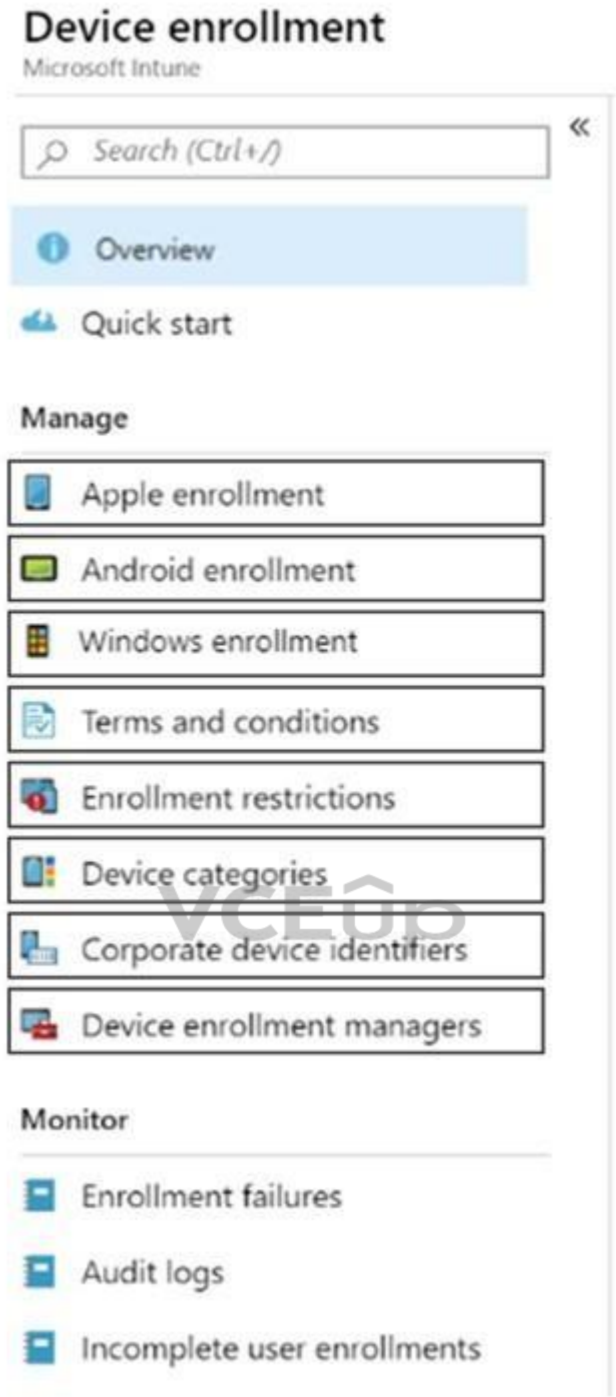
From the Device Management admin center, you set Microsoft Intune as the MDM authority.

You need to ensure that when the members of a group named Marketing join a device to Azure Active Directory (Azure AD), the device is enrolled automatically in Intune. The Marketing group members must be limited to five devices enrolled in Intune.

Which two options should you use to perform the configurations? To answer, select the appropriate blades in the answer area.

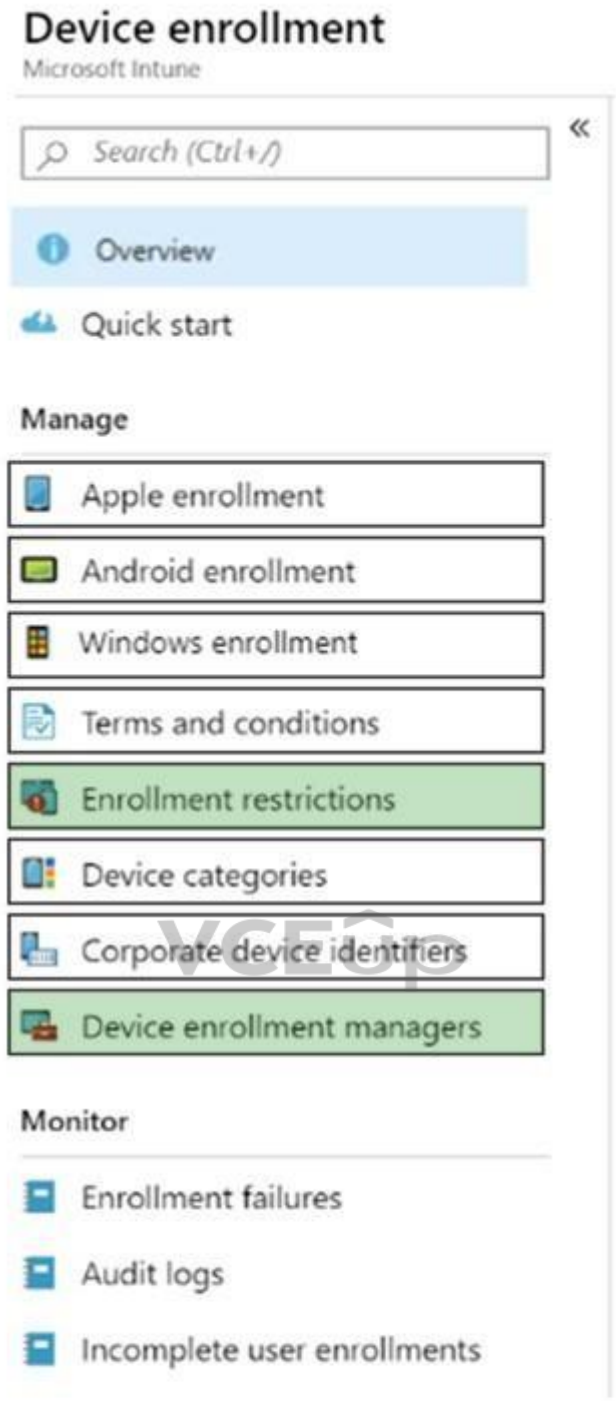
NOTE: Each correct selection is worth one point.

Hot Area:



Device enrollment
Microsoft Intune

Correct Answer:



Device enrollment

Microsoft Intune

Section: [none]
Explanation

Explanation/Reference:
Explanation:

Device enrollment manager (DEM) is an Intune permission that can be applied to an Azure AD user account and lets the user enroll up to 1,000 devices

You can create and manage enrollment restrictions that define what devices can enroll into management with Intune, including the: ▪ Number of devices.
▪ Operating systems and versions.

The Marketing group members must be limited to five devices enrolled in Intune

References:
https://docs.microsoft.com/en-us/intune/enrollment/device-enrollment-manager-enroll

https://docs.microsoft.com/en-us/intune/enrollment/enrollment-restrictions-set

QUESTION 39 You have a Microsoft 365 subscription.

You plan to enable Microsoft Azure Information Protection.

You need to ensure that only the members of a group named PilotUsers can protect content.

What should you do?

A. Run the `Set-AadrmOnboardingControlPolicy` cmdlet.
B. Run the `Add-AadrmRoleBasedAdministrator` cmdlet.
C. Create an Azure Information Protection policy.
D. Configure the protection activation status for Azure Information Protection.

Correct Answer: C
Section: [none]
Explanation

Explanation/Reference:
Reference: https://blogs.technet.microsoft.com/kemckinn/2018/05/17/creating-labels-for-azure-information-protection/

QUESTION 40 Your company has a Microsoft 365 subscription.

You need to identify which users performed the following privileged administration tasks:

- Deleted a folder from the second-stage Recycle Bin of Microsoft SharePoint
- Opened a mailbox of which the user was not the owner
- Reset a user password

What should you use?

A. Microsoft Azure Active Directory (Azure AD) audit logs
B. Security & Compliance content search
C. Microsoft Azure Active Directory (Azure AD) sign-ins
D. Security & Compliance audit log search

Correct Answer: A
Section: [none]
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/azure/azure-monitor/platform/activity-logs-overview

QUESTION 41 You have a Microsoft 365 subscription.

You have a user named User1.

You need to ensure that User1 can place a litigation hold on all mailbox content.

Which role should you assign to User1?

A. eDiscovery Manager from the Security & Compliance admin center

B. Compliance Management from the Exchange admin center
C. User management administrator from the Microsoft 365 admin center
D. Information Protection administrator from the Azure Active Directory admin center

Correct Answer: A
Section: [none]
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/Exchange/permissions/feature-permissions/policy-and-compliance-permissions?view=exchserver-2019

QUESTION 42 You have a Microsoft 365 subscription.

All users are assigned a Microsoft 365 E3 license.

You enable auditing for your organization.

What is the maximum amount of time data will be retained in the Microsoft 365 audit log?

A. 2 years
B. 1 year
C. 30 days
D. 90 days

Correct Answer: D
Section: [none]
Explanation

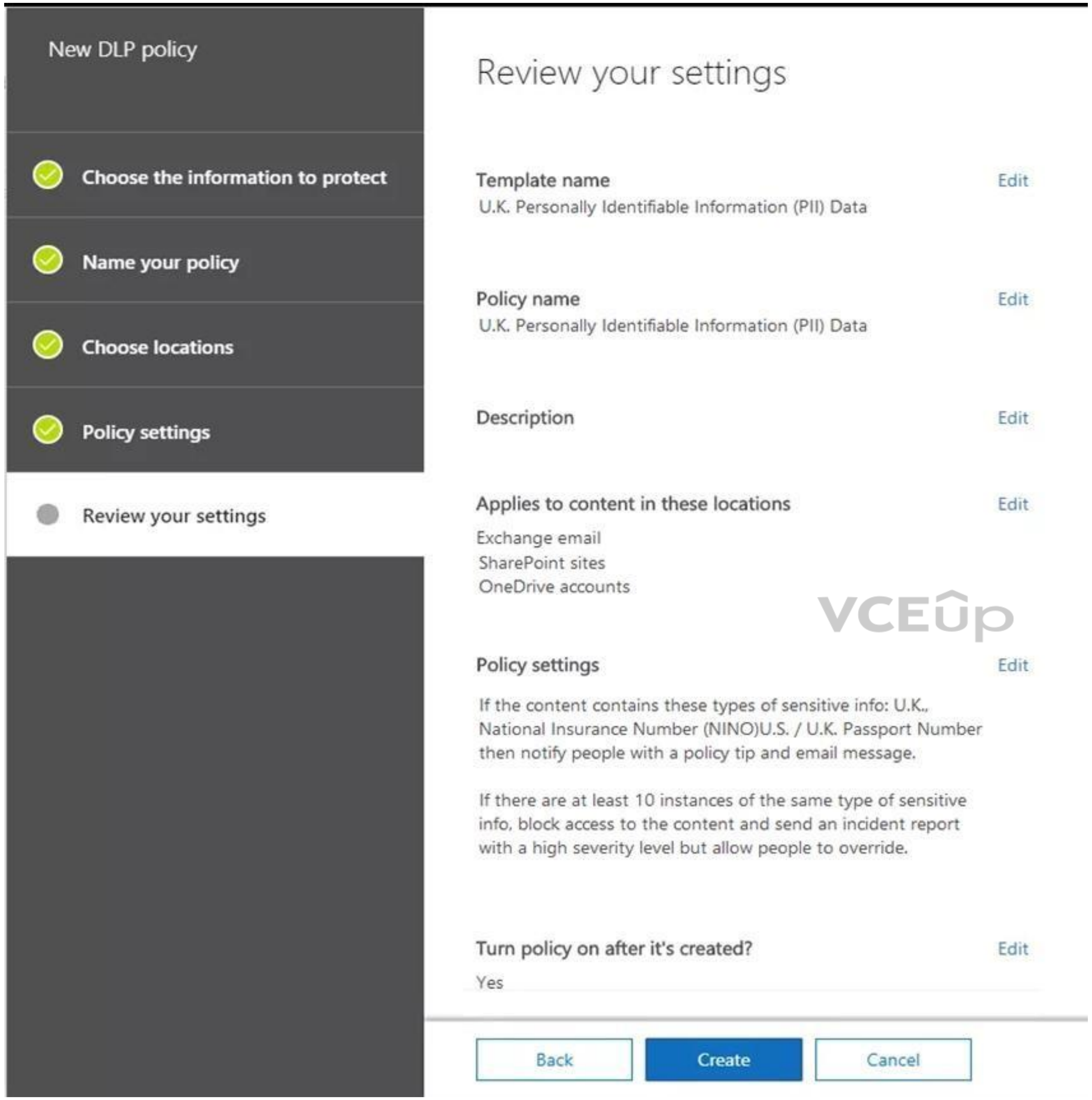
Explanation/Reference:
References: https://docs.microsoft.com/en-us/office365/securitycompliance/search-the-audit-log-in-security-and-compliance

QUESTION 43
HOTSPOT

Your company is based in the United Kingdom (UK).

Users frequently handle data that contains Personally Identifiable Information (PII).

You create a data loss prevention (DLP) policy that applies to users inside and outside the company. The policy is configured as shown in the following exhibit.



Review your settings

Template name
U.K. Personally Identifiable Information (PII) Data

Policy name
U.K. Personally Identifiable Information (PII) Data

Description

Applies to content in these locations
Exchange email
SharePoint sites
OneDrive accounts

Policy settings

If the content contains these types of sensitive info: U.K., National Insurance Number (NINO)U.S. / U.K. Passport Number then notify people with a policy tip and email message.

If there are at least 10 instances of the same type of sensitive info, block access to the content and send an incident report with a high severity level but allow people to override.

Turn policy on after it's created?
Yes

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:

Correct Answer:

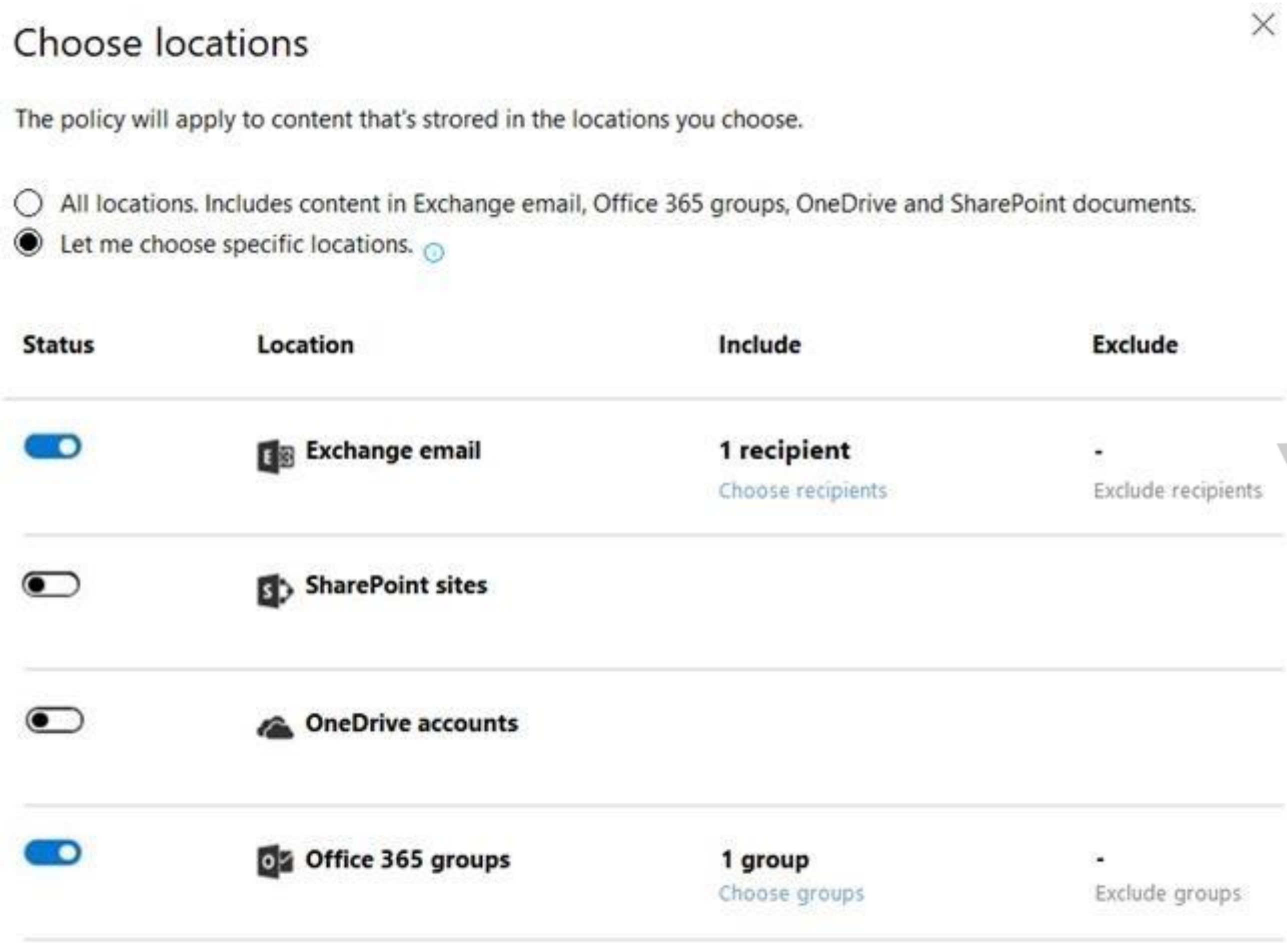
Section: [none]
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/office365/securitycompliance/data-loss-prevention-policies

QUESTION 44
HOTSPOT

You have a Microsoft 365 subscription that contains all the user data.

You plan to create the retention policy shown in the Locations exhibit. (Click the **Locations** tab.)



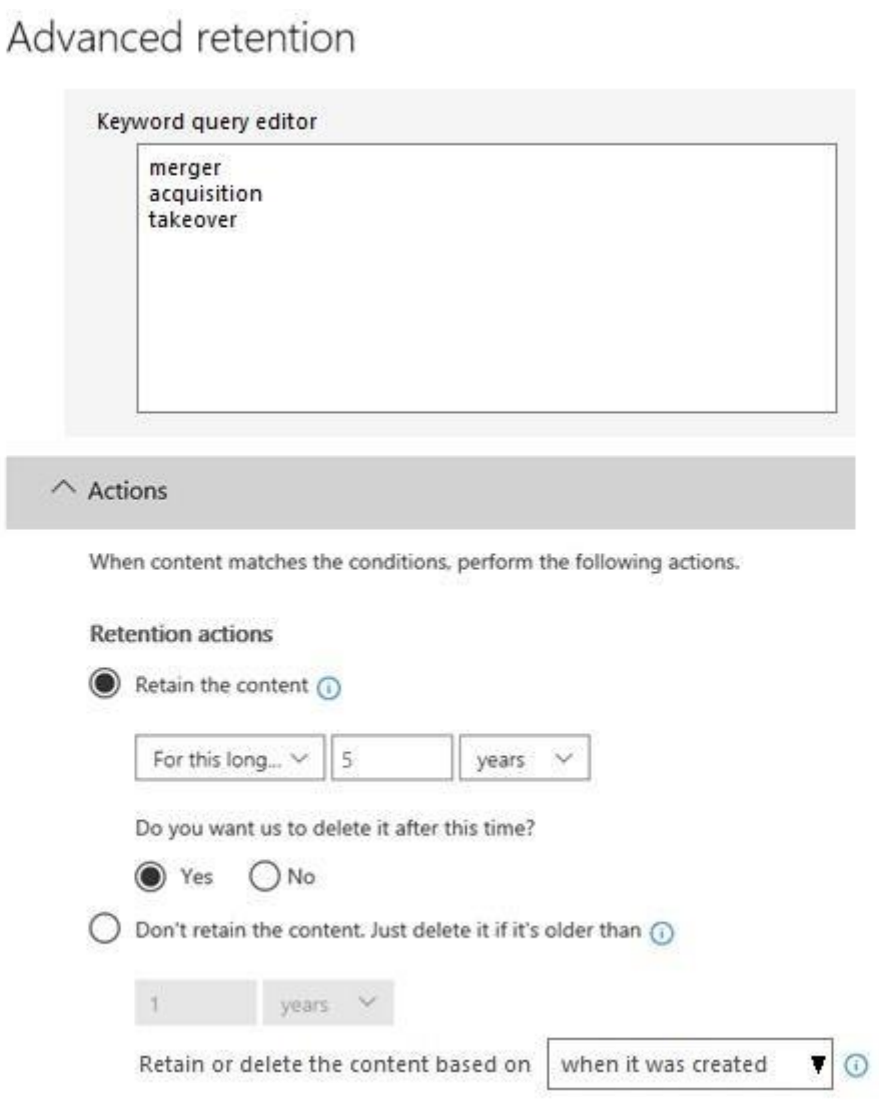
Choose locations

The policy will apply to content that's stored in the locations you choose.

○ All locations. Includes content in Exchange email, Office 365 groups, OneDrive and SharePoint documents.
● Let me choose specific locations.

Status	Location	Include	Exclude
●	Exchange email	1 recipient Choose recipients	- Exclude recipients
○	SharePoint sites		
○	OneDrive accounts		
●	Office 365 groups	1 group Choose groups	- Exclude groups

You configure the Advanced retention settings as shown in the Retention exhibit. (Click the **Retention** tab.)



Advanced retention

Keyword query editor

```
merger
acquisition
takeover
```

Actions

When content matches the conditions, perform the following actions.

Retention actions

● Retain the content

For this long... | 5 | years

Do you want us to delete it after this time?

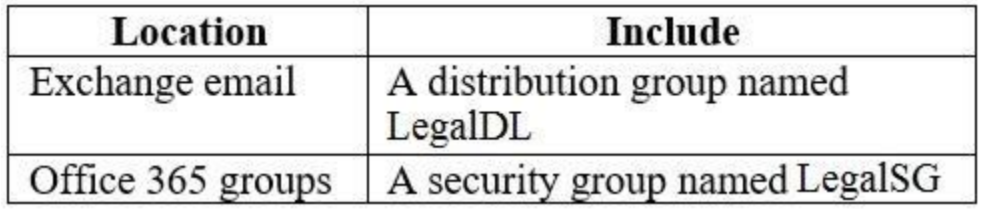
● Yes ○ No

○ Don't retain the content. Just delete it if it's older than

1 | years

Retain or delete the content based on: when it was created

The locations specified in the policy include the groups shown in the following table.

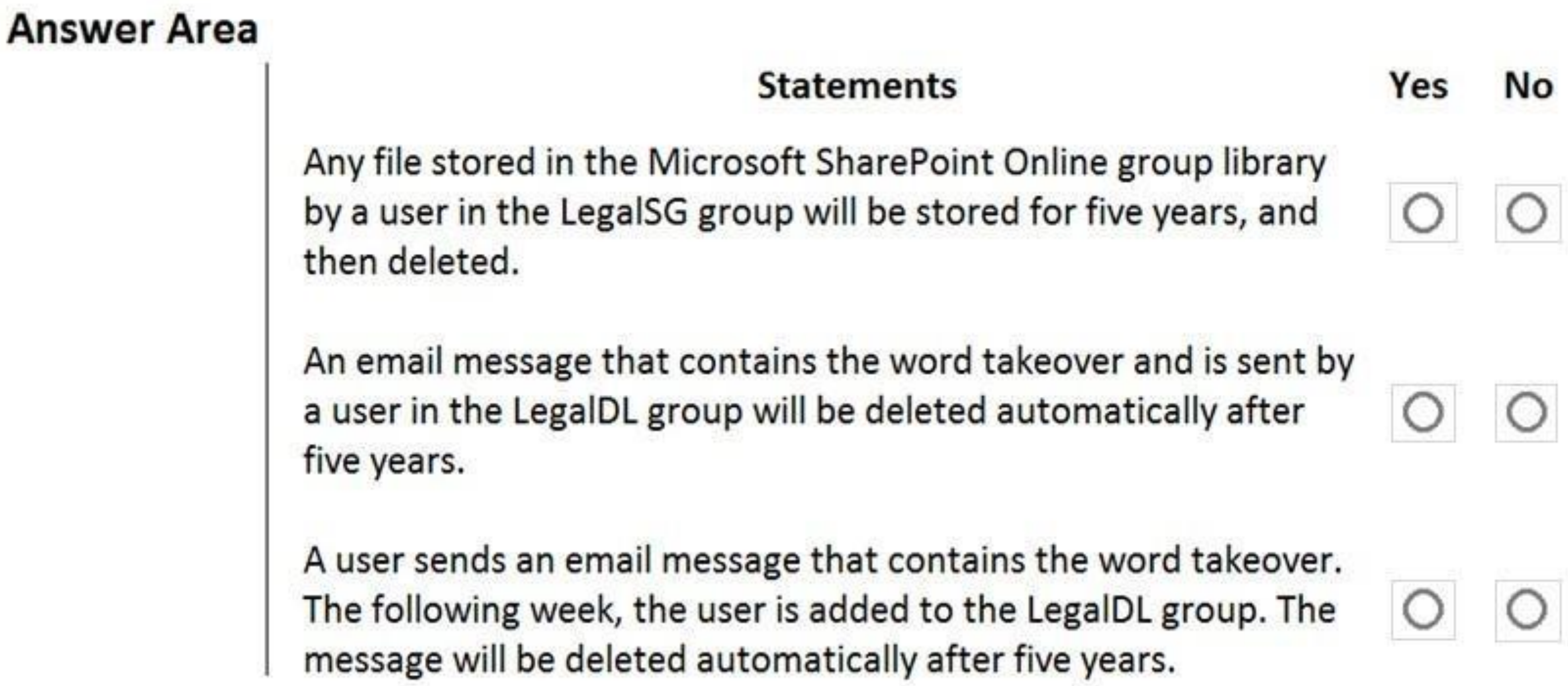


Location	Include
Exchange email	A distribution group named LegalDL
Office 365 groups	A security group named LegalSG

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

NOTE: Each correct selection is worth one point.

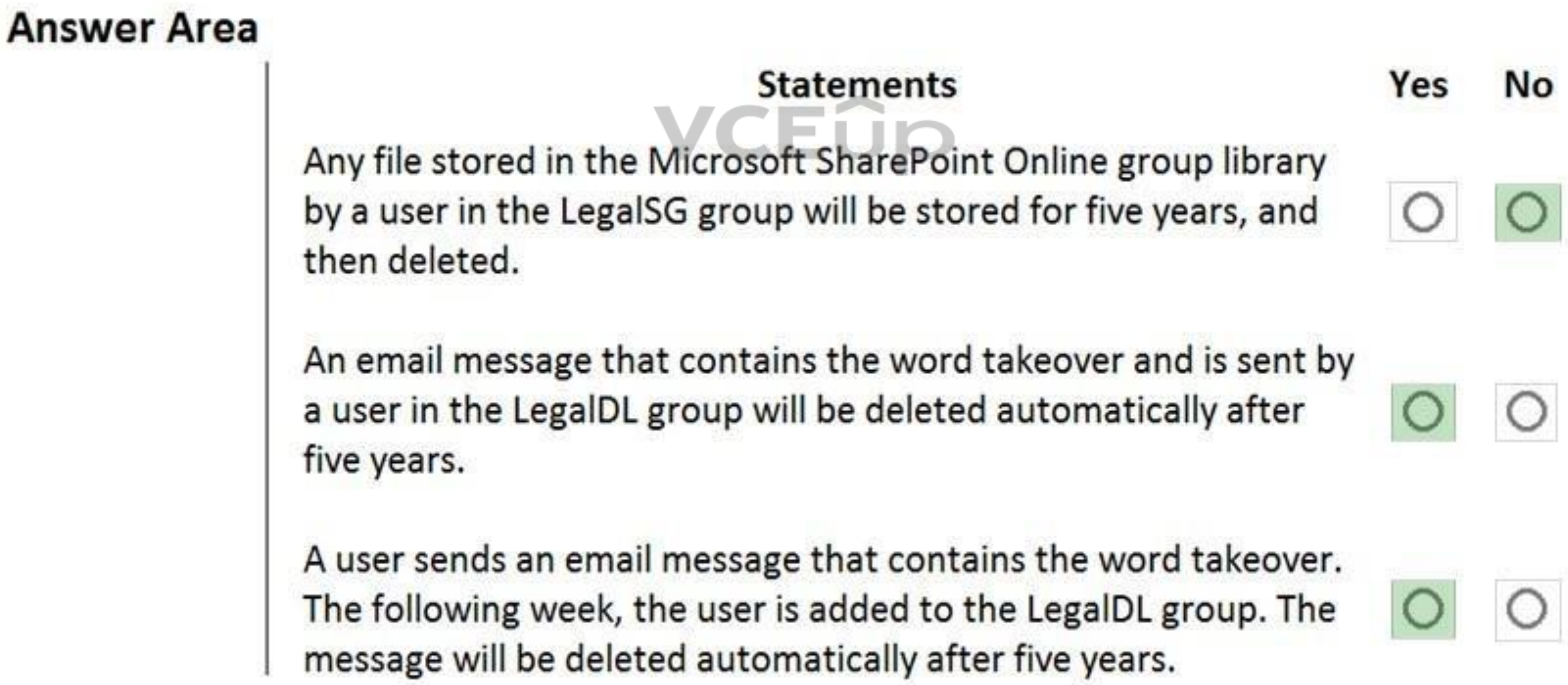
Hot Area:



Answer Area

Statements	Yes	No
Any file stored in the Microsoft SharePoint Online group library by a user in the LegalSG group will be stored for five years, and then deleted.	○	○
An email message that contains the word takeover and is sent by a user in the LegalDL group will be deleted automatically after five years.	○	○
A user sends an email message that contains the word takeover. The following week, the user is added to the LegalDL group. The message will be deleted automatically after five years.	○	○

Correct Answer:



Answer Area

Statements	Yes	No
Any file stored in the Microsoft SharePoint Online group library by a user in the LegalSG group will be stored for five years, and then deleted.	○	[✓ ○]
An email message that contains the word takeover and is sent by a user in the LegalDL group will be deleted automatically after five years.	[✓ ○]	○
A user sends an email message that contains the word takeover. The following week, the user is added to the LegalDL group. The message will be deleted automatically after five years.	[✓ ○]	○

Section: [none]
Explanation

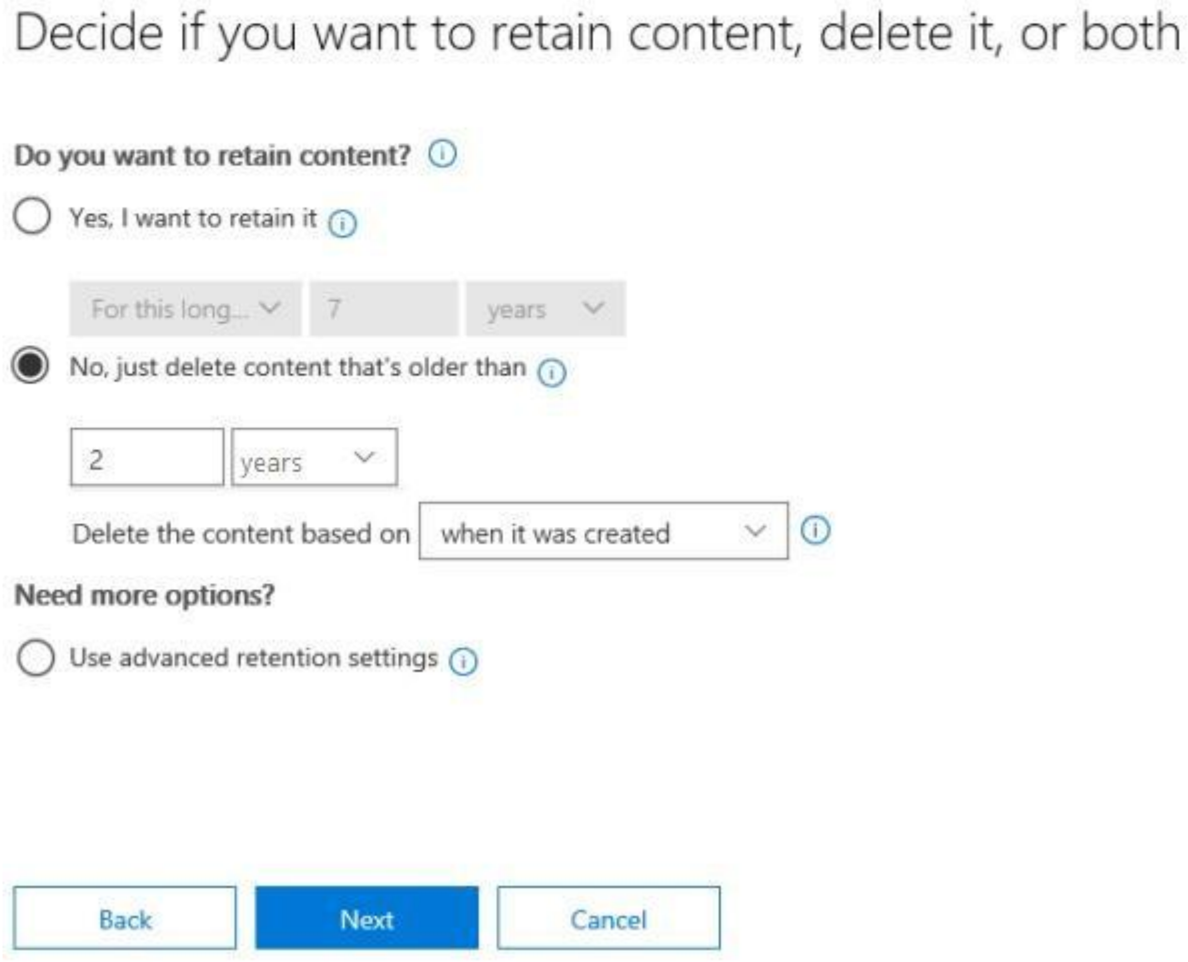
Explanation/Reference:
References: https://docs.microsoft.com/en-us/office365/securitycompliance/retention-policies

QUESTION 45
HOTSPOT

You have retention policies in Microsoft 365 as shown in the following table.

Name	Location
Policy1	OneDrive accounts
Policy2	Exchange email, Exchange public folders, Office 365 groups, OneDrive accounts, SharePoint sites

Policy1 is configured as shown in the Policy1 exhibit. (Click the **Policy1** tab.)



Decide if you want to retain content, delete it, or both

Do you want to retain content?

○ Yes, I want to retain it

For this long... 7 years

● No, just delete content that's older than

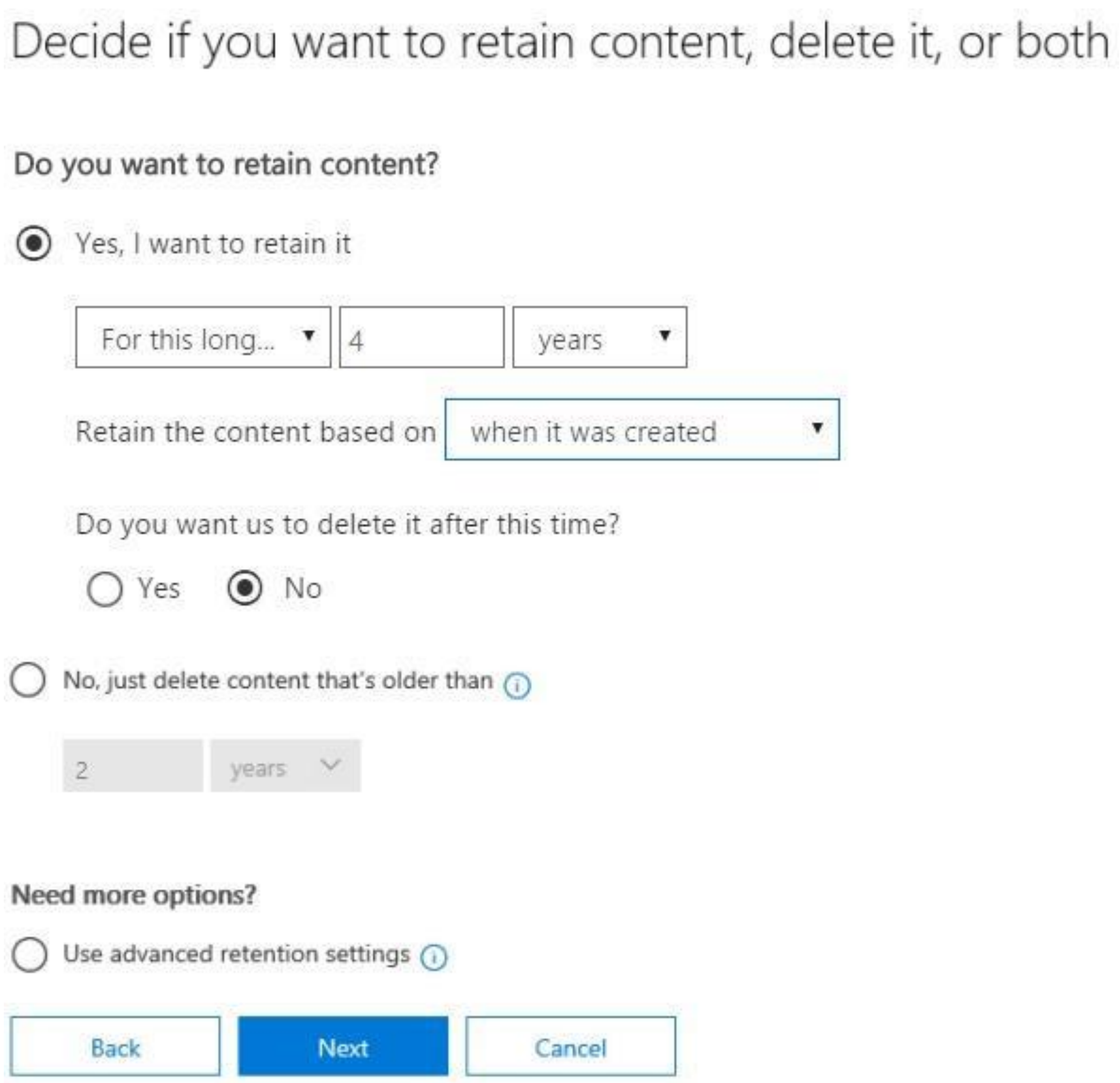
2 years

Delete the content based on when it was created

Need more options?

○ Use advanced retention settings

Policy2 is configured as shown in the Policy2 exhibit. (Click the **Policy2** tab.)



Decide if you want to retain content, delete it, or both

Do you want to retain content?

● Yes, I want to retain it

For this long... ▾ | 4 | years ▾

Retain the content based on: when it was created ▾

Do you want us to delete it after this time?

○ Yes ● No

○ No, just delete content that's older than ⓘ

2 | years ▾

Need more options?

○ Use advanced retention settings ⓘ

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:

Section: [none]
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/office365/securitycompliance/retention-policies#the-principles-of-retention-or-what-takes-precedence

QUESTION 46 You have a Microsoft 365 subscription.

You configure a data loss prevention (DLP) policy.

You discover that users are incorrectly marking content as false positive and bypassing the DLP policy.

You need to prevent the users from bypassing the DLP policy.

What should you configure?

A. incident reports
B. actions
C. exceptions
D. user overrides

Correct Answer: D
Section: [none]
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/office365/securitycompliance/data-loss-prevention-policies

QUESTION 47 You have a Microsoft 365 subscription.

All users have their email stored in Microsoft Exchange Online.

In the mailbox of a user named User1, you need to preserve a copy of all the email messages that contain the word ProjectX.

What should you do?

A. From the Security & Compliance admin center, create an eDiscovery case.
B. From the Exchange admin center, create a mail flow rule.
C. From the Security & Compliance admin center, start a message trace.
D. From Microsoft Cloud App Security, create an access policy.

Correct Answer: A
Section: [none]
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/office365/securitycompliance/ediscovery-cases#step-2-create-a-new-case

QUESTION 48 You have a Microsoft 365 E5 subscription.

You run an eDiscovery search that returns the following Azure Rights Management (Azure RMS) – encrypted content:

- Microsoft Exchange emails
- Microsoft OneDrive documents
- Microsoft SharePoint documents

Which content can be decrypted when you export the eDiscovery search results?

A. Exchange emails only
B. SharePoint documents, OneDrive documents, and Exchange emails
C. OneDrive documents only
D. SharePoint documents and OneDrive documents only
E. SharePoint documents only

Correct Answer: A
Section: [none]
Explanation
Explanation/Reference:

Reference: https://docs.microsoft.com/en-us/microsoft-365/compliance/export-search-results?view=o365-worldwide

QUESTION 49 You have a Microsoft
365 subscription.

You plan to connect to Microsoft Exchange Online PowerShell and run the following cmdlets:

▪ Search-MailboxAuditLog
▪ Test-ClientAccessRule
▪ Set-GroupMailbox ▪ Get-
Mailbox

Which cmdlet will generate an entry in the Microsoft Office 365 audit log?

A. Search-MailboxAuditLog

B. Test-ClientAccessRule

C. Set-GroupMailbox

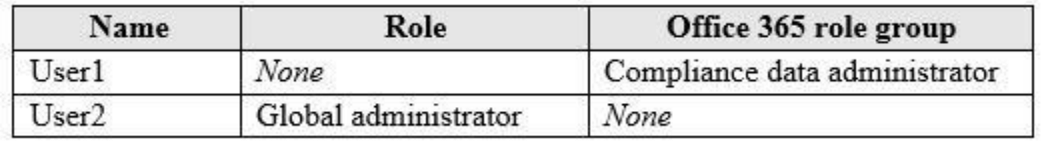
D. Get-Mailbox

Correct Answer: C
Section: [none]
Explanation

Explanation/Reference:
Reference: https://docs.microsoft.com/en-us/microsoft-365/compliance/search-the-audit-log-in-security-and-compliance?view=o365-worldwide#exchange-admin-audit-log

QUESTION 50
HOTSPOT

Your company has a Microsoft 365 subscription that uses an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant contains the users shown in the following table.



Name	Role	Office 365 role group
User1	*None*	Compliance data administrator
User2	Global administrator	*None*

You create a retention label named Label1 that has the following configurations:

- Retains content for five years
- Automatically deletes all content that is older than five years

You turn on Auto labeling for Label1 by using a policy named Policy1. Policy1 has the following configurations:

- Applies to content that contains the word Merger
- Specifies the OneDrive accounts and SharePoint sites locations

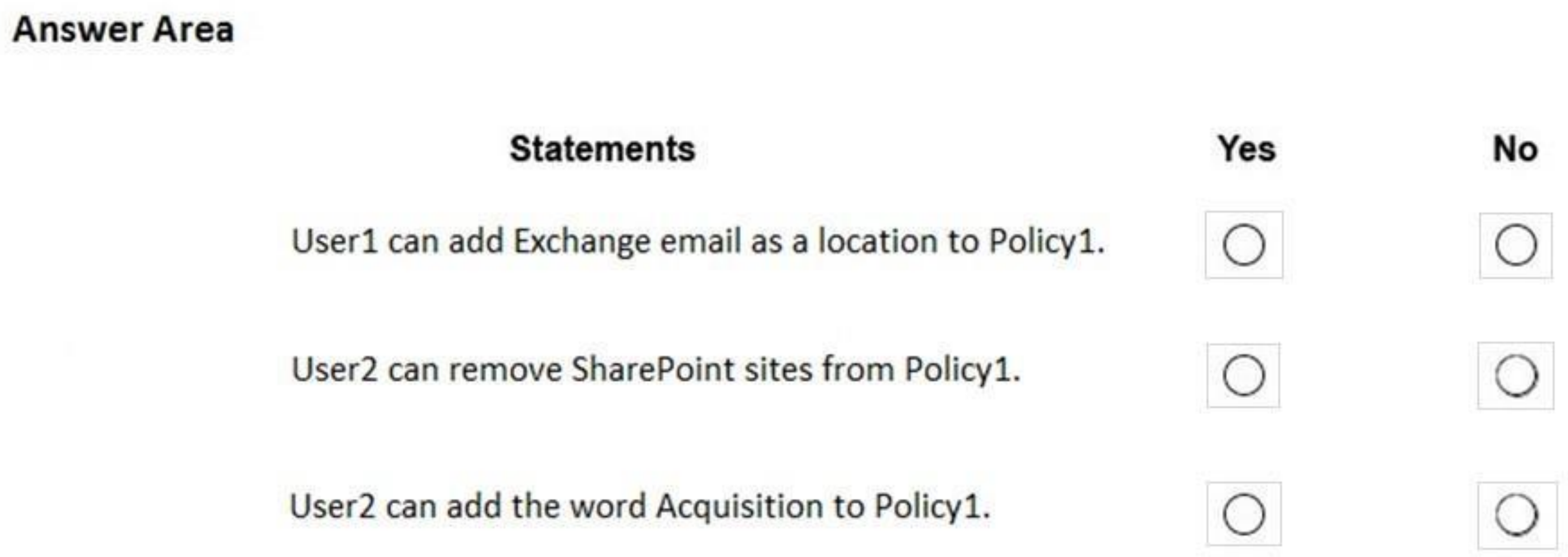
You run the following command.

```
Set-RetentionCompliancePolicy Policy1 -RestrictiveRetention $true -
Force
```

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

NOTE: Each correct selection is worth one point.

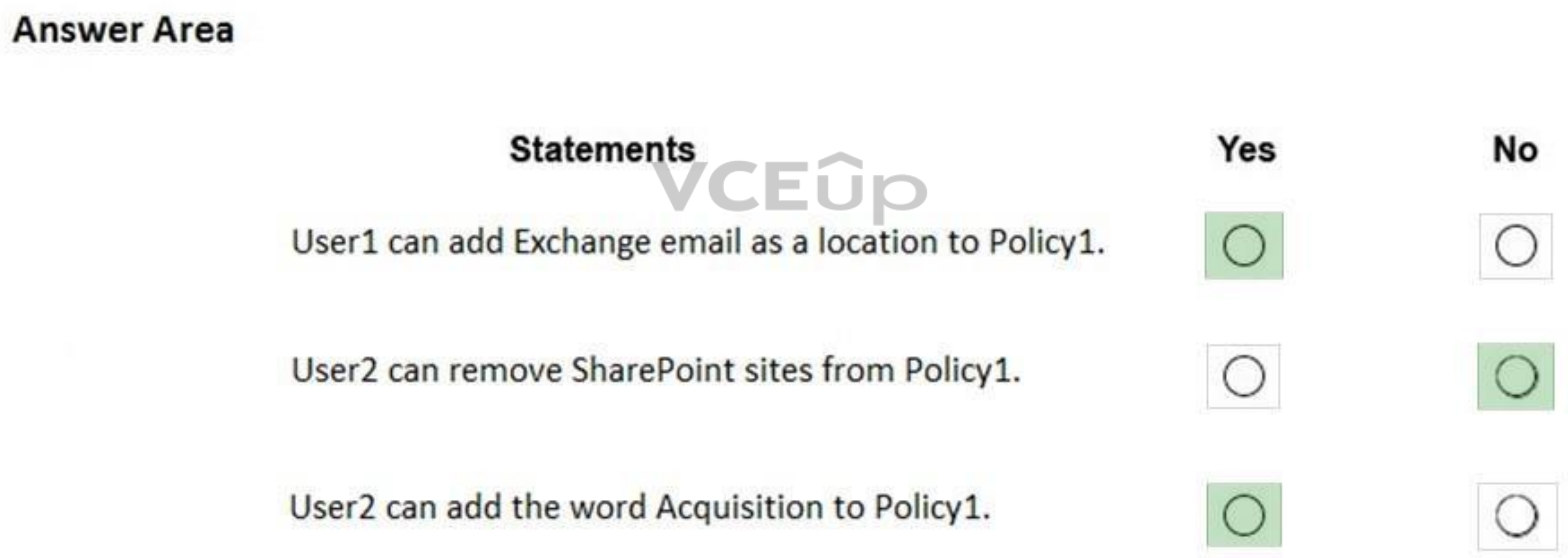
Hot Area:



Answer Area

Statements	Yes	No
User1 can add Exchange email as a location to Policy1.	○	○
User2 can remove SharePoint sites from Policy1.	○	○
User2 can add the word Acquisition to Policy1.	○	○

Correct Answer:



Answer Area

Statements	Yes	No
User1 can add Exchange email as a location to Policy1.	[✓ ○]	○
User2 can remove SharePoint sites from Policy1.	○	[✓ ○]
User2 can add the word Acquisition to Policy1.	[✓ ○]	○

Section: [none]
Explanation

Explanation/Reference:
Reference: https://docs.microsoft.com/en-us/powershell/module/exchange/policy-and-compliance-retention/set-retentioncompliancepolicy?view=exchange-ps

QUESTION 51
HOTSPOT

You have an Azure Active Directory (Azure AD) tenant that contains two users named User1 and User2.

On September 5, 2019, you create and enforce a terms of use (ToU) in the tenant. The ToU has the following settings:

- Name: Terms1
- Display name: Terms1 name

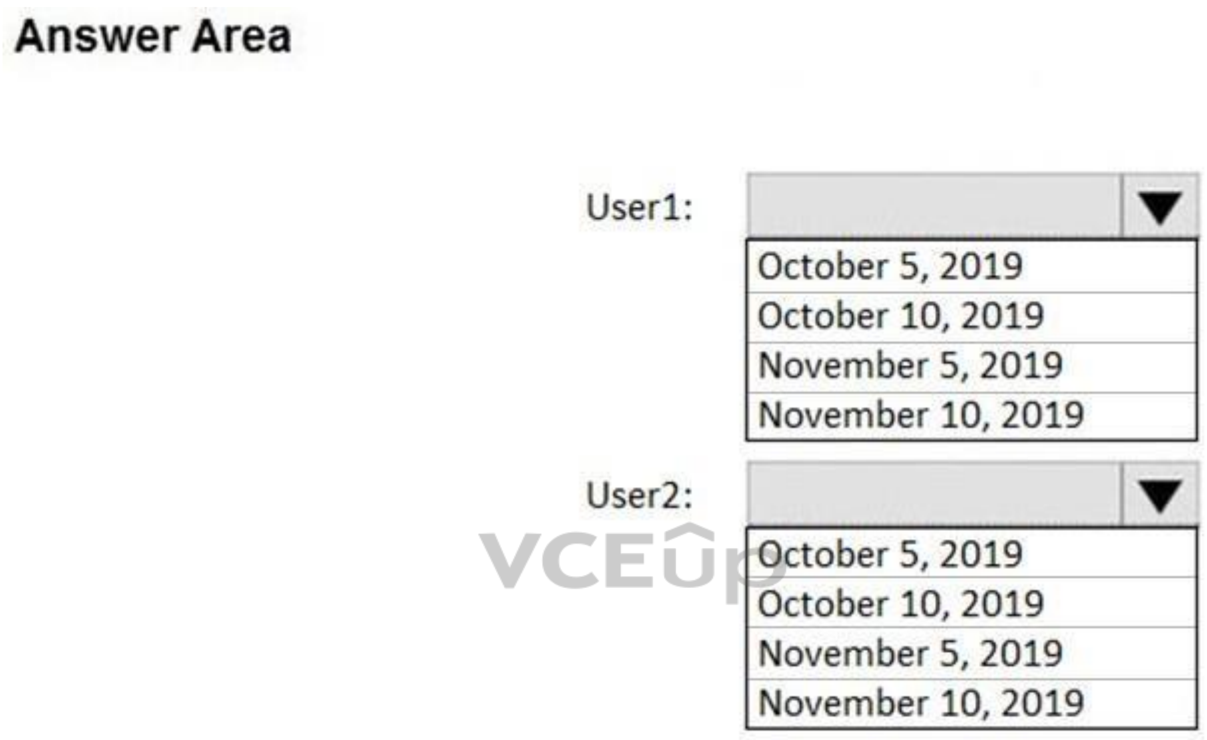
- Require users to expand the terms of use: Off
- Require users to consent on every device: Off
- Expire consents: On
- Expire starting on: October 10, 2019 ▪
Frequency: Monthly

User1 accepts Terms1 on September 5, 2019. User2 accepts Terms1 on October 5, 2019.

When will Terms1 expire for the first time for each user? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

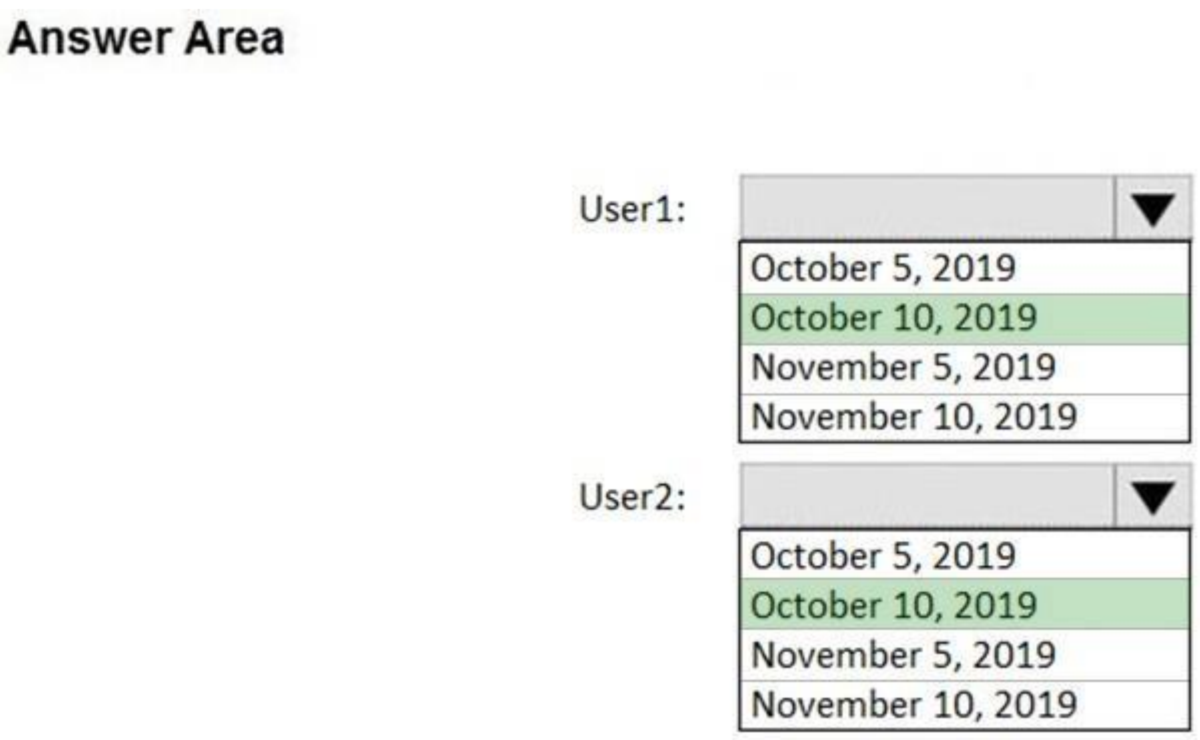


Answer Area

User1:
- October 5, 2019
- October 10, 2019
- November 5, 2019
- November 10, 2019

User2:
- October 5, 2019
- October 10, 2019
- November 5, 2019
- November 10, 2019

Correct Answer:



Answer Area

User1:

- October 5, 2019
- [✓ October 10, 2019]
- November 5, 2019
- November 10, 2019

User2:

- October 5, 2019
- [✓ October 10, 2019]
- November 5, 2019
- November 10, 2019

Section: [none]
Explanation

Explanation/Reference:
Reference: https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/terms-of-use

QUESTION 52
Your company uses on-premises Windows Server File Classification Infrastructure (FCI). Some documents on the on-premises file servers are classified as Confidential.

You migrate the files from the on-premises file servers to Microsoft SharePoint Online.

You need to ensure that you can implement data loss prevention (DLP) policies for the uploaded files based on the Confidential classification.

What should you do first?

A. From the SharePoint admin center, configure hybrid search.
B. From the SharePoint admin center, create a managed property.
C. From the Security & Compliance Center PowerShell, run the `New-DataClassification` cmdlet.
D. From the Security & Compliance Center PowerShell, run the `New-DlpComplianceRule` cmdlet.

Correct Answer: D
Section: [none]
Explanation

Explanation/Reference:
Reference: https://docs.microsoft.com/en-us/powershell/module/exchange/policy-and-compliance-dlp/new-dataclassification?view=exchange-ps

QUESTION 53 You have a Microsoft 365 subscription.

From the Security & Compliance admin center, you create a content search of all the mailboxes that contain the work ProjectX.

You need to export the results of the content search.

What do you need to download the report?

A. a certification authority (CA) certificate
B. an export key
C. a password
D. a user certificate

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:
Reference: https://docs.microsoft.com/en-us/office365/securitycompliance/export-search-results

QUESTION 54
HOTSPOT

You have a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com.

You have three applications named App1, App2, and App3. The apps use files that have the same file extensions.

Your company uses Windows Information Protection (WIP). WIP has the following configurations:

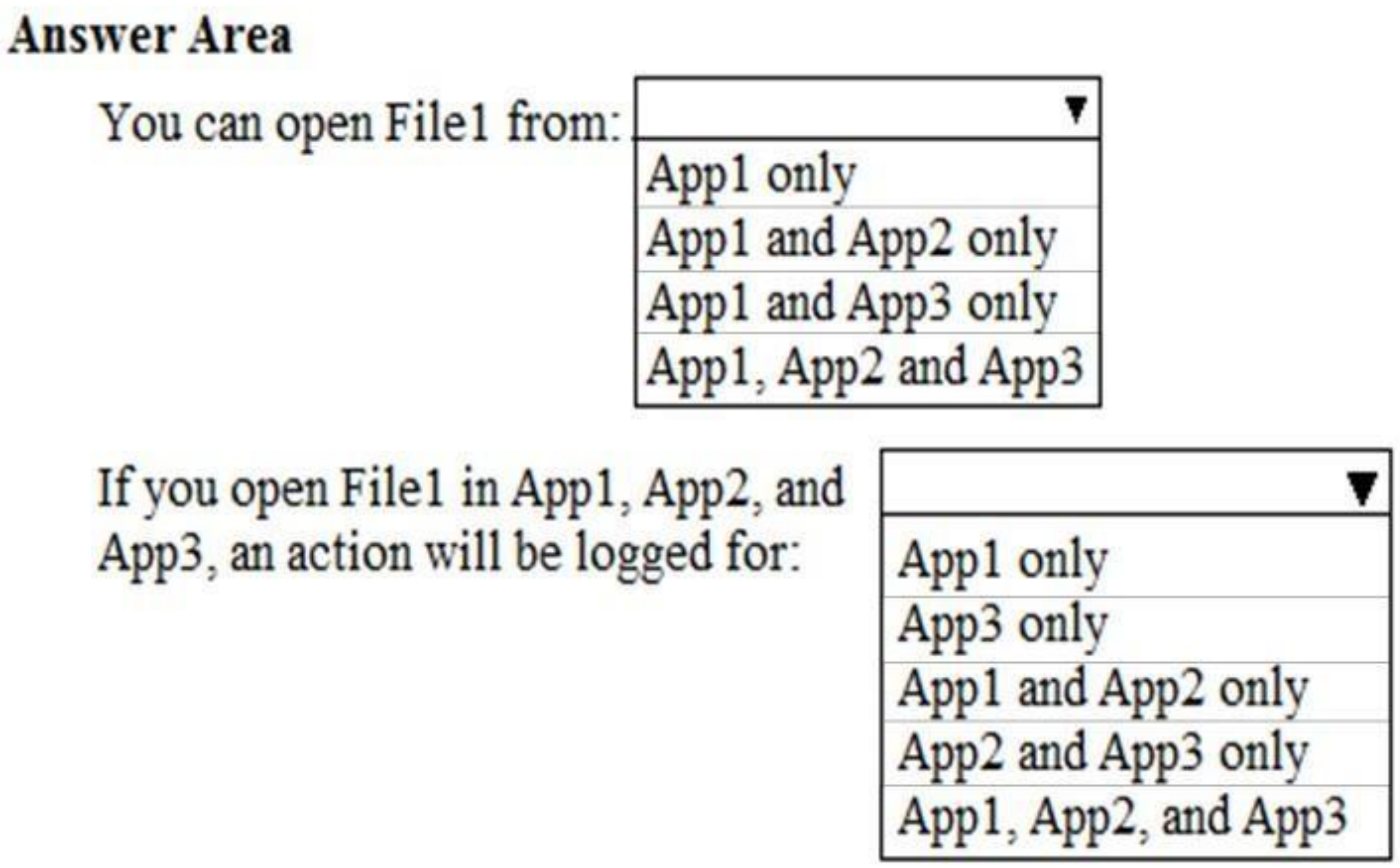
▪ Windows Information Protection mode: Silent
▪ Protected apps: App1 ▪
Exempt apps: App2

From App1, you create a file named File1.

What is the effect of the configurations? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

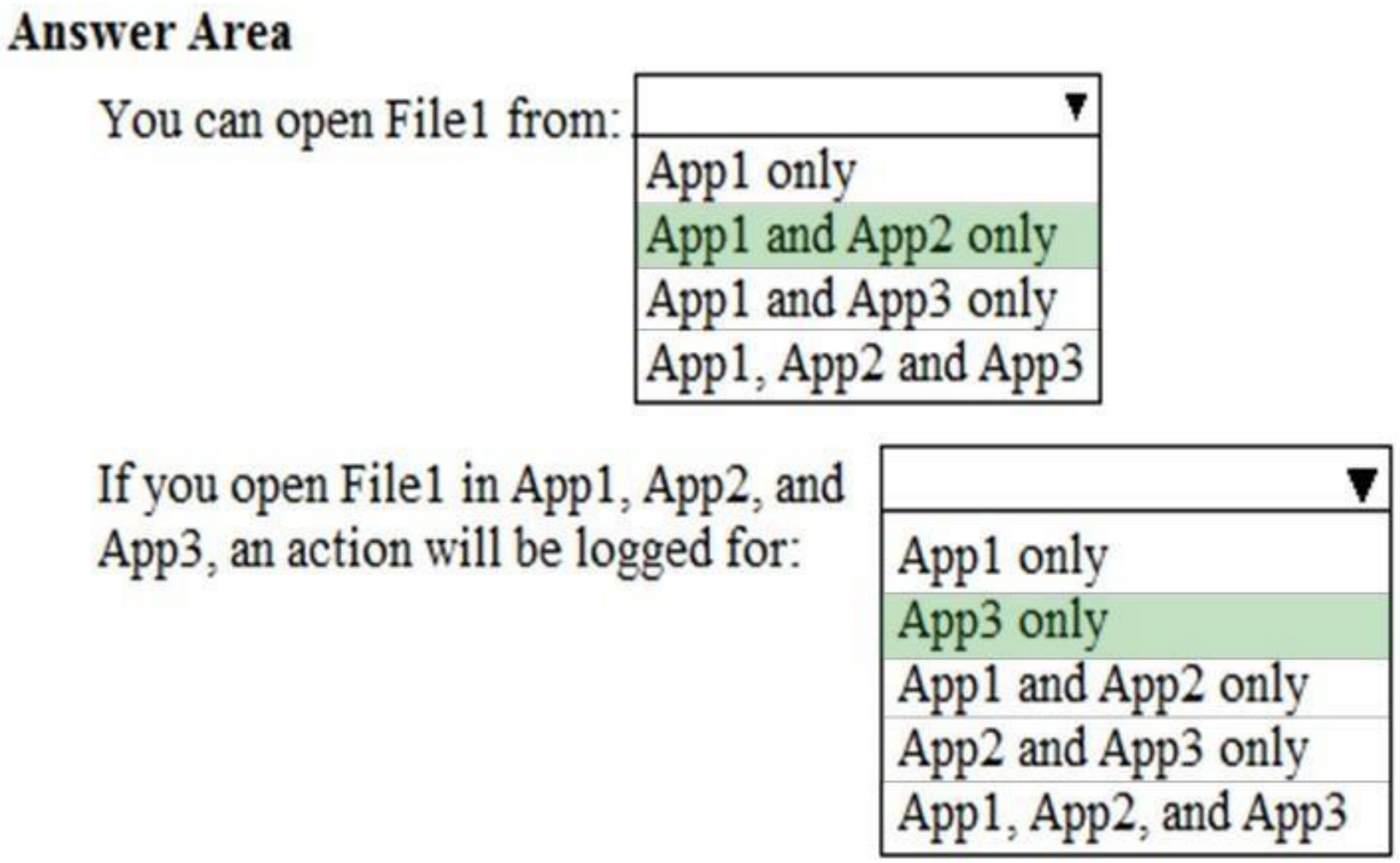
You can open File1 from:

- App1 only
- App1 and App2 only
- App1 and App3 only
- App1, App2 and App3

If you open File1 in App1, App2, and App3, an action will be logged for:

- App1 only
- App3 only
- App1 and App2 only
- App2 and App3 only
- App1, App2, and App3

Correct Answer:



Answer Area

You can open File1 from:

- App1 only
- [✓ App1 and App2 only]
- App1 and App3 only
- App1, App2 and App3

If you open File1 in App1, App2, and App3, an action will be logged for:

- App1 only
- [✓ App3 only]
- App1 and App2 only
- App2 and App3 only
- App1, App2, and App3

Section: [none]
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/windows/security/information-protection/windows-information-protection/create-wip-policy-using-intune-azure

QUESTION 55
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.

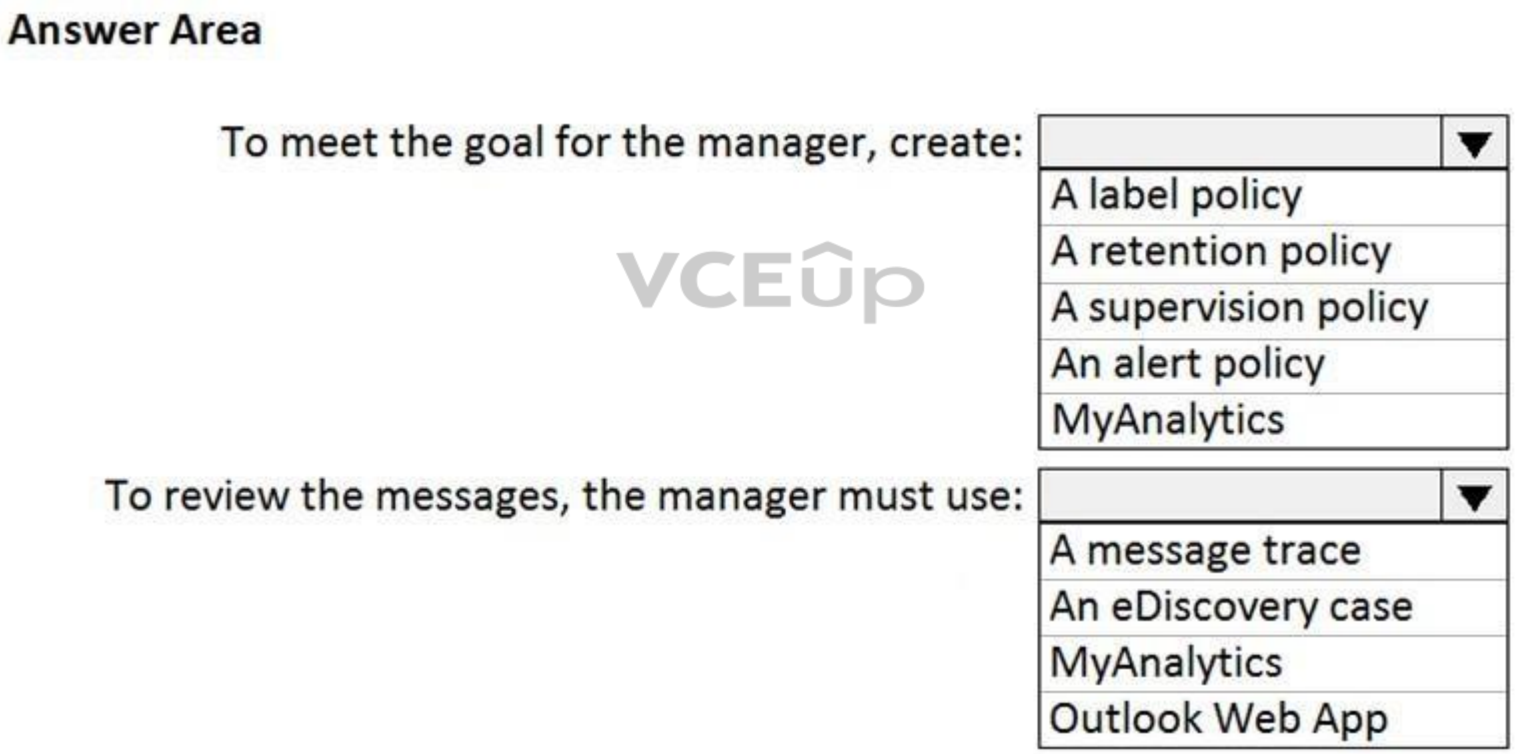
The manager of the Support group wants to randomly review messages that contain attachments.

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.

Hot Area:



Answer Area

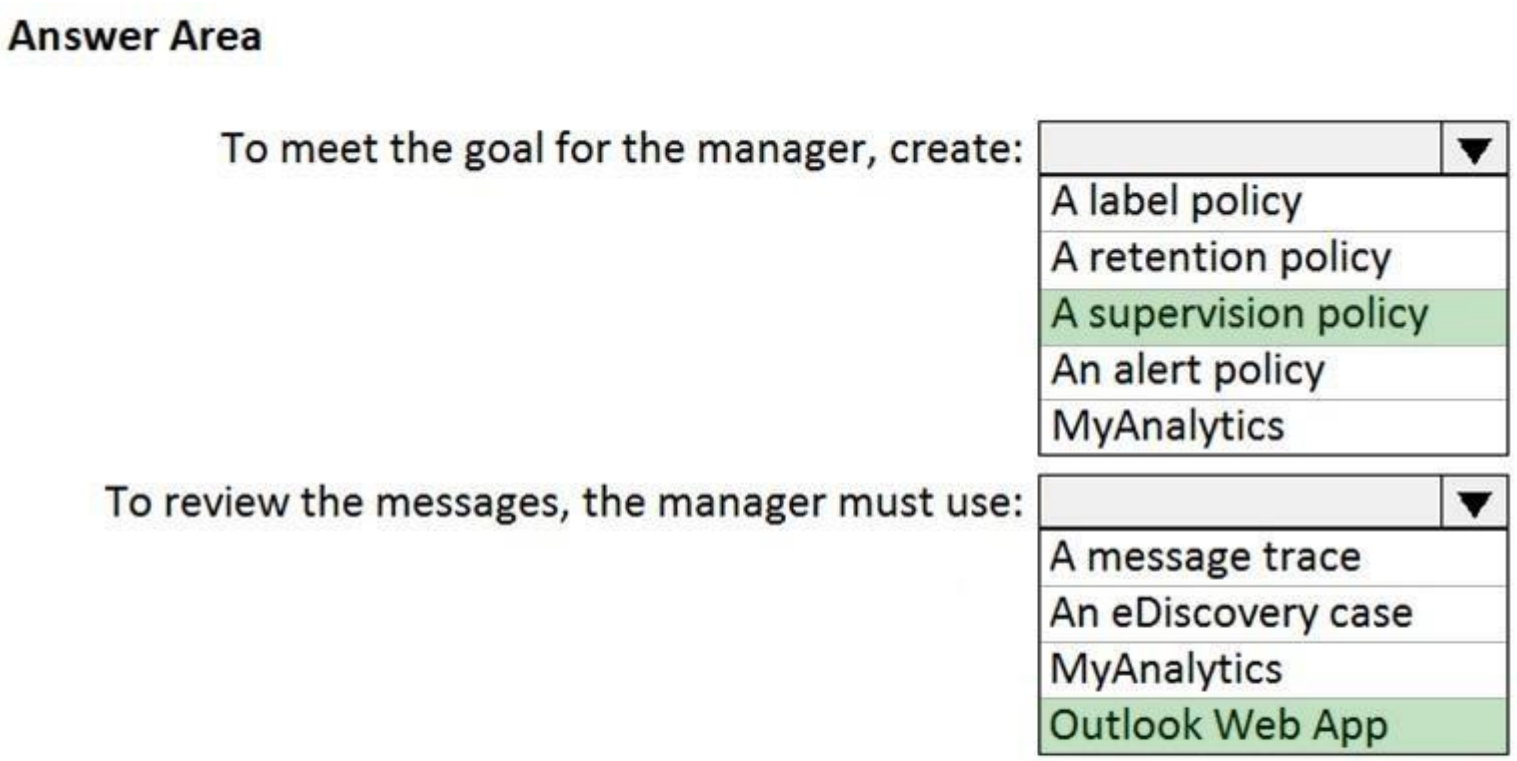
To meet the goal for the manager, create: ▼

- A label policy
- A retention policy
- A supervision 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:



Answer Area

To meet the goal for the manager, create: ▼

- A label policy
- A retention policy
- [✓ A supervision policy]
- An alert policy
- MyAnalytics

To review the messages, the manager must use: ▼

- A message trace
- An eDiscovery case
- MyAnalytics
- [✓ Outlook Web App]

Section: [none]
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/office365/securitycompliance/supervision-policies

QUESTION 56 Your company has a Microsoft 365 subscription.

You implement Microsoft Azure Information Protection.

You need to automatically protect email messages that contain the word Confidential in the subject line.

What should you create?

A. a mail flow rule from the Exchange admin center
B. a message trace from the Security & Compliance admin center
C. a supervision policy from the Security & Compliance admin center
D. a sharing policy from the Exchange admin center

Correct Answer: A
Section: [none]
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/azure/information-protection/configure-exo-rules

QUESTION 57 You have a Microsoft 365 subscription.

You need to investigate user activity in Microsoft 365, including from where users signed in, which applications were used, and increases in activity during the past month. The solution must minimize administrative effort.

Which admin center should you use?

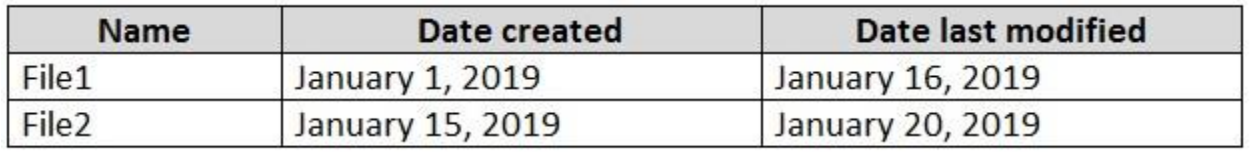
A. Azure ATP
B. Security & Compliance
C. Cloud App Security
D. Flow

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/office365/securitycompliance/search-the-audit-log-in-security-and-compliance

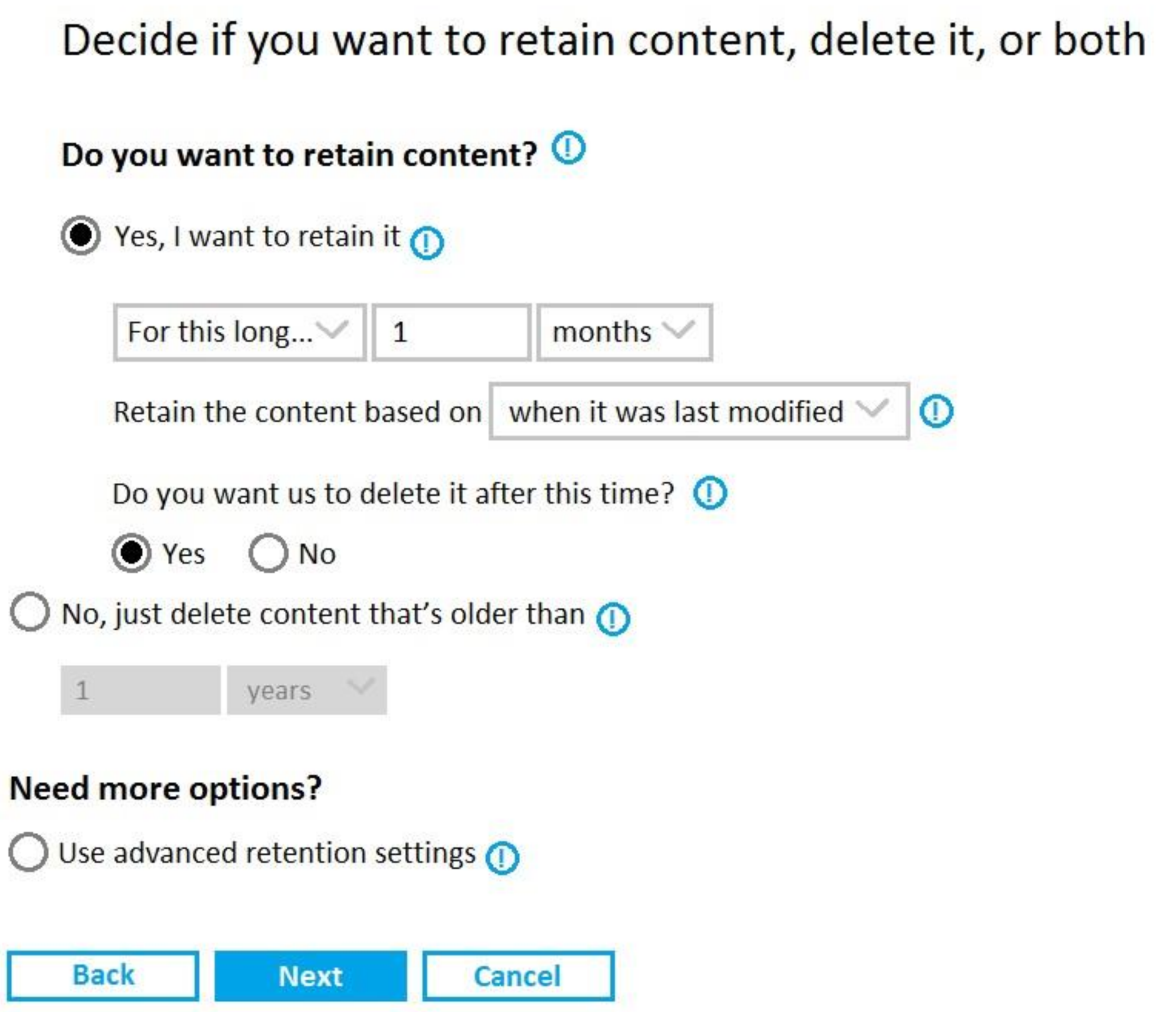
QUESTION 58
HOTSPOT

A user named User1 has files in Microsoft OneDrive as shown in the following table.



Name	Date created	Date last modified
File1	January 1, 2019	January 16, 2019
File2	January 15, 2019	January 20, 2019

On February 1, 2019, you apply a retention policy named Policy1 as shown in the following exhibit.



Decide if you want to retain content, delete it, or both

Do you want to retain content?

● Yes, I want to retain it

For this long... | 1 | months

Retain the content based on: when it was last modified

Do you want us to delete it after this time?

● Yes ○ No

○ No, just delete content that's older than

1 | years

Need more options?

○ Use advanced retention settings

On February 5, 2019, User1 edits File2.

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:

Section: [none]
Explanation

Explanation/Reference:

QUESTION 59 You have a Microsoft 365 subscription that uses a default domain named contoso.com.

You have two users named User1 and User2.

From the Security & Compliance admin center, you add User1 to the eDiscovery Manager role group.

From the Security & Compliance admin center, User1 creates a case named Case1.

You need to ensure that User1 can add User2 as a case member. The solution must use the principle of least privilege.

To which role group should you add User2?

A. eDiscovery Manager
B. eDiscovery Administrator
C. Security Administrator

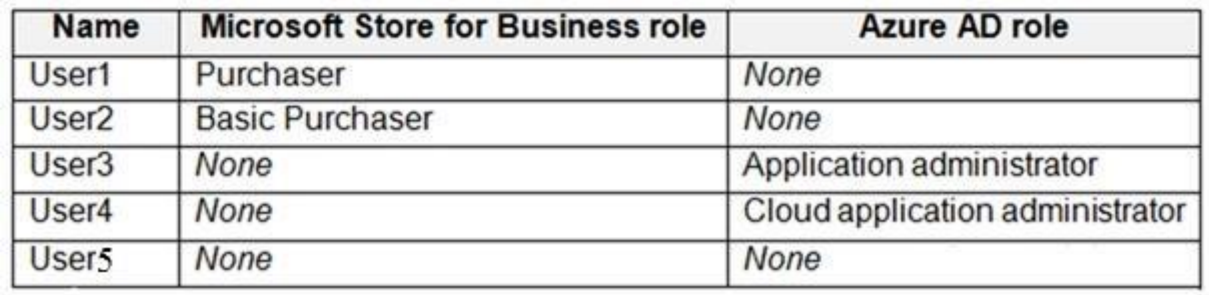
Correct Answer: A
Section: [none]
Explanation

Explanation/Reference:
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/add-or-remove-members-from-a-case-in-advanced-ediscovery?view=o365-worldwide

QUESTION 60 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?

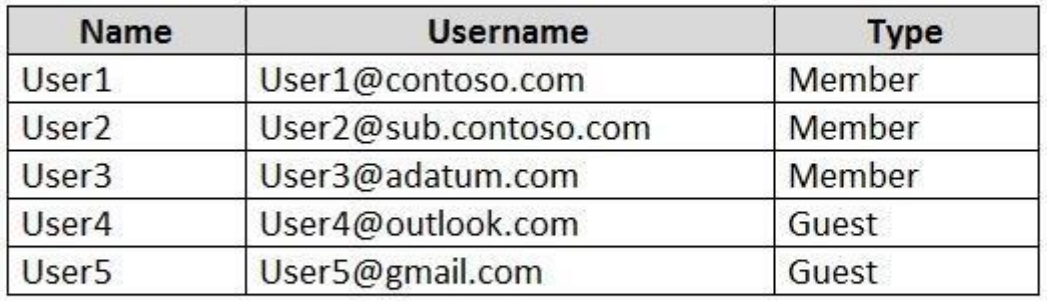
A. User1 and User2 only
B. User1 only
C. User1, User2, User3, and User4 only
D. User3 and User4 only
E. User1, User2, User3, User4, and User5

Correct Answer: A
Section: [none]
Explanation

Explanation/Reference:
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.

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

QUESTION 61
You have a Microsoft 365 subscription that contains an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant contains the users shown in the following table.



Name	Username	Type
User1	User1@contoso.com	Member
User2	User2@sub.contoso.com	Member
User3	User3@adatum.com	Member
User4	User4@outlook.com	Guest
User5	User5@gmail.com	Guest

You create and assign a data loss prevention (DLP) policy named Policy1. Policy1 is configured to prevent documents that contain Personally Identifiable Information (PII) from being emailed to users outside your organization.

To which users can User1 send documents that contain PII?

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

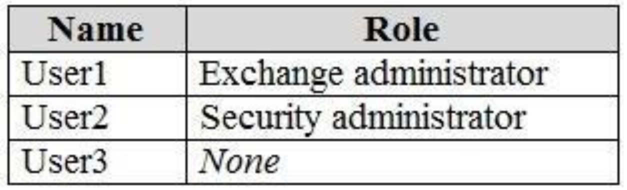
Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:
Explanation:
Guest accounts are considered “outside your organization”. Users who have non-guest accounts in a host organization's Active Directory or Azure Active Directory tenant are considered as people inside the organization.

Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/data-loss-prevention-policies?view=o365-worldwide

QUESTION 62
HOTSPOT

You have a Microsoft 365 subscription that contains the users shown in the following table.



Name	Role
User1	Exchange administrator
User2	Security administrator
User3	*None*

You run the following cmdlet.

```
Set-MailboxAuditBypassAssociation -Identity User2 -
AuditByPassEnabled $true
```

The users perform the following actions:

▪ User1 accesses an item in the mailbox of User2.
▪ User2 modifies a mailbox item in the mailbox of User3. ▪ User3
signs in to her mailbox.

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

NOTE: Each correct selection is worth one point.

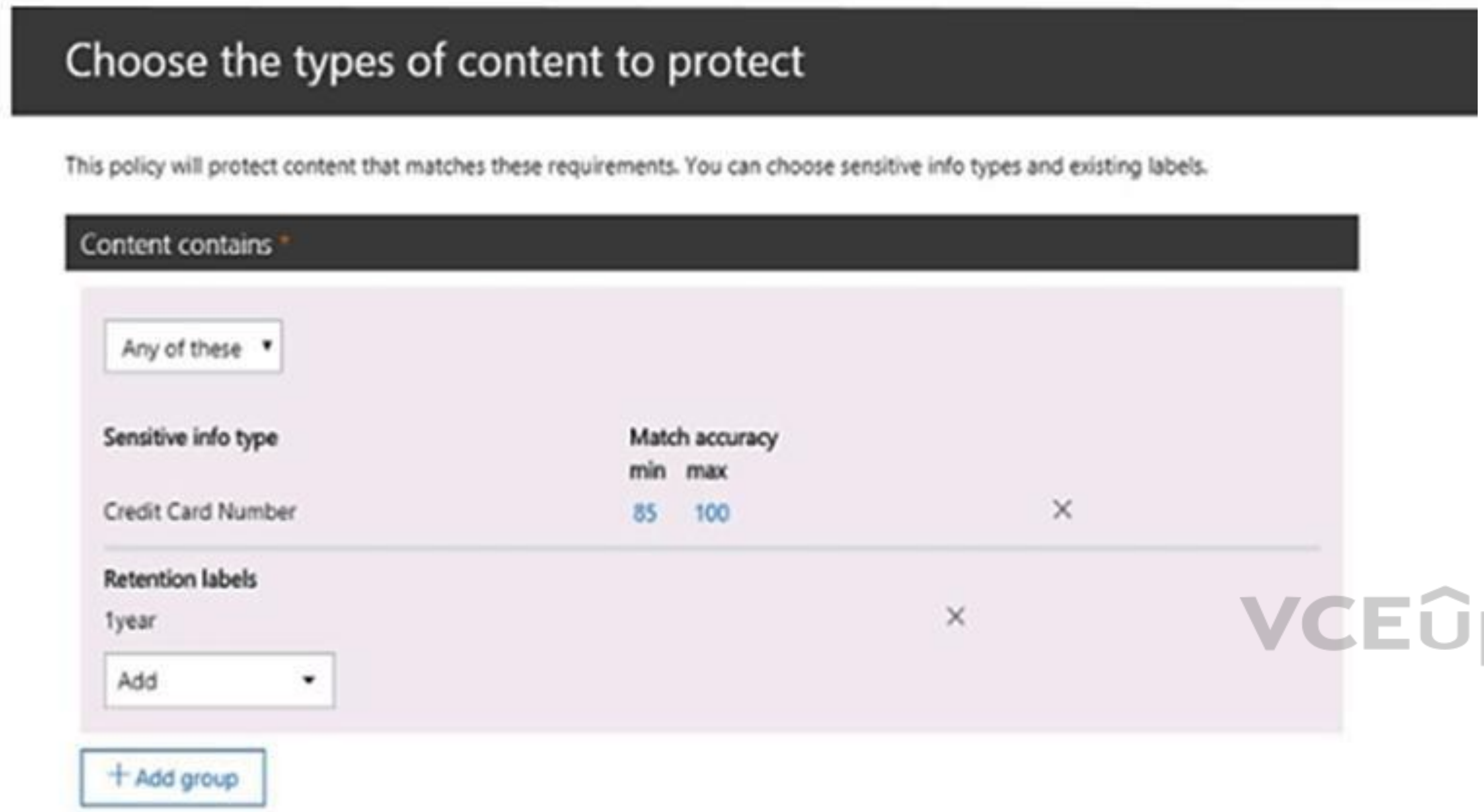
Hot Area:
Correct Answer:

Section: [none]
Explanation

Explanation/Reference:
Reference: https://docs.microsoft.com/en-us/powershell/module/exchange/set-mailboxauditbypassassociation?view=exchange-ps

QUESTION 63
HOTSPOT

You configure a data loss prevention (DLP) policy named DLP1 as shown in the following exhibit.



Choose the types of content to protect

This policy will protect content that matches these requirements. You can choose sensitive info types and existing labels.

Content contains *

Any of these

Sensitive info type	Match accuracy min max
Credit Card Number	85 100

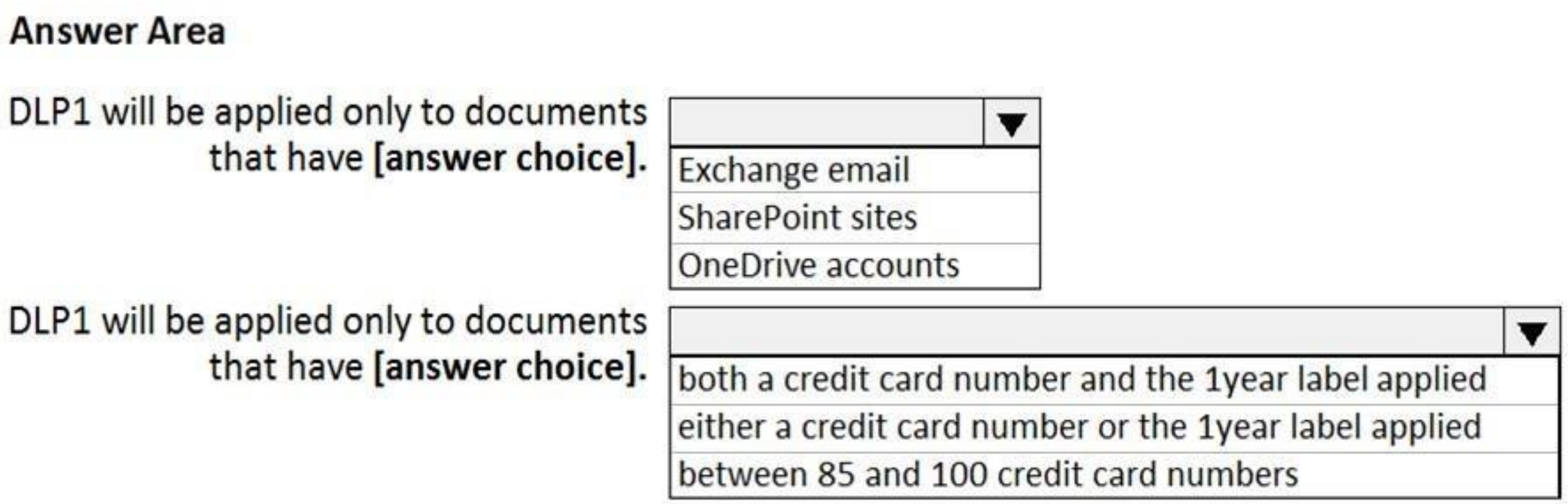
Retention labels

1year

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:



Answer Area

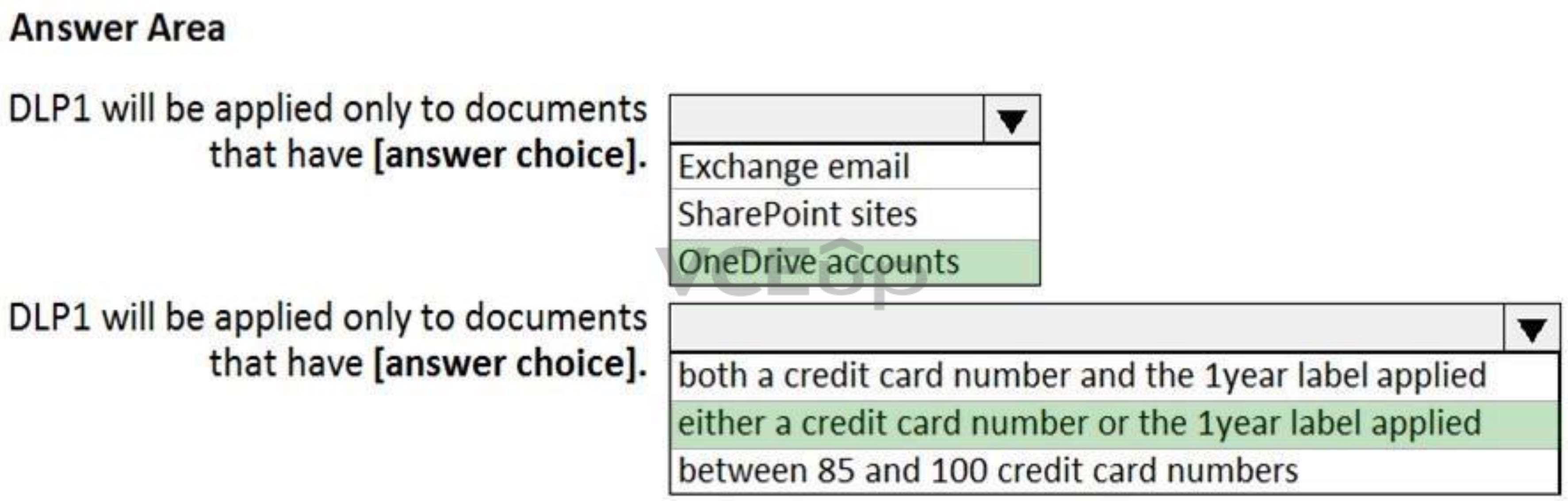
DLP1 will be applied only to documents that have [answer choice].

- Exchange email
- SharePoint sites
- OneDrive accounts

DLP1 will be applied only to documents that have [answer choice].

- both a credit card number and the 1year label applied
- either a credit card number or the 1year label applied
- between 85 and 100 credit card numbers

Correct Answer:



Answer Area

DLP1 will be applied only to documents that have [answer choice].

- Exchange email
- SharePoint sites
- [✓ OneDrive accounts]

DLP1 will be applied only to documents that have [answer choice].

- both a credit card number and the 1year label applied
- [✓ either a credit card number or the 1year label applied]
- between 85 and 100 credit card numbers

Section: [none]
Explanation

Explanation/Reference:
Reference: https://docs.microsoft.com/en-us/microsoft-365/compliance/data-loss-prevention-policies?view=o365-worldwide

QUESTION 64
HOTSPOT

You have a Microsoft 365 subscription.

Your network uses an IP address space of 51.40.15.0/24.

An Exchange Online administrator recently created a role named Role1 from a computer on the network.

You need to identify the name of the administrator by using an audit log search.

For which activities should you search and by which field should you filter in the audit log search? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Correct Answer:

Section: [none]
Explanation

Explanation/Reference:

QUESTION 65 You have a Microsoft 365 subscription that uses Security & Compliance retention policies.

You implement a preservation lock on a retention policy that is assigned to all executive users.

Which two actions can you perform on the retention policy? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point?

A. Add locations to the policy
B. Reduce the duration of policy
C. Remove locations from the policy
D. Extend the duration of the policy
E. Disable the policy

Correct Answer: AD
Section: [none]
Explanation

Explanation/Reference:

QUESTION 66 You have a Microsoft 365 subscription.

Your company has a customer ID associated to each customer. The customer IDs contain 10 numbers followed by 10 characters. The following is a sample customer ID: 12-456-7890-abc-de-fghij.

You plan to create a data loss prevention (DLP) policy that will detect messages containing customer IDs.

What should you create to ensure that the DLP policy can detect the customer IDs?

A. a sensitive information type
B. a sensitivity label
C. a supervision policy
D. a retention label

Correct Answer: A
Section: [none]
Explanation

Explanation/Reference:
Reference: https://docs.microsoft.com/en-us/microsoft-365/compliance/custom-sensitive-info-types?view=o365-worldwide

QUESTION 67 You have a Microsoft 365 subscription that contains a user named User1.

You need to ensure that User1 can search the Microsoft 365 audit logs from the Security & Compliance admin center.

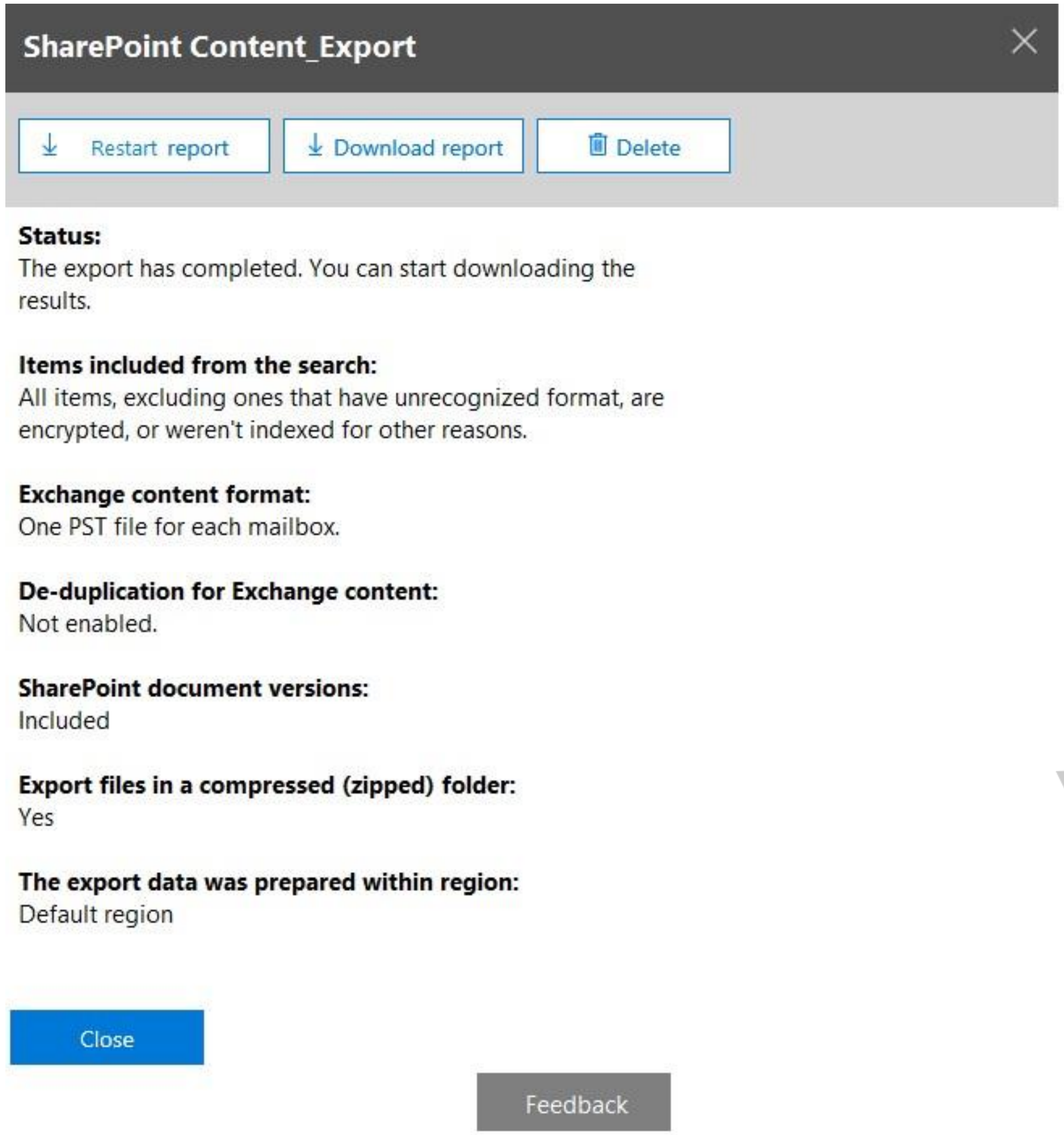
Which role should you assign to User1?

A. View-Only Audit Logs in the Security & Compliance admin center
B. View-Only Audit Logs in the Exchange admin center
C. Security reader in the Azure Active Directory admin center
D. Security Reader in the Security & Compliance admin center

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:
Reference: https://docs.microsoft.com/en-us/microsoft-365/compliance/search-the-audit-log-in-security-and-compliance?view=o365-worldwide

QUESTION 68
From the Security & Compliance admin center, you create a content export as shown in the exhibit. (Click the **Exhibit** tab.)



Status:
The export has completed. You can start downloading the results.

Items included from the search:
All items, excluding ones that have unrecognized format, are encrypted, or weren't indexed for other reasons.

Exchange content format:
One PST file for each mailbox.

De-duplication for Exchange content:
Not enabled.

SharePoint document versions:
Included

Export files in a compressed (zipped) folder:
Yes

The export data was prepared within region:
Default region

What will be excluded from the export?

A. a 10-MB XLSX file
B. a 5-MB MP3 file
C. a 5-KB RTF file
D. an 80-MB PPTX file

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:
Explanation:
Unrecognized file formats are excluded from the search.

Certain types of files, such as Bitmap or MP3 files, don't contain content that can be indexed. As a result, the search indexing servers in Exchange and SharePoint don't perform full-text indexing on these types of files. These types of files are considered to be unsupported file types.

Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/partially-indexed-items-in-content-search?view=o365-worldwide https://docs.microsoft.com/en-us/office365/securitycompliance/export-a-content-search-report

QUESTION 69
You are testing a data loss prevention (DLP) policy to protect the sharing of credit card information with external users.

During testing, you discover that a user can share credit card information with external users by using email. However, the user is prevented from sharing files that contain credit card information by using Microsoft SharePoint Online.

You need to prevent the user from sharing the credit card information by using email and SharePoint.

What should you configure?

A. the locations of the DLP policy
B. the user overrides of the DLP policy rule
C. the status of the DLP policy
D. the conditions of the DLP policy rule

Correct Answer: A
Section: [none]
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/office365/securitycompliance/data-loss-prevention-policies

QUESTION 70 You have a Microsoft 365 subscription.

You need to view the IP address from which a user synced a Microsoft SharePoint Online library.

What should you do?

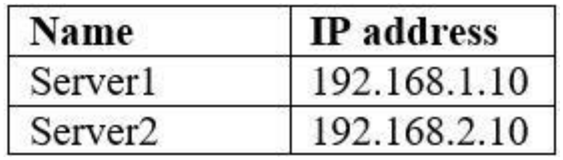
A. From the SharePoint Online admin center, view the usage reports.
B. From the Security & Compliance admin center, perform an audit log search.
C. From the Microsoft 365 admin center, view the usage reports.
D. From the Microsoft 365 admin center, view the properties of the user’s user account.

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/office365/securitycompliance/search-the-audit-log-in-security-and-compliance

QUESTION 71
HOTSPOT

Your network contains an Active Directory domain named contoso.com. The domain contains the file servers shown in the following table.



Name	IP address
Server1	192.168.1.10
Server2	192.168.2.10

A file named File1.abc is stored on Server1. A file named File2.abc is stored on Server2. Three apps named App1, App2, and App3 all open files that have the .abc file extension.

You implement Windows Information Protection (WIP) by using the following configurations:

- Exempt apps: App2
- Protected apps: App1
- Windows Information Protection mode: Block
- Network boundary: IPv4 range of: 192.168.1.1-192.168.1.255

You need to identify the apps from which you can open File1.abc.

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:

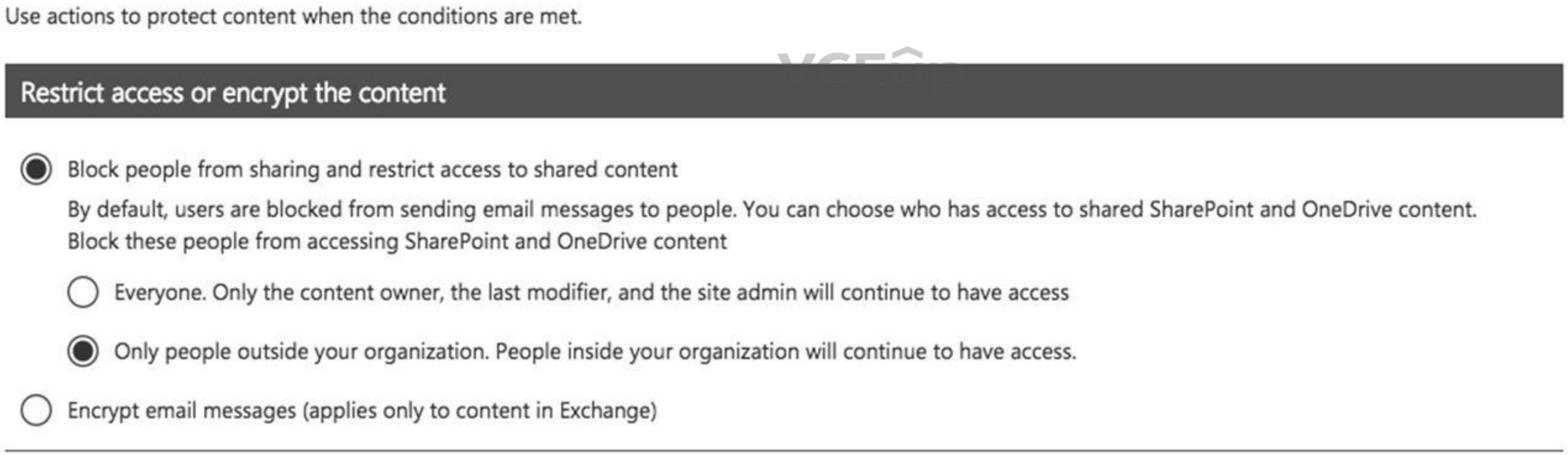
Correct Answer:

Section: [none]
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/windows/security/information-protection/windows-information-protection/create-wip-policy-using-intune-azure

QUESTION 72
In Microsoft 365, you configure a data loss prevention (DLP) policy named Policy1. Policy1 detects the sharing of United States (US) bank account numbers in email messages and attachments.

Policy1 is configured as shown in the exhibit. (Click the **Exhibit** tab.)



Use actions to protect content when the conditions are met.

Restrict access or encrypt the content

● Block people from sharing and restrict access to shared content

By default, users are blocked from sending email messages to people. You can choose who has access to shared SharePoint and OneDrive content.
Block these people from accessing SharePoint and OneDrive content

○ Everyone. Only the content owner, the last modifier, and the site admin will continue to have access

● Only people outside your organization. People inside your organization will continue to have access.

○ Encrypt email messages (applies only to content in Exchange)

You need to ensure that internal users can email documents that contain US bank account numbers to external users who have an email suffix of contoso.com.

What should you configure?

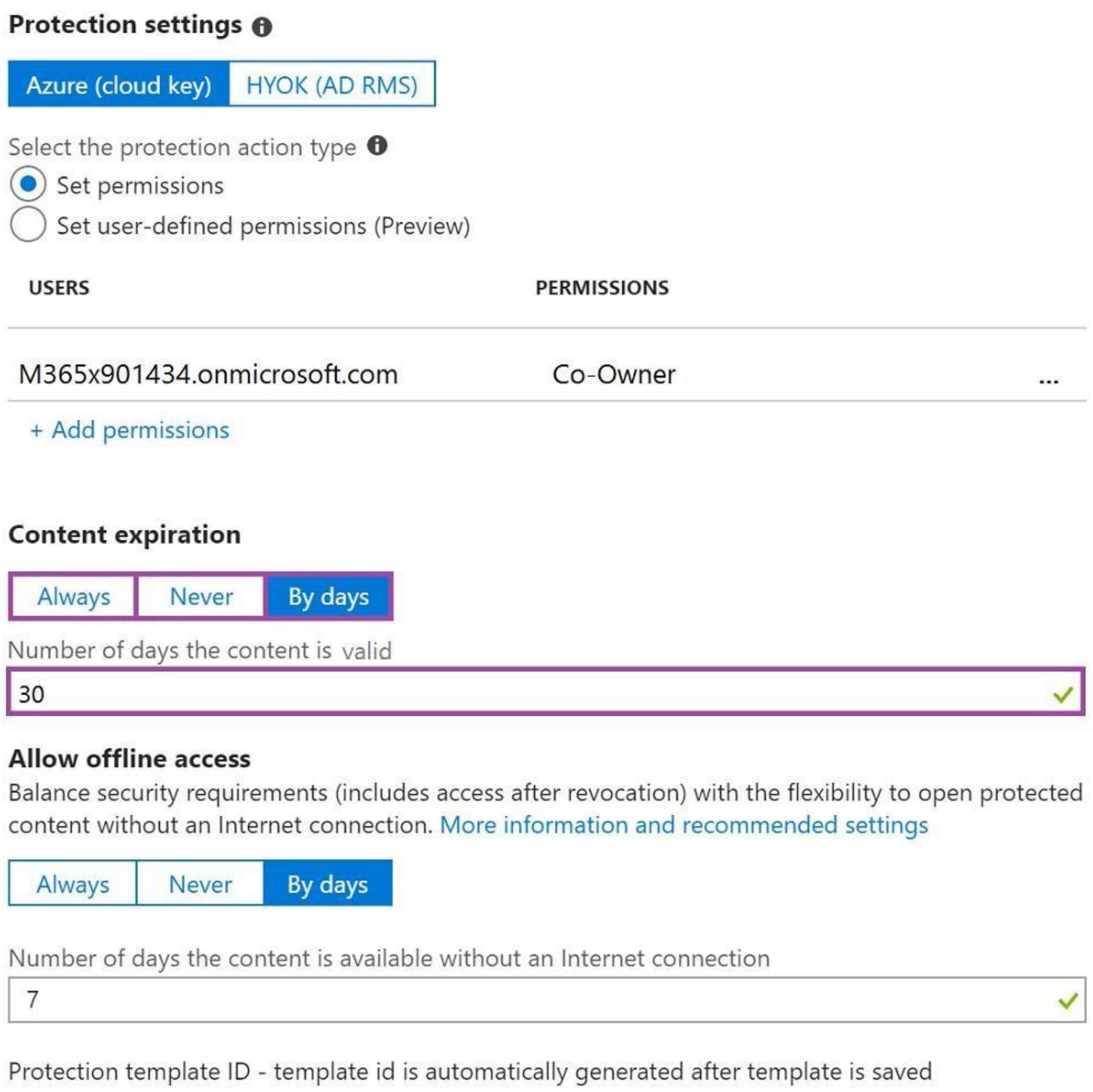
A. an exception
B. an action
C. a condition
D. a group

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/office365/securitycompliance/data-loss-prevention-policies#how-dlp-policies-work

QUESTION 73
HOTSPOT

You have a document in Microsoft OneDrive that is encrypted by using Microsoft Azure Information Protection as shown in the following exhibit.



Protection settings

Select the protection action type

● Set permissions

○ Set user-defined permissions (Preview)

USERS	PERMISSIONS	
M365x901434.onmicrosoft.com	Co-Owner	...

Content expiration

Number of days the content is valid: 30 ✓

Allow offline access

Balance security requirements (includes access after revocation) with the flexibility to open protected content without an Internet connection. More information and recommended settings

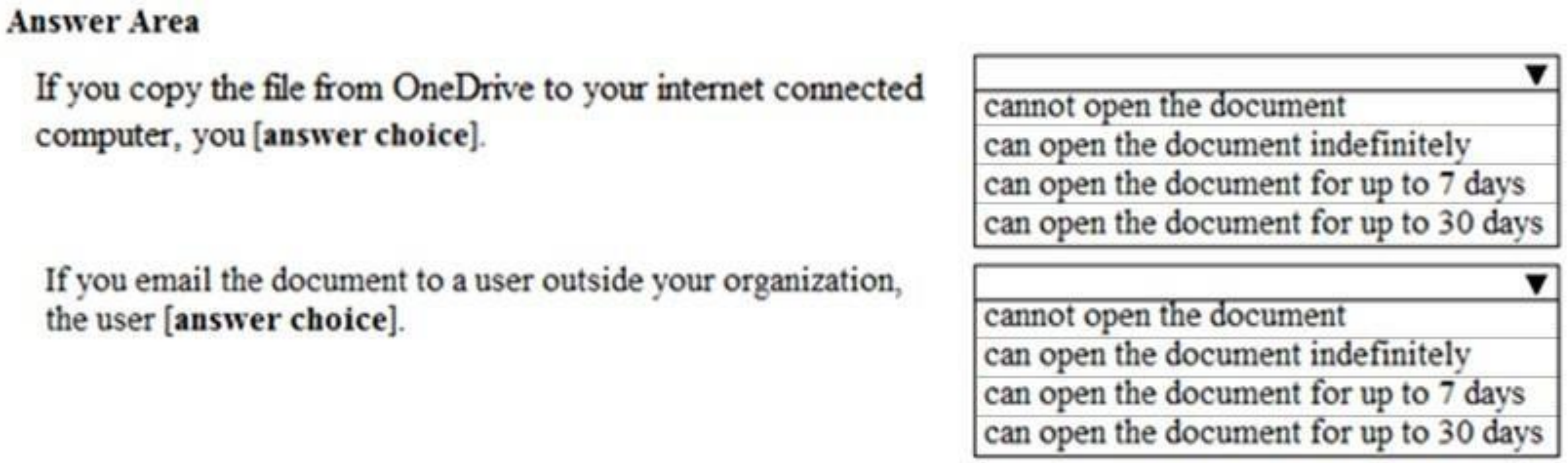
Number of days the content is available without an Internet connection: 7 ✓

Protection template ID - template id is automatically generated after template is saved

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:



Answer Area

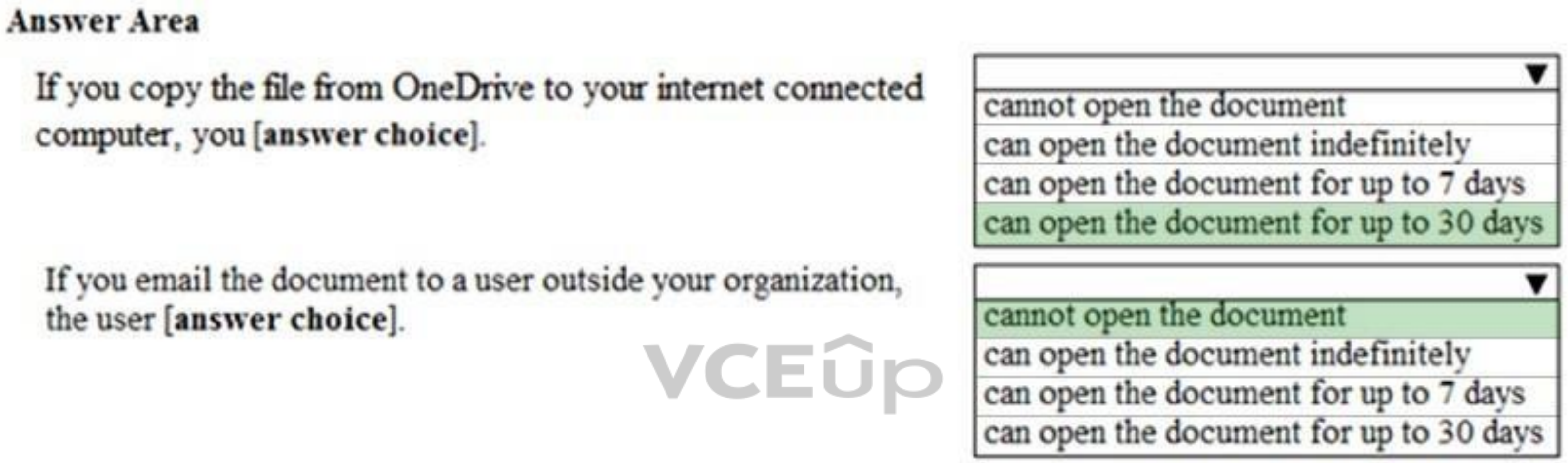
If you copy the file from OneDrive to your internet connected computer, you [**answer choice**].

▼
- cannot open the document
- can open the document indefinitely
- can open the document for up to 7 days
- can open the document for up to 30 days

If you email the document to a user outside your organization, the user [**answer choice**].

▼
- cannot open the document
- can open the document indefinitely
- can open the document for up to 7 days
- can open the document for up to 30 days

Correct Answer:



Answer Area

If you copy the file from OneDrive to your internet connected computer, you [**answer choice**].

▼
- cannot open the document
- can open the document indefinitely
- can open the document for up to 7 days
- [✓ can open the document for up to 30 days]

If you email the document to a user outside your organization, the user [**answer choice**].

▼
- [✓ cannot open the document]
- can open the document indefinitely
- can open the document for up to 7 days
- can open the document for up to 30 days

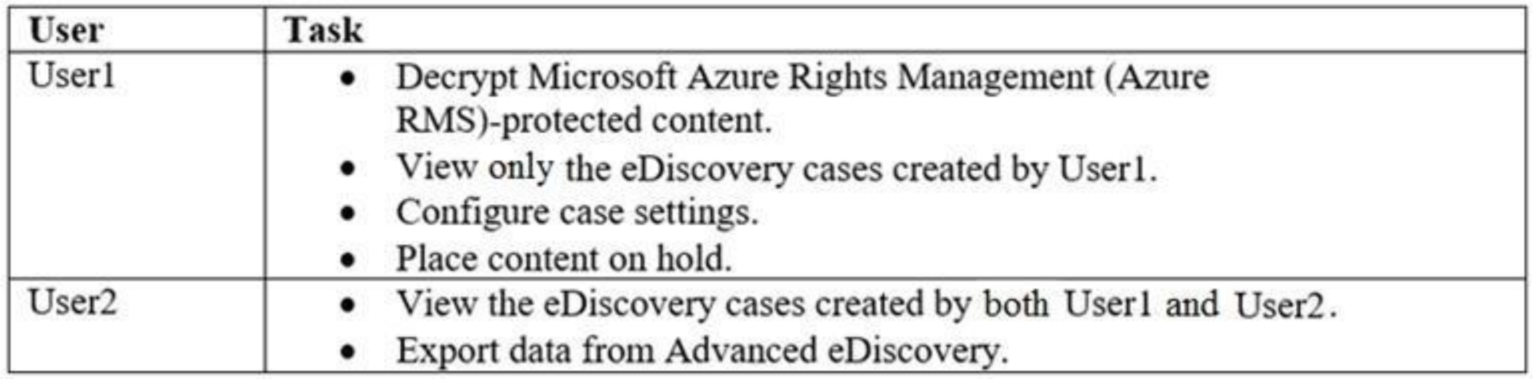
Section: [none]
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/azure/information-protection/configure-policy-protection

QUESTION 74
HOTSPOT

You have a Microsoft Office 365 subscription.

You need to delegate eDiscovery tasks as shown in the following table.



User	Task
User1	• Decrypt Microsoft Azure Rights Management (Azure RMS)-protected content. • View only the eDiscovery cases created by User1. • Configure case settings. • Place content on hold.
User2	• View the eDiscovery cases created by both User1 and User2. • Export data from Advanced eDiscovery.

The solution must follow the principle of the least privilege.

To which role group should you assign each user? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Correct Answer:

Section: [none]
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/office365/securitycompliance/assign-ediscovery-permissions

QUESTION 75 You have a Microsoft 365 subscription.

You need to identify which administrative users performed eDiscovery searches during the past week.

What should you do from the Security & Compliance admin center?

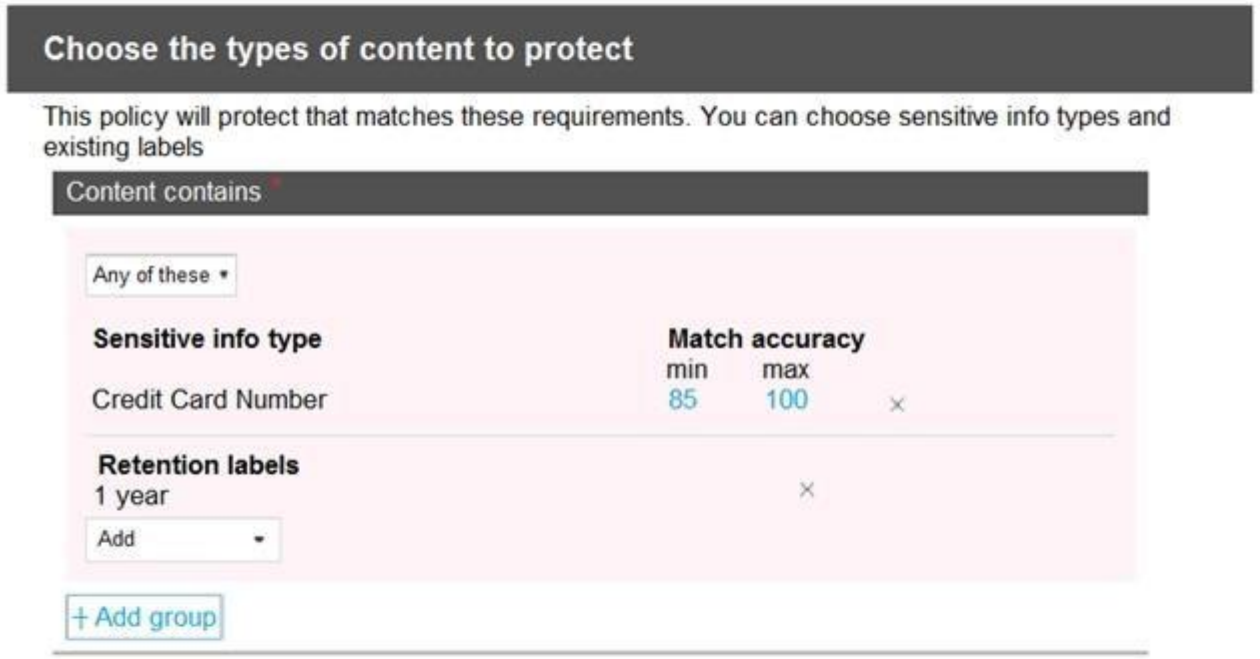
A. Perform a content search
B. Create a supervision policy
C. Create an eDiscovery case
D. Perform an audit log search

Correct Answer: D
Section: [none]
Explanation

Explanation/Reference:

QUESTION 76
HOTSPOT

You configure a data loss prevention (DLP) policy named DLP1 as shown in the following exhibit.



Choose the types of content to protect

This policy will protect that matches these requirements. You can choose sensitive info types and existing labels

Content contains

Any of these ▾

Sensitive info type	Match accuracy min	 max
Credit Card Number	85	100

Retention labels

1 year

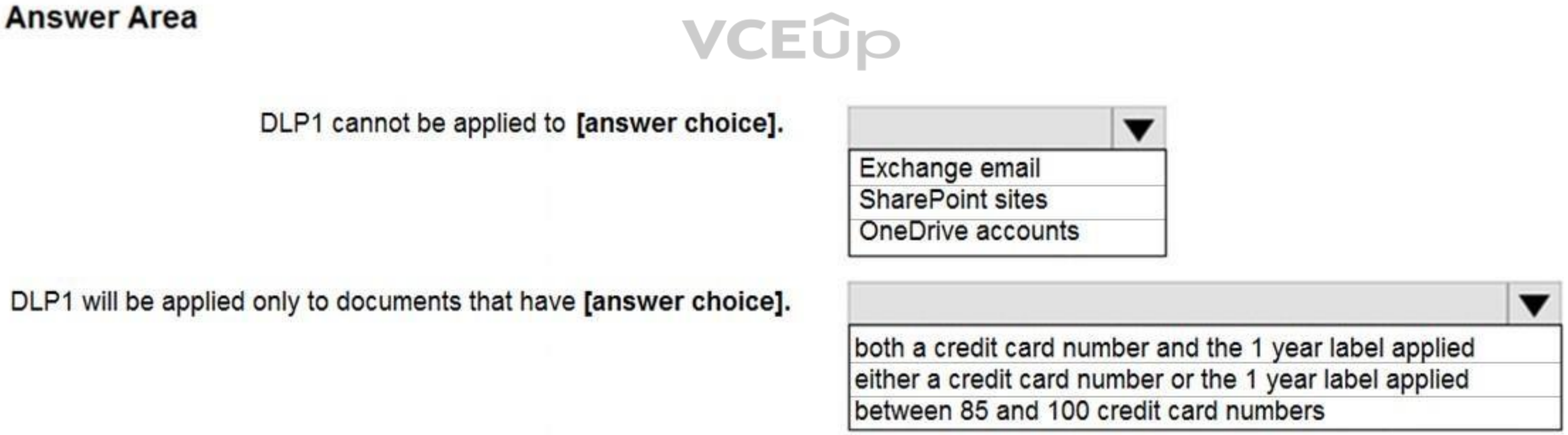
Add ▾

+ Add group

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:



Answer Area

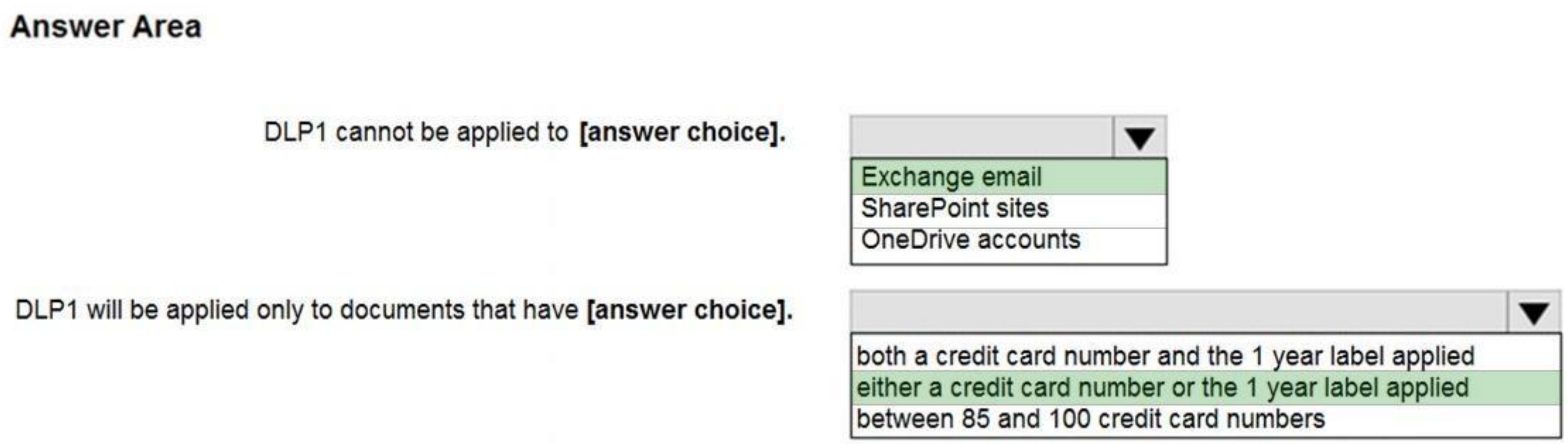
DLP1 cannot be applied to **[answer choice].**

- Exchange email
- SharePoint sites
- OneDrive accounts

DLP1 will be applied only to documents that have **[answer choice].**

- both a credit card number and the 1 year label applied
- either a credit card number or the 1 year label applied
- between 85 and 100 credit card numbers

Correct Answer:



Answer Area

DLP1 cannot be applied to **[answer choice].**

- Exchange email
- SharePoint sites
- OneDrive accounts

DLP1 will be applied only to documents that have **[answer choice].**

- both a credit card number and the 1 year label applied
- either a credit card number or the 1 year label applied
- between 85 and 100 credit card numbers

Section: [none]
Explanation

Explanation/Reference:
Explanation:

Using a retention label in a policy is only supported for items in SharePoint Online and OneDrive for Business.

Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/data-loss-prevention-policies?view=o365-worldwide#using-a-retention-label-as-a-condition-in-a-dlp-policy

QUESTION 77
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 subscription.

From the Security & Compliance admin center, you create a role group named US eDiscovery Managers by copying the eDiscovery Manager role group.

You need to ensure that the users in the new role group can only perform content searches of mailbox content for users in the United States.

Solution: From Windows PowerShell, you run the `New-ComplianceSecurityFilter` cmdlet with the appropriate parameters.

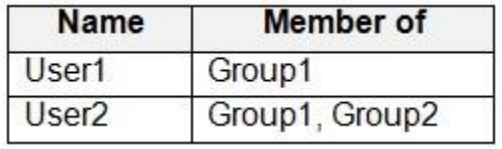
Does this meet the goal?

A. Yes
B. No

Correct Answer: A
Section: [none]
Explanation

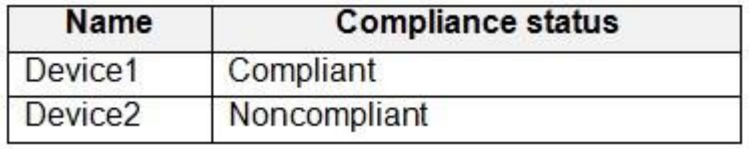
Explanation/Reference:
References: https://docs.microsoft.com/en-us/office365/securitycompliance/permissions-filtering-for-content-search https://docs.microsoft.com/en-us/powershell/module/exchange/policy-and-compliance-content-search/new-compliancesecurityfilter?view=exchange-ps **QUESTION 78** HOTSPOT

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



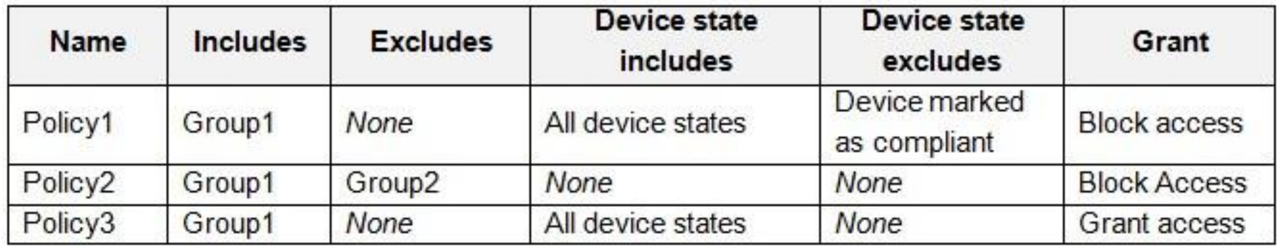
Name	Member of
User1	Group1
User2	Group1, Group2

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.

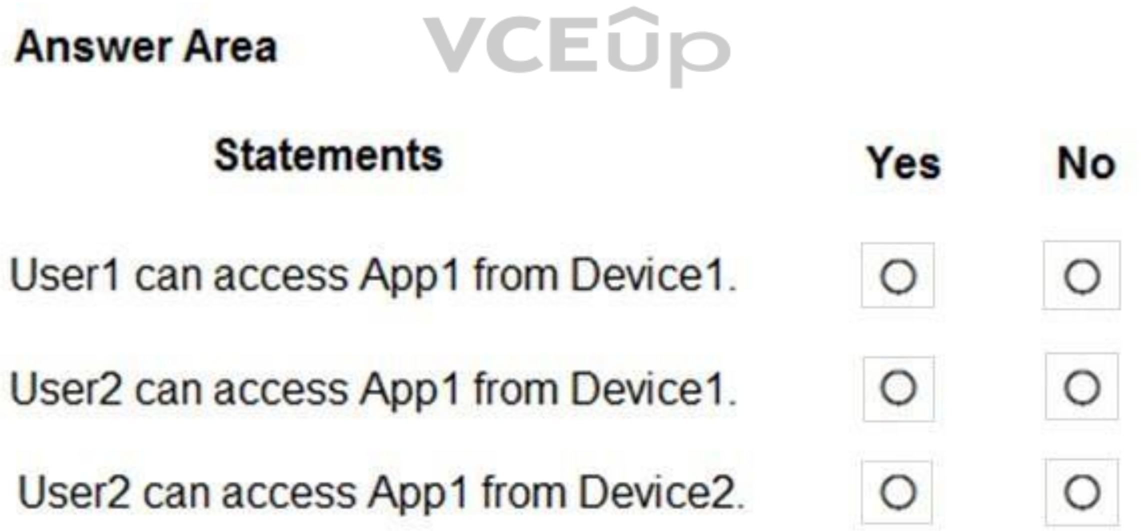


Name	Includes	Excludes	Device state includes	Device state excludes	Grant
Policy1	Group1	*None*	All device states	Device marked as compliant	Block access
Policy2	Group1	Group2	*None*	*None*	Block Access
Policy3	Group1	*None*	All device states	*None*	Grant access

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

NOTE: Each correct selection is worth one point.

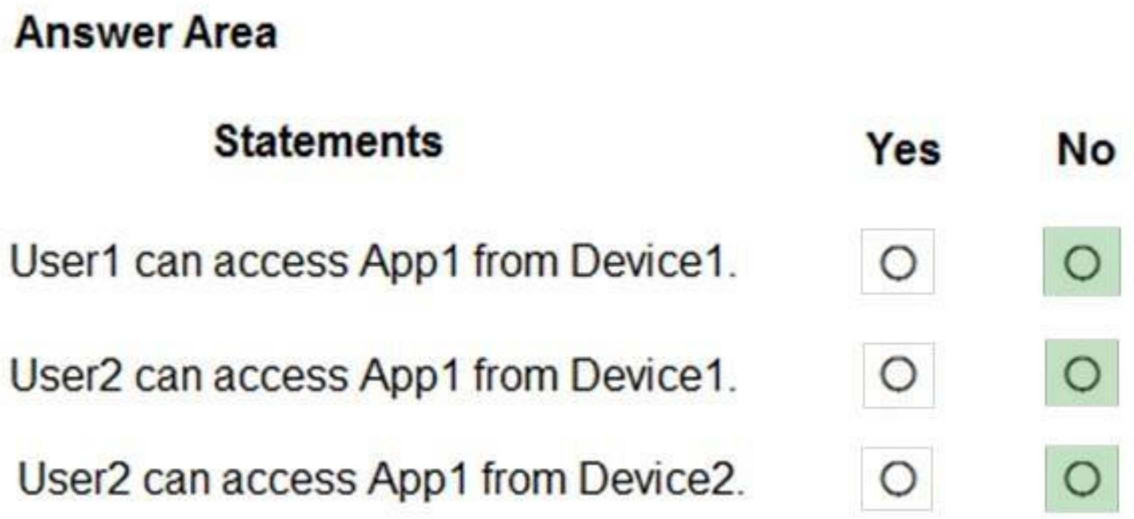
Hot Area:



Answer Area

Statements	Yes	No
User1 can access App1 from Device1.	○	○
User2 can access App1 from Device1.	○	○
User2 can access App1 from Device2.	○	○

Correct Answer:



Answer Area

Statements	Yes	No
User1 can access App1 from Device1.	○	[✓ ○]
User2 can access App1 from Device1.	○	[✓ ○]
User2 can access App1 from Device2.	○	[✓ ○]

Section: [none]
Explanation

Explanation/Reference:
Explanation:

Note: Block access overrides Grant access

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

QUESTION 79 You have a Microsoft 365 subscription.

You need to create a data loss prevention (DLP) policy that is configured to use the Set headers action.

To which location can the policy be applied?

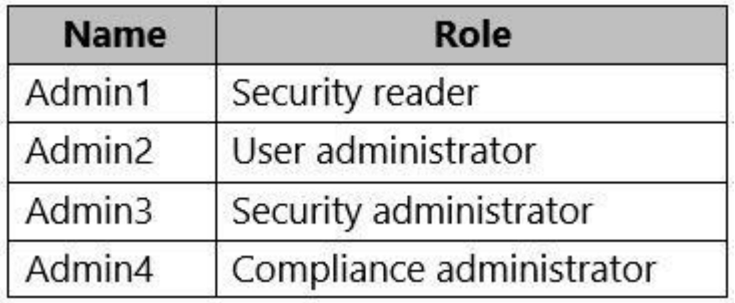
A. OneDrive accounts
B. Exchange email
C. Teams chat and channel messages
D. SharePoint sites

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:

QUESTION 80 You enable the Azure AD Identity Protection weekly digest email.

You create the users shown in the following table.



Name	Role
Admin1	Security reader
Admin2	User administrator
Admin3	Security administrator
Admin4	Compliance administrator

Which users will receive the weekly digest email automatically?

A. Admin2, Admin3, and Admin4 only
B. Admin1, Admin2, Admin3, and Admin4
C. Admin2 and Admin3 only
D. Admin3 only
E. Admin1 and Admin3 only

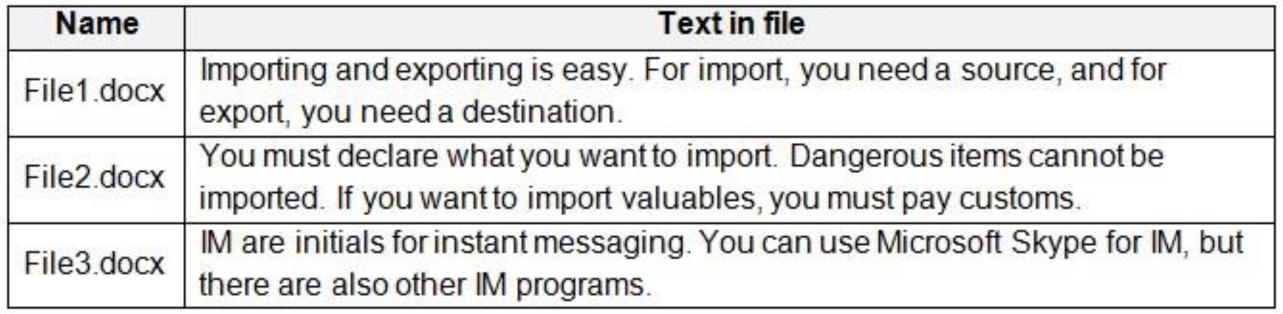
Correct Answer: E
Section: [none]
Explanation

Explanation/Reference:
Explanation:
By default, all Global Admins receive the email. Any newly created Global Admins, Security Readers or Security Administrators will automatically be added to the recipients list.

QUESTION 81
HOTSPOT

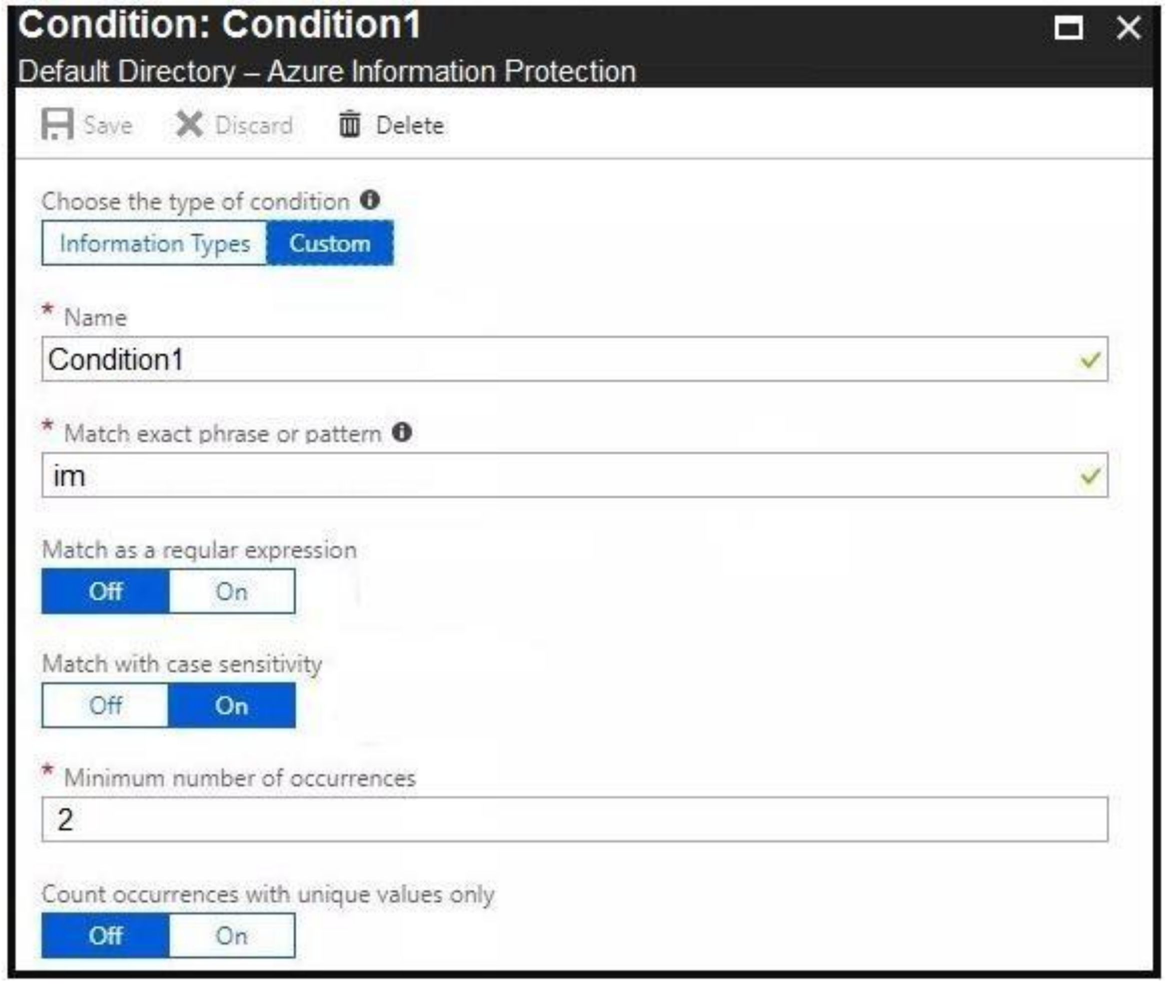
You have a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com.

A user named User1 has files on a Windows 10 device as shown in the following table.



Name	Text in file
File1.docx	Importing and exporting is easy. For import, you need a source, and for export, you need a destination.
File2.docx	You must declare what you want to import. Dangerous items cannot be imported. If you want to import valuables, you must pay customs.
File3.docx	IM are initials for instant messaging. You can use Microsoft Skype for IM, but there are also other IM programs.

In Azure Information Protection, you create a label named Label1 that is configured to apply automatically. Label1 is configured as shown in the following exhibit.



Condition: Condition1

Default Directory – Azure Information Protection

Choose the type of condition: Information Types / **Custom**

* Name: Condition1

* Match exact phrase or pattern: im

Match as a regular expression: **Off** / On

Match with case sensitivity: Off / **On**

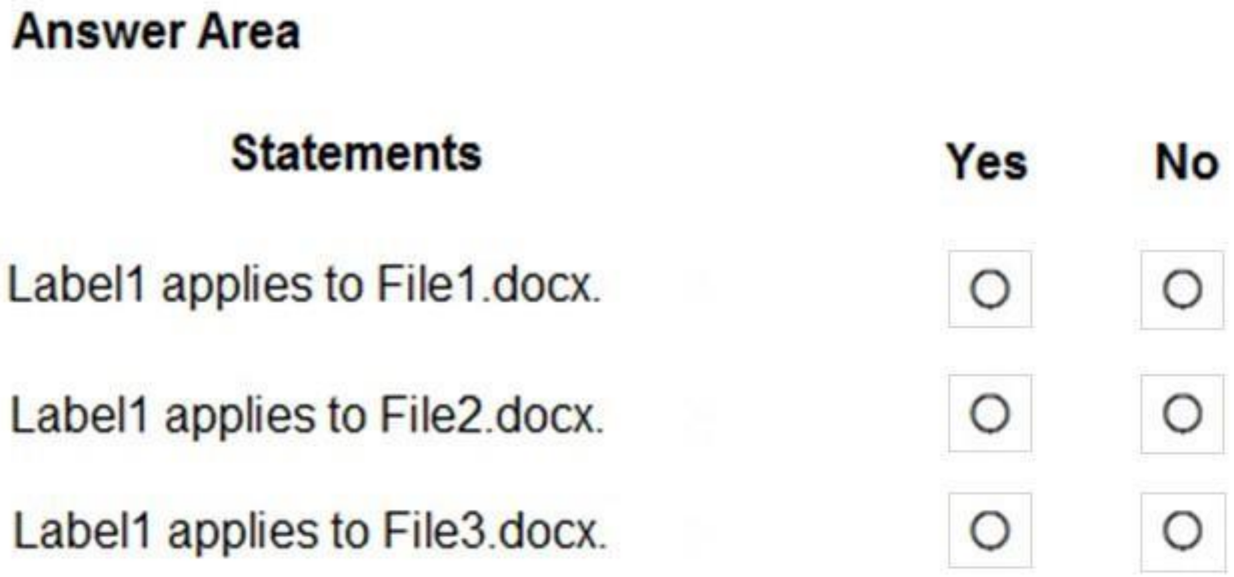
* Minimum number of occurrences: 2

Count occurrences with unique values only: **Off** / On

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

NOTE: Each correct selection is worth one point.

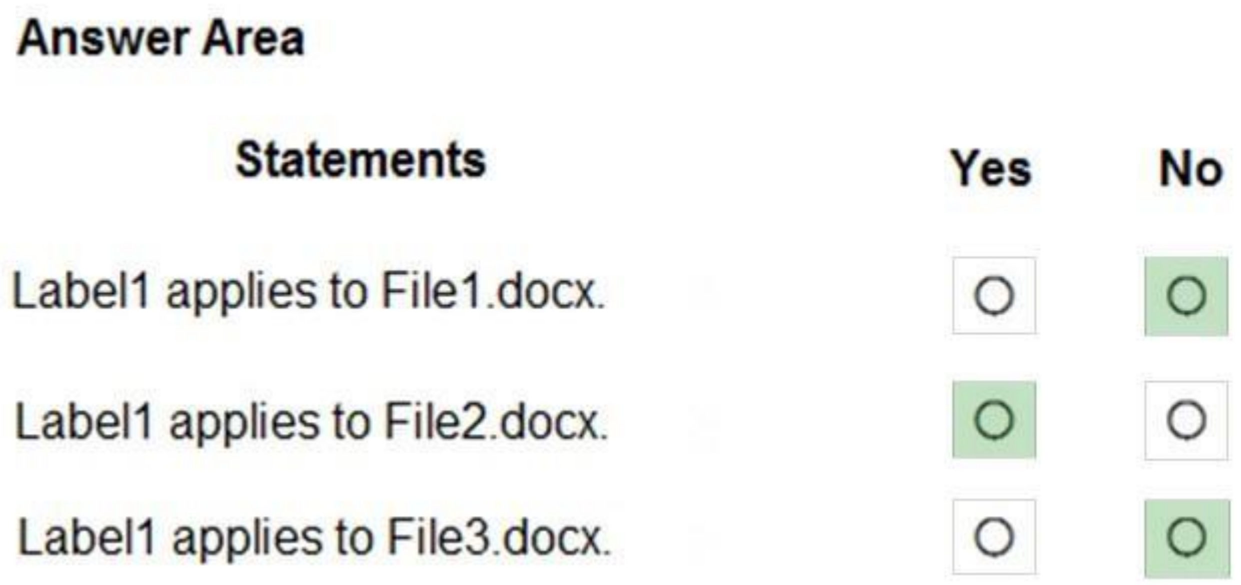
Hot Area:



Answer Area

Statements	Yes	No
Label1 applies to File1.docx.	○	○
Label1 applies to File2.docx.	○	○
Label1 applies to File3.docx.	○	○

Correct Answer:



Answer Area

Statements	Yes	No
Label1 applies to File1.docx.	○	[✓ ○]
Label1 applies to File2.docx.	[✓ ○]	○
Label1 applies to File3.docx.	○	[✓ ○]

Section: [none]
Explanation

Explanation/Reference:
Explanation:

The phrase to match is "im" and it is case sensitive. The phrase must also appear at least twice.

Box 1: No
File1.docx contain the word "import" once only

Box 2: Yes
File2.docx contains two occurrences of the word "import" as well as the word "imported"

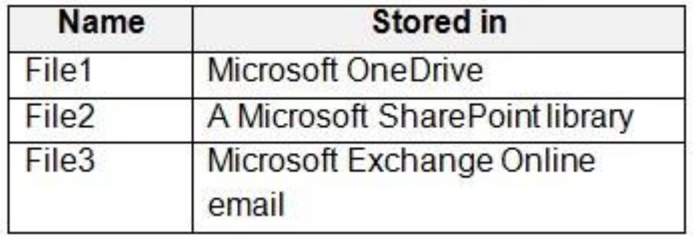
Box 3: No
File3.docx contains "IM" but his is not the correct letter case.

References: https://docs.microsoft.com/en-us/azure/information-protection/configure-policy-classification

QUESTION 82
HOTSPOT

You have a Microsoft 365 subscription that uses a default domain named contoso.com.

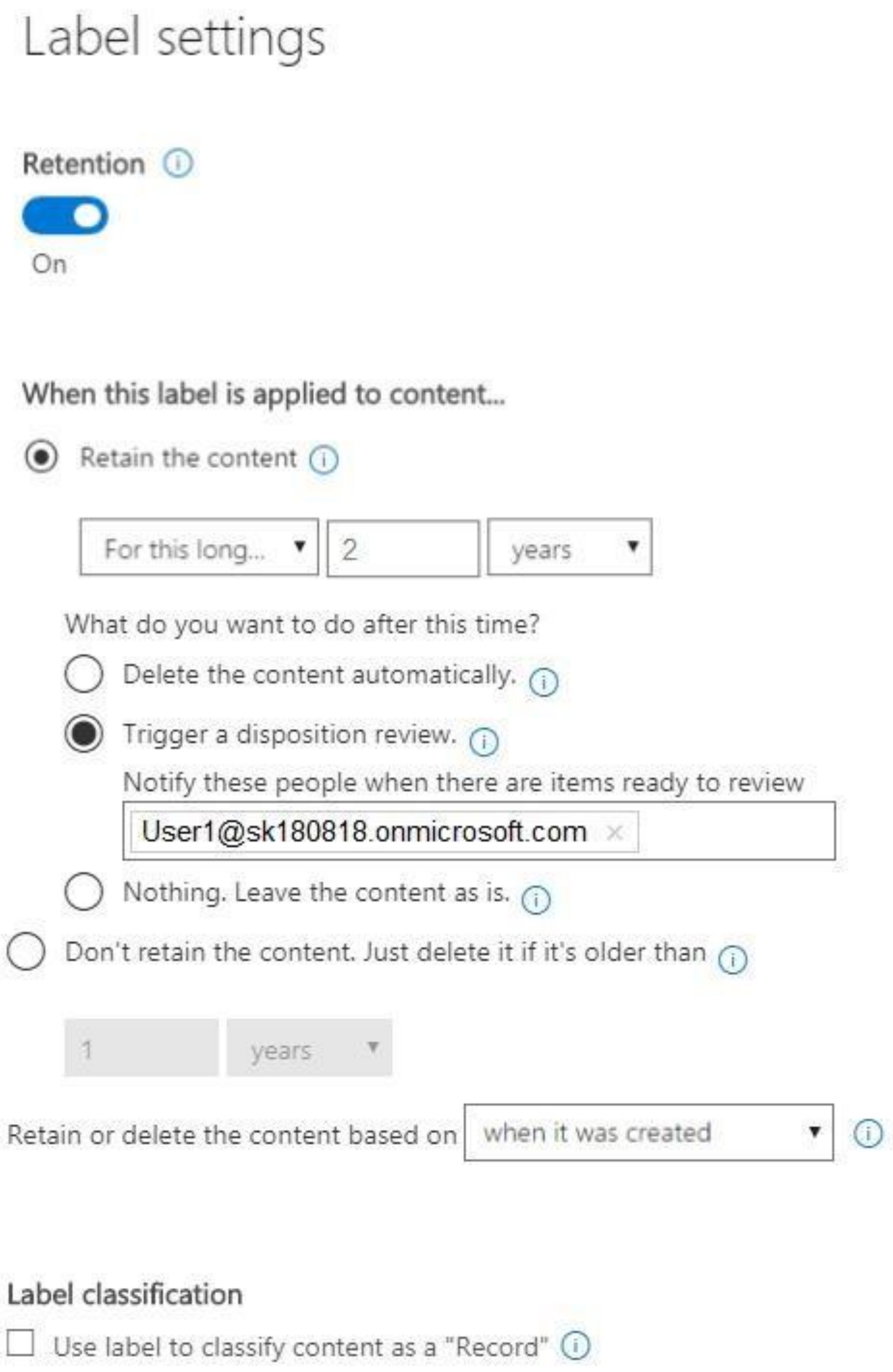
Three files were created on February 1, 2019, as shown in the following table.



Name	Stored in
File1	Microsoft OneDrive
File2	A Microsoft SharePoint library
File3	Microsoft Exchange Online email

On March 1, 2019, you create two retention labels named Label1 and Label2.

The settings for Lable1 are configured as shown in the Label1 exhibit. (Click the **Label1** tab.)



Label settings

Retention
On

When this label is applied to content...

● Retain the content

For this long... ▾ | 2 | years ▾

What do you want to do after this time?

○ Delete the content automatically.

● Trigger a disposition review.

Notify these people when there are items ready to review

User1@sk180818.onmicrosoft.com ×

○ Nothing. Leave the content as is.

○ Don't retain the content. Just delete it if it's older than

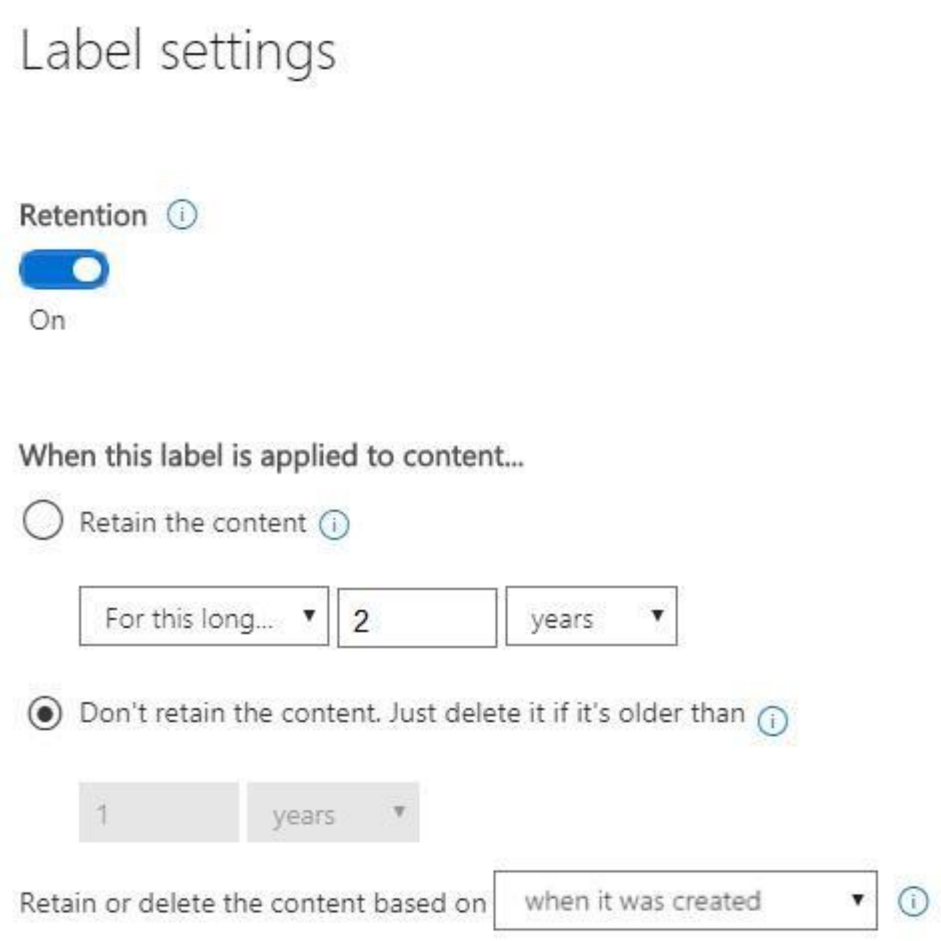
1 | years ▾

Retain or delete the content based on when it was created ▾

Label classification

□ Use label to classify content as a "Record"

The settings for Lable2 are configured as shown in the Label2 exhibit. (Click the **Label2** tab.)



Label settings

Retention

On

When this label is applied to content...

○ Retain the content

For this long... ▾ | 2 | years ▾

● Don't retain the content. Just delete it if it's older than

1 | years ▾

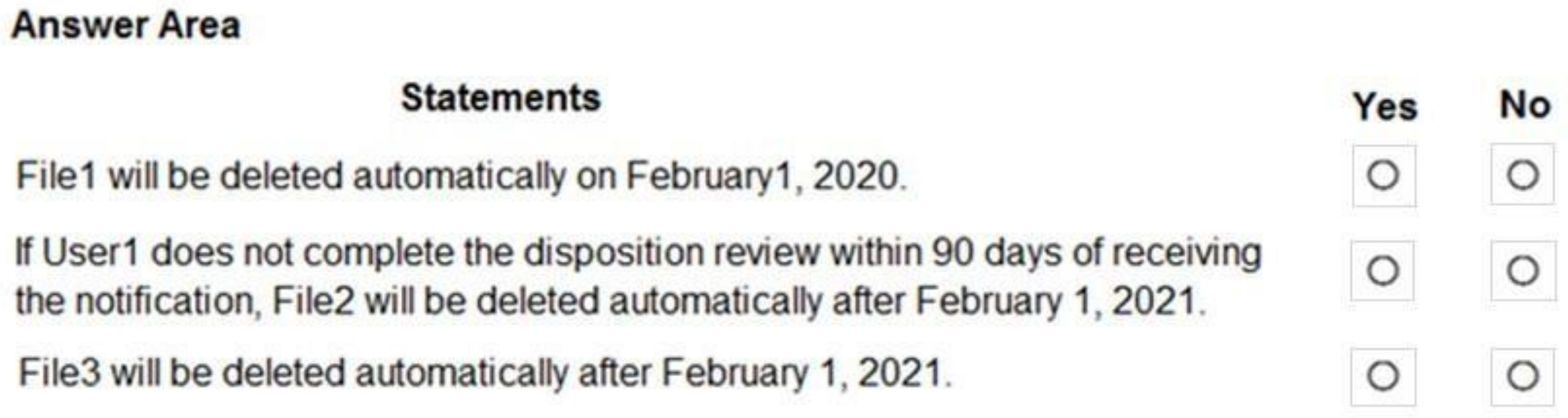
Retain or delete the content based on | when it was created ▾

You apply the retention labels to Exchange email, SharePoint sites, and OneDrive accounts.

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

NOTE: Each correct selection is worth one point.

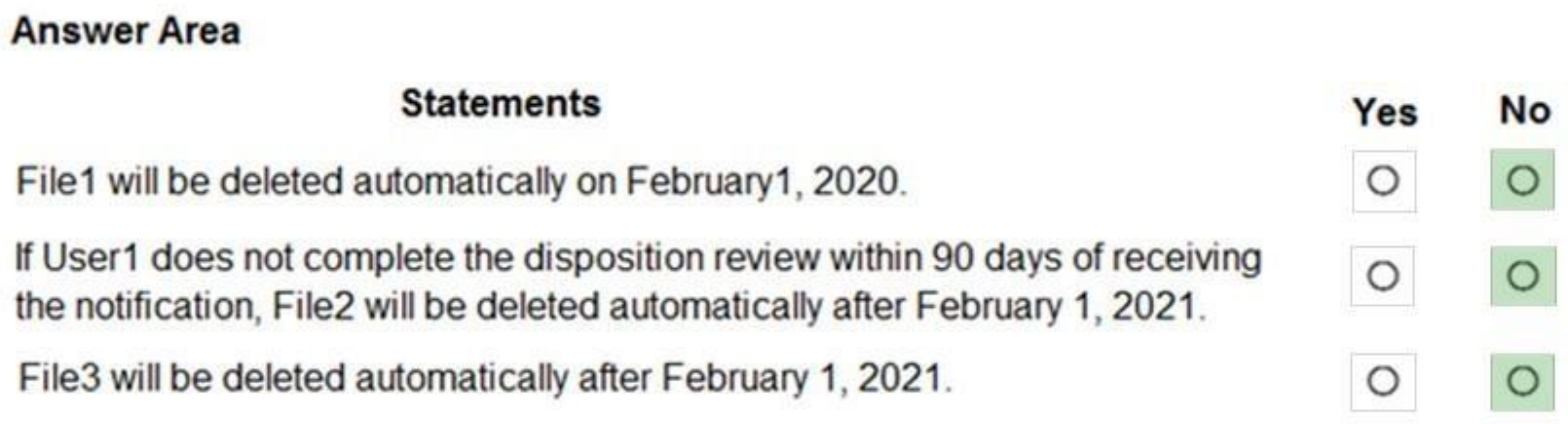
Hot Area:



Answer Area

Statements	Yes	No
File1 will be deleted automatically on February1, 2020.	○	○
If User1 does not complete the disposition review within 90 days of receiving the notification, File2 will be deleted automatically after February 1, 2021.	○	○
File3 will be deleted automatically after February 1, 2021.	○	○

Correct Answer:



Answer Area

Statements	Yes	No
File1 will be deleted automatically on February1, 2020.	○	[✓ ○]
If User1 does not complete the disposition review within 90 days of receiving the notification, File2 will be deleted automatically after February 1, 2021.	○	[✓ ○]
File3 will be deleted automatically after February 1, 2021.	○	[✓ ○]

Section: [none]
Explanation

Explanation/Reference:
Explanation:

Box 1: No
Retention overrides deletion.

Box 2: No
Content in a document library will be moved to the first-stage Recycle Bin within 7 days of disposition, and then permanently deleted another 93 days after that. Thus 100 days in total.

Box 3: No
Items in an Exchange mailbox will be permanently deleted within 14 days of disposition.

References: https://docs.microsoft.com/en-us/office365/securitycompliance/labels
https://docs.microsoft.com/en-us/office365/securitycompliance/disposition-reviews

QUESTION 83
DRAG DROP

You have a Microsoft 365 subscription.

In the Exchange admin center, you have a data loss prevention (DLP) policy named Policy1 that has the following configurations:

- Block emails that contain financial data.
- Display the following policy tip text: Message blocked.

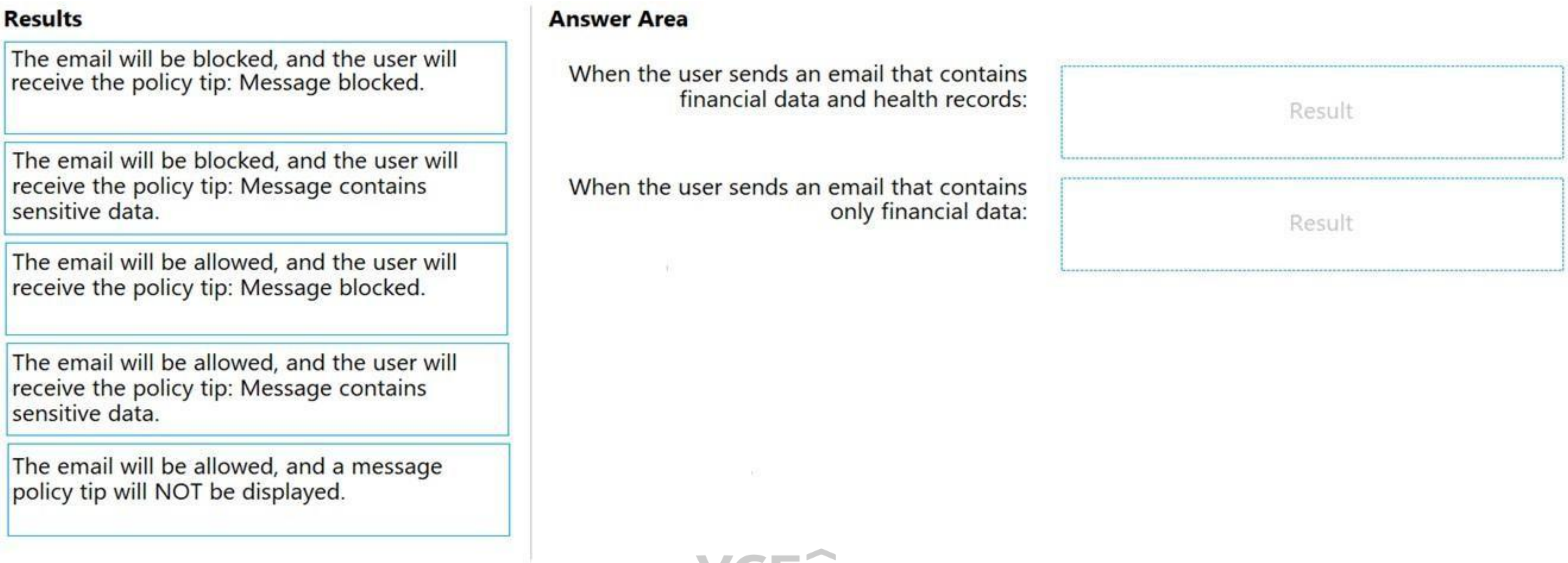
From the Security & Compliance admin center, you create a DLP policy named Policy2 that has the following configurations:

- Use the following location: Exchange email.
- Display the following policy tip text: Message contains sensitive data.
- When a user sends an email, notify the user if the email contains health records.

What is the result of the DLP policies when the user sends an email? To answer, drag the appropriate results to the correct scenarios. Each result may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:



Results

The email will be blocked, and the user will receive the policy tip: Message blocked.

The email will be blocked, and the user will receive the policy tip: Message contains sensitive data.

The email will be allowed, and the user will receive the policy tip: Message blocked.

The email will be allowed, and the user will receive the policy tip: Message contains sensitive data.

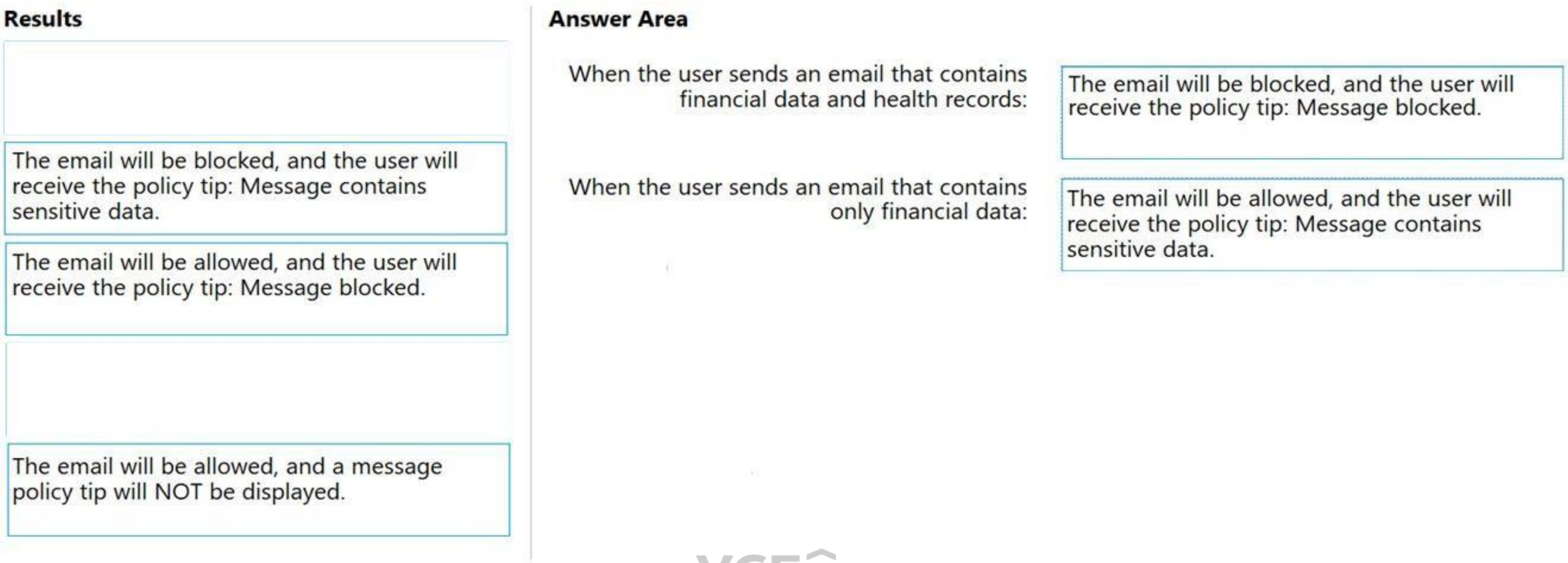
The email will be allowed, and a message policy tip will NOT be displayed.

Answer Area

When the user sends an email that contains financial data and health records: Result

When the user sends an email that contains only financial data: Result

Correct Answer:



Results

The email will be blocked, and the user will receive the policy tip: Message contains sensitive data.

The email will be allowed, and the user will receive the policy tip: Message blocked.

The email will be allowed, and a message policy tip will NOT be displayed.

Answer Area

When the user sends an email that contains financial data and health records: The email will be blocked, and the user will receive the policy tip: Message blocked.

When the user sends an email that contains only financial data: The email will be allowed, and the user will receive the policy tip: Message contains sensitive data.

Section: [none]
Explanation

Explanation/Reference:
Explanation:

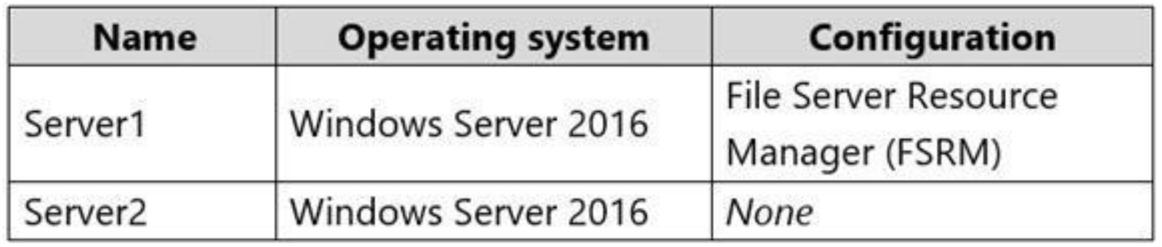
Box 1: The email will be blocked, and the user will receive the policy tip: Message blocked.
If you've created DLP policies in the Exchange admin center, those policies will continue to work side by side with any policies for email that you create in the Security & Compliance Center. But note that rules created in the Exchange admin center take precedence. All Exchange mail flow rules are processed first, and then the DLP rules from the Security & Compliance Center are processed.

Box 2: The email will be allowed, and the user will receive the policy tip: Message contains sensitive data.

Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/how-dlp-works-between-admin-centers

QUESTION 84
DRAG DROP

Your network contains an on-premises Active Directory domain that syncs to Azure Active Directory (Azure AD). The domain contains the servers shown in the following table.



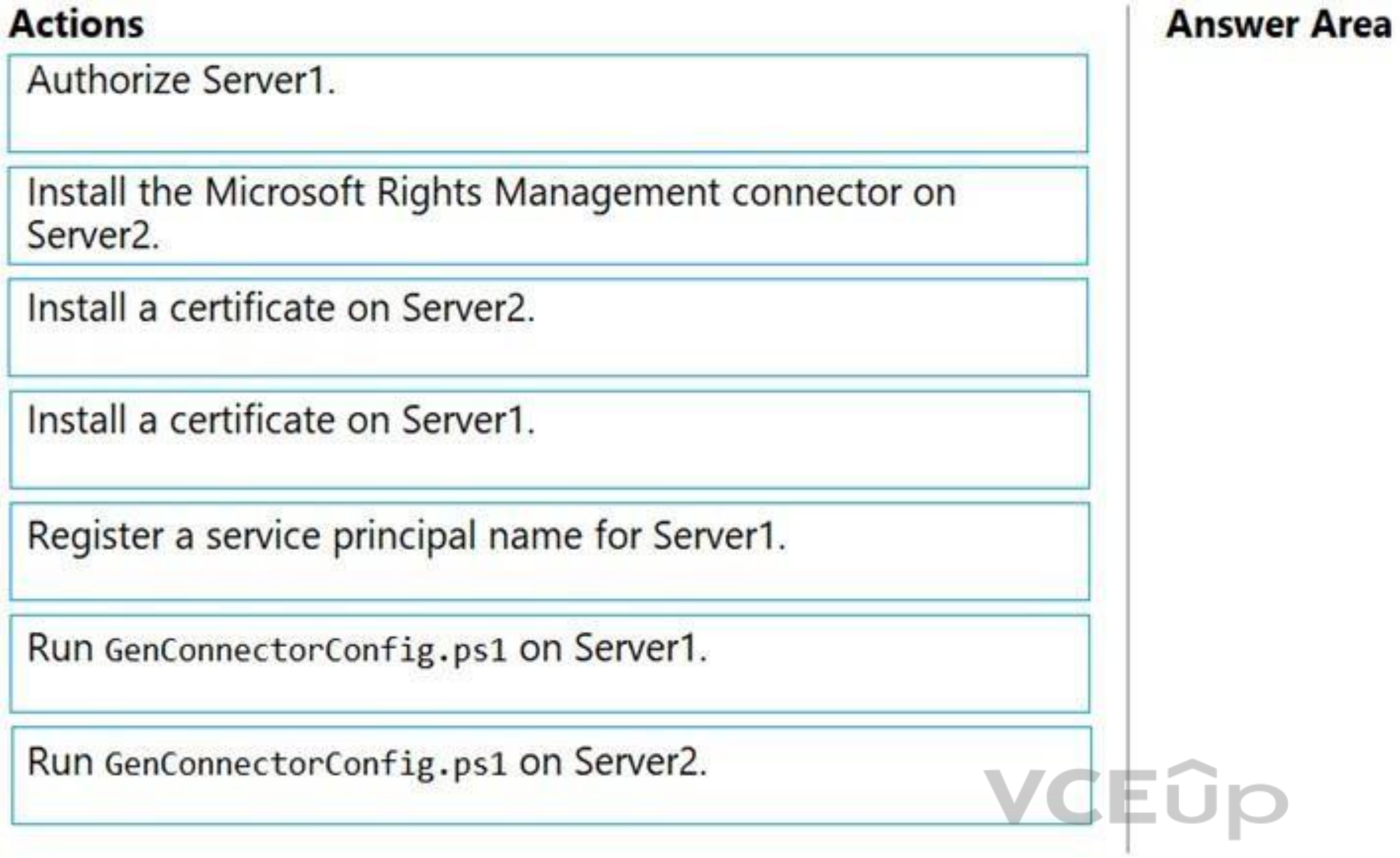
Name	Operating system	Configuration
Server1	Windows Server 2016	File Server Resource Manager (FSRM)
Server2	Windows Server 2016	*None*

You use Azure Information Protection.

You need to ensure that you can apply Azure Information Protection labels to the file stores on Server1.

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.

Select and Place:

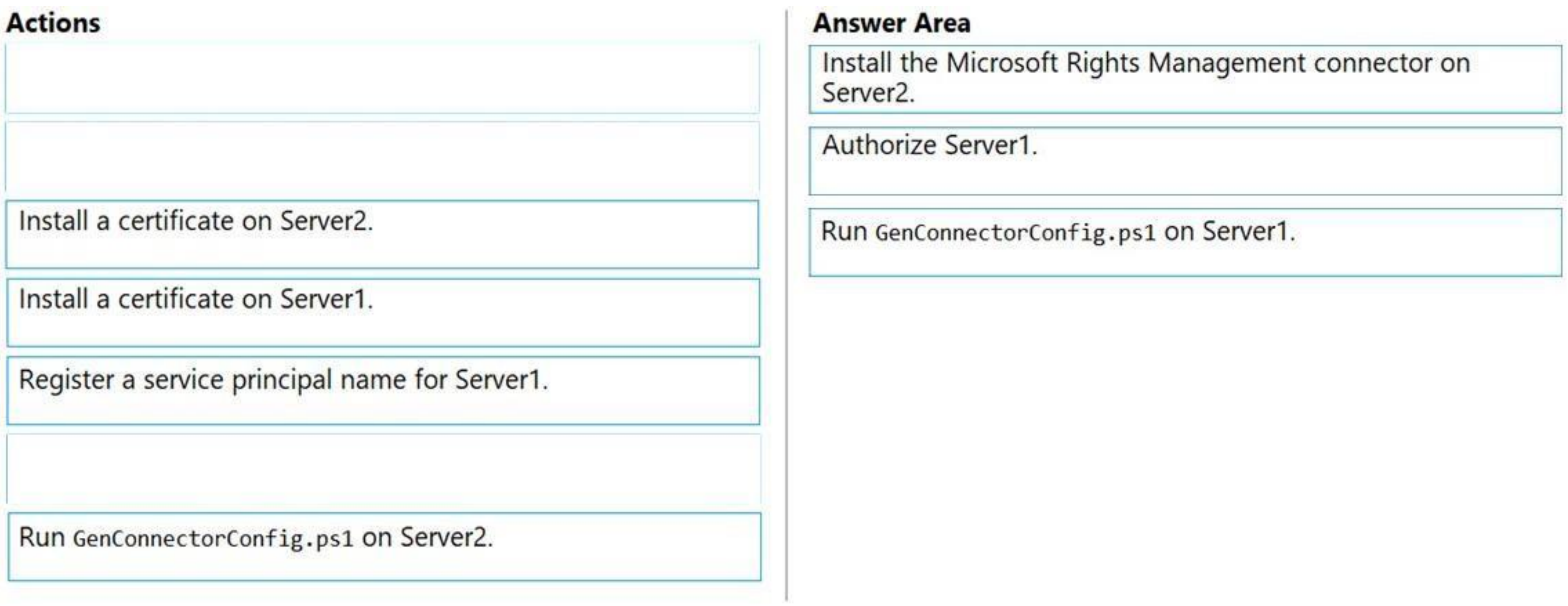


Actions

- Authorize Server1.
- Install the Microsoft Rights Management connector on Server2.
- Install a certificate on Server2.
- Install a certificate on Server1.
- Register a service principal name for Server1.
- Run `GenConnectorConfig.ps1` on Server1.
- Run `GenConnectorConfig.ps1` on Server2.

Answer Area

Correct Answer:



Actions

Install a certificate on Server2.

Install a certificate on Server1.

Register a service principal name for Server1.

Run `GenConnectorConfig.ps1` on Server2.

Answer Area

Install the Microsoft Rights Management connector on Server2.

Authorize Server1.

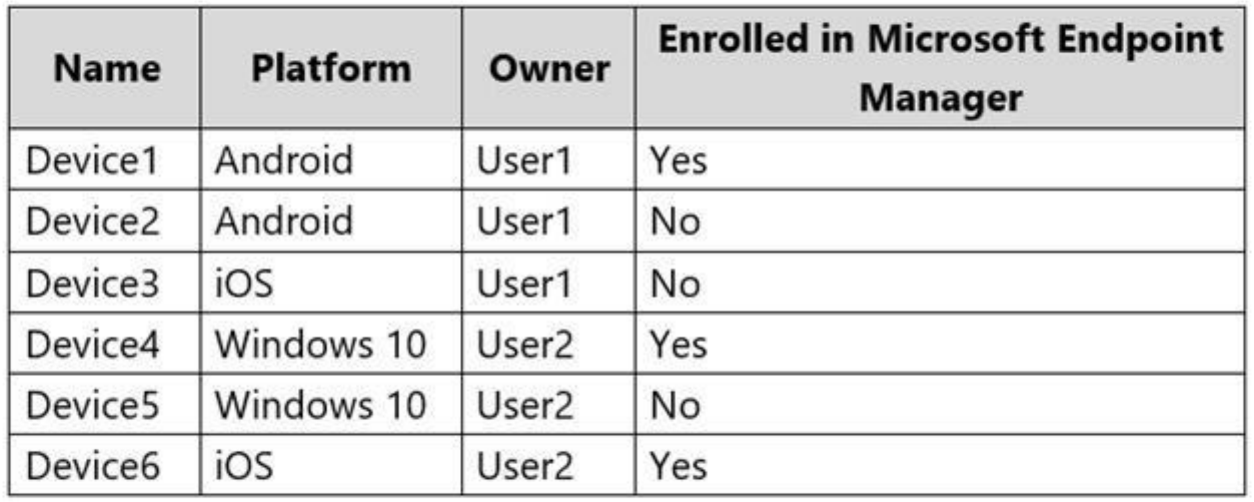
Run `GenConnectorConfig.ps1` on Server1.

Section: [none]
Explanation

Explanation/Reference:
Reference: https://docs.microsoft.com/en-us/azure/information-protection/install-configure-rms-connector https://docs.microsoft.com/en-us/azure/information-protection/configure-servers-rms-connector

QUESTION 85 You have a Microsoft 365 E5 subscription.

Users have the devices shown in the following table.



Name	Platform	Owner	Enrolled in Microsoft Endpoint Manager
Device1	Android	User1	Yes
Device2	Android	User1	No
Device3	iOS	User1	No
Device4	Windows 10	User2	Yes
Device5	Windows 10	User2	No
Device6	iOS	User2	Yes

On which devices can you manage apps by using app configuration policies in Microsoft Endpoint Manager?

A. Device1, Device4, and Device6
B. Device2, Device3, and Device5
C. Device1, Device2, Device3, and Device6
D. Device1, Device2, Device4, and Device5

Correct Answer: C
Section: [none]
Explanation

Explanation/Reference:
Explanation:
You can create and use app configuration policies to provide configuration settings for both iOS/iPadOS or Android apps on devices that are and are not enrolled in Microsoft Endpoint Manager.

Reference: https://docs.microsoft.com/en-us/mem/intune/apps/app-configuration-policies-overview

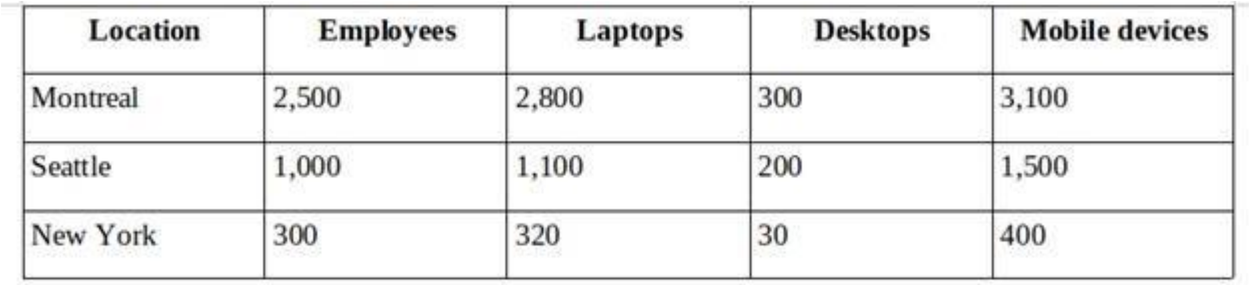
Testlet 2

Case Study

Overview

Contoso, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.

The company has the employees and devices shown in the following table.

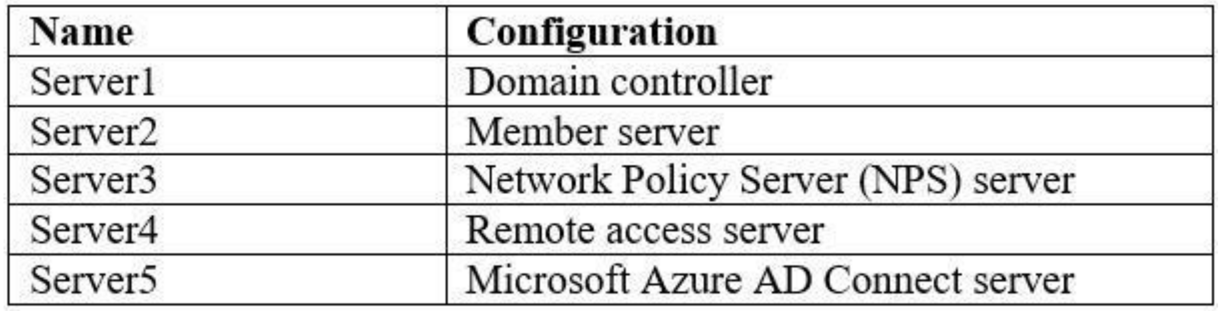


Location	Employees	Laptops	Desktops	Mobile devices
Montreal	2,500	2,800	300	3,100
Seattle	1,000	1,100	200	1,500
New York	300	320	30	400

Contoso recently purchased a Microsoft 365 E5 subscription.

Existing Environment

The network contains an on-premises Active Directory forest named contoso.com. The forest contains the servers shown in the following table.

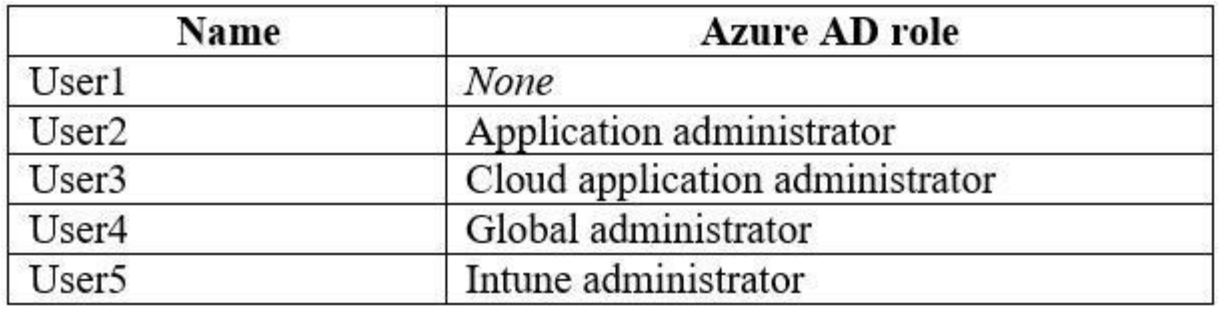


Name	Configuration
Server1	Domain controller
Server2	Member server
Server3	Network Policy Server (NPS) server
Server4	Remote access server
Server5	Microsoft Azure AD Connect server

All servers run Windows Server 2016. All desktops and laptops run Windows 10 Enterprise and are joined to the domain.

The mobile devices of the users in the Montreal and Seattle offices run Android. The mobile devices of the users in the New York office run iOS.

The domain is synced to Azure Active Directory (Azure AD) and includes the users shown in the following table.



Name	Azure AD role
User1	*None*
User2	Application administrator
User3	Cloud application administrator
User4	Global administrator
User5	Intune administrator

The domain also includes a group named Group1.

Requirements

Planned Changes
Contoso plans to implement the following changes:

- Implement Microsoft 365.

- Manage devices by using Microsoft Intune.
- Implement Azure Advanced Threat Protection (ATP).
- Every September, apply the latest feature updates to all Windows computers. Every March, apply the latest feature updates to the computers in the New York office only.

Technical Requirements

Contoso identifies the following technical requirements:

- When a Windows 10 device is joined to Azure AD, the device must enroll in Intune automatically.
- Dedicated support technicians must enroll all the Montreal office mobile devices in Intune.
- User1 must be able to enroll all the New York office mobile devices in Intune.
- Azure ATP sensors must be installed and must **NOT** use port mirroring.
- Whenever possible, the principle of least privilege must be used. ▪ A Microsoft Store for Business must be created.

Compliance Requirements

Contoso identifies the following compliance requirements:

- Ensure that the users in Group1 can only access Microsoft Exchange Online from devices that are enrolled in Intune and configured in accordance with the corporate policy. ▪ Configure Windows Information Protection (WIP) for the Windows 10 devices.

QUESTION 1 You need to meet the compliance requirements for the Windows 10 devices.

What should you create from the Endpoint Management admin center?

A. a device compliance policy
B. a device configuration profile
C. an app protection policy
D. an app configuration policy

Correct Answer: C
Section: [none]
Explanation

Explanation/Reference:
Reference:
https://docs.microsoft.com/en-us/windows/security/information-protection/windows-information-protection/create-wip-policy-using-intune-azure

Testlet 3

Case Study

Overview

ADatum Corporation is an international financial services company that has 5,000 employees.

ADatum has six offices: a main office in New York and five branch offices in Germany, the United Kingdom, France, Spain, and Italy.

All the offices are connected to each other by using a WAN link. Each office connects directly to the Internet.

Existing Environment

Current Infrastructure

ADatum recently purchased a Microsoft 365 subscription.

All user files are migrated to Microsoft 365.

All mailboxes are hosted in Microsoft 365. The users in each office have email suffixes that include the country of the user, for example, user1@us.adatum.com or user2@uk.adatum.com.

Each office has a security information and event management (SIEM) appliance. The appliance comes from three different vendors.

ADatum uses and processes Personally Identifiable Information (PII).

Problem Statements

ADatum entered into litigation. The legal department must place a hold on all the documents of a user named User1 that are in Microsoft 365.

Requirements

Business Goals

ADatum wants to be fully compliant with all the relevant data privacy laws in the regions where is operates.

ADatum wants to minimize the cost of hardware and software whenever possible. **Technical**

Requirements

ADatum identifies the following technical requirements:

- Centrally perform log analysis for all offices.
- Aggregate all data from the SIEM appliances to a central cloud repository for later analysis.
- Ensure that a SharePoint administrator can identify who accessed a specific file stored in a document library.
- Provide the users in the finance department with access to Service assurance information in Microsoft Office 365.
- Ensure that documents and email messages containing the PII data of European Union (EU) citizens are preserved for 10 years.
- If a user attempts to download 1,000 or more files from Microsoft SharePoint Online within 30 minutes, notify a security administrator and suspend the user's user account.
- A security administrator requires a report that shown which Microsoft 365 users signed in. Based on the report, the security administrator will create a policy to require multi-factor authentication when a sign-in is high risk.
- Ensure that the users in the New York office can only send email messages that contain sensitive U.S. PII data to other New York office uses. Email messages must be monitored to ensure compliance. Auditors in the New York office must have access to reports that show the sent and received email messages containing sensitive U.S. PII data.

QUESTION 1 Which report should the New York office auditors view?

A. DLP incidents
B. Top Senders and Recipients
C. DLP false positives and overrides
D. DLP policy matches

Correct Answer: A
Section: [none]
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/office365/securitycompliance/data-loss-prevention-policies

QUESTION 2 You need to meet the technical requirement for the EU PII data.

What should you create?

A. a data loss prevention (DLP) policy from the Security & Compliance admin center
B. a data loss prevention (DLP) policy from the Exchange admin center
C. a retention policy from the Exchange admin center

D. a retention policy from the Security & Compliance admin center

Correct Answer: D
Section: [none]
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/office365/securitycompliance/retention-policies

QUESTION 3 You need to protect the U.S. PII data to meet the technical requirements.

What should you create?

A. a data loss prevention (DLP) policy that contains a domain exception
B. a Security & Compliance retention policy that detects content containing sensitive data
C. a Security & Compliance alert policy that contains an activity
D. a data loss prevention (DLP) policy that contains a user override

Correct Answer: C
Section: [none]
Explanation

Explanation/Reference:
References: https://docs.microsoft.com/en-us/office365/securitycompliance/create-activity-alerts

QUESTION 4
DRAG DROP

You need to meet the requirement for the legal department.

Which three actions should you perform in sequence from the Security & Compliance admin center? 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:

Section: [none]
Explanation

Explanation/Reference:
References: https://www.sherweb.com/blog/ediscovery-office-365/

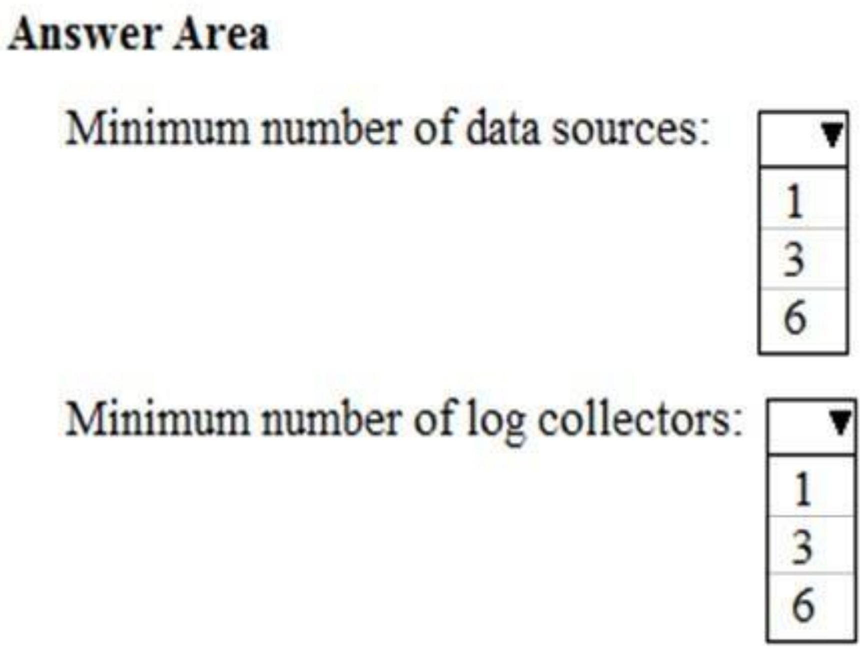
QUESTION 5 HOTSPOT

You need to meet the technical requirement for log analysis.

What is the minimum number of data sources and log collectors you should create from Microsoft Cloud App Security? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

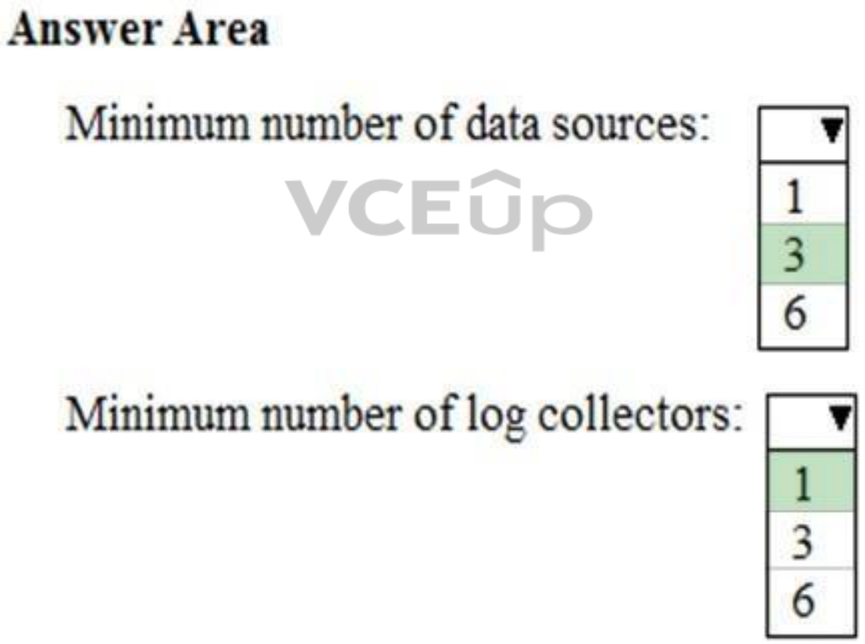


Answer Area

Minimum number of data sources: ▼
1
3
6

Minimum number of log collectors: ▼
1
3
6

Correct Answer:



Answer Area

Minimum number of data sources: ▼
1
[✓ 3]
6

Minimum number of log collectors: ▼
[✓ 1]
3
6

Section: [none]
Explanation
Explanation/Reference:
References: https://docs.microsoft.com/en-us/cloud-app-security/discovery-docker

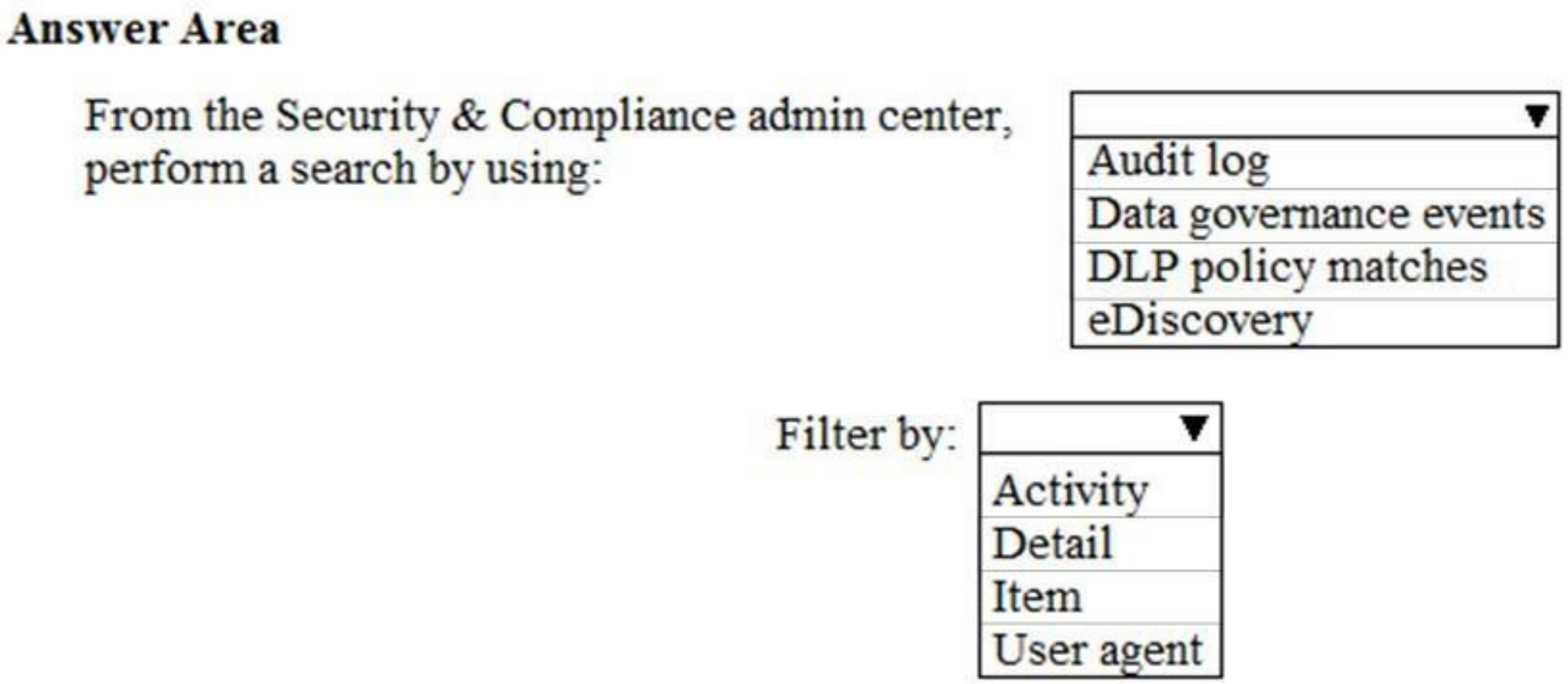
QUESTION 6 HOTSPOT

You need to meet the technical requirement for the SharePoint administrator.

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

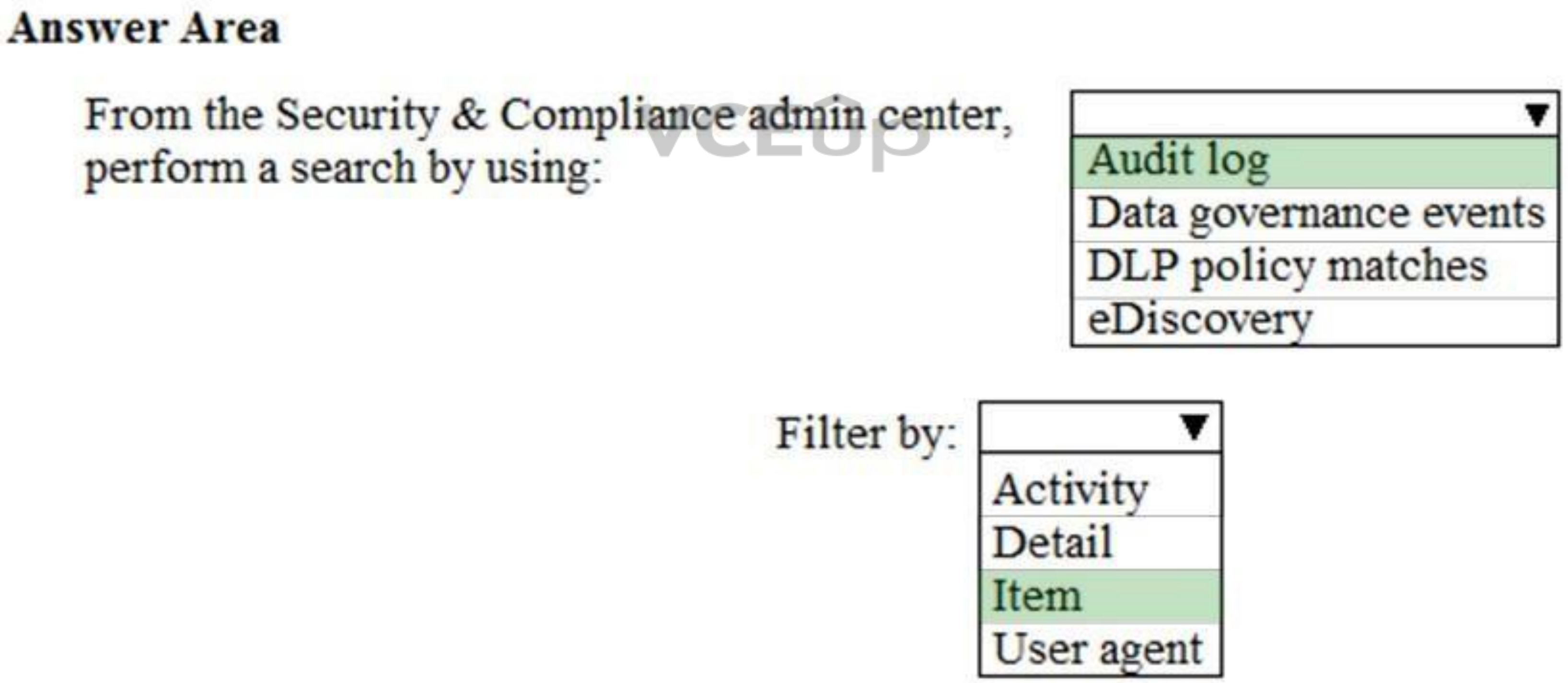
From the Security & Compliance admin center, perform a search by using:

- Audit log
- Data governance events
- DLP policy matches
- eDiscovery

Filter by:

- Activity
- Detail
- Item
- User agent

Correct Answer:



Answer Area

From the Security & Compliance admin center, perform a search by using:

- [✓ Audit log]
- Data governance events
- DLP policy matches
- eDiscovery

Filter by:

- Activity
- Detail
- [✓ Item]
- User agent

Section: [none]
Explanation

Explanation/Reference:
References:
https://docs.microsoft.com/en-us/office365/securitycompliance/search-the-audit-log-in-security-and-compliance#step-3-filter-the-search-results